DARKTRACE

Darktrace / Attack Surface Management

Experience Advanced AI-Powered Defense for Your Attack Surface in Real Time

The Attack Surface is Constantly Growing

The attack surface is constantly expanding with the adoption of remote heal and hybrid work and the rise of interconnected devices, migration to the cloud and increased adoption of Internet of Things (IoT) usage. This exponential growth creates a complex digital environment for organizations, making it difficult for security teams to track all internet-facing assets and identify potential vulnerabilities.

According to research conducted by ESG, **62%** of organizations' attack surface increased over the past two years, driven by additional third-party connections, increasing use of IoT and operational technology, and more use of public cloud infrastructure.[1]

Security Teams are Overwhelmed

More and more security teams struggle with limited attack surface visibility, which leads to an inability to respond quickly to zero days, an ever-growing backlog of repairs, and unclear risk prioritization due to the overwhelming volume of alerts.

Business benefits

Discovery all internet-facing assets
using AI techniques to understand what makes an external asset yours.

Get complete visibility of your attack surface
With continuous monitoring and internet crawling so nothing gets missed.

Understand and prioritize risk
with risk scoring and mapping to your potentially exposed assets

Get threat context and instant updates
With threat monitoring via the newsroom feature

Harden your security defenses
With integrations with Darktrace / Email and Darktrace / Proactive Exposure Management

Legacy Solutions Don't Provide the Whole Picture

Traditional attack surface management solutions often miss discovering all digital assets and lack continuous updates with infrequent scanning, leaving gaps that attackers can exploit. Additionally, they fail to provide contextual intelligence for proper risk prioritization, leading to inefficient resource allocation and increased risk exposure. As a result, organizations remain vulnerable to sophisticated and evolving cyber threats.

Darktrace / Attack Surface Management Provides AI-Drive, Real-Time Protection

Darktrace / Attack Surface Management provides continuous, tailored detection of external exposed assets and potential risk. Using AI techniques, it identifies internet-facing assets unique to your organization and provides a comprehensive view of your external attack surface in real time. Continuous monitoring ensures potential risks and high-impact vulnerabilities relative to your business are discovered eliminating gaps and blind spots, while risk scoring and vulnerability mapping allow you to prioritize mitigating risk on exposed critical assets.

Darktrace / Attack Surface Management uses AI-driven analysis to give you comprehensive insights into your attack surface and digital risks. By adopting a brand-centric approach, Attack Surface Management identifies internet-facing assets unique to your organization, ensuring zero-scope, zero-touch implementation. Drawing from a diverse set of information sources, Darktrace / Attack Surface Management detects potential threats beyond known servers and networks. It can provide continuous, tailored detection of externally exposed assets, allowing for immediate detection and response to emerging threats, and providing a dynamic and proactive approach to managing your digital security.

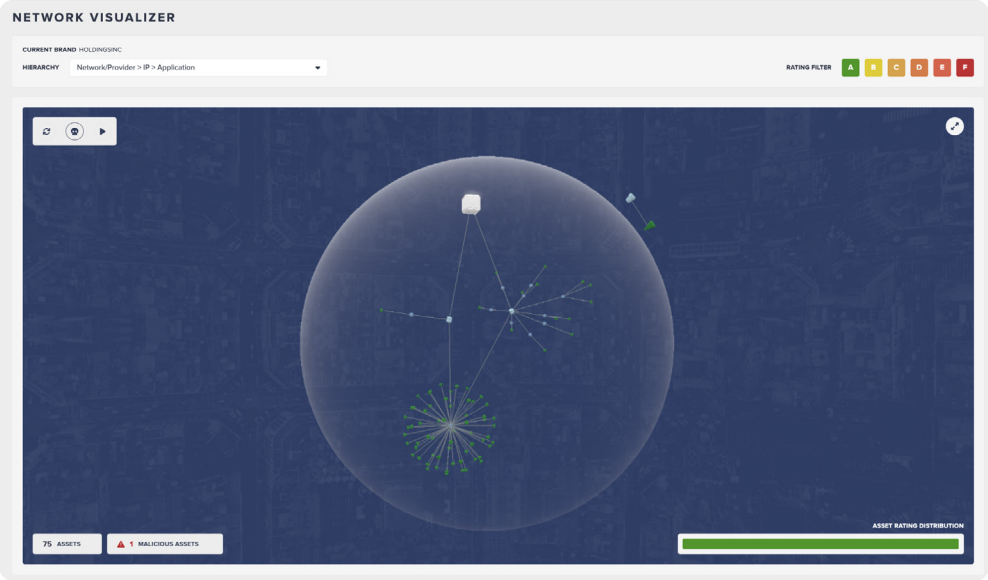
1. Security Hygiene and Posture Management Remains Decentralized and Complex, Enterprise Strategy Group 2023.

Key Capabilities of Darktrace / Attack Surface Management

Unparalleled Asset Discovery

Leverage AI to discover up to 30-50% more assets than before

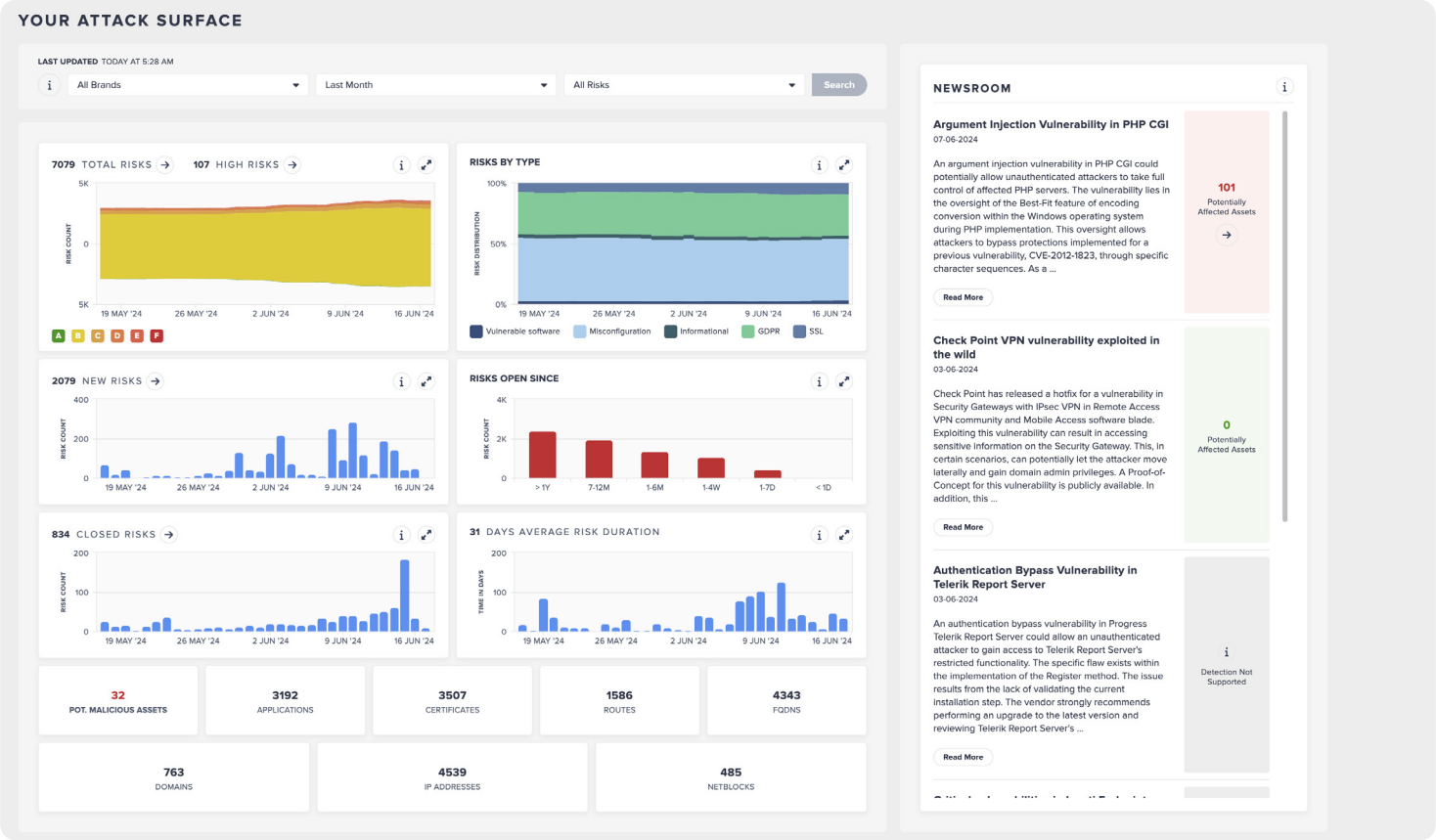
Darktrace / Attack Surface Management uses a range of AI techniques, including natural language processing (NLP), to understand what makes an external asset yours – searching beyond known servers, networks, and IPs, to discover more assets than your organization may realize it has. Unlike other attack surface management solutions, Darktrace requires no technical input: no IP ranges, no other parameters – your brand name is all that's needed. Drawing from a wide array of information sources, Attack Surface Management can uncover assets that either have a technical link with your core infrastructure or can be associated with your brand based on publicly available information – ensuring nothing gets missed.



Comprehensive Risk Detection & Prioritization

Identify every potential risk before an attacker strikes.

Attack Surface Management effectively identifies exposed assets from the perspective of potential adversaries, creating a comprehensive risk profile of your digital estate. It uncovers a wide array of vulnerabilities including supply chain risks, potential phishing domains, misconfigurations, brand abuse and third-party risks. Darktrace / Attack Surface Management can uniquely identify complex use cases, such as risks from network routing issues and shadow IT domain registrations, which most vendors typically do not do. Its risk rating model and risk open time feature enable the identification and prioritization of the most critical vulnerabilities relative to your business, facilitating efficient patching, updating, and management of internet-facing assets.



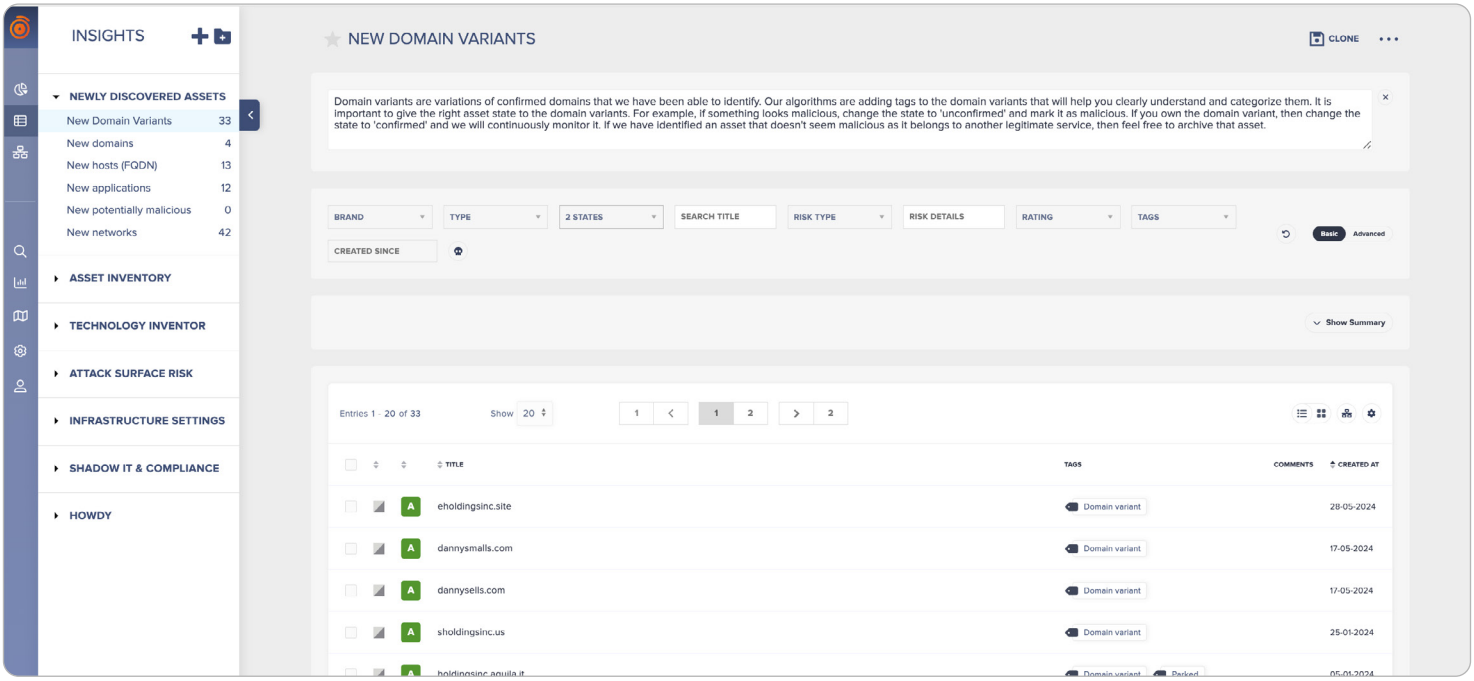
Continuous Monitoring

Eliminate blind spots in your attack surface.

Unlike traditional methods that provide a static snapshot or update on a weekly/monthly cadence, Darktrace / Attack Surface Management continuously monitors your digital estate – identifying risks, high-impact vulnerabilities, and external threats quickly.

The continual crawling ensures any new or unconfirmed assets are accounted for, and any potential new risks or vulnerabilities are detected.

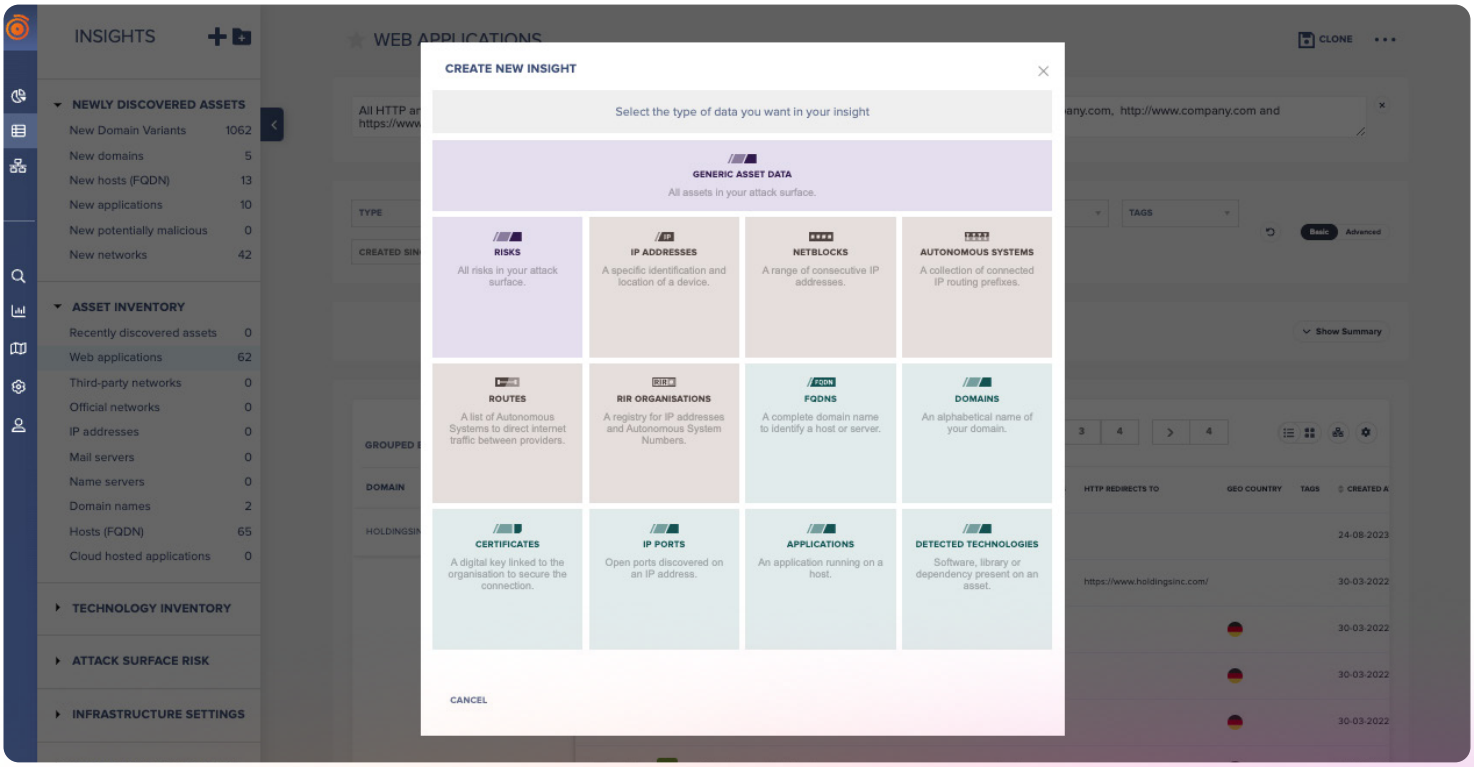
> Knowing that Attack Surface Management is continuously looking for assets and constantly doing vulnerability testing provides me further confidence, assurance, and peace of mind in our cyber security program.
>
> ■ **VP of IT**
> Direct Federal Credit Union



Customized Reporting

Contextual insights specific to your business

Attack Surface Management offers visibility into essential risk metrics, such as the number of critical vulnerabilities on your attack surface. These deep contextual insights enable security teams to prioritize and make effective context-based decisions. Custom reports for specific uses cases can also be created to deliver tailored insights based on your business's needs and priorities.

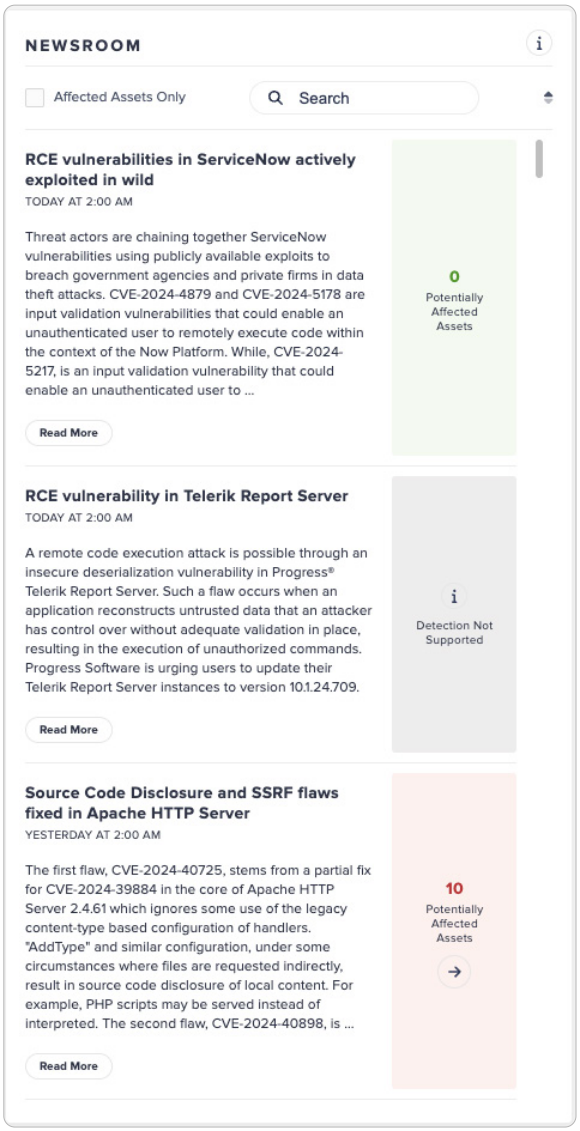


Newsroom

Take preventative action against critical vulnerabilities

Attack Surface Management via Newsroom monitors threat feeds and information sources to deliver immediate threat context and instant updates on high-impact vulnerabilities.

It then reveals all assets on your external attack surface that could potentially be affected by a new critical vulnerability, providing actionable insights. This lets your team focus on preventative measures, rather than having to spend time manually monitoring intelligence sources and news feeds or managing a vulnerability response process.



Deployment

Darktrace / Attack Surface Management is a cloud-hosted SaaS product that requires no input from the client or end user and can be set up in minutes. For customers with multiple brands, specific assets or brands are added to the environment by request via customer support.

Operational Benefits

Eliminate gaps and blind spots
With complete visibility over all digital assets, including shadow IT and cloud instances, allowing your security team to identify and manage potential vulnerabilities more effectively

Focus on what matters
by assessing and prioritizing risk based on potential impact, ensuring that the most critical threats to your company are addressed first

Keep security teams up to date
With continuous and automated monitoring that ensures your attack surface is current and new external assets are accounted for

Get ahead of threats
with automated threat intelligence updates, ensuring your security team has visibility into the latest threats and vulnerabilities without the need for manual updates.

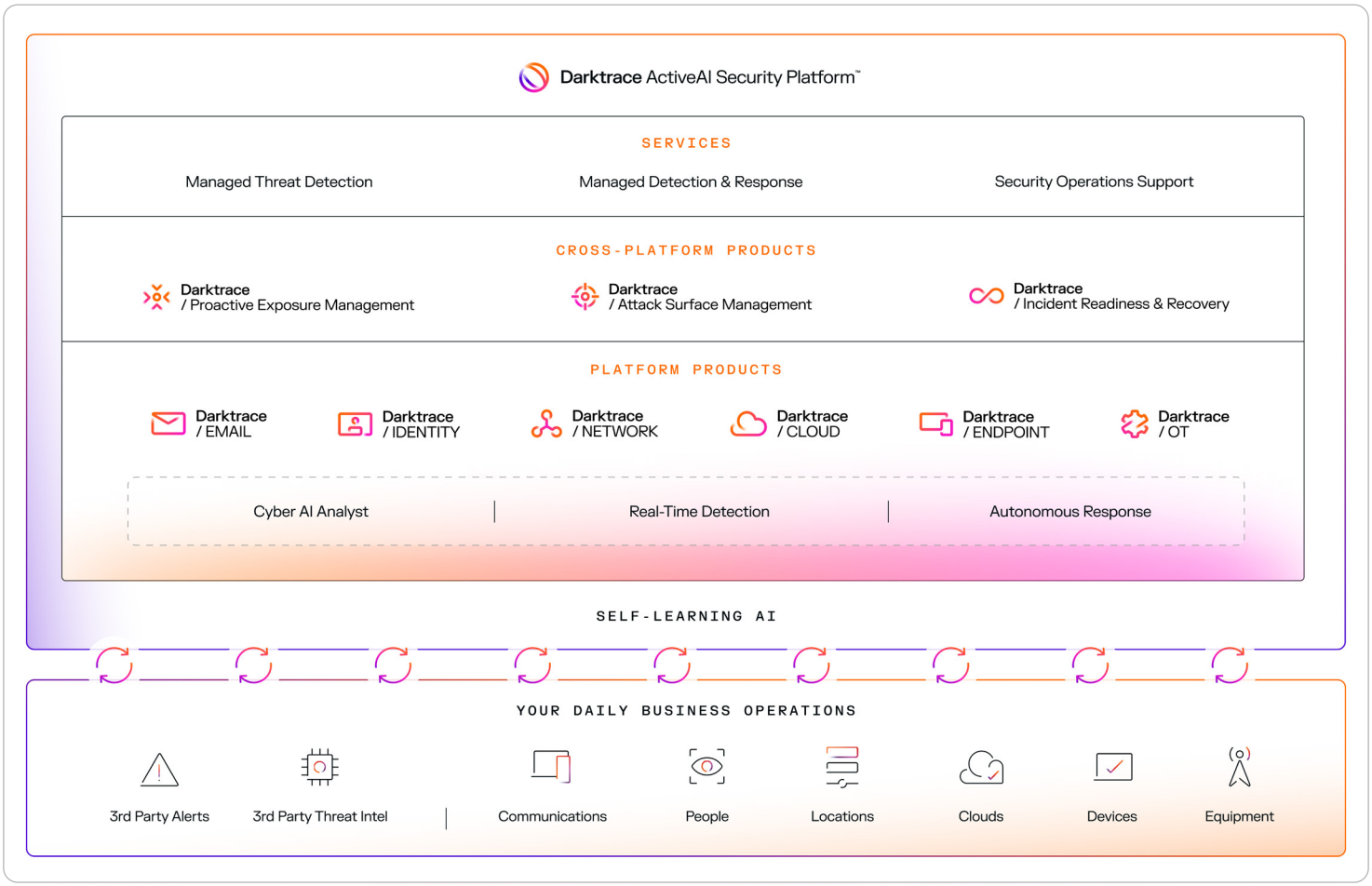
Maximize your security investments
with native product integrations across the ActiveAI platform to harden defenses across your organization and proactively protect against the latest threats

Proactively harden defenses with the Darktrace ActiveAI Platform

Darktrace / Attack Surface Management is part of the Darktrace ActiveAI platform, providing proactive attack surface management across your security stack. Through integration with Darktrace/ Proactive Exposure Management, it offers unified visibility and high-fidelity coverage, linking externally identified assets with internal observations for end-to-end threat mitigation. It seamlessly amplifies Darktrace / Email protections by pre-emptively forewarning against spoofed domains impersonating your organization.

It also enhances detection and response mechanisms at the endpoint and network layer while providing Cyber AI Analyst with external data to enhance its investigations.

Darktrace ActiveAI Security Platform revolutionizes your cyber defenses by helping you proactively prevent cyberattacks, quickly recover from incidents and continually strengthen your security posture, all within a single platform.



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