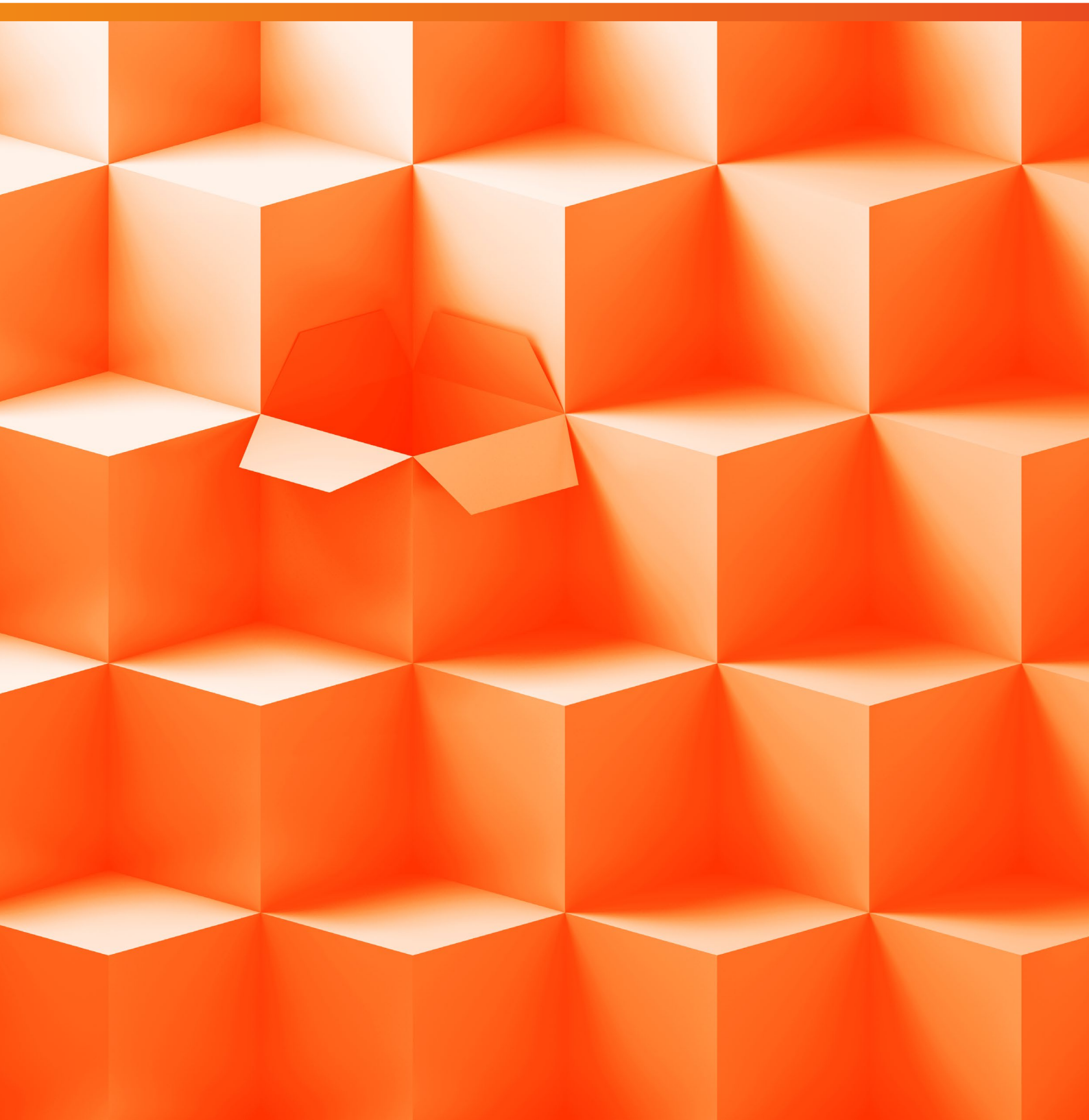
DARKTRACE

# Darktrace Packages

Version 4 - July 3rd 2023



## CONTENTS - DARKTRACE PACKAGES







# Darktrace Packages

Darktrace helps 8,400+ organizations of all sizes and industry to minimize cyber disruption, through a Cyber AI Loop built on a deep, bespoke understanding of the organization. Its interconnected set of cyber security products form an always-on feedback system that creates a virtuous cycle in which each capability strengthens and hardens the entire security ecosystem. This reduces cyber risk and provides protection across the entire digital environment – from email, cloud, applications, to IoT, endpoints, cyber-physical systems, and the traditional network. These unique developments come from our AI Research Centre in Cambridge, comprised of mathematicians and experts in multiple disciplines including astrophysics, linguistics, and data science.

The Cyber AI Loop represents the world's first always-on, end-to-end, interconnected set of cyber security solutions. It empowers defenders to reduce cyber risk at every stage of the attack lifecycle. Darktrace PREVENT™ allows organizations to anticipate attacks and reduce risk by hardening defenses, while Darktrace DETECT™ spots threats instantly and in real time. Darktrace RESPOND™ then takes targeted action to disarm cyber-attacks in seconds, and if an attack does get through, Darktrace HEAL™ will restore normal operations.

Each of these capabilities is powered by Self-Learning AI that understands its unique digital surroundings. Rather than being trained on attack data, it learns the bespoke details of your organization, so it can identify subtle patterns that indicate a vulnerability or an emerging threat. And each capability feeds back into the Loop as a whole, autonomously and continuously strengthening the entire system.

This Darktrace Packages Data Sheet sets forth the description of each of the different packages and subscription usage.

Darktrace is the only cyber security technology that protects the entire digital enterprise. By bringing its Self-Learning AI to your data, wherever it resides, Darktrace DETECT, RESPOND and Cyber AI Analyst offers a unified approach to cyber defense across diverse and fractured digital environments.

## Darktrace DETECT™

### See attacks instantly

Powered by a bespoke, continuously evolving understanding of self, Darktrace DETECT delivers instant visibility of threats – even those using novel malware strains or new techniques. Darktrace DETECT learns what makes your organization unique, from the ground up and without any prior assumptions as to what constitutes a threat.

This understanding allows it to detect subtle patterns that reveal deviations from the norm, making it possible for the security team to identify attacks in real time, not after the damage has been done.

## Darktrace RESPOND™

### Disarm within seconds

By making a series of micro-decisions at machine speed, Darktrace RESPOND disarms an attack in seconds. It uses Darktrace's evolving and bespoke understanding of your organization to pinpoint signs of a potential attack, interrupt the malicious activity, while letting your normal business operations continue. These autonomous actions can be taken against zero-day attacks, compromised cloud credentials, advanced spoofing campaigns, and more.

## Cyber AI Analyst™

### Bringing the human into the loop

At every stage of the Cyber AI Loop, Cyber AI Analyst runs in the background, using Explainable AI to generate meaningful outputs that a human team can easily understand. With DETECT, AI Analyst automatically investigates every security event, autonomously triaging and reporting on the full scope of the security incident, dramatically reducing the time to meaning for security teams. And with RESPOND, AI Analyst helps human security teams immediately understand what action the AI took, if any, and why, helping teams build trust in the AI's decision-making over time.

| | Darktrace Employee Suite | | Darktrace Infrastructure Suite | | Darktrace Platform | | |
|---|---|---|---|---|---|---|---|
| | Standard | Premium | Standard | Premium | Standard | Premium | Platinum |
| **Capabilities** | | | | | | | |
| Darktrace DETECT™ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Darktrace RESPOND™ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Darktrace Cyber AI Analyst™ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Areas of Coverage** | | | | | | | |
| Email | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| Network | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cloud | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Endpoint | | ✓ | | ✓ | | ✓ | ✓ |
| Microsoft 365 / Google Workspace | Select any 2 | Select any 4 | Select any 1 | Select any 3 | Select any 2 | Select any 4 | Unlimited |
| Zero Trust | | | | | | | |
| Apps | | | | | | | |
| **Services** | | | | | | | |
| Customer Portal Access | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Darktrace Services/ Ask the Expert | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Darktrace Services/ Proactive Threat Notification | × | Discounted | Additional | Discounted | Additional | Discounted | ✓ |
| Darktrace Services/Training | Live/Interactive | Live/Interactive | Live/Interactive | Live/Interactive | Live/Interactive | Live/Interactive | Darktrace Certified |

# Employee Suite

The Darktrace Employee Suite is essential for protecting your employees in the areas where they are most at risk. The Standard package offers detection and response capabilities in the inbox and across your apps, and the Premium package adds protection to your endpoint devices, and offers AI-powered investigation with Cyber AI Analyst. We can deploy our email technology within five minutes, and with Darktrace Self-Service, you can deploy Darktrace rapidly yourself.

## Standard: Email, Apps & Zero Trust

### Products:

- Darktrace DETECT™: real time threat detection
- Darktrace RESPOND™: autonomous response
- Cyber AI Analyst™: augment and uplift your team with AI powered investigations

### Coverage Areas:

- Email – defend your employees from spear phishing, impersonation attempts and account takeovers with Darktrace/Email, Darktrace's Autonomous Response technology for the inbox
- Apps and Zero Trust – protect your choice with any two of the following: Microsoft 365, Google Workspace, Salesforce, Sharepoint, OneDrive, Box, Dropbox, Slack, Zoom, JumpCloud, Okta, Duo and/or Zscaler

### Darktrace Services:

- 24/7 Ask the Expert service included
- Live and interactive training with Darktrace's world-class training team
- Opt in to additional product deployments via Darktrace Customer Portal

| Employee Band | Device Limit | Email Volume | Appliances (On-Prem) | Cloud Master (Cloud) |
|---|---|---|---|---|
| 1-50 | - | 3,300 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 51-75 | - | 4,900 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 76-100 | - | 6,500 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 101-125 | - | 8,100 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 126-150 | - | 9,800 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 151-175 | - | 11,400 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 176-200 | - | 13,000 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 201-225 | - | 14,600 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 226-250 | - | 16,300 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 251-275 | - | 17,900 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 276-300 | - | 19,500 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 301-350 | - | 22,800 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 351-400 | - | 26,000 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 401-450 | - | 29,300 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |
| 451-500 | - | 32,500 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | - |

# Premium: Email, Apps, Zero Trust & Endpoint

## Products:

- Darktrace DETECT™: real time threat detection
- Darktrace RESPOND™: autonomous response
- Cyber AI Analyst™: augment and uplift your team with AI powered investigations

## Coverage Areas:

- Email – defend your employees from spear phishing, impersonation attempts and account takeovers with Darktrace/Email, Darktrace's Autonomous Response technology for the inbox
- Apps and Zero Trust – protect your choice with any four of the following: Microsoft 365, Google Workspace, Salesforce, Sharepoint, OneDrive, Box, Dropbox, Slack, Zoom, JumpCloud, Okta, Duo and/or Zscaler
- Endpoint – protect your remote workers with detection, investigation and response for your Endpoint devices

## Darktrace Services:

- 24/7 Ask the Expert service included
- Proactive Threat Notification available at a discounted rate
- Live and interactive training with Darktrace's world-class training team
- Opt in to additional product deployments via Darktrace Customer Portal

| Employee Band | Device Limit | Email Volume | Appliances (On-Prem) | Cloud Master (Cloud) |
|---|---|---|---|---|
| 1-50 | - | 3,300 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 51-75 | - | 4,900 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 76-100 | - | 6,500 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 101-125 | - | 8,100 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 126-150 | - | 9,800 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 151-175 | - | 11,400 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 176-200 | - | 13,000 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 201-225 | - | 14,600 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 226-250 | - | 16,300 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 251-275 | - | 17,900 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 5-10k |
| 276-300 | - | 19,500 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 10-40k |
| 301-350 | - | 22,800 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 10-40k |
| 351-400 | - | 26,000 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 10-40k |
| 401-450 | - | 29,300 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 10-40k |
| 451-500 | - | 32,500 | 1 x /Appliance (Email)<br>1 x /Appliance (S) | 10-40k |

# Infrastructure Suite

The Darktrace Infrastructure Suite provides the best combination of products to protect your business infrastructure. The Standard package focuses on your cloud, apps and network, and Premium adds critical detection, investigation, and response for Endpoint devices. The Infrastructure Suite gives you complete visibility over your digital business, providing a structured solution for enterprise-wide defense.

## Standard: Network, Cloud, Apps & Zero Trust

### Products:

- Darktrace DETECT™: real time threat detection
- Darktrace RESPOND™: autonomous response
- Cyber AI Analyst™: augment and uplift your team with AI powered investigations

### Coverage Areas:

- Network – contain threats across the network and wider infrastructure, with complete visibility over your enterprise
- Cloud – detect and respond to unpredictable and unknown attacks across hybrid and multi-cloud environments
- Apps & Zero Trust – protect your choice with one of the following: Microsoft 365, Google Workspace, Salesforce, Sharepoint, OneDrive, Box, Dropbox, Slack, Zoom, JumpCloud, Okta, Duo and/or Zscaler

### Darktrace Services:

- 24/7 Ask the Expert service included
- Proactive Threat Notification available for an additional charge
- Live and interactive training with Darktrace's world-class training team
- Opt in to additional product deployments via Darktrace Customer Portal





| Employee Band | Device Limit | Email Volume | Appliances (On-Prem) | Cloud Master (Cloud) |
|---|---|---|---|---|
| 1-50 | 140 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 0-5k |
| 51-75 | 210 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 0-5k |
| 76-100 | 280 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 0-5k |
| 101-125 | 350 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 126-150 | 420 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 151-175 | 490 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 176-200 | 560 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 201-225 | 630 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 226-250 | 700 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 251-275 | 770 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 276-300 | 840 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 301-350 | 980 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 351-400 | 1,120 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 401-450 | 1,260 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 451-500 | 1,400 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |

# Premium: Network, Cloud, Apps, Zero Trust & Endpoint

## Products:

- Darktrace DETECT™: real time threat detection
- Darktrace RESPOND™: autonomous response
- Cyber AI Analyst™: augment and uplift your team with AI powered investigations

## Coverage Areas:

- Network – contain threats across the network and wider infrastructure, with complete visibility over your dynamic workforce
- Cloud – detect and respond to unpredictable and unknown attacks across hybrid and multi-cloud environments
- Apps & Zero Trust – protect your choice with any three of the following: Microsoft 365, Google Workspace, Sales-force, Sharepoint, OneDrive, Box, Dropbox, Slack, Zoom, JumpCloud, Okta, Duo and/or Zscaler
- Endpoint – protect your remote workers with detection, investigation and response for your Endpoint devices

## Darktrace Services

- 24/7 Ask the Expert service included
- Proactive Threat Notification available at a discounted rate
- Live and interactive training with Darktrace's world-class training team
- Opt in to additional product deployments via Darktrace Customer Portal

| Employee Band | Device Limit | Email Volume | Appliances (On-Prem) | Cloud Master (Cloud) |
|---|---|---|---|---|
| 1-50 | 140 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 51-75 | 210 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 76-100 | 280 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 101-125 | 350 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 126-150 | 420 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 151-175 | 490 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 176-200 | 560 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 5-10k |
| 201-225 | 630 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 226-250 | 700 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 251-275 | 770 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 276-300 | 840 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 301-350 | 980 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 351-400 | 1,120 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 401-450 | 1,260 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |
| 451-500 | 1,400 | - | 1 x /Appliance (M)<br>1 x /Appliance (S) | 10-40k |

# Darktrace Platform

The Darktrace Loop package brings Self-Learning AI-powered detection, investigation, and autonomous response to every corner of your digital estate – including cloud, email, network and endpoint. Your entire enterprise is protected from sophisticated cyber-threats, including ransomware and zero-day attacks.

This can be deployed on-premise, in the cloud or for hybrid working models, making this security unique to your environment. This enterprise-wide approach provides unified protection for hybrid working models, ensuring that attackers have nowhere to hide.

## Standard: Email, Network, Cloud, Apps & Zero Trust

### Products:

- Darktrace DETECT™: real time threat detection
- Darktrace RESPOND™: autonomous response
- Cyber AI Analyst™: augment and uplift your team with AI powered investigations

### Coverage Areas:

- Email – defend your employees from spear phishing, impersonation attempts and account takeovers with Darktrace/Email, Darktrace's Autonomous Response technology for the inbox
- Network – contain threats across the network and wider infrastructure, with complete visibility over your dynamic workforce
- Cloud – detect and respond to unpredictable and unknown attacks across hybrid and multi-cloud environments
- Apps & Zero Trust – protect your choice with any two of the following: Microsoft 365, Google Workspace, Salesforce, Sharepoint, OneDrive, Box, Dropbox, Slack, Zoom, JumpCloud, Okta, Duo and/or Zscaler

### Darktrace Services:

- 24/7 Ask the Expert service included
- Proactive Threat Notification available for an additional charge
- Live and interactive training with Darktrace's world-class training team
- Opt in to additional product deployments via Darktrace Customer Portal





| Employee Band | Device Limit | Email Volume | Appliances (On-Prem) | Cloud Master (Cloud) | Hybrid Deployment |
|---|---|---|---|---|---|
| 1-50 | 140 | 3,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 0-5k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 51-75 | 210 | 4,900 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 0-5k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 76-100 | 280 | 6,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 0-5k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 101-125 | 350 | 8,100 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 126-150 | 420 | 9,800 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 151-175 | 490 | 11,400 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 176-200 | 560 | 13,000 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 201-225 | 630 | 14,600 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 226-250 | 700 | 16,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 251-275 | 770 | 17,900 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 276-300 | 840 | 19,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 301-350 | 980 | 22,800 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 351-400 | 1,120 | 26,000 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 401-450 | 1,260 | 29,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 451-500 | 1,400 | 32,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |

# Premium: Email, Network, Cloud, Apps, Zero Trust & Endpoint

## Products:

- Darktrace DETECT™: real time threat detection
- Darktrace RESPOND™: autonomous response
- Cyber AI Analyst™: augment and uplift your team with AI powered investigations

## Coverage Areas:

- Email – defend your employees from spear phishing, impersonation attempts and account takeovers with Darktrace/Email, Darktrace's Autonomous Response technology for the inbox
- Network – contain threats across the network and wider infrastructure, with complete visibility over your dynamic workforce
- Cloud – detect and respond to unpredictable and unknown attacks across hybrid and multi-cloud environments
- Apps & Zero Trust – protect your choice with any four of the following: Microsoft 365, Google Workspace, Sales-force, Sharepoint, OneDrive, Box, Dropbox, Slack, Zoom, JumpCloud, Okta, Duo and/or Zscaler
- Endpoint – protect your remote workers with detection, investigation and response for your Endpoint devices

## Darktrace Services

- 24/7 Ask the Expert service included
- Proactive Threat Notification available at a discounted rate
- Live and interactive training with Darktrace's world-class training team
- Opt in to additional product deployments via Darktrace Customer Portal

| Employee Band | Device Limit | Email Volume | Appliances (On-Prem) | Cloud Master (Cloud) | Hybrid Deployment |
|---|---|---|---|---|---|
| 1-50 | 140 | 3,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 51-75 | 210 | 4,900 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 76-100 | 280 | 6,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 101-125 | 350 | 8,100 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 126-150 | 420 | 9,800 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 151-175 | 490 | 11,400 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 176-200 | 560 | 13,000 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 201-225 | 630 | 14,600 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 226-250 | 700 | 16,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 251-275 | 770 | 17,900 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 276-300 | 840 | 19,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 301-350 | 980 | 22,800 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 351-400 | 1,120 | 26,000 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 401-450 | 1,260 | 29,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 451-500 | 1,400 | 32,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |

# Darktrace Platform

## Platinum: Email, Cloud, Network, Endpoint, Zero Trust & Apps + Darktrace Services + Training Certification

Our Platinum Loop package offers our most comprehensive level of coverage. Darktrace's detection, investigation and autonomous response capabilities work in tandem across all parts of your digital infrastructure to deliver proactive cyber defense and power a truly self-defending business.

By bringing its Self-Learning AI to your data, wherever it resides, Darktrace offers a unified approach to cyber defense across fractured digital environments. By learning the 'patterns of life' for all users and devices – wherever they are located – the technology can identify and disrupt cyber-attacks, wherever they emerge.

### Products:

- Darktrace DETECT™: real time threat detection
- Darktrace RESPOND™: autonomous response
- Cyber AI Analyst™: augment and uplift your team with AI powered investigations

### Coverage Areas:

- Email – defend your employees from spear phishing, impersonation attempts and account takeovers with Darktrace/Email, Darktrace's Autonomous Response technology for the inbox
- Network – contain threats across the network and wider infrastructure, with complete visibility over your dynamic workforce
- Cloud – detect and respond to unpredictable and unknown attacks across hybrid and multi-cloud environments
- Apps & Zero Trust – unlimited Apps and Zero Trust coverage
- Endpoint – protect your remote workers with detection, investigation and response for your Endpoint devices

### Darktrace Services:

- 24/7 Ask the Expert service included
- Proactive Threat Notification included
- Darktrace Services/Certifications and training available to your entire team
- Opt in to additional product deployments via Darktrace Customer Portal

| Employee Band | Device Limit | Email Volume | Appliances (On-Prem) | Cloud Master (Cloud) | Hybrid Deployment |
|---|---|---|---|---|---|
| 1-50 | 140 | 3,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 51-75 | 210 | 4,900 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 76-100 | 280 | 6,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 101-125 | 350 | 8,100 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 5-10k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 126-150 | 420 | 9,800 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 151-175 | 490 | 11,400 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 176-200 | 560 | 13,000 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 201-225 | 630 | 14,600 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 226-250 | 700 | 16,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 251-275 | 770 | 17,900 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 276-300 | 840 | 19,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 301-350 | 980 | 22,800 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 351-400 | 1,120 | 26,000 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 401-450 | 1,260 | 29,300 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |
| 451-500 | 1,400 | 32,500 | 1 x /Appliance (Email)<br>1 x Appliance (S)<br>1 x /Appliance (M) | 10-40k | 1 x /Appliance (S)<br>1 x /Appliance (M) |

# Darktrace Services/Training

Darktrace Education offers training services that allows you to rapidly learn how to use and get the best value from Darktrace solutions. Our training accelerates the knowledge transfer, supports user adoption and lowers your total cost of ownership. With a global team of experienced instructors and subject matter experts, our mission is to deliver the best possible learning experience.

## Online Training

Darktrace Education provides a comprehensive rolebased curriculum, allowing customer to easily identify the relevant training courses. Our courses are modular by design allowing customers to focus on specific learning objectives and each course provides participants with fully documented training manuals which set out the tasks and lessons planned.

Complimentary to all customers and partners of Darktrace, our Education team operates an open public training schedule around the world. Delivered online, all you need to do is register for a course via the Customer Portal.

The sessions will be lecture format using a public cloud instance of Darktrace's world-leading Cyber AI platform. Hands-on exercises will also allow attendees to practice what they have learnt. Questions will be gathered via chat and answered both via chat and live during the presentation as appropriate. An additional audio question and answer period will be available after the session for those interested in participating.

Scheduled on a regular basis, our public training service makes learning more accessible, allowing geographically dispersed teams to access the training from wherever they are located, and saving valuable time by permitting the student to stay in the workplace during the training sessions. Our course durations are typically 2 – 4 hours, allowing you to learn and manage your day job. Furthermore, participants can attend as many training sessions as they need – it's unlimited, allowing for refresher or new staff training.

## Darktrace Services/Certification

Darktrace Services/Certification training creates well rounded experts with a badge and digital certificate after the course is completed. We offer foundational and role-based training paths:

- The Certified Engineer path verifies your competency to install, configure and administer Darktrace's Cyber AI Platform (Version 5), as well as networking and security fundamentals
- Certified Analyst path focuses more on using the Threat Visualizer interface and investigating threats on your network
- The Darktrace/Email Certified path is a product-centric certification that tests your knowledge and skills specifically for the Darktrace/Email interface.

By attending the public classes, you will have the opportunity to complete attendance tests following the webinars. On the completion of each course test, you will be able to proceed towards certification. Material can be reviewed on-demand via the instructional eLearning videos, and revising from the comprehensive training manuals can equip you further to sit the appropriate examination.

These certifications require you to undertake two examinations. In each case you will first need to pass the theory element, which consists of multiple choice questions. Successful candidates will then be expected to display their practical skills in our hands-on lab environment.
All exams are proctored by a Darktrace instructor and can be registered for via the Customer Portal.





# Darktrace Services

Darktrace is committed to ensuring that you receive the maximum value from our world-class Self-Learning AI technology and expert analysts. In order to best support you, our service options can be customized to uplift and and extend your security and IT teams. Services can be delivered by Darktrace's Cyber Analysts, experts in threat analysis and cyber intelligence, or Darktrace Certified Partners. Most importantly, these offerings are crafted based on experience across all sizes of companies and sectors to give you a custom fit.

## 24/7 Proactive Threat Notification

Darktrace's Security Operations Centers (SOC), located in Cambridge, San Francisco, and Singapore, provide you with around-the-clock coverage of significant incidents identified within your digital ecosystem, as flagged by your Darktrace deployment. Manned by our world-class Darktrace Cyber Analysts, this service notifies you of unusual activity or deviations in behavior which may be indicative of an in-progress attack. These incidents are rapidly triaged on demand, and our Cyber Analysts will provide you with the information you need to take action on events as they occur.

Darktrace Services/ Proactive Threat Notification ensure that high-fidelity incidents, which are strong indicators of an emerging attack, are funneled directly into the global Darktrace SOC for triage and assessment by our expert team of Cyber Analysts.

The alerts monitored by Darktrace as part of the Darktrace Services/ Proactive Threat Notification service can be identified by the Enhanced Monitoring tag within the Darktrace DETECT and can be viewed by filtering in the Threat Visualizer and Model Editor. The Enhanced Monitoring tag also enables you to see exactly which model breaches have been escalated into the SOC for triage.

Once a Darktrace Services/ Proactive Threat Notification is promoted into the Darktrace SOC it will be triaged by one of our global Cyber Analysts. Note that not all alerts are triaged, only incidents that are highly indicative of attack are marked with the Enhanced Monitoring tag and will be triaged by Darktrace Services/ Proactive Threat Notification analysts. Should Darktrace find strong evidence of attack during the triage phase, your team will be contacted immediately and provided with the intelligence ascertained in order to take action. Darktrace would suggest that any Darktrace Services/ Proactive Threat Notification alert be treated as high priority. Fully triaged alerts will be encrypted.

Using a shared secret key and emailed to a named distribution list within your organization. You can also receive automated telephone calls and/or SMS messages if a Darktrace Services/ Proactive Threat Notification email alert has been issued. You can configure SOC contacts and messaging delivery methods via the Customer Portal in your account preferences.

## 24/7 Ask the Expert

Accessible from within the Threat Visualizer and Customer Portal, Darktrace Services/Ask the Expert is a feature that can be enabled so that you and your security team can send queries to a Darktrace Cyber Analyst for expert assistance during live threat investigations. You will receive rapid feedback on new or advanced threats in your environment.

Accessing Darktrace Services/Ask the Expert via the Threat Visualizer gives you the ability to drag and drop graphics and traffic flow data into queries. This method of support enables your team to work collaboratively with Darktrace Analysts on a wide range of topics. When a Cyber Analyst responds to an Darktrace Services/Ask the Expert question, the answer will be available via 'Help -> View Questions' in the drop-down menu. These can also be seen in the Customer Portal.

There is no limit to the number of queries you can generate with Darktrace Services/Ask the Expert, but at times the Cyber Analyst may redirect you to internal training or technical operations teams if the question is less about analysis and more about software functionality. Software/Hardware Support services and feature requests must still be raised via the Customer Portal.

All Darktrace Services/Ask the Expert queries are queued for access to the global Darktrace Cyber Analyst team. While Darktrace Services/Ask the Expert is not a direct chat feature, if you are facing a real-time attack, Darktrace will prioritize access to the SOC and provide close support and rapid feedback during the initial investigation to ensure you have access to the data and intelligence generated from the Darktrace Immune System platform.

## Service Delivery and Customer Data

Access to our 24/7 services will depend upon your subscription agreement. The Darktrace Services/ Proactive Threat Notification service requires a standard Call Home connection from your master appliance to the Darktrace Management Center in Cambridge, UK.

Darktrace provides for and monitors full audit logging from the Darktrace Management Center to record actions completed by Darktrace employees during the execution of the contracted services. Darktrace employees are required to give audited reasoning as to why they are accessing any give account before being granted an access token.

The service offerings available require analysis and reporting to occur outside of the Darktrace platform. All data entered into Ask The Expert, both from your employees and the Darktrace Cyber Analyst team, is stored inside the Darktrace Customer Portal which is hosted by Darktrace in the Darktrace Management Center. Closed tickets remain in the portal archive for your review.

# Deployment Information

Darktrace can be installed with hardware, on-prem for your network or virtually with a Cloud Master.

| Package & Deployment Type | Explanation | Deployment Components Please see opposite page for more information |
|---|---|---|
| Darktrace Employee Suite: Cloud | Any combination of Email, Apps and Endpoint services will be hosted in a Darktrace controlled cloud environment. | Cloud Master<br>Endpoints (Premium Only)<br>Apps<br>Darktrace/Email Cloud |
| Darktrace Employee Suite: On-Premise | Any combination of Email and Apps services will be hosted at a customer location with on-premise appliances.<br>If Endpoint is included Darktrace will host additional cloud infrastructure to feed relevant meta data into on-premise appliances. | Endpoints (Premium Only)<br>Apps<br>Darktrace/Email On-Premise Appliance<br>DETECT On-Premise Appliance* |
| Darktrace Infrastructure Suite: Cloud | All services will be hosted in a Darktrace controlled cloud environment even if data is fed from on-premise or 3rd party-cloud solutions. | Cloud Master<br>Network Coverage<br>Endpoints (Premium Only)<br>IaaS<br>Apps<br>Darktrace/Network |
| Darktrace Infrastructure Suite: On-Premise | All services will be hosted at a customer location with on-premise appliances. Even if fed from 3rd party-cloud solutions.<br>If Endpoint is included Darktrace will host additional cloud infrastructure to feed relevant meta data into on on-premise appliances. | Cloud Master<br>Network Coverage<br>Endpoints (Premium Only)<br>IaaS<br>Apps<br>Darktrace/Network |
| Darktrace Platform: Hybrid<br>Darktrace/Email: Cloud<br>Darktrace DETECT: On-Premise | Any Email and Endpoint services will be hosted in a Darktrace controlled cloud environment feeding into on-premise appliances.<br>All other services will be hosted in on-premise equipment at a customer location. Even if fed from 3rd party-cloud solutions. | Endpoints (Premium and Platinum Only)<br>IaaS<br>Apps<br>Darktrace/Email Cloud<br>DETECT On-Premise Appliance* |
| Darktrace Platform: Cloud | All services will be hosted in a Darktrace controlled cloud environment even if fed from on-premise or 3rd party-cloud solutions. | Endpoints (Premium and Platinum Only)<br>IaaS<br>Apps<br>Darktrace/Email Cloud<br>DETECT On-Premise Appliance* |
| Darktrace Platform: On-Premise | Services will be hosted at a customer location with on-premise appliances. Even if fed from 3rd party-cloud solutions.<br>If Endpoint is included Darktrace will host additional cloud infrastructure to feed relevant meta data into on-premise appliances. | Endpoints (Premium and Platinum Only)<br>IaaS<br>Apps<br>Darktrace/Email Cloud<br>DETECT On-Premise Appliance* |

*For Darktrace DETECT On-Premise Application information, please refer to page 2





## Deployment Components

### Cloud Master

Darktrace provides virtualized Darktrace DETECT deployments by hosting a cloud-based master instance within Darktrace cloud environments (AWS and Azure). Virtualized deployments receive data from local probes in the customer network (physical or virtualized), from host-based Client sensors, from integrated third-party services (such as Apps or Cloud) or from connected Darktrace products such as Darktrace/Email.

You are licensed by connections per minute; if this number is exceeded you may incur an additional cost:

- >5,000 CPM
- 5,000 - 10,000 CPM
- 10,000 - 40,000 CPM
- 40,000 - 90,000 CPM
- 90,000 - 150,000 CPM
- 150,000 - 300,000 CPM

### Network Coverage

Darktrace can deploy Physical or Virtual Sensors to ingest raw traffic via a SPAN port or network tap. The number and size of sensors required depends on the peak volume of traffic in that part of the organization.

### Endpoint Coverage

Darktrace deploys lightweight agents onto the endpoint to extend visibility and autonomous response to branch offices and remote workers off the VPN. This allows the system to analyze real-time traffic of remote workers in the same way it analyzes full traffic in the corporate network, correlating a web of connections to learn an evolving understanding of workforce behavior. These agents deliver key data and metadata to the Darktrace DETECT; remote devices are then surfaced alongside devices in on-premises data centers, Apps user behavior and insights from email traffic. The Darktrace agent is provided as an installation package for Windows, MacOS or Linux endpoint devices.

### Infrastructure-as-a-Service (IaaS)

Depending on the deployment scenario and CSP, Darktrace coverage in IaaS environments can include 'vSensors' and 'osSensors' that ingest real-time cloud traffic, as well as 'Security Modules' that ingest event logs highlighting admin activity, such as logins and resource creations. In AWS, Azure, and Google Cloud Platform (GCP), vSensors capture real-time traffic directly from AWS VPC Traffic Mirroring and GCP Packet Mirroring, respectively. The receiving vSensor processes the traffic and feeds the necessary meta data back to a central Darktrace instance for analysis.

### Apps

Provider-specific Darktrace Apps deliver unified visibility across cloud-based collaboration applications. Apps can be deployed remotely and work by integrating with the security APIs of the relevant Apps solutions, ingesting login and data access events and correlating them with 'patterns of life' in the rest of the organization.

### Autonomous Response

- **Darktrace/Network:** To autonomously respond to threats on the on-premise network, Darktrace/Network responses are sent via the management interface of the Darktrace appliance or vSensor, or can be taken by integrating with existing firewall infrastructure.
- **Darktrace/Email:**
  - **Cloud:** Darktrace/Email Cloud integrates seamlessly with a virtualized or on-premise master and can be deployed for Google Workspace, Microsoft 365 or Hybrid Exchange environments. Email data is delivered to Darktrace/Email via a journal rule, and Darktrace can autonomously respond to threats by integrating with the email provider's API.
  - **On-Prem:** The Darktrace/Email appliance integrates seamlessly with an on-premise appliance and is used to protect On-premises Exchange environments. Email data is delivered to Darktrace/Email via a journal rule, and Darktrace can autonomously respond to threats by integrating with the Exchange server's API.
- **Darktrace/Apps:** Darktrace RESPOND-enabled Apps are also available for Microsoft 365, Google Workspace, Duo, Zoom and Okta, enabling the extension of autonomous response into business critical third-party platforms via API integration.

# Darktrace Appliance Specifications

Darktrace appliances are highly tuned, high performance pieces of hardware that host the Darktrace platform. There are multiple types of Darktrace appliance, with different throughput capacities and options for data ingestion.

Darktrace's technical experts will help you decide which type of appliance you need based on the organization's bandwidth and the number of internal devices present.

**Deployment Usage Fees/Appliance (Small):** Ideal for small deployments with a limited number of devices. It can be configured as a probe to act as a collector in larger deployments. The /Appliance (S) appliance contains the following ports:

- 1 x out-of-band interface
- 1 x 1Gbe admin interface
- 3 x 1Gbe analysis ports

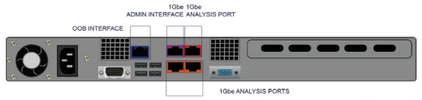



**Figure 1:** Deployment Usage Fees/Appliance (Small)

**Deployment Usage Fees/Appliance (Medium):** Small to Medium sized companies typically choose the Medium DCIP as they're 25x more powerful than a small in terms of connection count capacity. The /Appliance (M) appliance contains the following physical ports:

- 1 x out-of-band interface
- 1 x 1Gbe admin interface
- 3 x 1Gbe analysis port
- 2 x SFP+ analysis ports

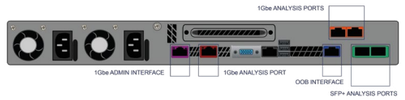



**Figure 2:** Deployment Usage Fees/Appliance (Medium)

**Deployment Usage Fees/Appliance (X2):** The Darktrace /Appliance (X2) series appliances are capable of ingesting data from multiple sources over different types of cable media. The X2 series is suitable for deployment in higher capacity environments and can operate as a master or probe as part of a distributed Darktrace deployment, or can function as a standalone device. The X2 series can be further expanded by additional network interface modules to provide further flexibility in deployment configuration. The /Appliance (X2) appliance contains the following physical ports:

- 1 x out-of-band interface
- 1 x 1Gbe admin interface
- 1 x 1Gbe analysis port
- 2 x 1Gbe / 10Gbe analysis ports
- 2 x SFP+ analysis ports

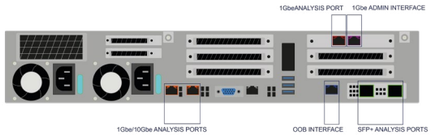



**Figure 3:** Deployment Usage Fees/Appliance (X2)

**Deployment Usage Fees/Appliance (Z):** The DCIP-Z series combine maximum processing power and high speed disk access. DCIP-Z appliances are suited to be placed as master appliances at the core of a high throughput master/probe distribution. The DCIP-Z appliance contains the following physical ports:

- 1 x out-of-band interface
- 1 x 1Gbe admin interface
- 1 x 1Gbe analysis port
- 2 x 1Gbe / 10Gbe analysis ports
- 2 x SFP+ analysis ports

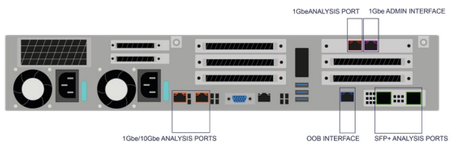



**Figure 4:** Deployment Usage Fees/Appliance (Z)

**Deployment Usage Fees/Appliance (XA):** The /Appliance (XA) appliance combines the hardware power of the /Appliance (X2) series with an FPGA NIC designed to pre-process incoming traffic. XA appliances are suited as probe appliances for high bandwidth environments, for situations that would otherwise require multiple probe appliances. The /Appliance (XA) appliance has the following physical network interfaces:

- 1 x 1Gbe admin interface
- 1 x Out of Band interface
- 4 x 10Gbe SFP+ analysis port OR 1 x 40Gbe QSFP+ analysis port

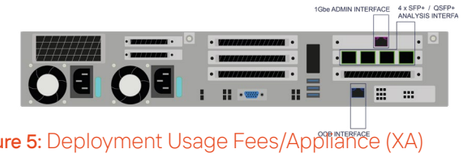



**Figure 5:** Deployment Usage Fees/Appliance (XA)





Peak sustained throughput, maximum unique internal devices and maximum connections per minute are dependent on the type of traffic analyzed, the behavior of the devices and the application of software features. The values in this table have been derived from real-world corporate networks, and refer to a sustained rate, allowing for traffic peaks. Every network is different and so these metrics should be used as a guide only. In addition, the exact throughput capacity of any metric is dependent on the type and nature of the traffic seen by Darktrace. Peak sustained throughput is the 95th percentile of bandwidth ingestion.

| | /Appliance (S) | /Appliance (M) / (Email) | /Appliance (X2) | /Appliance (Z) | /Appliance (XA) |
|---|---|---|---|---|---|
| Form factor | 1U rack mountable (half-deapth) | 1U rack mountable | 2U rack mountable | 2U rack mountable | 2U Rackmount |
| Dimensions (in) | 17.32" x 14.57" x 1.73" | 17.32" x 29.33" x 1.73" | 17.32" x 29.33" x 3.46" | 17.32" x 29.33" x 3.46" | 17.32" x 29.33" x 3.46" |
| Dimensions (cm) | 44cm x 37cm x 4.4cm | 44cm x 74.5cm x 4.4cm | 44cm x 74.5cm x 8.8cm | 44cm x 74.5cm x 8.8cm | 44cm x 74.5cm x 8.8cm |
| Weight (lbs / Kg) | 13.3 lbs / 6 Kg | 33 lbs / 15 kg | 51 lbs / 23 Kg | 51 lbs / 23 Kg | 51 lbs / 23 Kg |
| Racking | Fits 19" Rack | Fits 19" rack | Fits 19" rack | Fits 19" rack | Fits 19" rack |
| Interface admin ports | 1 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T | 10/100/1000 BASE-T |
| Remote management ports | 1 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T |
| Copper analysis ports | 3 x 10/100/1000 BASE-T | 3 x 10/100/1000 BASE-T | 1 x 10/100/1000 BASE-T<br>2 x 10 GBASE-T | 1 x 10/100/1000 BASE-T<br>2 x 10 GBASE-T | N/A |
| SFP+ analysis ports | n/a | 2 x 10Gbe/1Gbe SFP+ | 2 x 10Gbe/1Gbe SFP+ | 2 x 10Gbe/1Gbe SFP+ | 4 x 10 Gbe/1 Gbe SFP+ OR 1 x 40Gbe QSFP+ on FPGA NIC |
| Peak sustained throughput | Up to 300 Mbps | Up to 2Gbps | Up to 5Gbps | Up to 5Gbps | 20Gbps |
| Maximum unique internal devices | Up to 1000 devices analyzed | Up to 8,000 devices analyzed | Up to 36,000 devices analyzed | Up to 50,000 devices analyzed | N/A |
| Maximum connections per minute | 2,000 | 50,000 | 100,000 | 250,000 | 250,000 |
| Power supply | Single 350W IEC 13C 100/240V | Dual 750W IEC 13C 100/240V | Dual 1100W IEC 13C 100/240V | Dual 1100W IEC 13C 100/240V | Dual 1300W IEC C13 100/240V |
| Power consumption | Idle 26 W - 89 BTU/hr | Idle 120 W - 409 BTU/hr* | Idle: 128 W - 436 BTU/hr** | Idle: 128 W - 436 BTU/hr** | Idle: 128W - 436 BTU/hr |
| | 85% 89 W - 305 BTU/hr<br>Max 105 W – 358 BTU/hr | 85% 359 W - 1224 BTU/hr<br>Max 418 W – 1426 BTU/hr | 85%: 365 W - 1245 BTU/hr<br>Maximum: 426 W - 1453 BTU/hr | 85%: 365 W - 1245 BTU/hr<br>Maximum: 426 W - 1453 BTU/hr | 85%: 365W - 1245 BTU/hr, Max 426W 1453 BTU/hr |
| Supported Expansion Modules | Can support one expansion model:<br>2-port 1G/10G SFP+<br>2-port 1G RJ45 1000 BASE-T<br>4-port 1G RJ45 1000 BASE-T | Can support one expansion model:<br>2-port 1G/10G SFP+<br>2-port 10G RJ45 10000 BASE-T<br>2-port 1G RJ45 1000 BASE-T<br>4-port 1G RJ45 1000 BASE-T | Can support up to three expansion models:<br>2-port 1G/10G SFP+<br>2-port 10G RJ45 10000 BASE-T<br>2-port 1G RJ45 1000 BASE-T<br>4-port 1G RJ45 1000 BASE-T | Can support up to three expansion models:<br>2-port 1G/10G SFP+<br>2-port 10G RJ45 10000 BASE-T<br>2-port 1G RJ45 1000 BASE-T<br>4-port 1G RJ45 1000 BASE-T | N/A |
| Safety certificate | UL 60950-CSA 60950, EN 60950, IEC 60950 CB Certicate & Report, IEC 60950 | | | | |
| EMI Certification | FCC Part 15, Class A (CFR 47) (USA), ICES-003 Class A | | | | |

*In some cases, /Appliance (M) appliances will have a power supply of Dual 750W IEC 13C 100/240V.

**In some cases, /Appliance (X2)-11G and DCIP-Z appliances will have a power supply of Dual 1100W IEC 13C 100/240V

# Darktrace/Email – Data Storage and Security Schedule

## Summary

1. Darktrace/Email (formerly "Antigena Email") is an autonomous response module that takes action against email-borne attack campaigns. Hosted in one of Microsoft Azure or Amazon AWS the Darktrace/Email Cloud ("AEC") to provide insight and control over a Customer's email activity.
2. The AEC AI operates to extract metrics and meta data from Customer's Office365 (or equivalent cloud email system) email traffic to develop a 'pattern of life' for email activity. By correlating data across email and network traffic, AEC is able to evaluate the level of threat posed by an email and to spot unusual, anomalous emails that have bypassed existing email gateway tools.

## Data Transfer and Storage

3. All data is encrypted in transit and at rest within AEC.
4. Where data is stored on the cloud, Darktrace will maintain Customer Data in the hosted location specified on the Product Order Form (unless otherwise directed by Customer). As Darktrace has no control of Customer Data uploaded to AEC, it shall remain strictly Customer's responsibility to ensure that the uploading of such data complies with international data protection laws and regulations governing the international or cross- border data transfer of information.

## Data Retention and Transfer

5. Data is retained on the AEC at different rates which depend on the type of data. All data retention polices are in control of the client and can be configured via the 'Config' page. Data retention may be dynamically reduced by the instance to optimise performance. Retention categories include:

- Log Metrics
- Derived and aggregated data
- Raw email data
- Actioned email
- Flagged email

6. A full list of extracted and derived metrics is available within the Email Console 'Advanced' tabs. No searchable facility exists over the content of emails, or attachments or links contained therein. The ability to download emails from the user interface is not available for any account not under the control of Customer's organisation. The content and body of emails is not searchable by Darktrace and does not form part of the detection function other than as a source for the extraction of these metrics and to permit the end-user recovery options. Any original email buffered and maintained in storage is individually encrypted above and beyond the instance storage encryption. At the end of the applicable retention period as set forth in the policies, raw emails will be securely erased.
7. Customer's AEC will provide information to detect and respond to anomalous email activity. AEC will supply information to enable Customers to respond to email borne threats.
8. The telemetry data that is in the AEC is limited to the following:

- Probabilistic data structures which describe the pattern of activity, Darktrace rarity and frequency scores of visited hosts, domains, file hashes and links seen in the Darktrace monitored environment. These data structures do not include any of these details in an extractable format
- Hostname, IP, MAC address, Operating system, Device label and time of last seen are transferred
- Darktrace Alert information. Notifications of Alerts occurring as a result of anomalous network activity may be transferred to the AEC instance for the purposes of security forensics.
- A mapping between those properties and nominated AEC models
- Email addresses, naming, and groups found in emails and any associated email repositories

## Data Access by Darktrace

9. Access to AEC by Darktrace personnel is limited to the following purposes:

- Initial set up, configuration and traffic validation
- Access for the creation of customer reports (as part of trial, or as an on-going service agreement)
- Security incidents
- Support incidents

10. All email data access is logged and controlled. Logs of all data access, whether made by Customer or by Darktrace personnel, is available to Customer through the audit page in the interface. The body content of original emails is not available to Darktrace personnel through the interface and emails are individually encrypted.
11. There is no part of the workflow of any Darktrace personnel that requires access to original email.
12. Elements of emails, which already have a degree of anomaly associated with them, including attachment details and links and their derived properties may be collated by the Darktrace SOC (Security Operations Centre) for the purposes of analysis and security enhancement.

## Link Operations

13. Under certain circumstance, and as dictated by Darktrace or Customer models, links present in emails may be rewritten to redirect any user clicking that link via a Darktrace service. This link service will download the content of the destination of the original link and apply additional security checks on that destination and its content. Darktrace reserve the right to utilise third party services for elements of this security checking. No part of the service will identify to those third parties any details of the user, or organisation, performing the click action. Darktrace models will only re-write a link if some level of anomaly is detected that gives a reasonable suspicion that additional security checks may be necessary.

## Data Protection

14. Darktrace will protect any Customer Personal Data processed by AEC in accordance with the Data Protection Addendum at Appendix 2 of the Master Customer Agreement, and additionally subject to the following:

A. Details of Processing:

i. Subject Matter: Customer email traffic

ii. Duration: As set forth in the Product Order Form or as specified by system configuration

iii. Purpose: The provision of AEC

iv. Nature: Storage, compute and analysis of Customer email traffic

v. Type of Personal Data: Customer Data uploaded to AEC

vi. Categories of Data Subjects: May include Customer's customers, employees, suppliers and end-users

B. Sub-processors:

i. Customer hereby authorises Darktrace to use Amazon AWS or Microsoft Azure as applicable (the "Cloud Provider") as a sub-processor to fulfil its contractual obligations under the Agreement. Customer acknowledges that this authorisation will extend to and include the sub-processors used by the Cloud Provider, a list of which is available at the Cloud Provider's website.

ii. Darktrace will have in place with the Cloud Provider a written agreement equivalent to the terms contained herein to protect Personal Data.

iii. The Cloud Provider will ensure the security of any Personal Data processed by reason of this Agreement in accordance with its standard security measures and practices.

iv. Darktrace will remain responsible for all acts or omissions of the Cloud Vendor under this Agreement.

C. Transfers of Personal Data:

i. Customer will specify the location where Customer Data will be hosted (the "Region"). Once selected, neither Darktrace nor the Cloud Provider will transfer Customer Data from the Region except as necessary to provide the AEC offering or to comply law.

ii. The EU Model Clauses shall apply to the extent the processing of Personal Data by the Cloud Provider involves a transfer of Personal Data which originates in the EEA to a third country outside of the EEA. For such purposes, Customer hereby authorises Darktrace to enter into the EU Model Clauses with the Cloud Provider on Customer's behalf.

# Darktrace/Email For Onpremises Exchange

## Introduction

Darktrace/Email for Exchange (Onpremises) represents a powerful expansion of Darktrace DETECT and RESPOND autonomous, responsive capabilities into an area of operations traditionally difficult to manage and maintain. A ground-level departure from the legacy approach to securing the network against malicious emails, Darktrace/Email's contextualized actions rest entirely in wider patterns of activity identified across the business by Darktrace's powerful Cyber AI. It provides both visibility and unparalleled, intelligent response.

- Seamlessly integrates your existing Darktrace DETECT and RESPOND coverage with your email flow.
- Able to respond at any moment in the full attack life cycle to prevent delivery or to react to network events.
- Adjusts thresholds according to individual user behavior and reports on your most susceptible users.
- Prevent unknown malware
- Anti-spoofing detection
- Detects trusted account hijacking
- URL rewriting and Attachment neutralization
- Advanced detection of phishing attacks.
- Combined network and email security AI for complete coverage.

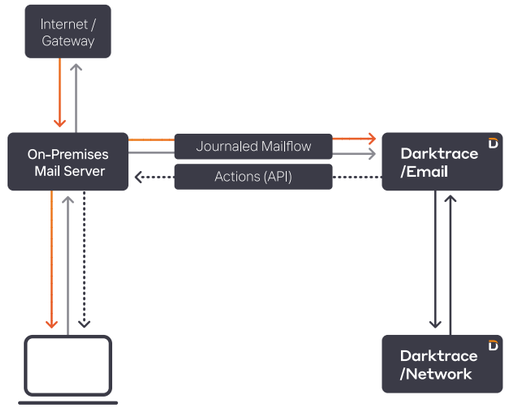
When the need arises to investigate a threat, to create models, and/or to gain better insight into the email hygiene of your organization, the dedicated Darktrace/Email interface provides a range of options for real-time threat investigation. Suspect emails are held for further inspection or authorization for release, user behavior and notable incidents are mapped, and detailed, comprehensive email logs can be filtered by a vast range of metrics including user, domain, attachments and model interaction.

## How It Works

Darktrace/Email works directly with an organization's Exchange Servers, utilizing the Journaling functionality to pass mailflow to the Darktrace/Email for inspection and analysis. In on-premises mailflow environments, a Darktrace/Email appliance is placed locally within the network to analyze and receive email at the source.

On initial configuration, Darktrace/Email will retrospectively process Active Directory and Exchange metadata to gain an intimate knowledge of users, email addresses, correspondents and routine operations. This operation is performed within the Darktrace/Email appliance and will not affect email activity.

In the early stages of deployment Darktrace/Email is run in passive mode, where any actions Darktrace/Email would take for each email are displayed but not performed. During the initial trial period, a customer may choose to enable live autonomous actions on a per-user basis or for specific groups.




## Considerations

The Darktrace/Email appliance should be situated within the same logical network area as the Exchange server to minimize latency in the journaled mailflow. Connectivity between the Darktrace appliance and the Darktrace/Email appliance must also be consistent.

Darktrace/Email works with Journaling rules to achieve full visibility; using Journal requires an email address to send undeliverable mail reports to. We strongly recommend a dedicated mailbox for this purpose, as Darktrace/Email cannot monitor or action emails to the mailbox used for undeliverable mail reports.

Darktrace/Email currently supports Exchange environments running Exchange Server 2013 SP1, or Exchange Server 2016 / 2019 with NTLM(v2) configured.

## Permissions

During the setup process, you will be required to login to your organizational Exchange Server with a Domain Administrator account to create the Connector and Journal rule. An Active Directory user must also be created which Darktrace/Email will utilize API access.

## Easy Deployment Process

1. The deployment of Darktrace/Email is simple: Ensure that an LDAP server is configured in the Darktrace Threat Visualizer before proceeding.
2. In your Firewall, allow the Darktrace/Email Appliance to contact the specified IPs over 22/SSH.
3. Create an Active Directory user for Darktrace/Email and provide the impersonation role.
4. Configure the Darktrace/Email appliance with NTP, SMTP, DNS and HTTPS in a location where it can access the Darktrace Master and your Exchange server.
5. Provide the Darktrace/Email appliance with your Exchange Server IP and the credentials of the user to impersonate.
6. Create a mailflow connector in your Exchange Server environment.
7. Create a Journaling rule in your Exchange Server environment.
8. Configure notifications between your Exchange Server and the Darktrace/Email appliance.
9. Darktrace/Email will then begin baselining all observed email traffic to establish an understanding of your organization's pattern of life.

The power of Darktrace/Email lies in leveraging this unique understanding of day-to-day user email behavior in relation to their past, to their peer group, and to the wider organization. Armed with the knowledge of what is 'normal' for a specific organization and specific individual, rather than what fits a predefined template of malicious communications, Darktrace/Email can identify subtle, sophisticated email campaigns which mimic benign communications and locate threats concealed as everyday activity.

# Darktrace and Google Workspace

## Introduction

Darktrace provides a wide range of components and integration methods that extend Darktrace Self-Learning AI coverage across the entirety of an organization's digital infrastructure - from virtualized networks to SaaS platforms - and ensure that Darktrace fits seamlessly into any existing security stack. The methods offered include Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules for third-party environments, virtualized probes and sensors, custom applications available in vendor stores and support for various industry-standard protocols and methods of interaction.

## Darktrace and Google Workspace

Google Workspace is a platform for enterprise communication, collaboration and business activity. Like many SaaS solutions, user interactions take place and organizational data is hosted in an environment managed by a third party, with a separate audit log and security interface. Because activity and logs are in a third-party environment, it can be a challenge for many security teams keeping track of alerts and activity across SaaS and network environments.

Darktrace offers two integrations for the Google Workspace platform to monitor user activity and provide autonomous response capability: Darktrace DETECT & RESPOND/Apps for Google Workspace module and Darktrace DETECT & RESPOND/Email for Gmail. Between these components, Darktrace DETECT and RESPOND coverage can be expanded to bring the extended digital estate within one platform and under award-winning 'pattern of life' anomaly detection.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules will provide access to the SaaS Console (Customer Portal), a specialized interface for investigating SaaS and Cloud activity. The SaaS console is powered by the Cyber AI Analyst and Darktrace's 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments, while maintaining existing workflows for operators that are already familiar with the Darktrace Threat Visualizer. The SaaS console contextualizes activity on a world map, visualizes anomalous behavior and presents detailed logs of user activity.

## Darktrace DETECT & RESPOND coverage with Darktrace/Apps for Google Workspace

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. The Darktrace/Apps Google Workspace module (Customer Portal) brings Darktrace self learning AI and Darktrace RESPOND autonomous response to the Google Workspace environment.

The module retrieves data from the Google Workspace audit logs; the typical events surfaced include login and access events, user administration and group modifications, calendar events and general administrative activity. Additional, optional event types can also be added to monitoring during configuration including Chrome event logs, data studi event logs and mobile audit information logs.

### Google Drive

The Google Workspace module can monitor Google Drive events such as file and folder modification (including creation and deletion), file visibility changes and sharing events. Additionally, Darktrace provides a selection of models to identify potential Data Loss incidents and anonymous file access events.

The module integrates with Google Workspace audit log via API. By default, one set of requests is made every minute. The data retrieved from Google Workspace is organized by Darktrace into categories which appear as metrics in the Darktrace Threat Visualizer and are available for custom model creation.

Additionally, as of Darktrace Threat Visualizer 5.2, the Google Workspace module support Darktrace RESPOND autonomous response. The module can forcibly logout or disable users acting anomalously in the Google Workspace environment.

### Example Deployment Process:

1. Create a new development project.
2. Enable Admin SDK and Enterprise License Manager API.
3. Create a new Service Account and grant it Domain-Wide Authority.
4. Enable API access.
5. Input details such as an optional Account Name, Admin Email and a JSON file created during the process into the Darktrace Threat Visualizer System Config page.





## Darktrace DETECT & RESPOND coverage with Darktrace/Email for Gmail

Darktrace/Email is a powerful expansion of Darktrace DETECT & RESPOND's autonomous, responsive capabilities into an area of operations traditionally difficult to manage and maintain. Darktrace/Email provides both visibility and unparalleled, intelligent response that integrates self learning AI across network and email security for complete coverage.

Darktrace/Email works directly with an organization's Gmail domains (Customer Portal), using Gmail Journaling functionality to pass mailflow to Darktrace/Email for inspection and analysis. A service account created as part of the configuration process works with the Gmail API to monitor and autonomously action email.

On initial configuration, Darktrace/Email will retrospectively process Google Workspace and Gmail metadata to learn users, email addresses, correspondents and routine operations. This learning is performed in the Darktrace/Email instance and will not affect email activity.

Darktrace/Email works collaboratively with the Darktrace/Apps Google Workspace module to ensure visibility across your Google Workspace environment. Where Darktrace/Email is also monitoring Gmail domains, the Google Workspace module will populate high severity model breaches from Darktrace/Email in the Threat Visualizer user activity logs for relevant Google Workspace users.

### Example Deployment Process:

1. Supply details such as email domains, approximate quantity of email addresses and mailflow, and contact information to your Darktrace representative or via the Darktrace Customer Portal
2. In your Google Workspace environment, create a new development project, enable relevant APIs, create a Service Account and grant the Service Account domain-wide authority.
3. Access the System Config page of the Darktrace Threat Visualizer and enter configuration details.
4. Return to Gmail to configure the journal rule and spam headers.

Darktrace/Email for Gmail is available with other Darktrace DETECT components or as a standalone environment

# Darktrace/Apps Microsoft 365 Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Apps Microsoft 365 module provides visibility over a number of sub-products including Sharepoint/ OneDrive for Business, Dynamics, Teams, and other Microsoft 365 services. Depending on the service, this user activity can include user management, file creation and sharing, and administrative events. Data is retrieved directly from the Microsoft unified audit log, returned information is therefore limited to the events that Microsoft chooses to audit and the data recorded as part of those audit log entries. Returned events will also be restricted to products that your organization has licensed with Microsoft 365.

Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Microsoft unified audit log - by default, one set of requests is made every minute. The unified audit log is populated by Microsoft 365 with aggregated "content blobs" for each service; when an auditable event is created, it can take up to 3 hours for the "blob" it is contained within to be made available in the log. The data retrieved from Microsoft 365 is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation.

Please note, Audit Log Search must be enabled for comprehensive monitoring.

### Sharepoint (OneDrive for Business)

Darktrace retrieves user activity for Sharepoint (OneDrive for Business) and activity produced by Microsoft 365 services which interact with Sharepoint. This activity includes file and folder creation, deletion and modification. Visibility changes and sharing events are also retrieved. Additionally, Darktrace provides a selection of models to identify potential Data Loss incidents and anonymous file access events.

### Dynamics 365

The module can surface Dynamics 365 user activity in the Threat Visualizer where compatible auditing has been configured in the Dynamics instance. Please see the relevant Microsoft documentation on configuring Dynamics 365 auditing. The events returned by the module will depend on the configuration settings of each Dynamics environment; entities with auditing enabled will produce create, read and modify events in the Darktrace Threat Visualizer.

*Please note, Microsoft does not produce audit logs for sandbox environments.*

### Teams

The Darktrace/Apps Microsoft 365 module can retrieve a subset of Microsoft Teams activity including logins and changes to team membership. Also retrieved are administrative actions such as Team and Channel creation and the addition or removal of Apps, Connectors and bots from Channels.

### Administration and Access

Microsoft 365 login activity is managed by Azure AD. Organizations with the Darktrace/Apps Microsoft 365 module will see a limited number of login and management events handled by Azure but will not have full visibility over all administrative activity. Events that will be retrieved include login and access activity, changes to recovery information and changes to multi-factor authentication use. User administration changes including role assignment and removal, group membership, user creation and user deletion will also be retrieved.

In addition to Microsoft 365 events handled by Azure, the module also processes administrative events from a number of services. This includes Microsoft 365 mailbox administration (see "License Requirements" below) as well as general administrative activity like quarantine management, licensing and app approval.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

### Contextual Information

Where Darktrace/Email is also monitoring Microsoft 365 email domains, the module will populate high severity model breaches from Darktrace/Email in these user activity logs for relevant Microsoft 365 users.

The Microsoft 365 module also supports population of contextual user information such as user roles, group membership, and licenses in the Threat Visualizer SaaS Console interface. This contextual data provides valuable insight when investigating user behavior and potentially anomalous access. If admin user roles are detected, the module will automatically tag user entities with the relevant role.

The information available to the module may vary due to role and permission restrictions; where relevant, further details are provided in the user permissions guidance.

## Considerations

Microsoft 365 imposes a complex and regularly updated limit policy on HTTPS requests. If this limit is regularly reached, it may be necessary to make the intervals between polls longer - doing so will increase the time lapse between the occurrence of an event and its detection. Please discuss implementing a larger interval with your Darktrace representative or a member of Darktrace support. The module will only make requests at the defined interval - default 1 minute - if the previous request cycle has completed within the interval. Therefore in high traffic environments, or where a large amount of activity has occurred, it may take longer than the defined interval for the next poll to occur.

The module requires access to specific endpoints in the third-party environment to retrieve event data. The required endpoints are listed on the System Configuration page. Please ensure these endpoints are allowed by any intermediary firewalls.

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

*Please note that it can take up to 12 hours for Microsoft 365 to produce the first event logs after enabling the unified audit log.*

## Autonomous Response

The Darktrace/Apps Microsoft 365 module supports Darktrace RESPOND autonomous response. The module can perform three actions in response to highly anomalous and potentially malicious activity - force a user to logout, disable a user and block an IP (or IP range). The available inhibitors and platforms will be expanded in future releases.

SaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or per-inhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

**Please note, modules authorized before Darktrace Threat Visualizer 5, or authorized solely for monitoring, must be reauthorized to add additional Darktrace RESPOND Permissions to the Graph API authorization. Please refer to the configuration guide for your chosen deployment method for more information.**

### Darktrace RESPOND Considerations

- An Azure P1 license is required for access to the Graph API.
- Due to restrictions on application-level permissions, admin users cannot be disabled or forced to logout using the default authentication method. Block IP actions can still be performed. Authentication with Device Code flow is required to perform these actions on administrative users.
- Where an on-premises Azure AD is synced via Azure AD Connect, actions taken against users in the cloud-based environment (force logout, disable user) will be overwritten.

**To prevent this, turn on "Repeat All Actions" within Darktrace RESPOND settings for the module. This setting will continuously apply the action, so any overwritten changes by Azure AD Connect are reinstated.**





## Permissions

In the default deployment mode, the Microsoft 365 module requires the following permissions to be granted by a Global Administrator user.

### Monitoring Permissions

- Read DLP policy events including detected sensitive data
- Read activity data for your organization
- Read service health information for your organization
- Read all users' full profiles
- Read all audit log data
- Read and write all applications
- Read directory data
- Sign in and read user profile

### RESPOND Only Permissions

- Read and write all users' full profiles
- Read your organization's policies
- Read your organization's security actions
- Read your organization's security events
- Read and write your organization's conditional access policies

The exact permissions requested differs slightly between the two deployment methods offered - full details are provided in the deployment guide.

### License Requirements

General monitoring is compatible with any license that includes access to the Security and Compliance Centre and Unified Audit Logging. These features are included in the Microsoft 365 Business Basic, Business Premium and Enterprise Licenses by default. Please see the Microsoft documentation for further information on whether your license is compatible.

By default, audit logs for mailbox administration activities are only created for users with an E5 license. For users with other license types, please refer to the Microsoft documentation on how to enable this logging in order to ensure these events are visible to Darktrace.

## Deployment Process

Two deployment modes are offered for the Darktrace/Apps Microsoft 365 module - the appropriate method will depend on your organizational policies. Selecting a method is described in more detail in Selecting a Deployment Mode for the Microsoft 365 Module.

The default method, for example, can be simplified to:

1. Access the 'Modules' section of the Darktrace System Config page and select Office 365.
2. Provide the domain of the authorizing user and then in the authorization prompt, click the link.
3. Login in with a Global Admin account and grant the requested permissions. Successful authorization will redirect to darktrace.com
4. Return to the System Config page to confirm the setup was successful.

# Darktrace/Apps Google Workspace Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate Darktrace DETECT and RESPOND capabilities with enterprise SaaS software and Cloud platform solutions, bringing visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module introduces the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloudbased environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Apps Google Workspace module provides visibility over user activity, user management, file creation and sharing, and administrative events. Data is retrieved directly from the Google Workspace audit log, returned information is therefore limited to the events that Google Workspace chooses to audit and the data recorded as part of those audit log entries. Typically, the following events will be recorded and fed through to the Threat Visualizer:

- Login events (including failed)
- Access method changes (multi-factor authentication usage)
- User and Role creation/modification
- Group membership changes
- Calendar event creation and invites
- File and folder modification events including creation and deletion
- File visibility changes or sharing events
- General administrative activity such as organizational unit changes, licensing and app approval

Monitoring is achieved via sets of HTTPS requests made with API access to the Google Workspace (formerly G Suite) audit log - by default, one set of requests is made every minute. In order to achieve highly accurate, real-time monitoring, high frequency polling is recommended. This polling interval can be altered by a member of Darktrace support if desired. The Google Workspace module makes at least two HTTPS requests per loop, and this increases linearly with the number of events being created (which depends on the number of users and how frequently they do things).

Returned events are organized by Darktrace into categories which appear as metrics in the Darktrace Threat Visualizer. This allows events to be easily identified and for models to be written which can identify similar unusual activity across a range of different modules.

### Additional Event Types

By default, the module retrieves audit activity logs of the following types: Admin, Calendar, Drive, GCP (Cloud Login API only), Groups (including Enterprise), Login, Token and User Accounts. In addition to the default coverage, the following additional event types can be added during configuration: Chat, Chrome, Context Aware Access, Data Studio, Meet, Mobile, Rules and SAML.

These event types can be added to existing Google Workspace modules at any time; re-authentication is not necessary.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules will provide access to the SaaS Console (Customer Portal), a specialized interface for investigating SaaS and Cloud activity. The SaaS console is powered by the Cyber AI Analyst and Darktrace's 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments, while maintaining existing workflows for operators that are already familiar with the Darktrace Threat Visualizer. The SaaS console contextualizes activity on a world map, visualizes anomalous behavior and presents detailed logs of user activity.

### Contextual Information

Where Darktrace/Email is also monitoring Gmail domains, the module will populate high severity model breaches from Darktrace/Email in these user activity logs for relevant Google Workspace users.

The Google Workspace module also supports population of contextual user information such as user roles, group membership, and linked apps in the Threat Visualizer SaaS Console interface. This contextual data provides valuable insight when investigating user behavior and potentially anomalous access. If admin user roles are detected, the module will automatically tag user entities with the relevant role.

To retrieve this contextual information, additional scopes must be granted to the module during authentication. The information available to the module may also vary due to role and permission restrictions; where relevant, further details are provided in the user permissions guidance.

## Considerations

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

Google Workspace imposes a complex and regularly updated limit policy on how many HTTPS requests can be made in a given time period. Due to this limit, please consider the following factors when selecting an appropriate polling policy or modifying the default configuration for your environment:

- Time lapse between the occurrence of an event and its detection
- Cost of increasing the number of HTTPS requests that can be made per day

**License Requirements:** Business Standard or higher is required for the Darktrace/Apps Google Workspace module to function.

## Autonomous Response

The Darktrace/Apps Google Workspace module supports Darktrace RESPOND autonomous response. The module can perform two actions in response to highly anomalous and potentially malicious activity - force a user to logout and disable a user. The available inhibitors and platforms will be expanded in future releases.

SaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or perinhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

**Please note, modules authorized solely for monitoring must be reauthorized to add additional Darktrace RESPOND API scopes. Please refer to the configuration guide (Customer Portal).**

### Google Drive

To prevent desktop-based Google Drive sync applications syncing user changes to/from the cloud, the "Disable User" action should be applied. Whilst the "Disable User" action is active, syncing will be prevented.

Users will be required to sign in again to any desktop-based Google Drive sync applications after the "Disable User" action has cleared or expired. After the action is cleared or expired, syncing will resume and any changes made locally by the user will be synced to Google Drive. Therefore, it is recommended that a longer action period is used when performing this action manually so that all investigations can take place before the user is able to resume sync.

### Darktrace RESPOND/Apps for Google Workspace Considerations

- The Google Workspace super administrator user who performs the configuration/authorization process cannot be actioned using "Disable User".
- Users will be required to sign in again

## Permissions

Darktrace/Apps Google Workspace module requires access to the Google Workspace Admin Log to fetch events. A service account with the minimal, read-only Project > Viewer role is created during configuration to facilitate this.

## Deployment Process

The deployment process for Darktrace/Apps Google Workspace module is relatively straightforward and is described in more detail in the setup guide. Essentially the process comes down to:

1. Create a new development project and enable Admin SDK & Enterprise Manager License APIs (optional).
2. Create a new Service Account for the newly created project to be utilized by Darktrace and provide the Service Account with Domain-Wide authority.
3. Input details, such as an Account Name, your Admin Email and a JSON file created during the process into the Darktrace Threat Visualizer configuration page.

# Darktrace/Apps Salesforce Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Apps Salesforce module provides coverage over administrative, resource modification and file events. By default, it monitors a subset of sObjects - resources in the Salesforce environment - but this is easily expandable on the System Config page to ensure coverage over your desired resources. The module queries the Salesforce API for creation, modification and deletion of sObjects that it is actively monitoring. By default, the following classes are monitored:

- Account
- Contact
- Dashboard
- Content Document
- Document
- Event
- Task
- User

Login activity and modifications to the Setup area are also retrieved from auditing endpoints, separate from sObject monitoring.

In addition, the module retrieves and processes Salesforce Event Logs which cover the following events:

- Report creation
- Report exports/downloads
- File uploads
- File downloads
- Content document distribution (sharing)

Salesforce attempts to create a new Event Log every hour but will default to 24 hours if an error occurs - the module will request the Event Log hourly if available.

By default, the module for Salesforce polls every 60 seconds. In order to achieve more accurate, real-time monitoring, high frequency polling is recommended.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

Salesforce imposes a limit on the number of HTTPS requests executed by a company over a rolling 24 hour period, calculated by Salesforce license type. This limit is between 15,000 and 1,000,000 requests per day and is applied across all services querying the API of a specific Salesforce instance. In default configuration, the module makes 8 queries for sObjects, 2 queries for audit information (Login History and Setup modifications) and 1 query for Event Logs at a polling rate of every 5 minutes. Over 24 hours, this produces a minimum of 3,168 requests. Adding additional sObjects, or high volumes of user activity, will greatly increase the number of requests required.

Your Darktrace representative can alter the polling frequency if rate-limiting is occurring. Please consider the following factors when selecting an appropriate polling policy or modifying the default monitoring configuration for your environment:

- Number of sObject classes monitored
- Time lapse between the occurrence of an event and its detection
- Differentiation of separate events occurring within a short time frame on the same sObject, as queries only register the most recent modification
- Demand for API requests across all services querying Salesforce
- Cost of increasing the HTTPS request limit

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

**License Requirements:** Lightning Enterprise License or higher is required for the Darktrace/Apps Salesforce module to function.

The module is currently limited to Salesforce Sales Cloud. Salesforce Commerce Cloud (Demandware) and Marketing Cloud are not supported.





## Autonomous Response

The Darktrace/Apps Salesforce module supports Darktrace RESPOND autonomous response. The module can perform three actions in response to highly anomalous and potentially malicious activity - force a user to logout, freeze a user and disable a user.

SaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or per-inhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

No additional Salesforce permissions are required to enable RESPOND capabilities. If RESPOND is licensed for an existing Darktrace DETECT/Apps Salesforce module, the module "Account Permissions" field should automatically update to display "RESPOND" after the license is added; if not updated automatically, click the "Authorize" button to update.

## Darktrace RESPOND/Apps for Salesforce Considerations

- The "Disable User" action utilizes the "deactivated" state on Salesforce users. Under specific circumstances (please see Deactivate Users), deactivating the user may not be possible. In this case, the "Freeze User" inhibitor should be used as an alternative.
- The System Administrator user who performs the configuration/authorization process cannot be actioned using "Disable User".

## Permissions

Darktrace SaaS module for Salesforce requires permission to:

- Access your basic information
- Access and manage your data
- Provide access to your data via the web
- Access and manage your Chatter data
- Provide access to custom applications
- Allow access to your unique identifier
- Access custom permissions
- Access and manage your Wave data
- Access and manage your Eclair data
- Perform requests on your behalf at any time

These permissions are required in order to monitor for events, and so that Darktrace for Salesforce can continue monitoring with no further user interaction required.

## Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the System Config page. Select Modules from the left-hand menu.
2. Select Salesforce from the available Darktrace/Apps modules (under heading "Cloud/SaaS Security"). A new dialog will appear. Ensure the module is enabled.
3. Click the "New Account" button to create an account - if an account is already configured, the button is located underneath the existing entry. Add an Account Name - this field will be displayed in the Threat Visualizer alongside events from Salesforce.
4. Under Information, click the authorization link.
5. Login in with an account with administrative permissions over the domains you wish Darktrace to monitor and grant the requested permissions. Generate the authorization code and URL.
6. Return to the Darktrace Threat Visualizer System Config page and enter the authorization code and URL into the appropriate fields. For security reasons, the code will expire after a short period so this step must be performed immediately after generation.
7. Click the "Authorize" button to begin monitoring your Salesforce environment. After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the Status section

**The module is now authorized and monitoring your domains. Please note, if changes are made to your Salesforce domains or the user who performed the authorization is modified or deleted, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.**

# Darktrace/Apps Box Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Apps Box Module utilizes the Box SDK to provide visibility over content management and user activity within the Box platform. Data is retrieved directly from the Admin logs generated by Box, returned information is therefore limited to the events that Box chooses to audit and the data recorded as part of those log entries. Typically, the following events will be surfaced in the Threat Visualizer:

- Login activity
- User management (creation, deletion)
- Collaboration actions
- Content uploads and downloads
- Content modification

Box makes events available to the Darktrace module within minutes of the event occurring. Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Box API - by default, one set of requests is made every minute.

The data retrieved from Box is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation. Additionally, Darktrace provides a selection of models to identify potential Data Loss incidents and anonymous file access events.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

Box makes at least one HTTPS request per loop. The number of HTTPS requests made increases linearly with the number of events being created (which depends on the number of users and how frequently they do things). Box imposes a limit on the number of HTTPS requests allowed in a given time period. This limit is 25,000 API calls per month for a Starter account, 50,000 for Business-tier accounts and 100,000 for an Enterprise account.

Due to this limit, please consider the following factors when selecting an appropriate polling policy or modifying the default configuration for your environment:

- Time lapse between the occurrence of an event and its detection
- Cost of upgrading the account to increase the number of HTTPS requests that can be made per day

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

## Permissions

Darktrace/Apps Box Module requires the following permissions in order to fetch events:

- Read and write all files and folders stored in Box
- Manage enterprise
- Manage users
- Manage groups
- Manage enterprise properties
- Manage retention policies
- Manage webhooks v2

Although these permissions must be granted by an Admin user, the module for Box module does not acquire any Admin permissions, and appears as a separate entity to the Box system.





## Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the System Config page. Select Modules from the left-hand menu.
2. Select Box from the available Cloud/SaaS Security modules. A new dialog will appear. Ensure the module is enabled.
3. Click the "New Account" button to create an account - if an account is already configured, the button is located underneath the existing entry. Add an Account Name - this field will be displayed in the Threat Visualizer alongside events from Box.
4. Under Information, click the authorization link.
5. Login in with an account with administrative permissions over the domains you wish Darktrace to monitor and grant the requested permissions.
6. Return to the Darktrace Threat Visualizer System Config page and enter the authorization code into the appropriate field. For security reasons, the code will expire after a short period so this step must be performed immediately after generation.
7. Click the "Authorize" button to begin monitoring your Box environment.

   After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the Status section

The module is now authorized and monitoring your domains. Please note, if changes are made to your Box domains or the user who performed the authorization is modified or deleted, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.

# Darktrace/Apps Dropbox Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Apps Dropbox Module provides visibility and analysis over file activity and administrative activity within Dropbox. Data is retrieved directly from the Dropbox API, returned information is therefore limited to the events that Dropbox makes available and the data recorded as part of those entries. Typically, the following events will be surfaced in the Threat Visualizer:

- Login activity and access changes
- File modifications and deletions
- File uploads and downloads
- File and folder access permissions changes
- Changes to group membership and user roles
- File sharing changes

Please note, customers with the Dropbox Standard Business plan will have visibility over login events only.

Monitoring is achieved by utilizing the Business API and relevant Dropbox SDK - by default, the module for Dropbox polls every 60 seconds. In order to achieve more accurate, real-time monitoring, high frequency polling is recommended. Dropbox event logs are updated in real time, allowing for real-time monitoring processes.

The data retrieved from Dropbox is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation. Additionally, Darktrace provides a selection of models to identify potential Data Loss incidents and anonymous file access events.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

Dropbox imposes a limit on the number of HTTPS requests allowed in a given time period; this limit is not made publicly available. Dropbox limits HTTPS requests on a per-app basis. This means that the number of requests utilized by the module for Dropbox will not impact other applications installed by the customer, and vice-versa.

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

License Requirements: It is highly recommended for customers with the Standard Business plan to upgrade to the Advanced Business plan, as this allows the Darktrace/Apps Dropbox Module to monitor all events related to files. For customers with the Dropbox Standard Business plan, the module for Dropbox can only detect login events.

## Permissions

Darktrace/Apps Dropbox Module requires access to the company's team information, as well as the team's detailed activity log. Although these permissions must be granted by an Admin user, the module for Dropbox does not acquire any Admin permissions and appears as a separate entity to the Dropbox system.

## Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the System Config page. Select Modules from the left-hand menu.
2. Select Dropbox from the available Cloud/SaaS Security modules. A new dialog will appear. Ensure the module is enabled.
3. Click the "New Account" button to create an account - if an account is already configured, the button is located underneath the existing entry. Add an Account Name - this field will be displayed in the Threat Visualizer alongside events from Dropbox.
4. Under Information, click the authorization link.
5. Login in with an account with administrative permissions over the domain you wish Darktrace to monitor and grant the requested permissions.
6. Generate the authorization code. Return to the Darktrace Threat Visualizer System Config page and enter the authorization code into the appropriate field. For security reasons, the code will expire after a short period so this step must be performed immediately after generation.
7. Click the "Authorize" button to begin monitoring your Dropbox environment.

   After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the Status section

The module is now authorized and monitoring your domains. Please note, if changes are made to your Dropbox domains or the administrator credentials change, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.

# Darktrace/Apps Slack Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Apps Slack module provides coverage over access, user modification, channel modification and platform administration within Slack. Activity is retrieved from the Slack Audit Logs API, returned information is therefore limited to the events that Slack makes available and the data recorded as part of each log event. Typically, the following events will be surfaced in the Threat Visualizer:

- Modifications to users including creation, deletion, guest creation and role changes.
- User logins, logouts and changes to authentication settings.
- Changes to channels including creation, deletion and membership.
- Administrative activities on workspaces and organization.
- File actions such as downloads and sharing.

The types of activity audited are frequently expanded - full details of the Slack activity covered by audit log monitoring can be found in the relevant Slack documentation. Information on any potential delay for the creation of audit logs is not made available. Returned events are organized by Darktrace into categories which appear as metrics in the Darktrace Threat Visualizer. This allows events to be easily identified and for models to be written which can identify similar unusual activity across a range of different modules.

Please note, the module monitors user action such as logins, role changes and channel management - it does not monitor message content or frequency of message creation.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

The Slack Audit Logs API utilized by Darktrace is rate limited to 50 calls per minute. If this limit is regularly reached, it may be necessary to make the intervals between polls longer - doing so will increase the time lapse between the occurrence of an event and its detection. Please discuss implementing a larger interval with your Darktrace representative or a member of Darktrace support.

Delays may be incurred where the SaaS or Cloud platform does not make events available to the Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

License Requirements: The Darktrace module requires a Slack Enterprise Grid license to operate.

## Permissions

The Slack module requires the User Token Scope auditlogs:read to be granted by an Organization Owner during the setup process.

## Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the System Config page. Select Modules from the left-hand menu.
2. Select Slack from the available Cloud/SaaS Security modules. A new dialog will appear. Ensure the module is enabled.
3. Click the "New Account" button to create an account - if an account is already configured, the button is located underneath the existing entry. Add an Account Name - this field will be displayed in the Threat Visualizer alongside events from Slack. Save your changes.
4. Under Information, select the authorization link.
5. Login in with an account with Organization Owner permissions over the Slack workspaces you wish Darktrace to monitor.
6. Ensure that the app is being installed at the Enterprise Grid level, rather than an individual workspace. The dropdown in the top right should state "My Grid Org", not "My Workspace".
7. Accept the scopes and generate the authorization code. Return to the Darktrace Threat Visualizer System Config page and enter the authorization code into the appropriate field. For security reasons, the code will expire after a short period so this step must be performed immediately after generation.
8. Click the "Authorize" button to begin monitoring your Slack environment. After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the Status section.

The module is now authorized and monitoring your Slack workspaces. Please note, if changes are made to your Slack organization or the user who performed the authorization is modified or deleted, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.

# Darktrace/Apps Zoom Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Apps Zoom module provides visibility over account and user administration and meeting activity.

To monitor sign in events and account modification, the module gathers and processes Operation Logs and Sign In/Sign Out logs generated by Zoom. Activity surfaced in the Threat Visualizer, therefore, is limited by the events that Zoom chooses to log and the data recorded as part of each entry. For example, failed login activity is not currently audited by Zoom and therefore is not retrievable. Typically, the Zoom module will retrieve the following user administration and access events:

- Sign in/Sign out events
- Account setting changes
- User modification, creation and deletion
- Role modification, creation and deletion
- Group modification, creation and deletion
- Changes to billing information.

Meeting activity is retrieved directly from the Zoom API by the module; meeting data is made available by Zoom after a meeting of two-or more participants has concluded and can take up to 30 minutes (after meeting end) to be produced. Details surfaced in the Darktrace Threat Visualizer will include:

- Meeting host activity
- Meeting participation activity
- Meeting information such as name, topic and whether the meeting was recorded.

Please note, dashboards must be enabled within your Zoom environment to retrieve meeting activity information.

Monitoring is achieved via sets of HTTPS requests to the Zoom API, authenticated by a Zoom app created during the configuration process - by default, one set of requests is made every minute. The data retrieved from Zoom is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation.

### Zoom Webinar

Webinar activity from Zoom Webinar can also be optionally retrieved. The details surfaced for these events are very similar to those for meeting activity as described above. This includes webinar host activity, participation activity and webinar information such as name, whether screenshare was used, and whether the webinar was recorded.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

Zoom imposes a limit on the number of API requests allowed in a 24hr period, calculated by both Zoom license type and endpoint requested. The module must make individual requests for each meeting and each participant, therefore high volumes of meeting activity and external meeting participants will greatly increase the number of requests required.

Please consider the following factors when selecting an appropriate polling policy or modifying the default monitoring configuration for your environment:

- Time lapse between the occurrence of an event and its detection
- Cost of increasing the HTTPS request limit

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

License Requirements: a Zoom Business, Education or API Plan is required for the Darktrace Security Module for Zoom to function.

## Autonomous Response

The Darktrace/Apps Zoom module supports both DETECT and RESPOND capabilities. The module can perform two actions in response to highly anomalous and potentially malicious activity: disable a user and forced logout.

SaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or per-inhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

Please note, the Darktrace module for Zoom is Darktrace RESPOND-enabled by default (license required). Re-authentication is not necessary when an Darktrace/Apps license is added.

## Darktrace RESPOND Considerations

- Due to limitations in the Zoom API, Admin or higher users cannot be disabled.
- Users who are logged out or disabled are not removed from meetings active at the time of action.
- Reverting the Zoom "disable user" action is a two-step process. In the event that the second step (license restoration) is interrupted, the user will be restored with a basic license.

## Permissions

The Darktrace/Apps Zoom module requires an app created within the Zoom environment to utilize for API access. The app must be created and authorized by a user with access to user activity logs (possessing the user activities reports role), such as an account owner.

The app created during configuration must be provided with the "report:read:admin", "dashboard_meetings:read:admin", "dashboard_webinars:read:admin" (optional for Zoom Webinar coverage) and "user:write:admin" (required for Darktrace RESPOND) scopes.

## Deployment Process

1. Access the Zoom Marketplace as an admin or account owner of the domain to be monitored.
2. Click on Develop and select Build App.
3. Choose OAuth, and create an app.
4. Select a name for the app - for example "Darktrace". Select Account-level App and deselect publishing the app.
5. In the app credentials section, enter the Redirect URL as: https://dista.darktrace.com/iry-hor/callback.html Also, add this URL as a whitelisted URL.
6. Navigate to the Information section and enter:
   - Suitable short and long descriptions for the app.
   - A developer name and email address. These fields are required for app creation but will not be used; we recommend using the email address of the user configuring the app.
7. Navigate to the Scopes section and click Add Scopes. Add the following scopes:
   - report:read:admin
   - dashboard_meetings:read:admin
   - user:write:admin
8. In the Activation section, an Installation URL should now be present. which can be used to generate your authorization code.
9. Keeping the Zoom window open, access the Darktrace Threat Visualizer and navigate to the System Config page (Main Menu > Admin).From the left-hand menu, select "Modules" and select Zoom from the available Cloud/SaaS Security modules. Click on the module to open a configuration window.
10. A new dialog will appear. Ensure the module is enabled. Click the "New Account" button to create an account.
11. Add an Account Name - this will appear alongside all events retrieved from Zoom.
12. In the Zoom window, locate App Credentials - a Client ID and Secret should be listed. Copy these values into the relevant fields of the Darktrace System Config page.
13. Access the URL generated during Zoom app configuration (Installation URL) and accept the permissions. An authorization code will be generated. Enter this code in the Darktrace System Config page.
14. Click the "Authorize" button to begin monitoring your Zoom environment.

After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the Status section

The module is now authorized and monitoring your domains. Please note, if changes are made to your Zoom domains or the user who performed the authorization is modified or deleted, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.

# Darktrace/Zero Trust Okta Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Zero Trust Okta module provides coverage over access, user sessions and platform administration within the Okta platform. Activity is retrieved directly from the Okta System Log API, returned information is therefore limited to the events that Okta makes available and the data recorded as part of each log event. Typically, the following events will be surfaced in the Threat Visualizer:

- Login activity to Okta and via Okta
- Modifications to groups and users
- Administrative actions
- Changes to apps and app approvals

Full details of Okta activity covered by API monitoring can be found in the relevant Okta documentation. Returned events are organized by Darktrace into categories which appear as metrics in the Darktrace Threat Visualizer. This allows events to be easily identified and for models to be written which can identify similar unusual activity across a range of different modules.

Okta makes events available to the Darktrace module within minutes of the event occurring. By default, the module polls every 60 seconds and retrieves the maximum number of events per request. In order to achieve accurate, real-time monitoring, high frequency polling is recommended.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

### Contextual Information

The Okta module supports population of contextual user information such as user roles, group membership, and linked apps in the Threat Visualizer SaaS Console interface. This contextual data provides valuable insight when investigating user behavior and potentially anomalous access. If admin user roles are detected, the module will automatically tag user entities with the relevant role (requires Super Admin).

The information available to the module may vary due to role and permission restrictions; further details are provided in the deployment guide Permissions section.

## Considerations

Okta imposes a complex and regularly updated limit policy on HTTPS requests, calculated by both Okta license type and endpoint requested. Limits are organization-wide for each endpoint; the Darktrace module must therefore share available requests with other services in your Okta environment that utilize the /api/v1/logs endpoint.

The module is designed to minimize the number of API calls required during operation, however environments with very large amounts of user activity may experience limiting. If this limit is regularly reached, please discuss implementing an alternative polling policy with your Darktrace representative or a member of Darktrace support. When considering a modification, please take into account event latency from reduced polling, possible cost of increasing the HTTPS request limit and demand for API requests across all services querying the System Logs endpoint.

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

Please note, organizations with an One App or Enterprise Okta license may receive notifications if the API limit is approached.





## Autonomous Response

The Darktrace/Zero Trust Okta module supports both DETECT and RESPOND capabilities. The module can disable a user ("Suspend") in response to highly anomalous and potentially malicious activity.

SaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or perinhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

Please note, modules authorized solely for monitoring must be reauthorized to enable Darktrace RESPOND functionality, even if the associated API token possessed the required permissions for Darktrace RESPOND actions. For more information, please refer to the Customer Portal guide - Adding Darktrace RESPOND Capabilities to an Existing Darktrace/Zero Trust Okta Module (Customer Portal)

## Darktrace RESPOND Considerations

- Due to limitations in the Okta API, the disable user action cannot forcibly end currently active sessions in third-party environments. All active user sessions are revoked, but this revocation will only be recognized by the third-party environment when the session expiry time in the environment is reached and a session refresh is attempted with Okta.

## Permissions

The Darktrace/Zero Trust Okta module requires an API key associated with an Okta account. Access to resources and ability to perform tasks programmatically is controlled by the roles of the user associated with the API token in Okta - please see the relevant Okta documentation on privilege level for more information.

The module requires the Okta roles Report Admin and Read Only Admin, and a custom role created during setup that grants three permissions required for Darktrace RESPOND ("Suspend users", "Unsuspend users", "Clear users' sessions").

Depending on your organizational policy, it may be preferable to create a service account limited to these permissions for Darktrace utilization. This approach is recommended; the module deployment guide includes the creation of a unique user for Darktrace utilization.

## Deployment Process

The deployment process for Darktrace/Zero Trust Okta module is described in more detail in the guide - Deploying Darktrace Okta Module (Customer Portal). Essentially, the process comes down to:

1. Create a user in Okta and assign the "Report Admin" and "Read-Only Admin" roles.
2. For Darktrace RESPOND, create a custom role and custom resource assignment and apply to the new user.
3. Access Okta as the newly created user and generate an API Token.
4. Provide the API token and required information on your Okta domain intended for monitoring on the Darktrace System Config page.
5. Click "Authorize" to begin monitoring your Okta environment.

# Darktrace/Zero Trust Duo Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How it works

The Darktrace/Zero Trust Duo module provides coverage over access, user sessions and platform administration within the Duo platform. The module retrieves both administrator and authentication logs from the Duo Admin API via an integration key created during configuration. Returned information is therefore limited to the events that Duo makes available and the data recorded as part of each log event. Typically, the following events will be surfaced in the Threat Visualizer:

- Login activity to Duo and via Duo
- Modifications to groups, directories and users
- Modifications to tokens and policies
- Administrative actions
- Changes to apps and app approvals

Login events are returned by the Duo Authentication log and all other events are returned from the Administrator log. Full details of the Duo activity covered by Administrator log monitoring can be found in the relevant Duo documentation. Returned events are organized by Darktrace into categories which appear as metrics in the Darktrace Threat Visualizer. This allows events to be easily identified and for models to be written which can identify similar unusual activity across a range of different modules.

Authentication events are made available to the module with a delay of 2 minutes. Information on any potential delay for the creation of administrative logs is not made available. By default, the module polls every 60 seconds- in order to achieve accurate, close to real-time monitoring, high frequency polling is recommended.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

The module is designed to minimize the number of API calls required during operation, however environments with very large amounts of user activity may experience limiting due to the restrictive nature of Duo API limits across all integrations. A maximum requests per minute setting can be configured to restrict polling if this limit is regularly reached. Please discuss implementing an alternative polling policy with your Darktrace representative or a member of Darktrace support.

## Autonomous Response

The Darktrace/Zero Trust Duo module supports both DETECT and RESPOND capabilities. The module can disable a user in response to highly anomalous and potentially malicious activity.

SaaS and IDaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or per-inhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace

RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

Please note, modules authorized solely for monitoring must be reauthorized to enable Darktrace RESPOND functionality after a Darktrace RESPOND license is added.

### Darktrace RESPOND Considerations

- Where Active Directory Sync is configured, due to limitations on how users synced from Active Directory can be managed in Duo, Darktrace RESPOND cannot take action against synced users.

Please refer to the relevant Duo documentation for more information on this restriction.

- Darktrace RESPOND cannot take action against Administrator users.
- Due to how Duo SSO handles session expiry, the disable user action cannot forcibly end currently active sessions in third-party environments. All active user sessions are revoked, but this revocation will only be recognized by the third-party environment when the session expiry time in the environment is reached and a session refresh is attempted with Duo.

Please refer to the Duo documentation on session expiry for more information.

## Permissions

The Darktrace/Zero Trust Duo module utilizes an integration key created by a user with the Owner role during the configuration process.

The application requires the "Grant read log" and, optionally, the "Grant read resource" permissions to be granted. Duo accounts can be identified by the Duo username or email address in the Threat Visualizer. If email address is desired, the Grant read resource permission is necessary.

For Darktrace RESPOND/Zero Trust, the "Grant write resource" permission must also be granted to the application associated with the integration key. This can be added during initial setup or added at a later date when RESPOND capabilities are added.

License Requirements: The module requires a paid (non-trial) Duo Beyond, Duo Access, or Duo MFA plan.

## Deployment Process

The following is an outline of the example steps needed to deploy the Darktrace/Zero Trust Duo module.

1. Create a new entry on the Darktrace System Config page.
2. In the Duo Admin Interface, as a user with the "Owner" role, add a new "Admin API" application.
3. Grant the application the required permissions.
4. Copy the tokens and API information from the application in Duo into the relevant fields of the Darktrace System Config page.
5. Click "Authorize" to begin monitoring your Duo environment.

The full deployment process for Darktrace/Zero Trust Duo module is described in more detail in the guide (Deploying Darktrace Duo Module).

# Darktrace/Zero Trust Jumpcloud Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How it works

The Darktrace/Zero Trust JumpCloud module provides coverage over administration of the JumpCloud platform and enables JumpCloud logins to be tracked against devices in the Darktrace Threat Visualizer. User activity is retrieved directly from the JumpCloud Directory Insights API, returned information is therefore limited to the events that JumpCloud makes available and the data recorded as part of each log event. Typically, the following events will be surfaced in the Threat Visualizer:

- Login Success
- Login Failure
- Group Modified
- New System Added
- Command Run
- App Added

In addition to events surfaced in the Threat Visualizer for users of the JumpCloud Platform, the module provides tracking information to Darktrace DETECT/Network for devices accessed via JumpCloud agents and for logins to those JumpCloud agents. If this functionality is desired, please ensure the IPs of devices accessed via JumpCloud are explicitly included in the Deployment Scope on the System Config page.

JumpCloud events makes events available to the Darktrace module within minutes of the event occurring. In order to achieve more accurate, real-time monitoring, high frequency polling is recommended. Returned events are organized by Darktrace into categories which appear as metrics in the Darktrace Threat Visualizer. This allows events to be easily identified and for models to be written which can identify similar unusual activity across a range of different modules.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Autonomous Response

The Darktrace/Zero Trust JumpCloud module supports both DETECT and RESPOND capabilities. The module can disable a user ("Suspend") in response to highly anomalous and potentially malicious activity. Disabled users are logged out from the JumpCloud user interface, are unable to create new device sessions or access resources through the JumpCloud interface.

SaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or per-inhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

No additional JumpCloud permissions are required to enable RESPOND capabilities. If RESPOND is licensed for an existing Darktrace DETECT/Zero Trust JumpCloud module, the module "Account Permissions" field should automatically update to display "RESPOND" after the license is added; if not updated automatically, click the "Authorize" button to update.

## Considerations

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

By default, the module polls every 60 seconds and makes at least one API call per loop. The module may make additional calls to determine the names of users, groups and apps associated with events. This polling interval can be altered by a member of Darktrace support if desired. If throttling problems are encountered, there are several contingency plans we can enact such as introducing a wait time between querying each different subscription to spread the requests out over a longer time period.

License Requirements: The JumpCloud module requires a JumpCloud license with the "Directory Insights" add-on.

## Darktrace RESPOND Considerations

- Due to limitations in the JumpCloud "Suspend" state, the disable user action cannot forcibly end remote login sessions. All active user sessions are revoked, but this revocation will only be recognized by the device when the user attempts to switch user accounts, log out, or reboot the device. Please refer to the relevant JumpCloud documentation for detailed information.
- If JumpCloud is integrated with Active Directory, ensure the JumpCloud Active Directory integration is not configured to remove or unbind users from the AD environment when suspended in JumpCloud. Please refer to UserDisableAction in the relevant JumpCloud documentation for detailed information.
- The "Suspend" action can only be applied to the JumpCloud User account type.

## Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the System Config page. Select Modules from the left-hand menu.
2. Select Jumpcloud from the available Cloud/SaaS Security modules. A new dialog will appear. Ensure the module is enabled.
3. Click the "New Account" button to create an account - if an account is already configured, the button is located underneath the existing entry. Add an Account Name - this field will be displayed in the Threat Visualizer alongside events from Jumpcloud. Save your changes.
4. Log in to the JumpCloud console as an administrator. Open the drop down menu in the top right corner by clicking on the email address of the administrator. Select the 'API Settings...' option.
5. Copy the API Key shown. Please note, if the API Key associated with this administrator is regenerated at any point, the Darktrace JumpCloud module will need to be re-authorized.
6. Return to the System Config page on the Darktrace Threat Visualizer and paste the API Key into the Administrator API Key field.
7. Click the "Authorize" button to begin monitoring your Jumpcloud environment. After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the Status section

Your JumpCloud Security Module is now authorized. Events should appear in the Threat Visualizer after a short delay. This is a one-time process and no maintenance should be required unless the administrator API Key is regenerated.

# Darktrace/Zero Trust Egnyte Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How it works

The Darktrace/Zero Trust Egnyte module provides visibility over login activity, file system modification and changes to file and folder access. Egnyte produces three audit reports on demand - Login Audit, File Audit and Permissions Audit - which are requested and processed by the module to achieve monitoring. Data is retrieved directly from each audit report, returned information is therefore limited to the events that Egnyte chooses to audit and the data recorded as part of each entry. Processing all reports provides coverage over the following events:

- Login activity
- File modifications
- File uploads and downloads
- File and folder access permissions changes

Login activity is available almost immediately, but file activity is only collated by Egnyte periodically. The module will retrieve and surface events in the Threat Visualizer as soon as they are made available to it. Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Egnyte API - by default, one set of audit report requests is made every 10 minutes.

The data retrieved from Egnyte is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation. Additionally, Darktrace provides a selection of models to identify potential Data Loss incidents and anonymous file access events.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

Egnyte restricts the maximum number of requests available to Darktrace module to 5,000 per day. Under default configuration options, the Egnyte module makes approximately 15 requests per cycle so should not reach this limit. If the polling frequency is altered manually and the cap is reached, the module will automatically double the time between poll cycles and wait until the request limit has reset. All events will still be retrieved, but there will be significant delay between the activity and their appearance in the Threat Visualizer.

The module regularly generates and deletes audit reports which may result in some notifications appearing on your Egnyte Dashboard. It is currently not possible to turn these notifications off in Egnyte. The reports referenced are deleted shortly after creation to avoid filling up cloud storage space.

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

The Darktrace/Zero Trust Egnyte module requires the domain selected for monitoring to have an Egnyte license that includes the 'Advanced Security Package'. This package is included by default in Business and Enterprise editions.





## Permissions

The Darktrace module for Egnyte requires the Egnyte.audit permission scope in order to generate and read audit reports. The permissions required also allow us to delete audit reports

## Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the System Config page. Select Modules from the lefthand menu.
2. Select Egnyte from the available Darktrace/Zero Trust modules (under heading "Cloud/SaaS Security"). A new dialog will appear. Ensure the module is enabled.
3. Click the "New Account" button to create an account - if an account is already configured, the button is located underneath the existing entry. Add an Account Name - this field will be displayed in the Threat Visualizer alongside events from Egnyte.
4. Under Information, click the authorization link.
5. Enter your Egnyte domain name in the following page, it will redirect to an Egnyte login page. Log in to Egnyte, generating a unique authorization code.
6. Return to the Darktrace Threat Visualizer System Config page and enter the authorization code into the appropriate field. For security reasons, the code will expire after a short period so this step must be performed immediately after generation.
7. Click the "Authorize" button to begin monitoring your Egnyte environment. After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the Status section

The module is now authorized and monitoring your domains. Please note, if changes are made to your Egnyte domains or the administrator credentials change, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.

# Darktrace/Cloud AWS Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

aws partner network

**Advanced**
Technology Partner

## How It Works

The Darktrace/Cloud AWS module monitors management and administration activity via interaction with AWS CloudTrail. AWS CloudTrail audits Management Events and Data Events (S3/Lambda) which are compiled into logfiles and stored in the AWS S3 bucket created during the configuration process. Data is processed directly from the CloudTrail logfiles, returned information is therefore limited to the events that AWS chooses to audit for each service via CloudTrail and the data recorded as part of each entry. The module can monitor AWS services including:

- EC2
- IAM
- S3
- VPC
- Lambda

Full information about AWS services which support CloudTrail monitoring can be found in the relevant AWS documentation. The AWS module does not currently support the monitoring of CloudTrails created via AWS ControlTower.

AWS CloudTrail events are produced up to 15 minutes after activity occurs. In high-traffic environments, the volume of events that must be retrieved in each polling cycle may result in latency between CloudTrail log production and appearance in the Threat Visualizer.

The diverse event types produced by AWS are organized by Darktrace into categories based on the action type and the AWS service that generates it. These categories then appear as metrics in the Darktrace Threat Visualizer which can be used for modeling.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

## Considerations

AWS works on a 'pay-as-you-go' policy for event logging and API calls. Hence there are small charges involved in CloudTrail detecting events, the API request performed by the Darktrace appliance to get these events and storage costs for the event logs. Costs are dependent upon the amount of activity within AWS, the interval between Darktrace polls and any additional configuration settings applied.

Darktrace/Cloud AWS module also automatically removes associated log files from S3 a day after they are generated, thereby preventing significant data build up. This setting can be disabled via the System Config page and is not available in *Restricted Mode*.

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

### Write-Only Mode

*Write-Only Mode* filters CloudTrail to only record AWS "Write" management events, significantly decreasing processing time in busy environments and reducing costs for log storage, API requests made, and number of events recorded. The filter utilizes the "read-only" and "write-only" settings available in AWS CloudTrail - more information can be found in the AWS documentation.

To use this mode, "Automatically Configure CloudTrail" and "CloudTrail Write Event Filter" must be enabled on the Darktrace System Config page.

## Permissions

Darktrace/Cloud AWS module requires the linked IAM user to have permission to see and modify AWS CloudTrails and have full access to the S3 bucket associated with monitoring. These permissions allow the module to access AWS CloudTrail logfiles, reconfigure the CloudTrail if a misconfiguration is detected, and modify the bucket containing logfiles to ensure there is not an increasing buildup of old logs. Detailed example policy statements are provided in the configuration guide.

Programmatic MFA is also supported on the linked IAM user from Darktrace Threat Visualizer 5.2.

### Restricted Mode

The module can also be deployed in a restricted mode where the linked IAM user is solely granted "read" and "list" permissions to the S3 bucket containing the monitoring logs, but is not granted access to CloudTrail.

### Automatic Account Retrieval

Account IDs are used to retrieve logs from CloudTrail; the module will only retrieve logs for accounts it is aware of. The module can automatically retrieve an up-to-date list of all accounts under the organization if provided an IAM user with the organizations:ListAccounts permission. This list can also be provided manually on the Darktrace System Config page.

## Deployment Process

The deployment process for Darktrace Customers using the Darktrace Security Module for AWS is relatively straightforward and is described in more detail in Deploying Darktrace AWS Security Module. For deployments in ***Restricted Mode*** or with alternative configuration settings, these steps may differ.

For default configuration, the process outline is:

1. Create a new Trail (in AWS CloudTrail); by default the Trail applies to all regions and outputs all logfiles into an S3 bucket.
2. Create an IAM user that has permission to access and modify the CloudTrail and associated S3 bucket.
3. Input configuration details, such as the new IAM user access keys, into the Darktrace Threat Visualizer configuration page.

**After performing these steps, your Darktrace Security Module for AWS will be authorized and begin monitoring events immediately.**

# Darktrace/Cloud Azure Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Cloud Azure Module provides visibility over Microsoft 365 administration and adds additional coverage over IaaS administration in Microsoft Azure.

### Access Management

The Darktrace/Cloud Azure Module provides visibility over management activity and user access handled by Azure AD; Azure Active Directory tracks user activity and sign-in metrics and creates audit log reports that can be retrieved via the Graph API. Data is retrieved directly from the Microsoft Azure audit log endpoint, returned information is therefore limited to the events that Microsoft chooses to audit and the data recorded as part of those audit log entries.

Returned events will also be restricted to products that your organization has licensed with Microsoft 365. Typically, the Azure module will provide coverage over:

- Group administration activity including creation, membership and deletion.
- Access control including management of Service Principals, app authorizations and licensing.
- Login activity such as failed logins, successful logins and changes to passwords.

Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Microsoft Graph API - by default, one set of requests is made every minute. The data retrieved from Azure is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation.

### Cloud Environment

The Darktrace/Cloud Azure Module also retrieves cloud infrastructure resource creation and management events from Microsoft Azure via reader access to the Azure Activity Log. Returned data and events are limited to those that Azure chooses to record and the data recorded as part of those log entries. There may also be a short delay between the event occurring and the Azure Activity Log entry creation. Typically, the following events will be recorded and fed through to the Threat Visualizer:

- Creation of virtual resources including virtual machines, data factories, virtual networks and Azure websites.
- Modification of resource visibility such as network security group changes, Public IP modification, API account creation and changes to the Front Door service.
- Subscription to and validation of cloud services including containerized services, Blockchain providers, Visual Studio and hosting plan changes.

This information is surfaced in the Darktrace Threat Visualizer as management events only - devices and subnets will not be created for virtual machines or other infrastructure which is seen in the activity log. For visibility over virtual resources at the network level, please discuss deploying Darktrace virtual sensors with your Darktrace representative.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.





## Considerations

Microsoft Azure imposes a complex and regularly updated limit policy on HTTPS requests. If this limit is regularly reached, it may be necessary to make the intervals between polls longer - doing so will increase the time lapse between the occurrence of an event and its detection. Please discuss implementing a larger interval with your Darktrace representative or a member of Darktrace support.

The module will only make requests at the defined interval - default 1 minute - if the previous request cycle has completed within the interval. Therefore in high traffic environments, or where a large amount of activity has occurred, it may take longer than the defined interval for the next poll to occur.

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

Please note, the module requires access to specific endpoints in the third-party environment to retrieve event data. The required endpoints are listed on the System Configuration page. Please ensure these endpoints are allowed by any intermediary firewalls.

### License Requirements

- The module is only available for customers with a "Premium P1" license or above, which grants access to Advanced Security/ Usage Reports.
- Azure only produces user activity audit logs for Microsoft 365 services and features that your organization has licensed.

*The module is currently limited to standard Microsoft Azure environments. National Clouds including Azure Government and Azure Germany are not supported.*

## Permissions

In the default deployment mode, the Azure module requires the following permissions to be granted by a Global Administrator user:

- Read all audit log data
- Read all usage reports
- Read and write all applications
- Read directory data
- Sign in and read user profile

## Deployment Process

Two deployment modes are offered to Darktrace Customers using the Darktrace Security Module for Azure - the appropriate method will depend on your organizational policies. For most organizations, the default method will be suitable and can be simplified to:

1. Access the 'Modules' section of the Darktrace System Config page and select Azure.
2. In the authorization prompt, click the link.
3. Login in with a Global Admin account and grant the requested permissions. Successful authorization will redirect to **darktrace.com.**
4. Optionally grant the module reader access in the Azure Portal to monitor virtual resources.
5. Return to the System Config page to confirm the setup was successful.

Selecting a method is described in more detail in Selecting a Deployment Mode for the Azure Module.

# Darktrace/Cloud Google Cloud Platform Module

## Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate Darktrace DETECT and RESPOND capabilities with enterprise SaaS software and Cloud platform solutions, bringing visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module introduces the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloudbased environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

## How It Works

The Darktrace/Cloud Google Cloud Platform module (GCP) provides visibility over administration and user activity within your Google Cloud environment. The module utilizes the Google Cloud logging API to retrieve GCP-audited events - information available to the module is therefore limited to the events that GCP chooses to audit, and the data recorded as part of those audit-log entries. Administration and system events logs are produced by default by GCP and provide the Darktrace module visibility over the creation of cloud resources, API activity and changes to cloud resource configurations. This includes events generated by users and system actions at both the organizational and project-level.

Typically, the following events will be recorded and passed to the Threat Visualizer:

- Resource creation through administrative actions or API calls, such as VM creation
- Resource modification through administrative actions or API calls, such as permission changes
- Resource configuration changes performed by system events
- User-driven API calls and changes to user-provided resource data (derived from Data Access logs, please see below)

A comprehensive list of GCP services which support Cloud Audit Log monitoring and the type of events that are audited can be found in the relevant Google documentation.

Optional Data Access logs can also be produced within GCP and processed by the module to gain additional insight into specific components. These logs are not enabled by default and can be enabled on a per-component basis to gain greater insight. Please note, Data Access audit logs do not record data-access operations on resources that are publicly shared (available to All Users or All Authenticated Users) or that can be accessed without logging into Google Cloud.

### Firebase

Some monitoring is also available over Google Firebase events - Firebase management activity is recorded to the Cloud Admin Activity log and the Cloud Data Access log. Full details of audited events can be found in the Firebase documentation. The production of Data Access logs is optional, therefore additional configuration is required to ensure these logs are produced and available to the module. This configuration is covered in the setup guide.

## Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules will provide access to the SaaS Console (Customer Portal), a specialized interface for investigating SaaS and Cloud activity. The SaaS console is powered by the Cyber AI Analyst and Darktrace's 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments, while maintaining existing workflows for operators that are already familiar with the Darktrace Threat Visualizer. The SaaS console contextualizes activity on a world map, visualizes anomalous behavior and presents detailed logs of user activity.

## Considerations

User access to GCP is authenticated and managed via the Google Workspace platform; this activity is not visible to the GCP module. To monitor logins, user activity, and resource creation/modification across the entire platform, it is recommended to deploy both modules (Darktrace/Apps Google Workspace and Darktrace/Cloud GCP). The deployment guide provides alternative deployment methods, including a dual deployment for fresh installations and an extension process for organizations that already use the Darktrace Google Workspace module.

Data Access logs are an optional part of the Google Cloud Logging service. This logging is largely free, but costs may be incurred above a certain volume of log creation/ingestion. For most organizations, this limit will not be reached (see the relevant Log Pricing resources from Google), but your Darktrace representative can limit the rate of data access events if such costs are a concern.

GCP Cloud Logs are restricted to 60 API requests per minute. By default, the module monitors all projects in the organization for which it is authenticated. If the module regularly makes more than 60 requests per minute, or specific projects like testing environments do not need to be monitored, this scope can be reduced by entering only the project IDs of interest.





Delays may be incurred if the external platform does not make events available to the Darktrace module for processing and analysis within the expected period. Such delays are the responsibility of the third-party platform. Latency between the time an event occurred and the time it was made available to the module are shown in the event metadata within the Threat Visualizer.

License Requirements: The GCP module requires that Google Cloud Operations Cloud Logging be enabled. This should be enabled on all license types by default. If you are not sure whether this available with your GCP license, please see the Google Cloud Operations documentation for more information.

## Permissions

Darktrace Security Module for GCP requires the roles Logging -> Private Logs Viewer and Resource Manager -> Organization Viewer to be granted to a Service Account at the Organizational level.

## Deployment Process

The deployment process for Darktrace/Cloud GCP module is covered in more detail in the configuration guide. Three deployment processes are offered for organizations who wish to just deploy GCP, to deploy both GCP and G Suite modules together or for those with an existing G Suite module who wish to extend its coverage.

Essentially the process comes down to:

1. Create a new development project and enable Cloud Logging APIs.
2. Create a new Service Account for the newly created project to be utilized by Darktrace and provide the Service Account with Domain-Wide authority.
3. Add the Service Account at the organizational level and grant it the required roles.
4. Input details such as an Account Name and a JSON file created during the process into the Darktrace Threat Visualizer configuration page.

## About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,400 organizations globally from advanced cyber-threats.

Scan to LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 4949 7696
info@darktrace.com
darktrace.com