DARKTRACE

WHITE PAPER

Why Point Solutions Fail

Best Practices for Consolidating Security Tools

Self-Learning AI

CONTENTS

PART I

Point Solutions Fall Short

Cyber security evolved in silos—but attacks do not.

As unique cyber threats appear, security teams are tasked with protecting each of their domains. Sometimes this involves having a host of solutions that can protect email, cloud, SaaS, endpoints, and more. Specialized tools may protect individual elements well, but in the complexity of the modern digital business, security teams are tasked with juggling a patchwork of tools. Integrations are time-consuming, and blind spots are left behind.

Building out defenses in a piecemeal fashion is a reactive approach to defending against the expanding threat landscape. In desperation to keep up with new threats, new solutions have been stacked on top of each other. However, in a world where things are inherently and inextricably connected, management, integration, and visibility over these systems is paramount for security.

Complexity obscures risk and exhausts resources

Aggregating point solutions to meet specific challenges creates diminishing returns. Even if IT had the resources to maintain shelves filled with underutilized point solutions – and most do not — the resulting "tool sprawl" would undermine operations. Aggregating data from too many siloed tools creates complex, disjointed, and redundant workflows that weaken instead of strengthen security.

This creates numerous security deficiencies and workload inefficiencies:

- Gaps between tools that don't interact create dangerous blind spots
- Relying on too many tools leads to alert overload
- Triage progresses in a linear, tool by tool, fashion instead of across multiple attack vectors simultaneously, making it difficult for teams to prioritize
- Slower "time to meaning" delays response
- Inability to track cyber-attacks as they move across multiple domains

Costs rise as efficiency falls. Operating redundant tools and services places excess strain on analyst teams and drives annual renewal and subscription costs up. Security professionals also need to engage multiple vendors and hold multiple calls to investigate events and coordinate incident response (IR).

Digital exposure is a by-product of growth. Cloud migration, mergers and acquisitions, and geographic expansion — all positive things for the business — cause your digital attack surface to expand.

For example, transitioning to the cloud might mean using multiple providers, each partly responsible for security. The dynamic nature of cloud risk imposes another overlay of complexity as security teams grapple with and fine-tune technologies using siloed controls. Blind spots between solutions can cause entire cloud instances and unencrypted data to go completely overlooked.

Platform-based security scales—and fully leverages AI

Consolidating siloed security functions sooner rather than later avoids risk and wasted investment. Aggregation streamlines workflows for securing access, managing privilege, accelerating detection and response, and meeting regulatory compliance goals — all while reducing the burden on your security team.

This paper will overview best practices for aggregating functionalities in an adaptive, AI-led platform to:

- Harden your security posture and improve performance with complete visibility across your environment, faster detection, and a more targeted, automated response
- Modernize and simplify operations to reduce cost, complexity, and compliance efforts

Whether across email, cloud, the network, or OT, cyber security point solutions take broadly the same approach when it comes to AI. They rely on a combination of supervised machine learning, deep learning, and transformers to train and inform their systems. This entails shipping your company's data out to a large data lake housed somewhere in the cloud where it gets blended with attack data from thousands of other organizations.

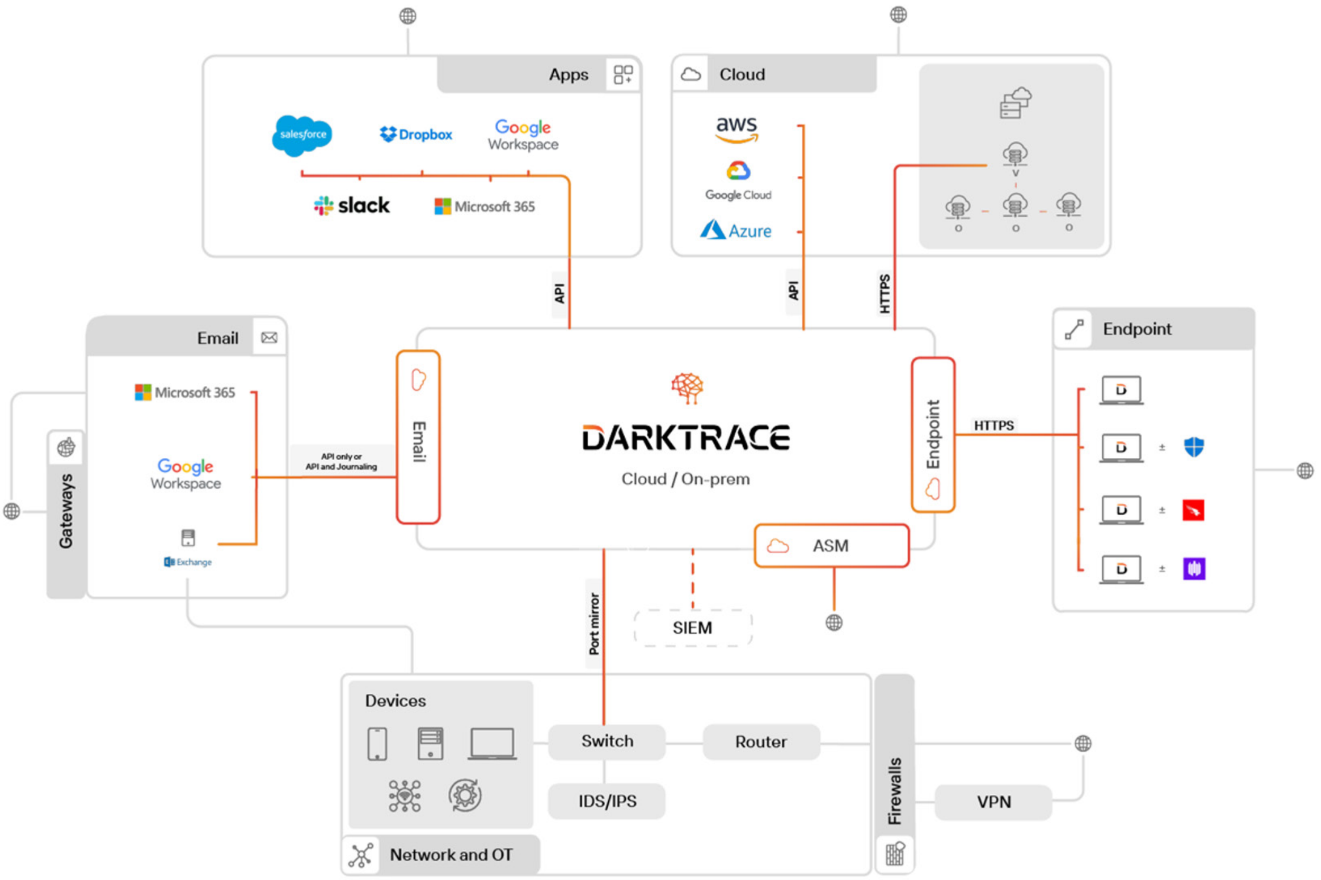

Figure 1: Darktrace Cyber AI Platform

The resulting homogenized data set gets used to train AI systems — yours and everyone else's — to recognize patterns of attack based on previously encountered threats.

While using AI in this way reduces the workload of security teams who would traditionally input this data by hand, it emanates the same risk. Namely, that AI systems trained on known threats cannot deal with the threats of tomorrow. Ultimately, it is the unknown threats that bring down an organization.

At its conception, this was a reasonably smart way of approaching cyber security. For a long time, the assumption that today's threats will resemble yesterday's attacks was a valid one. But in an age where the commoditization of cyber-crime has lowered the bar-to-entry for attackers, and where Generative AI and other open-source tools are enabling personalized attacks at scale, this is no longer the case.

Darktrace brings AI to the data at your organization. Wherever information exists or people are communicating, Darktrace's Self-Learning AI understands what constitutes 'normal' for any given device's pattern of life at an organization. The system then identifies subtle deviations in behavior that indicate a cyber-threat. This unique approach equips the platform to identify novel as well as known threats on the very first encounter – whether said threats arise in the cloud, email, endpoints, network, or OT environments.

Better detection is only half the battle. Darktrace also delivered the world's first proven Autonomous Response technology able to intelligently fight back against in-progress attacks before they do damage. Rather than generate mass quarantines that might lead to downtime, the platform neutralizes threats in seconds by enforcing normal behavior for a user or device that gets compromised.

The system also generates incident summaries that equip resource-constrained security analysts to take immediate action. The context provided includes insights on incidents involving novel attack techniques that cannot be countered using pre-defined playbooks.

> The usability and interconnectivity of Darktrace streamlines our workflow and makes our lives easier every single day. But we also know that when the unexpected does occur and we do come under attack, we have best- in-class AI-powered detection and response to keep our global business running smoothly.

/ Head of Global Infrastructure and Cyber Security, Retail

PART II

Consolidating to Improve Security Performance

Consolidating security controls overcomes the weaknesses inherent in patchworking too many point solutions together. Following modern best practices for leveraging advanced AI improves security performance through:

- Complete visibility with a unified view of risk across multiple domains
- Anomaly detection and behavioral analysis at machine speed and scale without relying on knowledge of past attacks to detect and respond to threats
- Fast, surgical autonomous response to block threats at the first sign of lateral movement
- Proactive assessment of risk to prevent more attacks

Step 1. Eliminate gaps in visibility

Threat actors see more than siloed solutions. Multi-vector attacks can combine and simultaneously launch techniques such as DDoS and ransomware to overwhelm responders and exploit weakness wherever they find it. Siloed security solutions will detect certain attacks they are trained to identify. However, they struggle to bring together the multiple events that constitute an attack's full lifecycle.

Without a unified view of risk, defending critical systems against multi-vector attacks proves nearly impossible. A modern cyber-attack may start in the email environment, move laterally through a network, and then spread to cloud or operational technology. By the time a threat triggers detection it may have finished doing what it came to do — steal or ransom data and disrupt operations.

Nuanced and phased attacks may surprise or gradually disarm security teams that use one dimensional point solutions that rely on a single point of reference. Individual tools send very narrow views of data, leaving analysts to pivot between dashboards to build a complete, actionable picture of risk

Comprehensive Protection Wherever You Need It

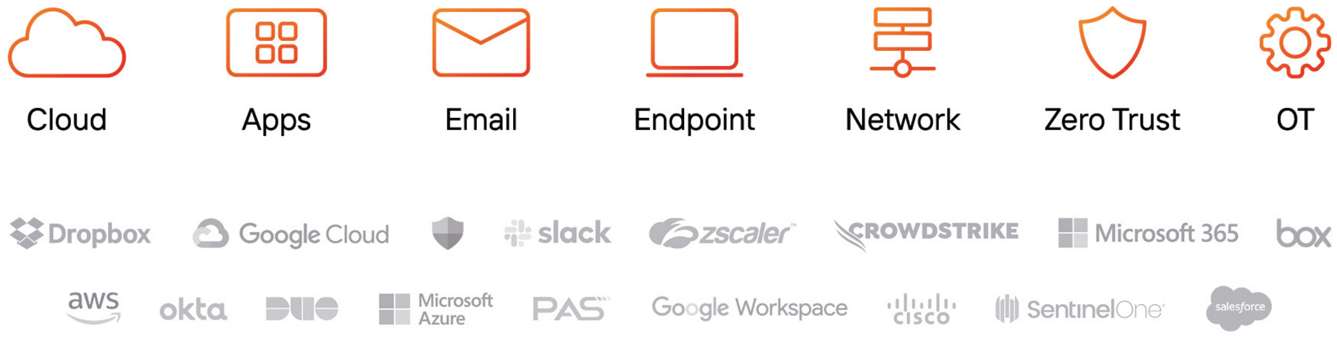

Figure 2: Darktrace provides complete lifecycle protection across the entire business and multiple domains

A platform-based approach unifies coverage across multiple domains

Costs rise as efficiency falls. Operating redundant tools and services places excess strain on analyst teams, leading to increased annual renewal and subscription costs. Security professionals often find themselves engaging with multiple vendors and holding numerous calls to investigate events and coordinate incident response.

In response to these challenges, end-to-end visibility across your entire environment becomes crucial. This equips defenders with a holistic understanding of their digital estate, enabling effective prioritization of sophisticated threats. The Darktrace platform is specifically designed to address these issues. It deploys seamlessly wherever data resides within an organization, providing security professionals with a unified view of data and risk. This spans corporate networks, cloud/ SaaS applications, endpoints, email, and even OT resources—all accessible through a single-pane-of-glass interface.

Moreover, the platform's unified interface consolidates email, Microsoft, Google, and other account activities, presenting security professionals with an easily accessible view for immediate insight. This consolidated approach empowers them to classify and respond to threats promptly.

Use Case: Consolidating Security in the Cloud

Darktrace combines cloud security posture management (CSPM) that reveals misconfigurations, compliance risks and organizational policy violations with a real-time external and internal assessment of cyber security readiness.

Rather than bombard security teams with 'to do' lists containing thousands of vulnerabilities, the platform provides context based on exposure and potential damage. Real-time threat detection and cloud-native response also help to contain emerging cloud risks.

Step 2. Accelerate "time to meaning"

Detection outpaces analysis. Even with AI, inefficient use of point solutions results in lengthy linear investigations. Many monitoring solutions leverage automation to detect threats and send them to analysts in near-real-time, but humans still need to evaluate and investigate them one-by-one to have a complete understanding of the attack lifecycle.

Most detection tools and even some consolidated platforms use static machine learning technology to train the system to recognize risk. With this rearview-mirror approach, each tool's frame of reference consists only of known attacks that occurred in the past. This approach lacks the ability to recognize unusual activity for your unique organization, a critical advantage for identifying both known and unknown threats on the first encounter

AI-led platform analyzes anomalies in real time—at the same time

Understanding normal behavior for individual users and devices allows Darktrace's AI to recognize anomalous activity. The platform notices behaviors that appear to be benign in isolation but, when viewed in context, clearly point to digital risk developing in your environment.

The AI learns your organization to spot sophisticated security incidents that consist of seemingly unrelated indicators of risk appearing across multiple domains. Then, it connects the dots, coalescing insights and using Explainable AI to enhance time-to-meaning for seemingly disparate events in a unified view.

Autonomous approach maintains itself. Compared with a static learning approach, Self-Learning AI continually updates itself and also adds to your analysts' understanding of what's normal for your business. Data remains current without analysts having to manually update multiple tools with the same information.

An integrated platform streamlines communication between teams (and tools that don't talk to one another). Rather than flood analysts with alerts, efficient platform-based tooling enhances their ability to illuminate and share the latest data, threat intelligence, and tribal knowledge across teams. Working from a single, reliable data set speeds and simplifies detection, investigation, mitigation, recovery, and compliance efforts.

Step 3. Automate response to stop threats in second

Coordinating insights across multiple systems delays response. Relying on a patchwork of point solutions to investigate and correlate threats and vulnerabilities slows things down — the exact opposite of what you want these tools to do. Individual tools may use AI to spot attacks in a given environment, but when the tools act independently of each other, security teams must work hard to pull the pieces of the puzzle together. Disparate or redundant efforts make it harder to coordinate response and increase the chance of human error.

According to IBM:

> "Organizations that used security AI and automation extensively within their approach experienced, on average, a 108-day shorter time to identify and contain the breach. Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches."[1]

/ IBM Cost of a Data Breach Report 2023

AI-led platform facilitates autonomous response

A modern AI-led platform should act to resolve risk on its own. Faster reconciliation of events helps analysts prioritize and mobilize to respond faster, but even that is no longer enough. The Darktrace platform uniquely automates response that goes beyond sending alerts or opening tickets.

Darktrace's dynamic understanding of your environment enables a truly autonomous and precise cloud-native response. Its understanding of 'normal' for every user and device allows it to enforce 'normal' – cutting out only the malicious activity, while allowing normal business to continue functioning.

How this response will take place will depend on where Darktrace is deployed in your environment. In the network, it might mean blocking specific, anomalous connections over a certain port. In the cloud, it could mean detaching EC2 instances and applying security groups to contain only assets at risk. In email, this could be locking links or flattening attachments.

Response actions can be initiatives either by Darktrace directly through native mechanisms, or via integrations with your organization's existing security controls.

Data breaches that occur at organizations that use AI and automation for security cost

$1.76M

less than at other companies

/ (IBM)

Step 4. Consolidate internal and external views of risk

Real-time detection and response is only part of the cyber security prism. Security teams are increasingly looking to proactively reduce cyber risk and prevent attacks before they're even launched. This often requires security solutions that support security staff in preparation for cyber-attacks by identifying vulnerabilities, emulating attacks, and more. The goal of this practice is to prevent attacks from happening in the first place. Doing so involves 'thinking like an attacker' to harden defenses.

Security teams operating preventative security measures today will be juggling some combination of Attack Surface Management (ASM), attack path modeling, red teaming, penetration testing, security awareness training, vulnerability management, and more. These tools and processes rarely interact with each other, and create significant overhead. Solutions that consolidate several prevention techniques into one unified platform, that also has the capability to inform detection and response, help mitigate cyber risk much more effectively. A more holistic approach to cyber risk reduction starts with a cohesive view of both internal and external risk.

End-to-end platform prevents more attacks

Combining an internal and external view of risk. Darktrace's end-to-end approach combines both ASM and attack path modeling to help anticipate and avoid attacks. This allows defenders to combine external insight (i.e. "Which areas of my infrastructure are most exposed to the outside world?") with internal perspective (i.e. "What are the quickest and easiest paths within my organization to my crown jewels?") for a comprehensive, actionable view of risk.

Combining preventative measures with detection and response. This comprehensive view of risk can then be combined with detection and response mechanisms for even greater efficiencies. ASM and attack path modeling show analysts the most risky and likely pathways of attack. This intelligence can be shared with detection and response systems so they can watch the assets along these paths closely and prioritize investigating unusual activity involving those assets. Within the platform, information from attack prevention techniques automatically feeds into detection and response solutions and vice versa. AI engines alert on particularly vulnerable paths and high-profile assets at risk so detection and response systems can be on heightened alert for unusual activity.

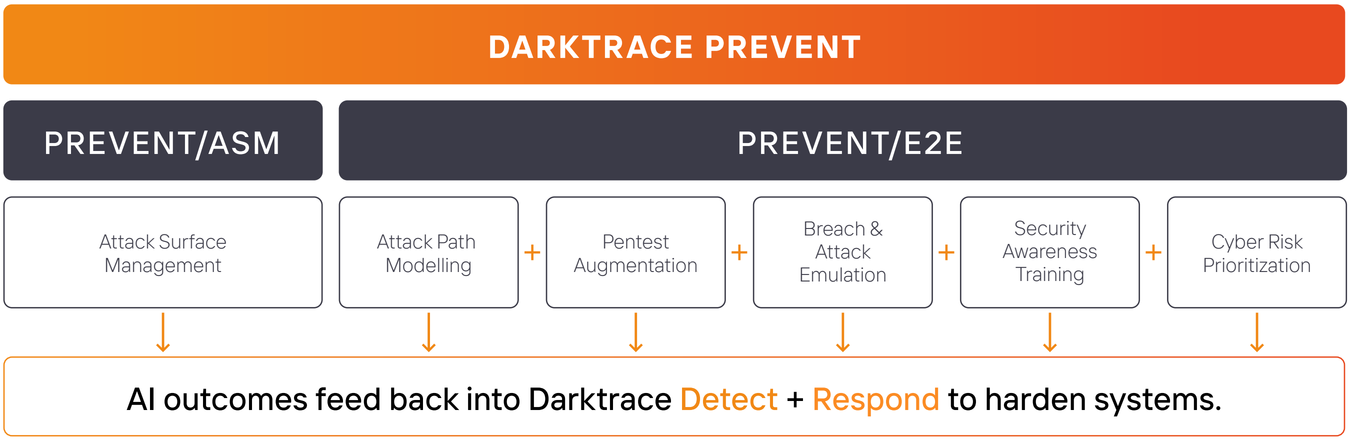
DARKTRACE PREVENT
PREVENT/ASM
PREVENT/E2E
Attack Surface Management
Attack Path Modelling
+
Pentest Augmentation
+
Breach & Attack Emulation
+
Security Awareness Training
+
Cyber Risk Prioritization
AI outcomes feed back into Darktrace Detect + Respond to harden systems.

Figure 3: Darktrace PREVENT combines several preventative security measures into one end-to-end solution

PART III

Consolidating to Level-up Operations

The math is straightforward: The more security functions companies consolidate within an integrated platform, the fewer tools professionals need to buy, and the less time it takes to integrate and manage them all. Fewer gaps between tools and within workflows simplifies governance and audit trails to avoid fines, liability, and potential damage to your brand reputation.

Step 5. Simplify integration

Point solutions provide limited integration features, particularly across infrastructures spanning multiple cloud environments. Each individual tool might only integrate within a particular environment (AWS, Azure, SCADA).

Consolidation streamlines initial setup while improving coverage

With an end-to-end platform approach, one tool integrates with all environments to eliminate redundant configuration and translation efforts. Flexible integrations allow the Darktrace platform solution to reach every corner of your business from cloud systems and endpoints to OT systems and traditional corporate networks. The platform integrates with your organization's existing security controls, allowing CISOs and security leaders to leverage and maximize prior investments to handle future attacks.

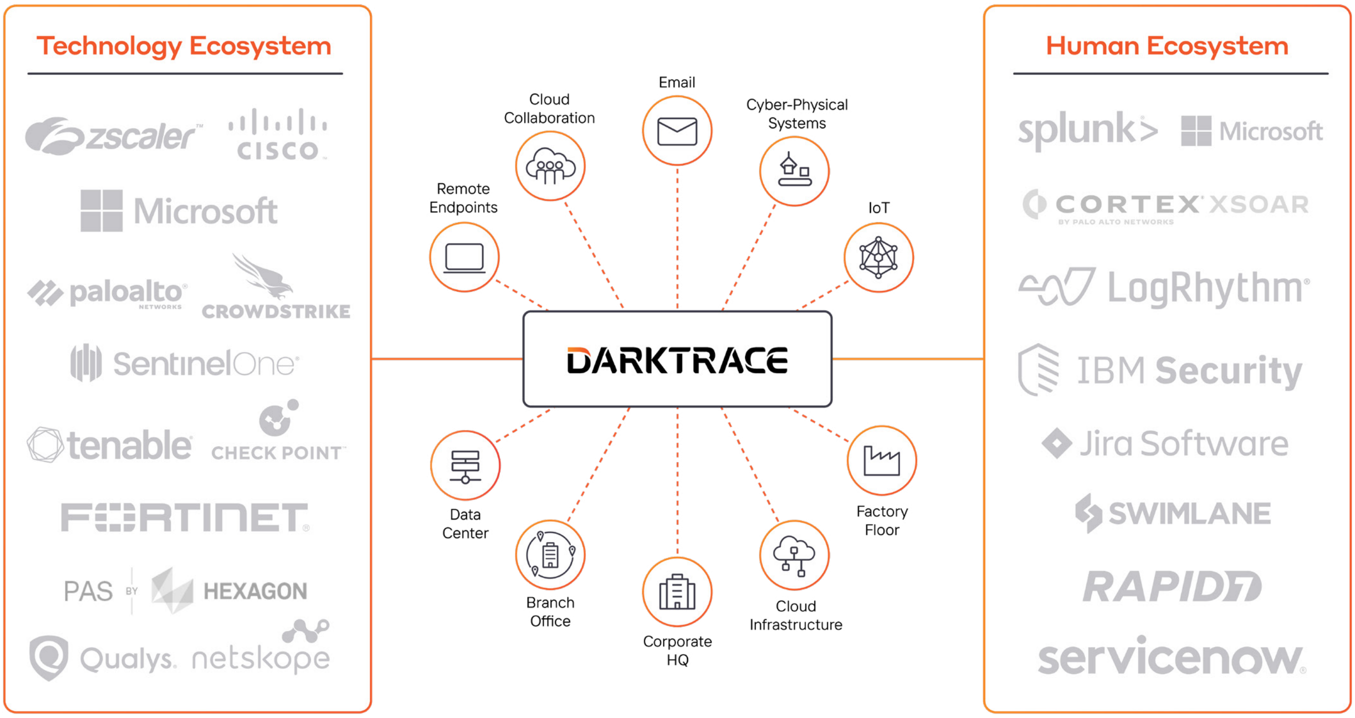

Figure 4: Darktrace is designed with an open architecture that makes it the perfect complement to your existing infrastructure and products

Step 6. Reduce cost & complexity

On the surface, buying point solutions to combat specific problems as they arise might appear to cost less than onboarding to a holistic platform, but in the long run:

Consolidation generates massive cost-efficiencies

By consolidating various functions and resources within one platform, Darktrace effectively reduces complexity and streamlines vendor management and support. Consolidated billing provides greater budgetary transparency and enhances cost management and resource allocation.

An AI-led platform approach allows security to evolve dynamically in step with the business. Additional capabilities can be turned on the moment they're needed without IT needing to source, test, and set up new vendors within purchasing systems.

Step 7. Streamline compliance and reporting

Organizations need to produce and provide evidence to demonstrate compliance with federal, state, and industry regulations surrounding data privacy. The benefits of consolidation for streamlining governance efforts include:

- Greater control over information and digital assets
- Improved management that ensures consistency across organizations
- Reduced cost and risk associated with data breaches and compliance violations
- A complete, cohesive trail that simplifies reporting and policy documentation following incidents

Darktrace introduces customizable compliance features that allow mapping of security controls to relevant best-practice frameworks from CISA, NIST, CIS-20, FERC, and NIS2. Events and anomalies occurring on critical attack paths automatically get tagged and mapped to MITRE ATT&CK to help with auditing and compliance reporting.

Darktrace's Cyber AI Analyst generates detailed reports in plain language that non-technical professionals can reference to document governance. Summaries generated at machine speed break down events step-by-step and help meet requirements to report cyber security incidents to authorities within a tight window of time (e.g. NIS2 specifies 24 hours).

PART IV

Choosing the Right Platform to Consolidate Security Tools

Part IV. Choosing the Right Platform to Consolidate Security Tools

Once the CISO decides on a platform-centric approach to security, the work of finding the ideal fit for your organization begins. A best-practice approach consolidates security elements and coverage across multiple domains to deliver:

- Visibility, detection, response, and prevention throughout your digital estate
- Faster, more accurate analysis of behaviors and events
- Surgical autonomous response to threats
- Streamlined regulatory compliance and reporting

AI that's not stuck in the past

Darktrace offers the industry's only Self-Learning AI that develops a cross-platform understanding of user behavior across email, network, cloud applications, and OT environments. By learning about your business from your business in real time, the platform recognizes and resolves nuance activity that point solutions and other platforms might miss. Darktrace reveals the full scope of an incident and clearly depicts and contextualizes each stage of an attack for security teams.

The right platform prepares defenders for whatever comes next. Consolidation to the Darktrace platform scales security to meet the changing needs of a growing business. Smarter use of AI hardens defenses, unburdens analysts, and maximizes the value of automation and human resources.

The journey starts here

Darktrace offers a 30-day free trial. To take the next step on your consolidation journey, see what Darktrace finds in your environment.

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 more than 145 patent applications filed. Darktrace employs 2,200+ people around the world and protects over 9,000 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 4949 7696

info@darktrace.com

darktrace.com