DARKTRACE

Reducing Cyber Risk

A Guide to Preventative IT Security

CONTENTS

Introduction

In the wake of increasingly sophisticated threat actors and more complex digital infrastructures, cyber risk – and how to manage and control it – has become a top agenda item, no longer just for the IT team but for business leaders and board members alike.

While protecting an organization from cyber disruption is demanding increasing budgets, much of this is devoted to cyber defence: real-time detection and response to ongoing attacks.

This is no doubt important. However, in a more recent trend, defenders are increasingly looking to 'move security to the left' – a reference to the MITRE ATT&CK framework that essentially means an increased emphasis on getting ahead of the attack and proactively hardening chokepoints and vulnerabilities to prevent an attack from occurring in the first place.

The logic behind this is clear: attack prevention is cheaper than incident response.

If organizations can get proactive about hardening their defences such that an attacker is unable to target an organization in the first place, then time and money can be saved in the absence of business disruption, reputational fallout, and a lengthy and resource-intensive incident response.

> As organizations contend with an increasingly complex set of cyber security challenges, a reactive approach does not go far enough. CISOs are starting to look at cyber security just like any other operational risk and are turning to a more proactive approach that pre-empts cyber-attacks before they happen, rather than waiting to be breached.

Research Director
/ International Data Corporation (IDC)

> Almost two-thirds of organizations do not have high confidence in identifying their greatest vulnerabilities or weaknesses, leaving them exposed to attack.

/ International Data Corporation (IDC)

The Changing Attack Surface

Rapid digitalization has become an inevitability across nearly every industry, but managing the potential risks of a fast-expanding attack surface can be daunting. As malicious actors recognize the profitability of cyber-attacks, their campaigns have become increasingly well-resourced and sophisticated. Moreover, cyber-crime is increasingly becoming commercialized, lowering the barrier-to-entry for cyber-criminals, and increasing organizations' exposure to a cyber-attack.

> Common cyber-attacks, like a data breach, average over **$4 million** in damages to businesses globally.
>
> **IBM's 2022 "Cost of a Data Breach" report**

CISOs and security teams are left juggling an assortment of different risk areas, including:

- Misconfigurations
- New emerging vulnerabilities
- Cloud adoption and migration
- Supply chain risk (Gartner now predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains.)
- Phishing and brand abuse
- Mergers, acquisitions & subsidiaries
  – Risk associated with newly acquired assets

Navigating the World of Preventative Cyber Security

Cyber Risk

Cyber risk addresses the potential scenario where a threat actor takes action that causes damage to an organization's assets in cyber space. That damage can manifest in a variety of ways – through loss of confidentiality (i.e. a data leak), integrity (i.e. faulty or misleading data) or availability (i.e. malfunctioning systems).

To manage cyber risk, organizations today are adopting a variety of loosely overlapping measures.

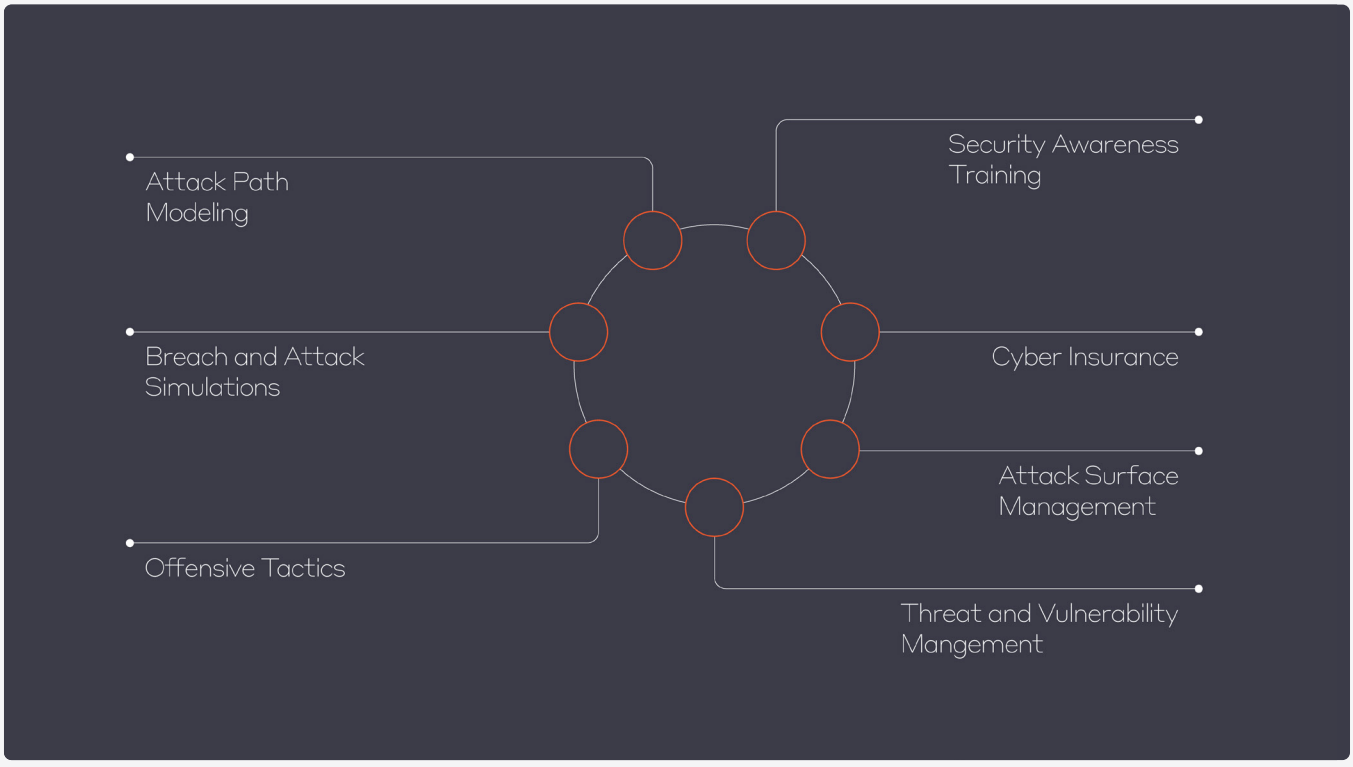


Figure 1: Organizations may have a range of disparate preventative security measures in place

Security Awareness Training

Organizations are increasingly investing in security awareness programs designed to encourage best practice and discourage risky behavior across the workforce. This activity may reduce risk, but security teams struggle to enforce sustainable best practices.

With bad habits inevitably returning once the training has passed and been forgotten, the challenge for security teams becomes instilling continuous awareness.

Threat and Vulnerability Management

Threat and vulnerability management involves continuously assessing new vulnerabilities, and to determine if these affect the devices, operating systems and cloud applications being used by the organization. With tens of thousands of vulnerabilities being disclosed every year, this can be a costly and time-consuming process that involves outside consultants and partners.

Understanding whether or not a vulnerability impacts you is one challenge, but getting a real sense of prioritization requires knowledge not just of the attack surface, but a comprehensive internal view of the organization to determine which assets and attack paths represent the greatest business risk.

Attack Surface Management

Attack surface management involves viewing an organization from the perspective of an attacker; assessing all publicly-facing assets for potential risk, helping organizations understand and take control of their exposed IT assets.

This outside-in view of an organization's attack surface can be valuable in highlighting external risk, but it requires an internal view of the organization to ensure countermeasures are prioritized in the context of how much business risk those measures are helping to mitigate.

Attack Path Modeling

Attack path modeling may involve hypothesizing and visually representing the steps an attacker could take to conduct a successful cyber-attack. It requires an understanding of the most vulnerable and exposed assets in an organization, which, if inputted manually, can be a time-consuming process.

Efficient attack path models would require continuous testing and streamlined data from your organization that can be tested but remain operational in the process. Attack paths are constantly changing, limiting the value of point-in-time assessments.

Offensive Tactics: Red Teaming / Penetration Testing

Many organizations look to hire in a 'red team' to try andbreach an organization and simulate an attack. The security insights of this type of exercise can be limited in scope: it may be confined to one area of the digital infrastructure the red team has targeted – or been told to target – and the service is only contracted for a finite period.

The goal of a penetration test is to reveal as many security flaws as possible, and this may create long to-do lists for IT and security teams, lacking that sense of prioritization on whether these measures have a meaningful impact on business risk.

These types of adversarial assessments are often carried out as a 'checkbox exercise' or as a result of a compliance requirement, but the lack of tangible insights can result in CISOs and security teams getting frustrated.

Cyber Insurance

Another way organizations can manage down cyber risk is to pass that risk off to another party in the form of cyber insurance. Cyber risk is increasing annually, applying upward pressure on premiums for cyber insurance. Furthermore, ensured parties need to be conscious of exactly what they are insuring and the limitations within their insurance policy, making cyber insurance an increasingly expensive and complex place to invest.

Compliance

Organizations now fall under increasing pressure to conform to an ever-changing set of regulations, standards, and frameworks. For example, the NIST Cyber Security Framework and SOCI Act have substantial impact on the way organizations in the United States and Australia understand, manage, and reduce their cyber-risk.

This often requires more spending on security systems and labor, across detection and response systems, but also with asset management and risk assessment.

In addition to inducing higher spending, compliance policies also require evidence that your organization is complying to the laws. Effective security tools need to be able to generate the appropriate reporting and risk scoring to meet these criteria. Customizable compliance features are necessary so a security team can configure their system to address specific compliance frameworks that apply to their organization.

Harden Your Defenses Inside and Out

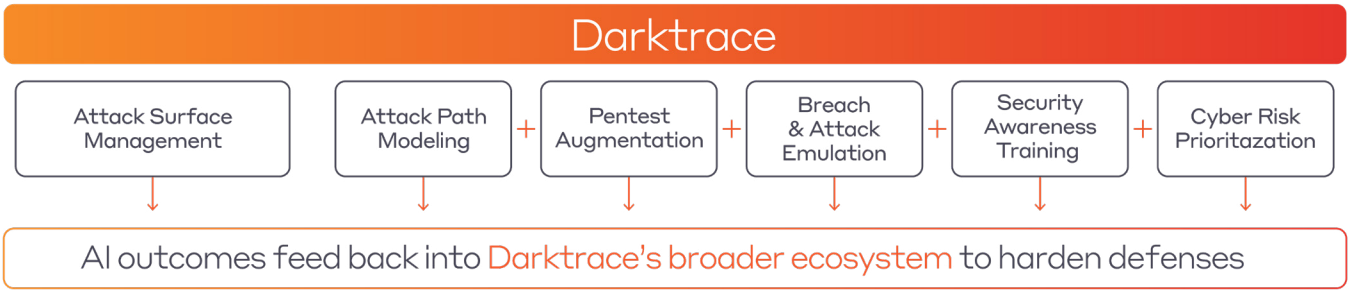
While each of the preventative security measures described above might play an important part in reducing the cyber risk posture of an organization, simultaneously managing them is resource-intensive, time consuming, and costly. They generally provide a single-point-in-time snapshot of an organization's risk posture, meaning they become antiquated as soon as the IT infrastructure changes.

A Single Solution for Reducing Cyber Risk

Darktrace brings together many aspects of the preventative security methods described above into a single end-to-end solution that allows defenders to prioritize and harden defences, both inside and out.

The technology combines an outside-in view of an organization with an internal view of an organization's every user, device, and how they communicate. It uses AI to continuously analyze every possible attack path and then outputs easily-understandable, prioritized mitigation advice to the security team, while simultaneously feeding back into the wider security ecosystem.

The preventative product family empowers CISOs and security staff to become an AI-powered red team, simulate attacks, identify critical assets, and test pathways of vulnerability.



Darktrace AI Research Centre

Darktrace's research-led solutions are rooted in innovation. The Darktrace AI Research Centre based in Cambridge-UK, with more than 160 patents and patents pending, includes teams of mathematicians, software engineers, linguists, and other experts investigating how AI can be applied to real-world problems. The centre has produced numerous breakthroughs, which now form the AI capabilities comprising its products.

While Darktrace's roots are in the detection and response space, in 2020 the AI Research Centre turned its focus to attack prevention, recognizing many of the challenges security teams grapple with today in this area.

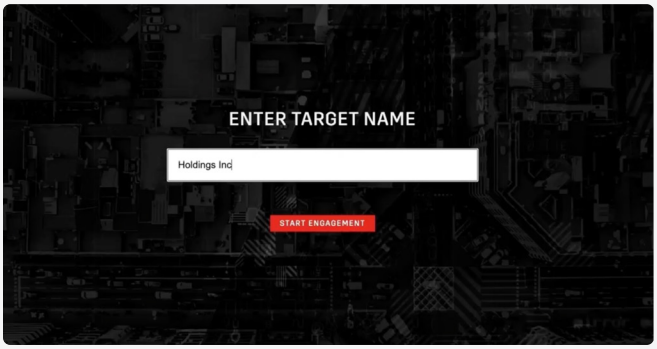
This research culminated in the launch of added attack path modeling and preventative solutions in 2022 and incident management and recovery capabilities in 2023.

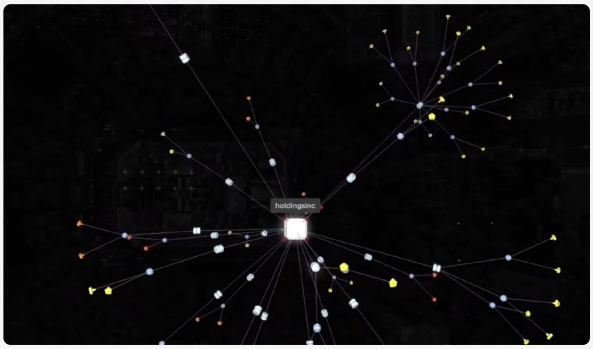
Continuous Evaluation of Your Attack Surface

Darktrace's attack surface management capabilities allow you to continuously monitor your external attack surface for risks, high-impact vulnerabilities and external threats.

Zero-Scope

Unlike other attack surface management solutions, Darktrace requires no technical input: no IP ranges, no other parameters – your brand name is all that's needed. It uses AI to understand what makes an external asset yours. This 'zero-scope' approach ensures unparalleled discovery, searching beyond known servers, networks, and IPs, and typically surfacing 30% - 50% more assets than an organization realizes it has.





Newsroom

Typical vulnerability management programs are resource intensive, involving the constant monitoring of news feeds and intelligence sources. Meanwhile, exposure tests from vulnerability scanners take time, when in fact security teams need a quick initial indicator of their exposure.

Darktrace's Newsroom feature alleviates the pain from managing a vulnerability response process by informing you of newly discovered critical vulnerabilities and providing timely mitigation suggestions that would help prevent potential exploits.

It continuously monitors open-source intelligence sources for new vulnerabilities and assesses your organization's exposure, and reveals all assets on your external attack surface potentially affected by a new critical vulnerability.

Continuous Monitoring

The solution does not provide a point-in-time snapshot, but rather continuously monitors the external attack surface, ensuring you have the most up-to-date understanding of all your assets at risk, high-impact vulnerabilities, and external threats.

Actionable Insights

The solution provides a high-level overview of the evolution of your attack surface and associated risks, presenting trends on key metrics such as the type of risks found and their criticality for prioritization. Darktrace is used by organizations to reveal shadow IT, supply chain risks, potential phishing domains, vulnerabilities and misconfigurations, and risks arising from mergers and acquisitions.

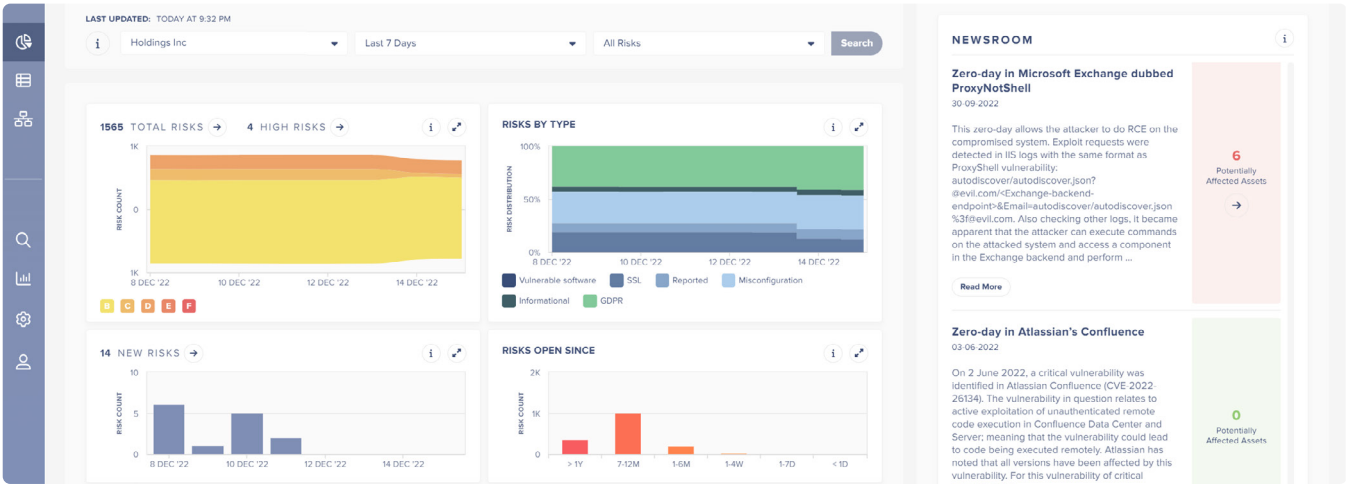


Figure 2: Darktrace's Newsroom feature highlights newly discovered critical vulnerabilities

Strengthen Your Internal Infrastructure

Darktrace identifies and prioritizes your high-value targets and pathways to secure vital internal systems and assets. It continuously learns all your internal users, devices, and the interactions between them to establish your most critical assets and attack paths. With this continuously updated understanding of your entire organization, it prioritizes and presents the most effective mitigation actions that will reduce risk to the greatest extent. And while your security team work on these countermeasures, Darktrace autonomously feeds back into it's own detection and response capabilities to harden defenses around your critical assets.

Attack Path Modeling

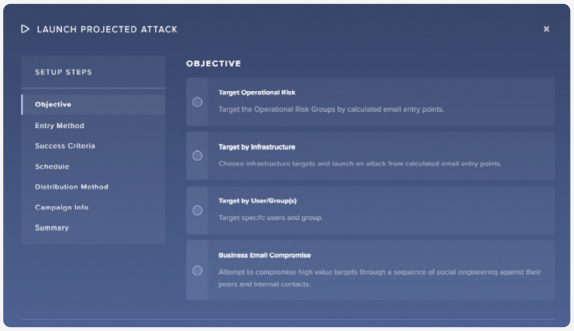
Darktrace continuously identifies all potential pathways and analyzes every digital touchpoint. From this, it assesses your most vulnerable and critical attack paths, learning the potential impact of each user, device and system, and then how exposed they are.

Risk Scoring

For security teams that are working on a tight budget, understanding critical attack paths is vital for prioritizing spending. With Darktrace you have a deep understanding of these attack paths and can allocate spending accordingly with evidence.

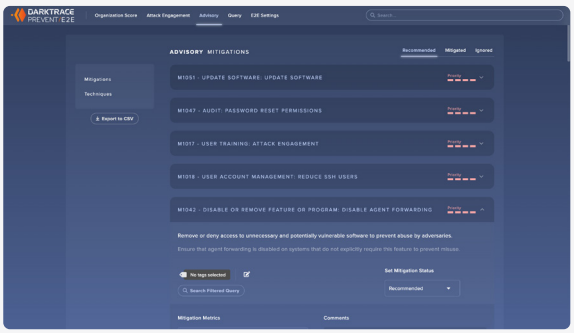
Breach and Attack Emulation

The technology can then use generative AI to simulate a real attack path, creating social engineering messages that mimic a sophisticated attack. This tests the validity of critical attack paths already established while feeding the information gained from the phishing simulation back into the detection engine to further harden the environment.



AI Advisory

Darktrace then produces prioritized mitigation advice through explainable AI, showing how to reduce risk. With zero impact to actual business operations, you have the capability to view ransomware risk scores, KPI scores for overall risk, and your domain ownership.



Autonomously Strengthen Defenses with an End-to-End Ecosystem

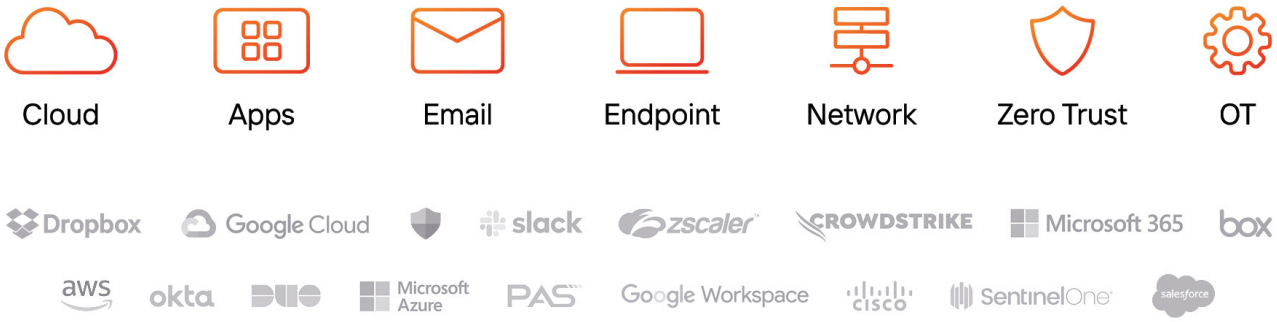
Darktrace offers an interconnected set of cyber security solutions for cloud, email, network, apps, zero trust, endpoint and OT, designed to augment humans at every stage of an incident life-cycle – from before an attack begins, to real-time detection and response to in-progress threats, through to incident management and post-incident recovery.

These AI engines are dynamically related: each capability continuously feeding back into the system as a whole, creating a virtuous cycle in which the state of an organization's cyber security is continuously improved.

Darktrace's preventative security function feeds autonomously into its detection and response functions, informing these AI engines of particularly vulnerable or potentially impactful assets and attack paths so that they can be on heightened alert should anything unusual or suspicious occur along these attack paths.

As a result, defenses are hardened and life is made more difficult for the attacker. Conversely, the detection and response functions feed back into preventative security: when these systems establish that an attack is taking place, it will feed that information back to predict and pre-empt an attacker's next move.

Comprehensive Protection Wherever You Need It



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. Breakthrough innovations from its R&D Centers have resulted in over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,900 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 97242 2011
info@darktrace.com
darktrace.com