DARKTRACE

Darktrace / Proactive Exposure Management

Prioritize risk, anticipate attacks and harden your security posture

Complexity, change & cyber risk

Uncover the 50% of technology risks you didn't know existed[1]

Cyber risk is a growing concern for leaders who face potential threats that have not yet materialized, or in some cases are entirely unknown. If left unattended, they pose a significant danger to their organization's assets and operations.

With pressure to achieve resilience, security teams are beginning to shift away from reactive security methods towards a proactive approach that stops threats before they happen.

However, they face several obstacles:

A growing interconnectivity of IT infrastructure brought about by cloud adoption and IT-OT convergence makes operations easier, but it also introduces new attack paths ready to be exploited.

Scaling organizations have complex team structures where the needs of each team are unpredictable, making human risks and cyber hygiene hard to measure.

On the security side, these structures have also distributed responsibilities, creating delays in management that give adversaries more time to exploit open risks. While some vulnerability management solutions address these obstacles in part, teams still struggle to determine what deserves high priority.

By 2026, organizations investing in programs based on continuous exposure management will be three times less likely to suffer from a breach[2]. Now more than ever, it is critical to take a proactive stance and prepare for threats using a combination of solutions adapted to the unique business, rather than a general view of risk.

Business benefits

Unify exposure across all your technologies
With an AI scoring system that gives visibility into risks across your different architectures, human communications and CVEs

Unprecedented ROI and cost insights
For your CVE risks including the potential $ implications of a security breach, patch latency vs discovery rates, and blind spots

Enhance employee awareness
Through sophisticated email phishing engagements that test susceptibility and supplement training programs

Align your proactive and reactive functions
Quickly determine the potential impact of compromised devices and see how these compromises could be prevented entirely

Strategically reduce risk with tailored advisories
Make the biggest impact with the smallest actions, specific to your business risks

1 Validated by business outcomes from existing customers
2 Gartner How to Manage Cybersecurity Threats, Not Episodes (2024)

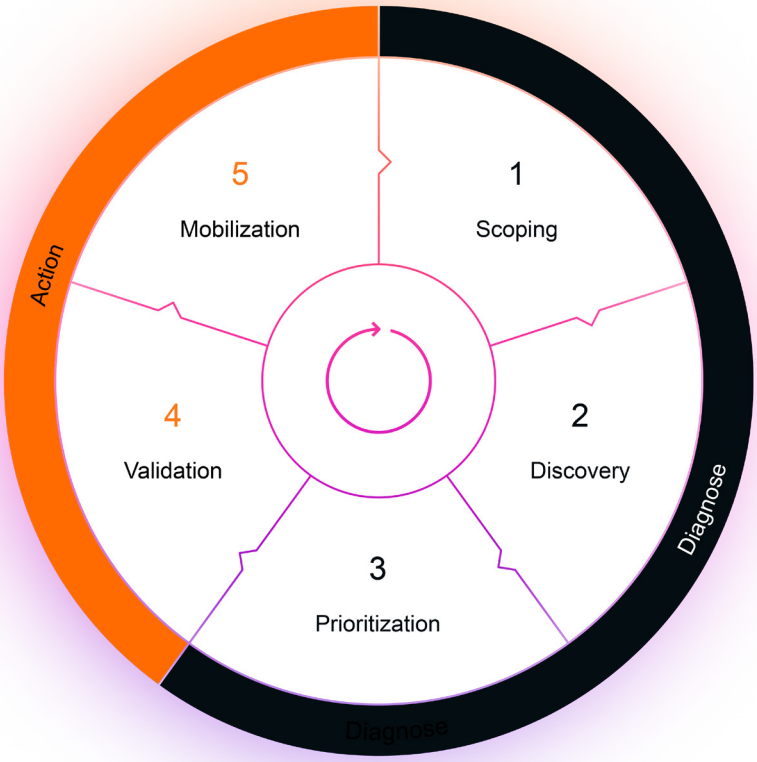
Moving to a continuous approach

Darktrace / Proactive Exposure Management shifts your understanding of cyber risk to an adversarial mindset that highlights your security exposures like never before.

Organizations can proactively secure their critical assets with a continuous understanding of the most vulnerable and high-value paths across their different architectures, based on a combined business context and knowledge of sophisticated MITRE APTs and ATT&CK techniques.

This clarity is achieved through an ongoing assessment of all your assets using industry leading Self-Learning AI that knows their relationships, behaviors, and exposures.

Motivated teams can test human weak points along these attack paths to demonstrate attack feasibility, whilst unrivaled threat and vulnerability management allows them to identify control gaps and mobilize with prioritized mitigation guidance. Maintain compliance standards and reduce their patch latency with vulnerability management that maps CVEs to your individual technology importance.



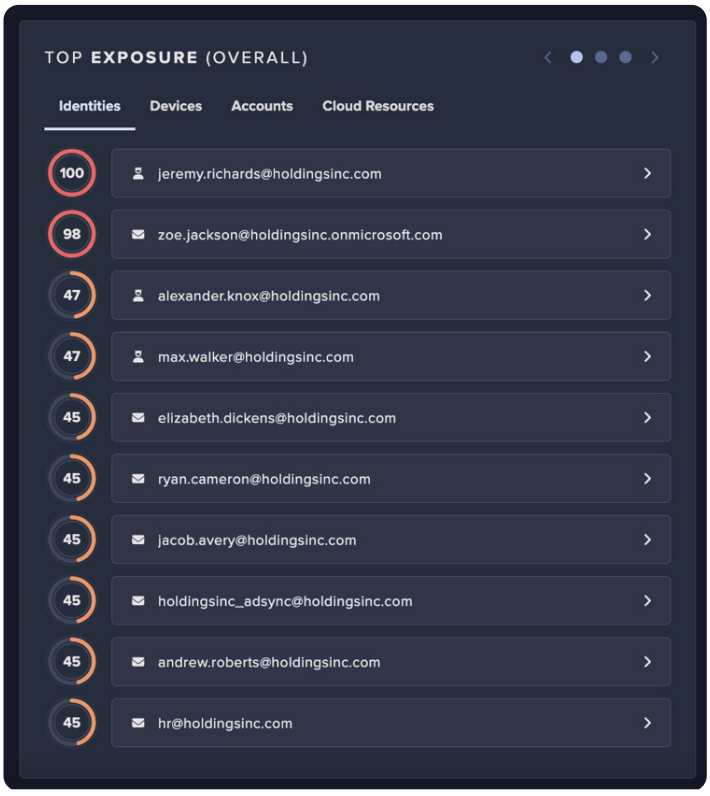
Gartner's Continuous Threat Exposure Management (CTEM) cycle defines a new approach that leads to stronger security postures and fewer real incidents

Key Capabilities

Proactive AI risk insights that reveal what's important to You

Instead of static CVE lists that contain no business context, Darktrace lets organizations understand their security exposure like never before.

Teams get detailed visibility with an AI-based risk scoring system designed for security workflows and executive reporting alike. Darktrace learns and understands all your technologies, human communication patterns, CVEs, and MITRE adversary techniques to assess potential damage, weaknesses, impact, and overall exposure- as well as the difficulty of potential attacks. These scores are continually updated through AI techniques including graph theory, clustering and supervised learning.



Top rankings and risk baselines provide an effective, prioritized view for cyber risk discovery and assessment that lets teams prioritize their biggest risks with the smallest effort.

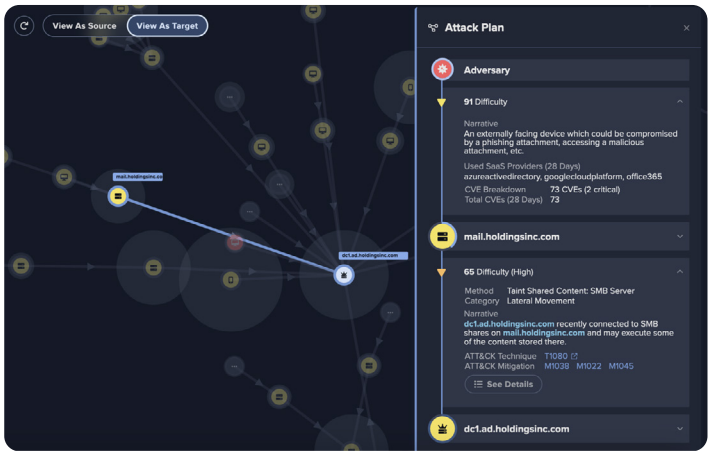
Now, they can skip analysis and jump straight to addressing the users, devices and vulnerabilities which pose the most severe risk of compromise.

Understand your security risk from an attacker's point of view

As teams consistently struggle to identify and correlate risks across their entire architecture, it's crucial they achieve a practical view of how they might impact their technologies if exploited.

Darktrace is one of few vendors to proactively secure your critical assets with AI-driven attack path modeling across all your technologies and human communications.

Users can uncover threat exposures across their whole digital ecosystem with a sociographic or line view of how they are related and the potential paths an adversary might take between them. These paths can be reviewed to identify critical choke points in any of their environments for a proactive approach that lets teams address the biggest risks first, or even predict the most impactful next steps of a live incident as part of the wider Darktrace ActiveAI Security Platform.



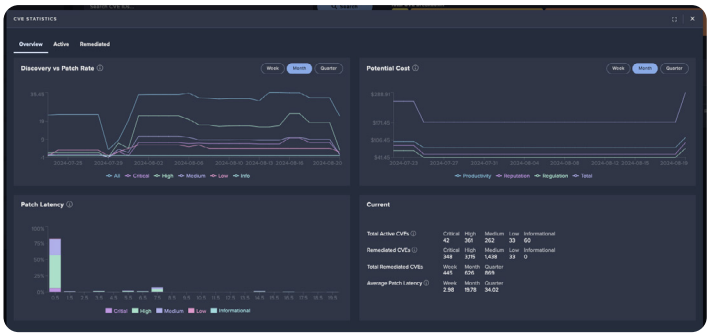
Instead of reviewing lists of techniques, organizations can see the MITRE ATT&CK behaviors that will most-likely affect your business. You'll understand the number of linked attack paths, their relative difficulty to address, potential damage, and the mitigation steps needed to reduce their success.

Close any user-created gaps with sophisticated email phishing engagements created to test employee susceptibility along attack paths. Custom scenarios reduce human-centric risk by exposing poor cyber hygiene, and can augment wider training programs with practical behavioral data. This link of human and technology risks gives security teams a better picture of their interconnected security posture.

Empower and mobilize with unrivaled threat and vulnerability management

With integration, Darktrace delivers strategic CVE management containing unprecedented ROI.

Security teams can see their most immediate vulnerability risks–not just in the context of common industry scoring (e.g. CVSS, EPSS), but in relation to data from each of their environments. Gain industry-first insights into whether patch efforts are keeping pace with CVE developments), reveal blind spots in assets that were missed in previous scans, and share the potential cost implications of a data breach with executive stakeholders.

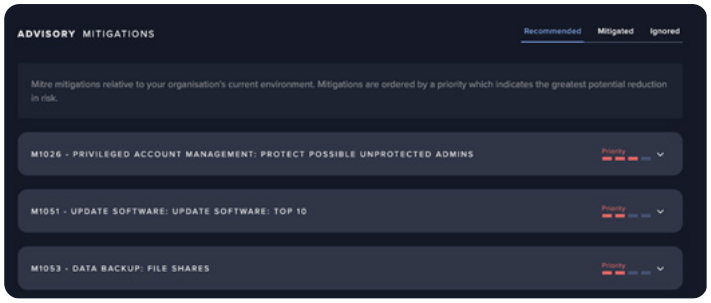


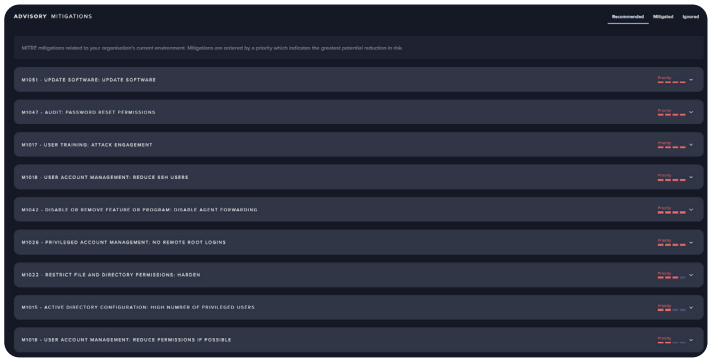
Darktrace maps adversary targeting and attack behaviors to your business profile to give you a better understanding of attack likelihood and your potential exposure against the most sophisticated threats. For organizations operating in more sensitive geographies or industries, this poses a unique perspective to help further reduce risk.

Minimize exposure before an exploit

Whilst many threat and vulnerability management (TVM) solutions consider mitigation an essential capability, Darktrace can go one step further by ranking mitigations based on how they will reduce the most risk.

Risk-reducing advisories proactively harden your security posture with tailored advice that goes beyond simple patch lists.





Get prioritized mitigation steps paired with their potential outcomes against risk, whilst giving security teams focus and direction in their proactive efforts. Darktrace makes it easier to take the steps needed to give your organization greater resilience. Now different organizations understand the mitigation priorities that are important to them.

Deployment

The Darktrace / Proactive Exposure Management solution requires deployment of Darktrace / NETWORK and either Darktrace / EMAIL, or a free mailbox connector for organizations using Microsoft 365. Optional Darktrace LDAP, Azure AD and Darktrace / ENDPOINT modules are easy to set-up and provide further enrichment and discovery. Further integrations are available for Darktrace endpoint security integrations and vulnerability scanners. For more information check the Darktrace website.

Operational benefits

See the biggest risks, with the smallest effort
Top rankings and risk baselines provide an effective, prioritized view for cyber risk discovery and assessment

Identify all your control gaps
Minimize exposure with tailored mitigation actions prioritized for your security teams to reduce successful exploits

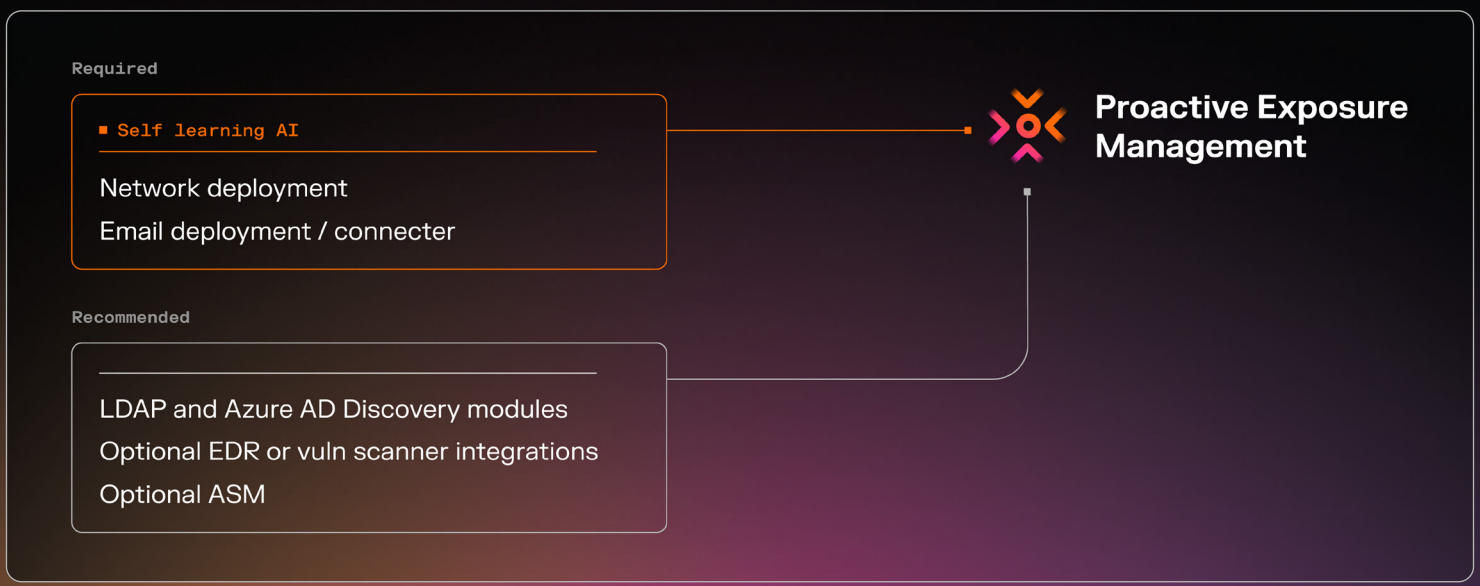
Augment your Red Team initiatives
Save time with high-value assets and critical attack paths for pen-testers to target and validate

Understand security choke points
Theorize complex multi-stage attacks that are only possible in your unique business context

Gain a practical adversary lens
Darktrace maps adversary targeting and MITRE attack behaviors to your business and its assets making them easier to harden

Deployment steps

01	Deploy Darktrace / NETWORK and Darktrace / EMAIL (or alternative connector)
02	Grant additional permissions to Darktrace / EMAIL from the console
03	Configure the Proactive Exposure Management vulnerability database
04	Configure a Darktrace Security Integration (optional, recommended)
05	Configure a Darktrace Vulnerability Scanning Integration (optional, recommended)
06	Configure LDAP enrichment (if not previously configured)
07	Configure Active Directory Discovery (LDAP) and/or Azure Discovery (Azure AD/Intune) modules
08	Grant user access to Darktrace / Proactive Exposure Management



Darktrace / Proactive Exposure Management collects data from a number of optional and recommended sources. Further integrations are available on our Website or Customer Portal for additional enrichment

Darktrace Platform & Portfolio

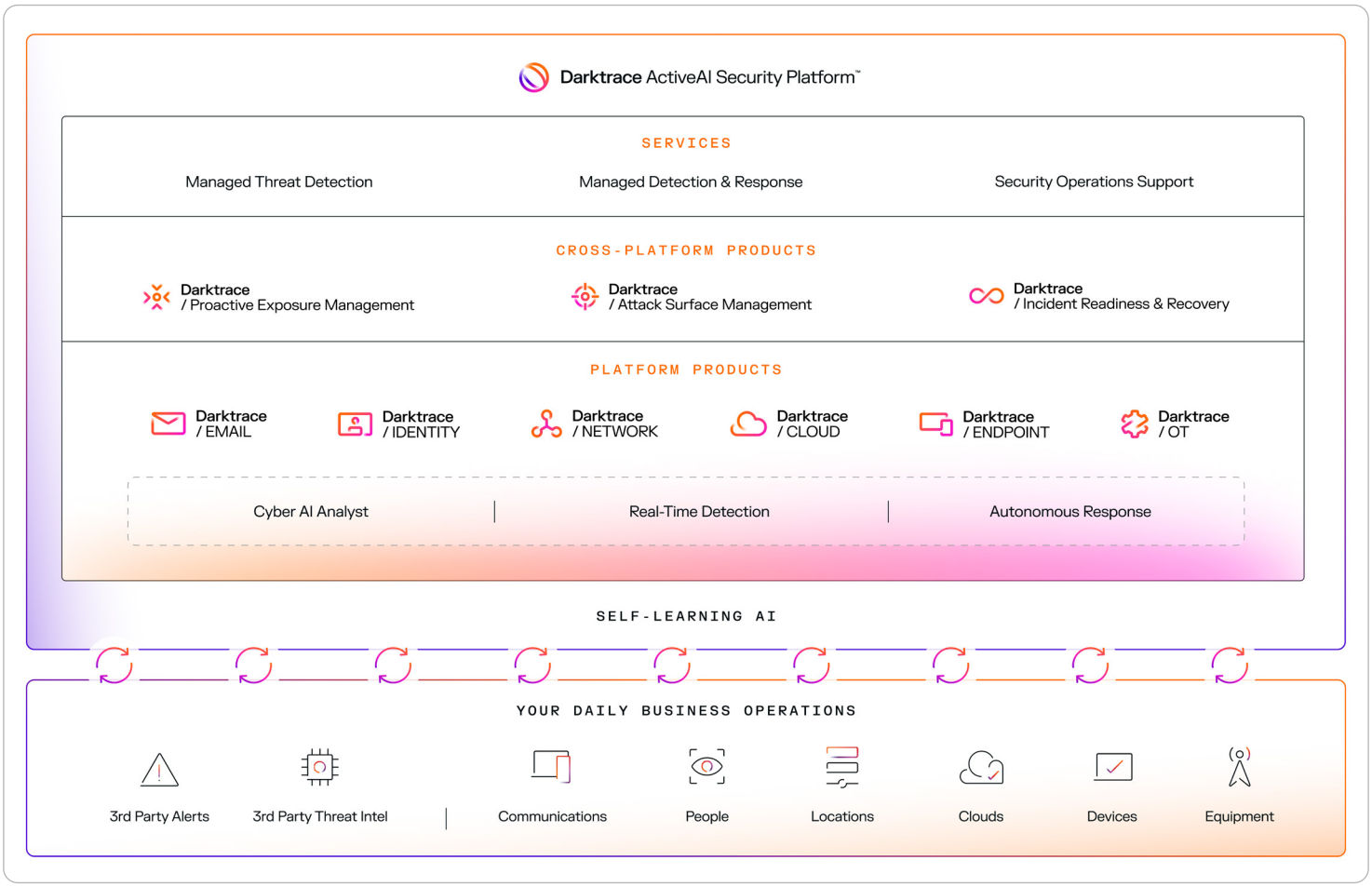
Exposure & the Darktrace ActiveAI Security Platform

Darktrace / Proactive Exposure Management acts as the heart of the proactive workflow within the Darktrace ActiveAI Security Platform.

> We know that the bad guys are gaining knowledge every day. We need to as well. And I think that this type of proactive approach is a requirement now. I don't think it is an option.
>
> ■ **Director of IT**
> Ongweowen Corp

By taking Darktrace's existing AI-based understanding of the business and applying it to the concept of risk rather than active threats, security teams can shift their dominant security functions towards activities earlier in the threat workflow and think about preventing threats rather than reacting to them as they emerge. Customers of multiple solutions benefit from increased capabilities. These range from new data inputs such as endpoint or the external attack surface that build a holistic view of your internal and external risks, through to improvements in threat preparedness. Organizations can see the next forecasted hop of a live attack and firmer responses for those incidents occurring along critical attack paths.

Darktrace is the first of its kind to provide proactive cyber defense in a single holistic platform. To achieve this, Darktrace pioneered the use of ActiveAI Security that continuously learns from your day-to-day business operations, applying context from your enterprise data ingested from internal native sources including email, cloud, operational technology, endpoints, identity, applications and networks, and external sources of third-party security tools and threat intelligence. Through this approach, Darktrace provides the ability to visualize and correlate security incidents uninhibited by the siloed approach of individual point.



About Darktrace

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a 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 help transform security operations and improve cyber resilience. Breakthrough innovations from its R&D Centers have resulted in more than 200 patent applications filed. Darktrace employs 2,400 people around the world and protects over 9,700 organizations globally from known, unknown and novel cyber-threats.

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

darktrace.com | info@darktrace.com