Darktrace for Small & Midsize Businesses

DARKTRACE

AT A GLANCE:

- Learns 'normal' for every organization to catch unknown and unpredictable threats
- Offers always-on, adaptive coverage of your entire workforce and business
- Automates threat investigations at speed and scale
- Easy to deploy, with hundreds of out-of-the-box AI models

The Challenges of Cyber Security

The threat landscape constantly evolves, leaving security teams to face novel and advanced attacks – which now use sophisticated AI tools such as ChatGPT – often moving at machine speed and hitting parts of the digital ecosystem that companies are not prepared to secure.

Just as the threat landscape evolves, so too does a business' digital infrastructure. Today's dynamic workforce is dispersed, agile, and unpredictable and modern businesses are relying on increasingly diverse technologies, from cloud and SaaS services to advanced IoT.

At the same time, security teams are facing a staffing and skills shortage, and must manage disparate security stacks that more often than not present too many alerts to triage appropriately – leaving the real threats unnoticed or improperly managed.

Given these challenges, cyber AI is a must have for any lean security team.

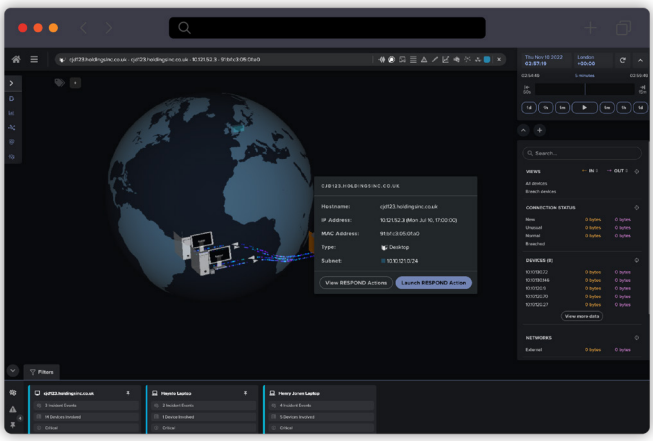


Figure 1: Darktrace autonomously detects and responds to threats with surgical precision, 24/7

Empowering Small Security Teams

Darktrace allows even the smallest security teams to protect their dynamic workforces from the most sophisticated threats, while enhancing the value of existing investments through shared intelligence and active integrations. It offers four interconnected AI engines that constantly communicate and improve an organization's defensive posture across the entire attack lifecycle — aiding in prevention, detection, response, and recovery.

Darktrace's learns your business data. The AI never sleeps – meaning your team can trust that there is always an intelligent solution autonomously detecting, investigating, and responding in real time to threats as they emerge, without the need for configuration or constant tuning.

Instead, Darktrace learns the unique 'pattern of life' of every business, effectively, what constitutes normal. It uses this deep understanding to spot even the most subtle deviations from normal behavior that point to an attack – from advanced threats like Dharma ransomware, to zero-day nation-state attacks like APT41.

The technology doesn't learn what's dangerous from historical data but from an in-depth understanding of each organization and its users.

The Cyber AI Analyst tool optimizes threat investigations by continuously examining every security threat that arises.

It spotlights the highest priority threats and rapidly synthesizes all of the context around an attack into a natural language report. The result is that time-to-meaning and time-to-response are dramatically reduced – allowing security team members time to use their expertise where it really matters. Since the AI learns continuously, it can easily adjust and scale to fit your business.

Highlights

- AI is always-on, for 24/7 coverage
- Solution works without configuration or constant tuning
- AI can adjust and scale to fit your dynamic business

Darktrace Solutions for Common Challenges

How Darktrace Solves Key Pain Points for Startups, Scale-ups, and Local Businesses

Challenge	Darktrace Capability	Learn More
Teams need solutions that work 24/7, even when employees are away.	Darktrace's use of AI allows it to work around the clock. The mobile app also helps ensure teams are informed even when they are away from their computers.	Pages 6 and 7
Attacks can strike quickly and the human team cannot respond in time to minimize business disruption.	Darktrace AI detects threats in real time and can take action at machine speed.	Page 6
There's a shortage of IT specialists, so software must be easy to use out of the box.	Darktrace can deploy with hundreds of out-of-the-box AI models ready to use. Teams can also completely customize their deployments so that the autonomous defense best matches business needs and policies.	Page 6
Security tools must be able to adapt and scale with the business.	Self-Learning AI continuously trains on your unique business data, so it can learn any changes and esaily scales up with your business.	Page 1
Smaller IT teams require optimized workflows to maximize time.	Cyber AI Analyst dramatically reduces time-to-meaning and time-to-response – allowing security team members time to use their expertise where it really matters.	Page 3

> Darktrace is a welcome addition to any cyber-security toolkit, increasing visibility while decreasing response times.
>
> / Vice President of Information Technology, Real Estate Investment

Autonomous Investigations and Reporting Maximize Your Time

Autonomous Investigations: Cyber AI Analyst Augments the Human

For teams that only have five minutes a day to use Darktrace, the most critical capability to leverage is Cyber AI Analyst, which allows you to see immediately the most significant threats happening in real time.

Cyber AI Analyst autonomously investigates every threat detected and highlights the highest-priority incidents at any one time – ensuring you see what needs attention right away.

The technology pulls together related events into a clear Incident Report, including an AI-generated natural language summary and a visual timeline of the threat. Security responders are able to grasp the severity of the incident immediately - ensuring severe threats like ransomware, data exfiltration, and a malicious insider attack are able to be actioned in minutes.

Incident Reports include a clear graphic pointing to where the threat sits in the kill chain. If there are several phases, it's likely a big attack and will need close, immediate attention. Security teams can easily skim through the related devices, subnets, scanning ports, sources, and the relevant details, which are all pulled into one place in the report. Cyber AI Analyst makes it easy to take just a few minutes to examine an incident and decide how to follow up.

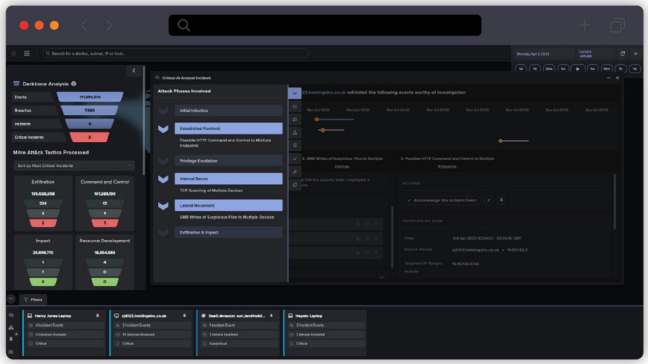


Figure 2: Cyber AI Analyst Incident Report with attack phases shown

Highlights

- Cyber AI Analyst conducts autonomous investigations to save your team time
- Darktrace can integrate with existing tools in your workflow

On-demand Investigations

While Incident Reports are always created for the most critical threats at any one time, investigations can be applied on demand to suspicious devices or users by simply selecting the time window, the device or user of interest, and then clicking the 'Investigate' button within the Threat Visualizer.

This provides the ability to easily confirm assumptions about suspicious activity, proactively threat hunt, effortlessly check on HR watchlists, or even help new starters on the security team understand how to pull together an investigation.

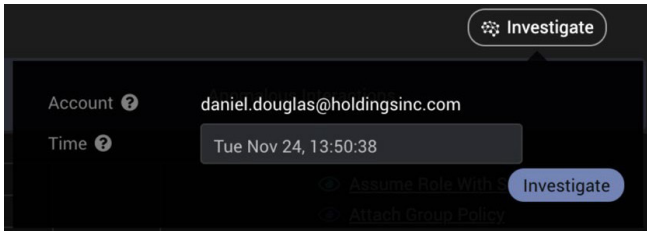


Figure 3: Easily trigger on-demand AI-driven investigations

Seamless Interoperability

Cyber AI Analyst technology can also be integrated with tools across your security stack, allowing investigations to be triggered based on data from third-party sources like Crowd-Strike or Carbon Black.

The rich context and insights of Incident Reports can additionally be exported to SIEM, SOAR, or ticketing systems to enhance your existing workflows.

This ability to integrate with other tools helps maximize ROI not only for Darktrace but other security investments as well.

> Darktrace Cyber AI Analyst provides high-fidelity alerts and incidents that I can send over to our SIEM as well as SOAR for automated actions. It's been a game-changer for the SOC.
>
> / Cyber Security Engineer, Chemical Manufacturing

A Look at the UI

Cyber AI Analyst Incident Tray

The Cyber AI Analyst incident tray is accessible within the Threat Visualizer. Incidents are categorized in order of significance, starting with the highest level of threat. Each incident lists the device name, the number of incident events, the number of other devices involved, and the threat status.

Cyber AI Analyst will always prioritize the most severe incidents in the tray for the specified time period. As it refines its understanding of each incident, incidents may reduce in severity or be replaced by emerging threats. The 'Show More Incidents' button can be used to retrieve incidents that you were previously investigating or wish to revisit, but are no longer highest in severity.

The 'Include Acknowledged' toggle shows or hides acknowledged incidents. Incidents can be acknowledged on an event-by-event basis, in their entirety in the Threat Visualizer, or in the Mobile App.

Acknowledging a Cyber AI Analyst incident does not acknowledge the underlying model breaches.

Any pinned Cyber AI Analyst incidents will always appear in the left-hand side of the incident tray. Click the 'Download Incidents' button to download a PDF report containing all current incidents in the tray.

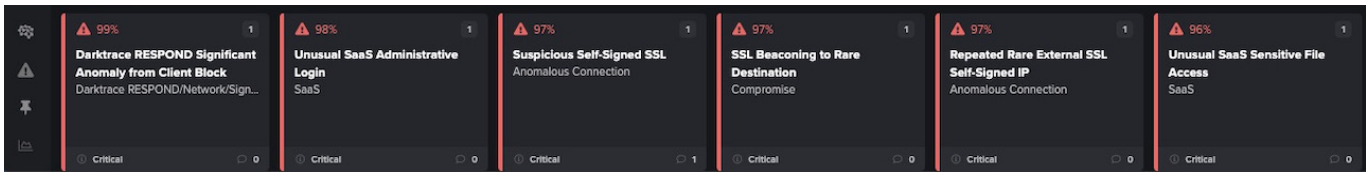


Figure 4: The Incident Tray shows the most significant incidents at any one time

Incident Timeline

Click on an incident in the tray to launch the Cyber AI Analyst pane. An incident is composed of one or more events: events are a group of detected actions (model breaches) investigated by Cyber AI Analyst that pose a likely cyber-threat. At the top of the page is a clear timeline representative of the incident. Detections that are associated with each event will appear as dots, where color indicates severity.

The activity associated with an event currently selected from the tabs below the timeline will be highlighted in blue. Long-lived events, such as large data transfers, may cover a large chronological period. Darktrace RESPOND activity is also shown in green on this timeline.

Like a human, Cyber AI Analyst uses an initial detection of unusual behavior as a starting point for investigations.

The behavioral analysis it performs may discover patterns of activity that were not the original trigger point for the detection but are worthy of investigation.

Consequently, the event period may not correspond with the model breach time.

Additionally, some model breaches require sustained behaviors such as repeated connections before breaching, so the final breach trigger may be later than the connection of interest.

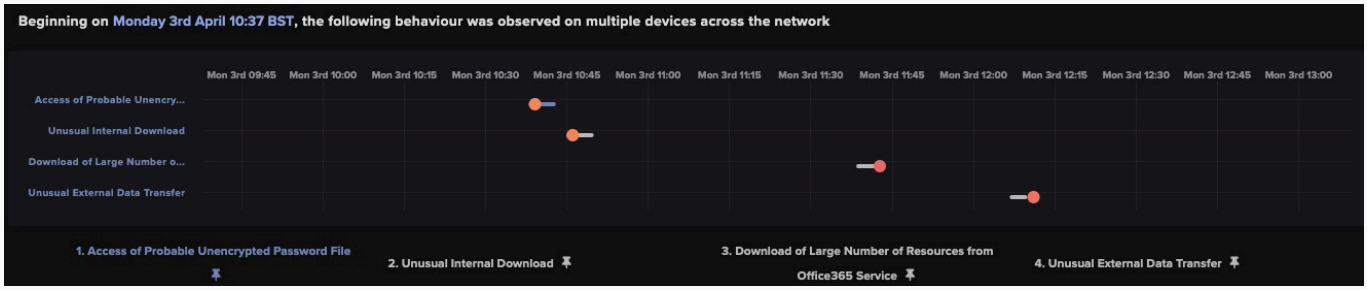


Figure 5: Each Incident Report shows a clear visual timeline of all the events involved

Attack Phases

Clicking the downward arrows on the left side of the pane will open a visual representation of attack phases involved in the incident. This view immediately indicates the scope and severity of the incident.

Download the Report

The 'Download' icon on the right offers the ability to easily download and share a PDF version of the Cyber AI Analyst Incident Report.

Incident Events

Each event will appear as a tab. The right panels will break down key elements of the event and the involved devices; the data is specific to each event type. The left panel gives a summary of the event.

Detections that triggered a Cyber AI Analyst investigation will be listed as related model breaches. Currently active or expired RESPOND actions will be listed below the related breaches.

The action section allows for the individual event to be pinned or acknowledged alongside all related model breaches.

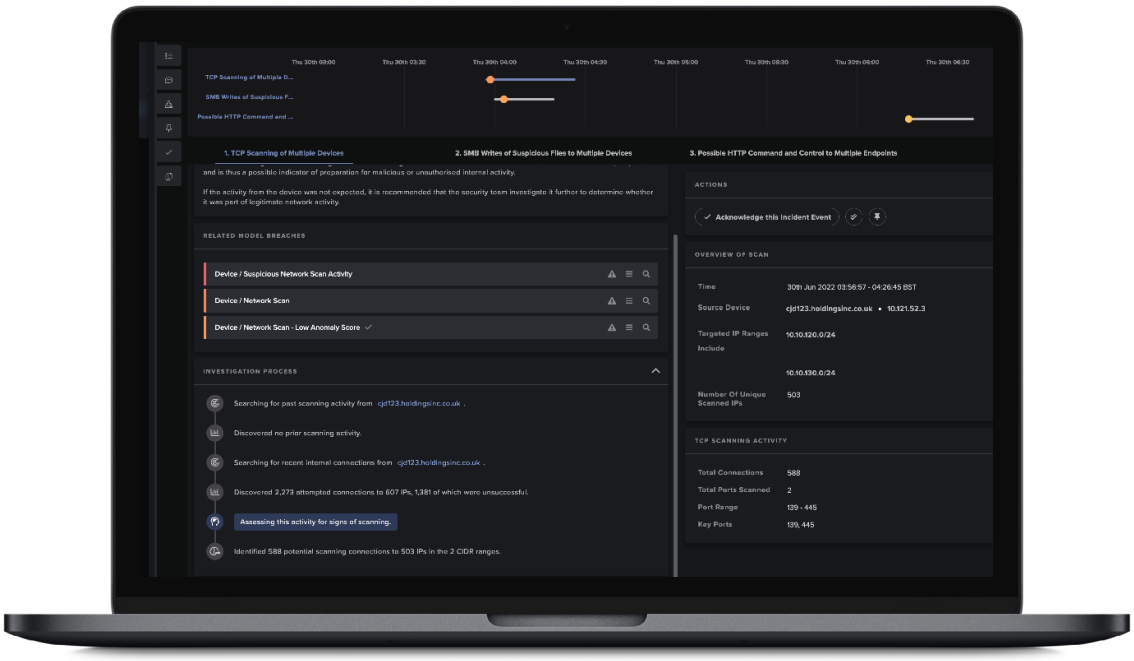


Figure 6: Incident Report showing related unusual behavior and connected device information

> "With AI Analyst, we've been able to exponentially reduce alerts, harden our environment, and get strategic."
>
> / CISO, Legal Services

Enhanced Monitoring: Highlighting Strong Indicators of Attack

Another key feature that teams can easily take advantage of is the Enhanced Monitoring model view.

Based on a bespoke set of parameters for each organization, they enable tailored defense of particularly sensitive data and vulnerabilities. When triggered, Enhanced Monitoring models are strong indicators of attack that immediately highlight to security teams the most heavy-hitting threats.

Enhanced Model detections are available via the Threat Visualizer by selecting Threat Tray Filters and choosing Enhanced Monitoring. When Self-Learning AI detects a threat related to an Enhanced Monitoring model, you can get automatic email alerts for additional real-time notification.

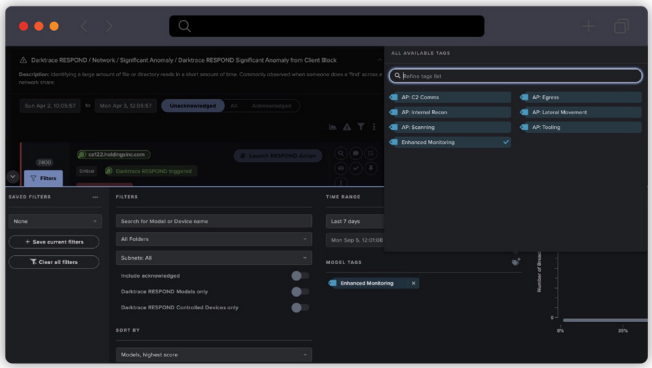


Figure 7: Filter for Enhanced Monitoring to see the most critical behavior detected

> It's autonomous – Darktrace and AI Analyst just work as expected for high-risk incidents, and we let it do its thing
>
> / Cyber Security Analyst, Construction

Autonomous Response Neutralizes Threats at Machine Speed

RESPOND: The Machine Fights Back

Darktrace provides real-time autonomous detection and response, neutralizing threats as they emerge – giving understaffed and overworked teams the critical time necessary to catch up.

Powered by Self-Learning AI, Darktrace is the first and only solution that can prevent, detect, and respond to attacks at machine speed and with precision, even if the threat is targeted or entirely unknown.

Every second, Darktrace stops an emerging cyber-attack – making it a critical tool for small teams to ensure workforces and workloads are always protected.

For small teams, the first step on the journey towards truly autonomous defense is setting up Darktrace to match your business needs.

Darktrace can deploy with hundreds of out of-the-box AI models ready to use. Teams can also completely customize their deployments so that the autonomous defense best matches business needs and policies.

To that end, the product can easily be configured according to a range of flexible parameters:

- **Degree of Automation:** Configure Darktrace to be fully autonomous or to require human approval before taking action
- **Use Cases:** Tailor Darktrace to cover specific business risks, from insider threats to external attacks
- **Timing:** Schedule distinct parameters for different times of the week, including over the weekends or during business hours
- **Scope:** Consider where and to what extent actions should apply, whether globally or per subnet, user, device, or threat model
- **Integration:** Deploy Darktrace to interface with third- party firewalls or network devices as a mechanism for response

Highlights

- Deploys out-of-the-box with hundreds of ready to use AI models
- Completely customize your deployment to fit specific business needs and policies

Access Your Security Any Time, Anywhere

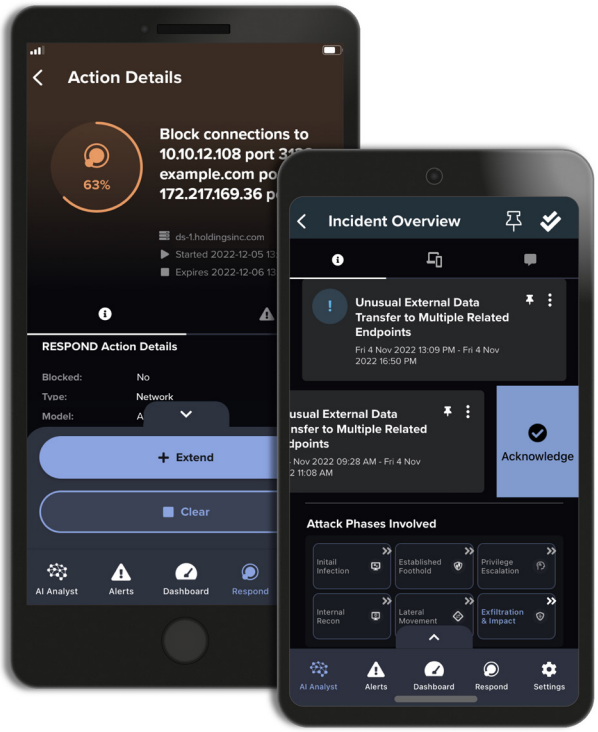


Figure 8: The Darktrace Mobile App lets you monitor your entire digital infrastructure on the go

Self-Learning AI on the Go: The Darktrace Mobile App

The Darktrace Mobile App lets you protect your dynamic workforce and monitor your entire digital infrastructure on the go.

Get real-time threat notifications, investigate the most significant incidents with Cyber AI Analyst, and take actions – all from your phone.

Self-Learning AI gives you enterprise-wide coverage that evolves and grows with your business, and with our Mobile App you can stay ahead of any threat that emerges.

Use the App to:

- Examine Cyber AI Analyst incident summaries
- Discover alert details around emerging threats
- Access dashboard for instant visibility
- View and adjust RESPOND actions and settings
- View and take action on your email environment

> Not only is the product top notch, but the customer service and staffing are excellent.
>
> / IT Security Specialist, Medical Not-For-Profit

Integrations Maximize All Your Security Investments

Easy Win Integrations

The Darktrace platform was designed with an open and extensible architecture that seamlessly integrates with your existing investments. Customers can enhance and extend their Darktrace deployment via one-click integrations, including the ability to immediately extend coverage to new cloud services, enrich the platform's analysis with new sources of log ingestion, and activate coordinated responses via integrations with other security defenses. If you don't see your chosen provider in Darktrace's configuration page, custom templates make it easy to set up bespoke integrations.

SIEMs and SOARs:
Sharing AI Insights

Native integrations via API and syslog allow Darktrace to feed AI detections and Cyber AI Analyst Incidents to SIEMs for analysis and correlation, as well as to SOAR solutions to trigger response playbooks.

Darktrace can also poll SIEM and SOAR solutions to ingest enrichment data, and SOAR playbooks can be configured to trigger custom models and Cyber AI Analyst investigations in Darktrace. Current customers can see the integrations guide here.

EDRs:
Extending Endpoint Protection

Darktrace can ingest EDR alerts as weak indicators that inform our AI's analysis across the business.

EDR alerts can also trigger Cyber AI Analyst investigations without the need for an underlying Darktrace detection. Current customers can see the integrations guide on alerting options here.

Single Sign On:
Seamless Access

For ease of use, Darktrace natively supports authentication and access via SAML 2.0 Single Sign On. Current customers can see the integrations guide here.

VPN & Zero Trust Technologies:
Defending the Dynamic Workforce

By integrating with VPN and zero trust services, Darktrace can extend its visibility across an increasingly distributed workforce. Low-effort native integrations and custom templates are available for any service in this area. Current customers can see the access control integrations guide here.

Firewalls:
Autonomous Response and Added Context

Darktrace can trigger RESPOND actions via integrations with firewalls and preventative controls for attacks that have gotten through.

Darktrace can also ingest logs from firewalls and network devices to extend visibility as needed. Current customers can see the integrations guide here.

LDAP:
Authentication and Enriched Visibility

Integration with LDAP servers, such as Active Directory, can support authenticated access to the Threat Visualizer, as well as enrichment of Darktrace's visibility by providing additional LDAP attributes for users. Darktrace also provides the option to create LDAP group tags for use in threat modeling. Current customers can see the integrations guide here.

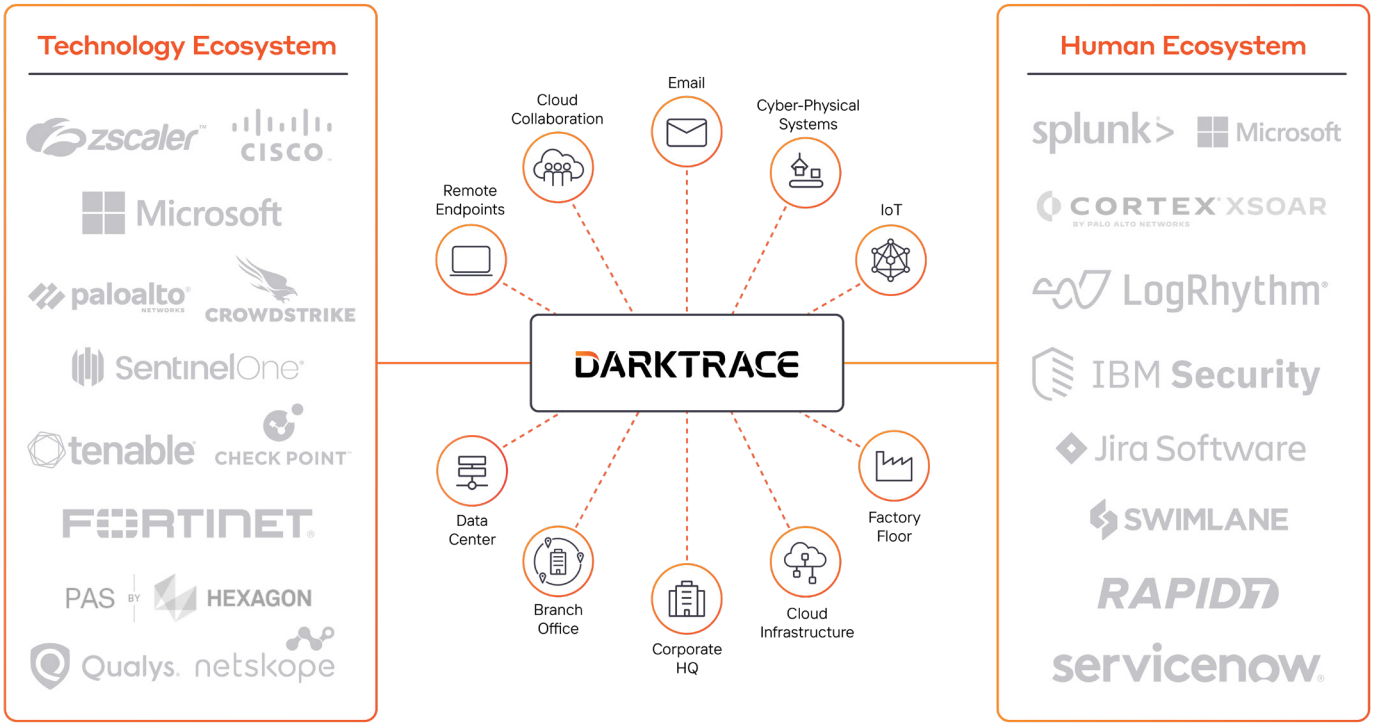


Figure 9: Darktrace integrates seamlessly across the security stack, improving productivity and ROI

> Tying Darktrace into all these various integration points has unlocked so much potential in our SOC.
>
> / Security Engineer, Business Consulting

© 2023 Darktrace Holdings Limited. All rights reserved. The Darktrace name, logo, and other trademarks used herein are trademarks of Darktrace Holdings Limited. The names of other companies, products and services are the property of their respective owners.