DIGITAL HAND MADE

Version 5: Extending the Darktrace Immune System

Version 5 of the Darktrace Immune System extends self-learning technology to cover more of the enterprise including SaaS tools and endpoint devices, supports one-click integrations to many security tools, and can now be delivered seamlessly from the cloud.

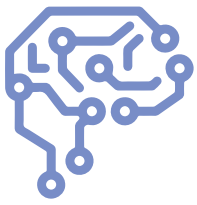
The ability to adapt to changing working conditions has introduced new challenges for security teams, redefining enterprise security in its wake. An increasingly dynamic workforce risks exposing data, creates new vulnerabilities, and is more susceptible to human error.

Security teams are adjusting how they view normal behavior when employees work from home or adopt different work patterns. With self-learning AI, the Darktrace Immune System adapts to these unknown and hidden threats. By increasing the reach of cyber security coverage to endpoints and email, as well as cloud and collaboration tools, Darktrace can actively protect gaps in protection across your enterprise.

Whether your organization is increasing its investment in securing innovative technologies, prioritizing operational speed, or trying to get more value from existing technologies, Version 5 has a lot to offer you. This upgrade represents an extension of the platform across three distinct areas.

AI Augmentation

Enhancements to Antigena Autonomous Response and Cyber AI Analyst



- Antigena expansion
- Cyber AI Analyst for cloud & industrial networks
- AI triage on third-party alerts
- On-demand AI investigations
- External API to share AI Incident Reports with SIEM, SOAR, and SOC systems

Workforce Coverage

Extended coverage across clients, cloud services, and collaboration platforms

- Client Sensors
- Dedicated SaaS Console
- Antigena for SaaS
- New Modules for Zoom, Okta, and more
- New integrations with zero-trust technologies
- Cyber AI Analyst for cloud & SaaS

Seamless Journey

Unified interfaces, flexible integrations, and cloud-delivered deployments

- Unified interfaces
- NOC dashboard
- One-click integrations
- OT Engineer View
- Enhanced Model Editor & Advanced Search UI
- Cloud-delivered deployments

What's New in Version 5?

AI Augmentation

The risks and complexity introduced by a dynamic workforce have not made life any easier for security teams. New technologies and services are being deployed; data flows and topologies are in flux; and static rules, policies, and playbooks have been unable to adapt to changing users and working practices, no matter how diligently and rapidly we rewrite them.

The challenge of managing complexity also stands quite apart from the novel tactics and techniques that Cyber AI continues to discover in the wild, which even the fastest rule writers would be unable to predict in advance. What we have seen and will continue to see in the industry is an urgent need for augmentation, and toward that end, Darktrace has enhanced its self-learning capabilities across two core areas of the platform: Autonomous Response and AI Investigation.

Darktrace Antigena: Autonomous Response

Extending Autonomous Response to SaaS applications

When the Darktrace Immune System detects an emerging cyber-threat, Antigena swiftly interrupts the attack with surgical precision. By containing novel threats in seconds, Autonomous Response enables security teams to prioritize strategic work even as the volume and speed of attacks continues to rise.

In the face of machine-speed threats, Antigena can either take self-directed action or integrate with existing investments as a mechanism for response, informing third-party systems about attacks that have gotten through. With Version 5, Antigena can now neutralize attacks in a wide variety of SaaS services – from email platforms in Microsoft 365, to cloud collaboration tools like Zoom and Teams, to cloud file storage applications like SharePoint and OneDrive.

Common use cases for Antigena SaaS include compromised SaaS or email credentials, insider threat, and admin abuse. By disabling users or blocking geographic access, Antigena can autonomously defend your crown jewels in the cloud without human intervention.

Microsoft 365

SharePoint

zoom

OneDrive

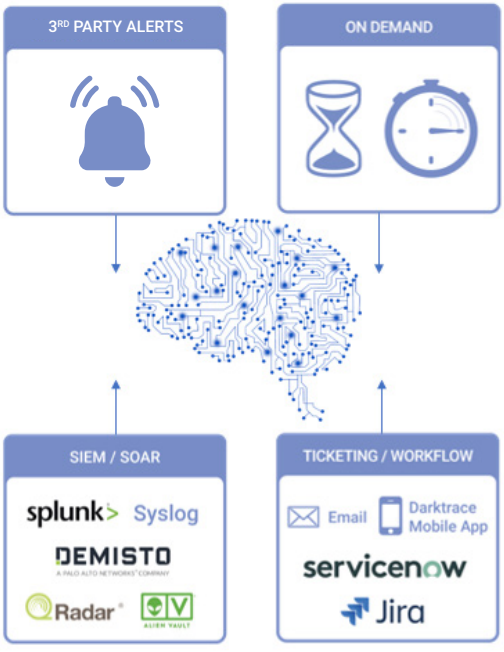
Cyber AI Analyst: AI Investigation

Extending AI Investigations across your workforce and security stack

Cyber AI Analyst is Darktrace's AI investigation technology, which automatically triages, interprets, and reports on the full scope of security incidents targeting your dynamic workforce. Trained on expert analyst behavior and proprietary AI, Cyber AI Analyst reduces time to triage by up to 92%, delivering critical AI augmentation for strained security teams.

By continuously and automatically investigating every security event that the Darktrace Immune System detects, Cyber AI Analyst produces a dynamic situational dashboard as well as written reports that immediately put security teams in a position to take action.

Version 5 extends the reach of Cyber AI Analyst beyond network events to SaaS applications, cloud infrastructure, and cyber-physical systems. It also enables Cyber AI Analyst to conduct on-demand investigations into users and devices of interest, ingest third-party alerts to trigger new investigations, and automatically feed AI-generated Incident Reports to any SIEM, SOAR, or downstream ticketing system.



Workforce Coverage

Today's dynamic workforce is dispersed, agile, and unpredictable. Critical data and applications now live in a host of unfamiliar cloud services, while workforce behavior more generally tends to show up outside of the familiar purview of traditional defenses. In this connection static and incompatible controls have often led to overly relaxed permissions, simple mistakes, and easy avenues of attack for cyber-criminals and insiders alike.

Against this backdrop, an adaptive and unified security strategy that evolves with your dynamic workforce has never been more critical, especially as organizations embrace zero-trust environments, cloud and SaaS applications and more fluid working practices for the long term.

Client Sensors

Extending network visibility to the disconnected endpoint

To cover branch offices and remote workers off the VPN, Darktrace can now deploy lightweight Client Sensors on a range of managed endpoints. This allows the system to analyze real-time traffic of remote workers in the same way it analyzes traffic in the network, correlating a web of connections to learn an evolving understanding of workforce behavior.

In the context of insider data theft, the ability to operate off the VPN is a key risk. Yet with Client Sensors, if a disgruntled employee stages data for exfiltration in, say, a SaaS environment, and then downloads it from home off the VPN, the Darktrace Immune System will detect and contain the incident in seconds.

Cloud, SaaS & Zero Trust

Extending coverage of workforce behavior

Perhaps the most critical locus of workforce activity today resides in SaaS applications, with users increasingly leveraging cloud services from Salesforce and GSuite, to Box, Dropbox, and Microsoft 365. These workforce applications aid efficiency and innovation at scale, and organizations of all shapes and sizes have adopted them for core business functions and operations.

Yet as we move operations to the cloud, native and third-party defenses built for SaaS offer little more than static and siloed 'protective skin'.

The Darktrace Immune System complements native cloud and SaaS defenses with a range of critical enhancements, including a dedicated SaaS Console, extensions of Autonomous Response and Cyber AI Analyst investigations to the cloud, and integrations with Zoom, Okta, Microsoft Teams, and more.

Equally, new ingestion capabilities for Zscaler and other VPN and zero-trust technologies enable Darktrace to protect employees wherever they operate.

Microsoft Teams zscaler

Microsoft Dynamics 365 okta

Darktrace SaaS Console

Seamless Journey, Cloud-Delivered

Unified interfaces

The Darktrace Immune System represents the only self-learning platform that learns normal across your entire digital business – from cloud, SaaS, and email, to endpoints, IoT, and cyber-physical systems.

Unlike legacy platforms with glued together point solutions, Darktrace's platform is anchored in a single cyber AI engine, which learns from a variety of data sources to detect, interpret, and respond to novel threats targeting your dynamic workforce.

While Version 5 introduces new interfaces to the platform – from a dedicated SaaS Console to a specialized OT Engineer View – one of the overarching design principles of the update is unification, and these interfaces are harmonized accordingly to facilitate seamless investigations and simplified workflows.

One-click integrations

The Darktrace Immune System was designed with an open and extensible architecture that seamlessly integrates with your existing investments. In Version 5, new functionality enables customers to enhance and extend their Darktrace deployment via one-click integrations.

This includes the ability to immediately extend coverage to new cloud services, enrich the platform's analysis with new sources of log ingestion, and activate coordinated Autonomous Response via integrations with other security defenses. As organizations accelerate digital transformation and prepare for the future of work, the ability to quickly adapt and integrate their security defenses will be more critical than ever.

Flexible Delivery

As we push the platform forward, a design principle of flexibility across autonomous systems also remains fundamental. Version 5 not only expands the Darktrace Immune System to new areas of the business, but also ensures that this expansion delivers a seamless experience for customers, regardless of where they start their journey with the platform. Delivery and expansion is now entirely flexible, with the option of 100% cloud-delivered deployments, or hybrid deployments that cover on-premise and cloud environments.

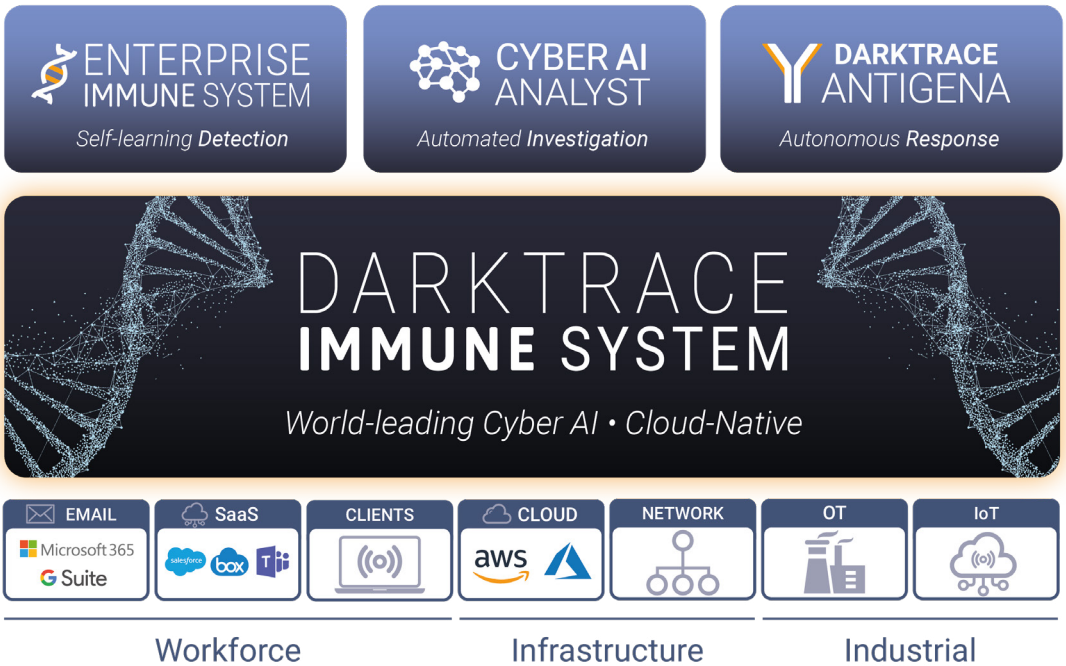


Figure 1: With Version 5, organizations can start their journey with the platform wherever they like, with cloud-delivered deployments and one-click integrations available for seamless expansion.