DARKTRACE

Darktrace ActiveAI Security Platform for Lean IT and Security Teams

The Challenge

As organizations rapidly adopt AI tools, copilots, and autonomous systems, security teams are being asked to secure environments that are becoming more dynamic and interconnected. In many cases, this adoption is happening faster than teams can adapt their existing controls, introducing new pathways across identity, SaaS, cloud, email, and endpoint systems.

At the same time, attackers are using AI and automation to spread activity across email, identity, SaaS, cloud, and network environments, avoiding single points of detection. By relying on low-and-slow techniques and legitimate credentials, they make malicious behavior appear routine, allowing threats to progress without triggering obvious alerts.

Building a security stack with fragmented tools creates new security challenges down the line. Each tool generates its own alerts and requires separate tuning, investigation, and maintenance. Detection is often based on known threats, leading to large alert volumes and uncertainty around what actually needs attention. Even when signals are stitched together, manual validation is required to understand what is happening and what to do next.

Teams need a consolidated security approach that combines AI, data-driven context, and the ability to close gaps in visibility over policy and process to improve mean times to identify and contain threats.

Darktrace ActiveAI Security Platform

The Darktrace ActiveAI Security Platform is designed for lean security teams to eliminate time spent on alert triage and investigations. The platform rapidly detects and responds to known and unknown threats while exposing risk gaps across your technologies and processes, so teams can shift to a proactive cyber approach.

The ActiveAI Security Platform is built on multi-layered, Self-Learning AI that continuously trains from your ever-changing business data wherever it is deployed, with further enrichment from external threat intelligence and third-party alerting.

Core Capabilities

Unprecedented visibility across the enterprise with a Self-Learning AI

Apply Self-Learning AI across network, AI systems, OT, cloud, email, endpoints, applications, and identities to build a holistic understanding of your unique environment, continuously adapt detections as your business changes, and automatically connect related anomalies to reduce integration effort, detection tuning, and time to understanding.

Detection and Response to sophisticated, multi-domain threats

Our AI's Self-Learning capabilities allow it to identify subtle behavioral anomalies that indicate a cyber-attack. Once these are detected, the AI can respond autonomously to neutralize the malicious activity and buy back time when teams are busy or during off hours.

Drastically reduce investigate time with Cyber AI Analyst

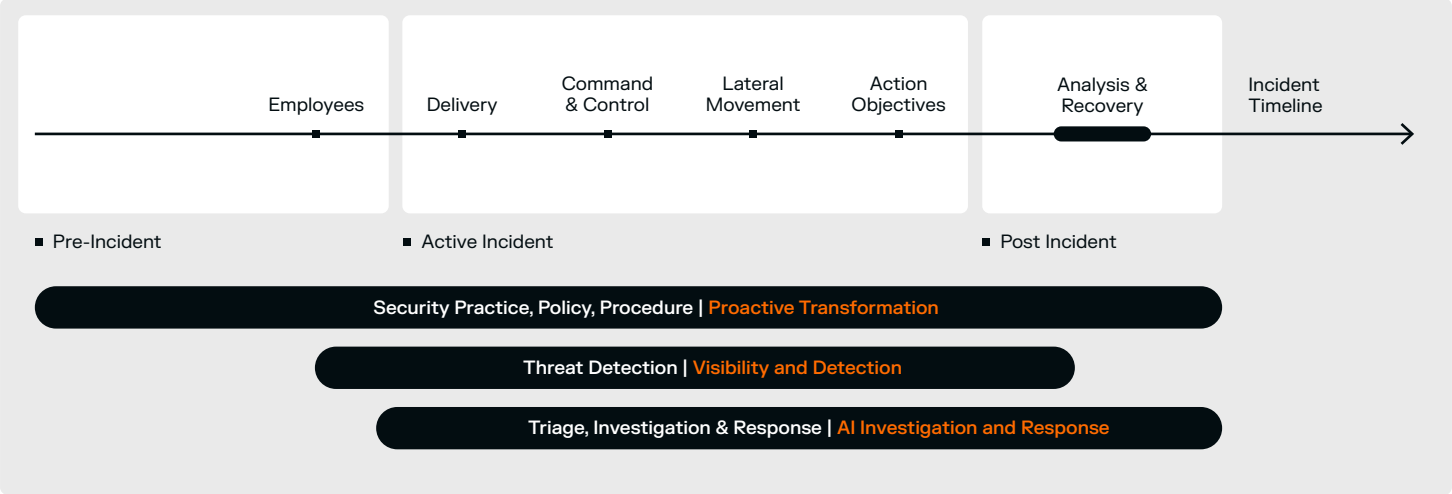
Reduce thousands of individual alerts into only a few incidents. This provides SOCs with up to 30 additional Full Time Employees performing Level 2 analysis and written reporting annually. This means teams no longer have to spend the bulk of their time on alert triage.

Gain insights to achieve a proactive cyber defense

Uncover hidden assets, monitor shadow IT and emerging external risks, and prioritize the most likely attack paths and vulnerabilities based on real business context, helping teams prevent security control failures before they are exploited.

AI-assisted readiness and recovery

Give security teams confidence through realistic incident simulations, readiness reporting, and AI-generated playbooks that assess technology gaps, reduce decision-making under pressure, and guide optimal recovery steps based on active investigations in their own environment.



Operational benefits

Detect threats that do not match known attack patterns

Identify known, unknown, and novel threats earlier by baselining normal behavior across users, devices, applications, network, cloud, and email. This enables detection of suspicious activity even when no signature or prior threat intelligence exists.

Maintain full visibility without managing multiple tools

Monitor activity across the entire digital environment from a single platform, reducing blind spots created by siloed security tools and limited integration between systems.

Prevent incidents by reducing exposure early

Identify exposed assets, attack paths, and vulnerabilities before they are exploited, helping teams prioritize the most meaningful risk reductions without extensive manual analysis.

Increase operational capacity without adding complexity

Automate routine investigation and reporting to free up time for higher-impact work, allowing teams to focus on decision-making, improvement, and prevention rather than constant alert handling.

Communicate risk and incidents clearly to stakeholders

Generate unified reporting and proactive insights that make it easier to explain security posture, incidents, and response actions to leadership without manual report building.

How VERTO simplified their security strategy while reducing costs

01 Managing strict compliance with a lean team

VERTO, a not-for-profit organization, provides employment, training, and community services to help individuals and communities. They needed to maintain continuous security coverage and meet strict compliance requirements with limited internal capacity. Managing multiple tools, responding to alerts after hours, and maintaining confidence during audits placed ongoing strain on day-to-day security operations.

02 Why Darktrace?

VERTO initially deployed Darktrace to provide continuous monitoring and investigation without relying on manual triage or outsourced SOC coverage. The platform's ability to operate autonomously and adapt to their environment made it viable to run alongside existing tools without increasing operational burden.

03 Initial results

Soon after deployment, Darktrace began automatically investigating security events at scale, filtering high-volume activity into a small number of actionable incidents. 8.4 billion events were filtered down to just 19 critical incidents, cutting alert noise by more than 99.9%. The majority of investigations were handled without human intervention, significantly reducing alert fatigue and freeing time for higher-priority work.

04 Long-term benefits / developed partnership

Over time, Darktrace became more than a security tool for VERTO, evolving into a trusted partner invested in their long-term success. The team valued the flexibility, proactive support, and collaborative approach from day one, reinforcing confidence in expanding their use of the platform as needs grew.

Today, VERTO relies on the Darktrace ActiveAI Security Platform as a core pillar of its security strategy, with coverage across multiple domains, including cloud, endpoint, email, identity, and network security, supported by automated investigation through Cyber AI Analyst. This expanded adoption reflects a relationship built on operational trust, measurable outcomes, and shared accountability for protecting the business as it scales.