DARKTRACE

Darktrace / IDENTITY

AI-Powered Identity Threat Detection and Response: Real-Time Protection for Every Identity, Everywhere.

Security siloes don't provide the big picture

Productivity suites and SaaS applications offer unparalleled speed and efficiency for businesses but have also expanded the attack surface to create new opportunities for attackers.

The measures taken to secure these applications are often siloed from the rest of the organization's infrastructure. Modern cyber-attacks traverse multiple domains, with data from cloud applications often representing just one piece of a much larger puzzle. As organizations increasingly adopt SaaS applications and remote work platforms, managing identities across diverse environments has become a significant challenge.

These fragmented ecosystems lead to visibility gaps, making it difficult to detect insider threats and malicious activities within critical applications such as Microsoft 365, Google Workspace, Okta, Zoom, and Salesforce.

Attackers exploit these vulnerabilities using advanced techniques like phishing, credential stuffing, and social engineering. Stolen credentials have been implicated in over 31% of breaches [1], demonstrating the urgent need for advanced identity protection that extends beyond traditional access controls. Compounding the challenge is the need to balance stringent data protection standards such as GDPR and CCPA with user convenience.

Managing compliance in dynamic hybrid environments is resource-intensive, requiring automated solutions to ensure consistent security and adherence to regulatory requirements.

Business Benefits

Proactive risk mitigation: Identifies and stops identity-based threats like credential theft and account takeovers before they escalate, reducing the risk of breaches.

Operational efficiency for security teams: Automates time-consuming detection, investigation, and response workflows, enabling SecOps teams to focus on high-priority tasks.

Streamlined compliance: Ensures continuous adherence to organizational standards with automated policy enforcement and real-time activity monitoring.

Comprehensive threat coverage: Unifies visibility and protection across SaaS applications, email systems, and cloud platforms, eliminating blind spots.

Minimized business disruption: Autonomously responds to threats while maintaining operational continuity, ensuring business processes remain unaffected.

Cost-effective security: Reduces the cost of breaches and the burden of manual operations with AI-driven automation, optimizing resource allocation.

Enhanced security posture: Delivers a unified platform that strengthens identity, cloud, and email security, building resilience against sophisticated attacks.

Confidence in security operations: Empowers CISOs and SecOps teams with real-time insights, actionable intelligence, and a proactive approach to identity security, fostering trust at all levels of the organization.

[1] Verizon 2024 Data Breach Investigations Report (DBIR)

Fragmented security leaves critical gaps in identity protection

Supported SaaS Applications

Existing identity security tools often fail to meet these challenges. Many struggle to integrate seamlessly into hybrid or multi-cloud infrastructures, leaving blind spots. Scalability is another common issue, with traditional solutions unable to adapt to organizational growth or evolving security needs. This lack of flexibility creates performance bottlenecks and increases risk exposure. Additionally, the reliance on static rules and manual workflows delays response times, giving attackers an opportunity to exploit security gaps. Organizations require a modern, integrated solution capable of providing comprehensive visibility, automated response, and proactive defense across their identity landscapes.

Redefining identity security in the cloud era

Darktrace / IDENTITY is an AI-native identity security solution built to address the complexities of identity security in today's multi-cloud environments. By leveraging Self-Learning AI, the solution delivers visibility, continuous monitoring, and automated responses to detect, mitigate, and respond to identity-based threats in real time. Its advanced capabilities ensure organizations can identify abnormal activities targeting user credentials, privileged accounts, and sensitive access points, empowering security teams to stay ahead of sophisticated threats that traditional tools often miss.

Darktrace / IDENTITY provides a unified view of identity activity across critical SaaS applications such as Microsoft 365, Okta, Salesforce, Slack, and more, ensuring no threats are overlooked even in fragmented environments. By monitoring user behavior beyond authentication, Darktrace / IDENTITY detects unauthorized administrative actions, excessive file downloads, and lateral movement within SaaS ecosystems. This comprehensive approach enhances security posture, minimizes operational disruptions, and enables organizations to proactively address identity threats before they escalate. With seamless integration, rapid deployment, and scalability, Darktrace / IDENTITY adapts to evolving business needs, providing robust identity protection while reducing operational burden.

Additionally, Darktrace / IDENTITY supports "bring your own" application behavioral detection and response with custom modular configuration through a REST API that supports JSON, OAUTH 2, and API key authentication. This flexibility allows organizations to adapt the platform to their unique environments, ensuring tailored, effective security measures across all identity touchpoints.

A holistic approach to securing identities

Unified protection across SaaS, email, and cloud

Darktrace / IDENTITY is a critical component of the Darktrace ActiveAI Security Platform, enabling customers to expand threat detection beyond email, cloud, and network environments to common SaaS applications. By integrating these modules, the platform leverages the power of Self-Learning AI and Cyber AI Analyst to deliver unparalleled visibility, contextual threat analysis, and rapid response capabilities. This unified approach ensures that user activity is continuously monitored, whether it originates within SaaS applications, cloud platforms, or email systems, and enables security teams to detect and respond to threats faster than ever before.

The integration of Darktrace / IDENTITY and Darktrace / CLOUD extends the reach of Self-Learning AI beyond the enterprise network, bringing anomaly detection and behavioral analysis to critical SaaS applications and cloud-based environments. The Darktrace / IDENTITY Console provides a dedicated interface for investigating user activity, offering global maps of activity, detailed logs, and visualizations of anomalous behavior chains. By correlating identity and cloud-based activities, the platform can detect sophisticated attack patterns, such as a compromised Microsoft 365 account used to exfiltrate data from Dropbox or unauthorized privilege escalations in AWS.

Adding Darktrace / EMAIL into this ecosystem enhances protection by addressing the threats originating from phishing attacks and credential theft attempts that are often the starting point for identity-based attacks. For example, if a phishing email targeting an executive is flagged by Darktrace / EMAIL, the platform can correlate this event with unusual login behavior detected by Darktrace / IDENTITY, such as an impossible travel scenario or the use of a previously unseen device. By connecting these insights, Darktrace can autonomously block the attacker's IP, terminate active sessions, and disable the compromised account, stopping the attack before it spreads further.

This unified approach also enables the platform to identify and respond to insider threats and Advanced Persistent Threats (APTs) that span multiple environments. For instance, an insider attempting to use legitimate credentials to access sensitive files in SharePoint and then share them externally via Slack can be detected by combining insights from Darktrace / IDENTITY and Darktrace / CLOUD.

Darktrace / EMAIL adds another layer of protection by analyzing email behaviors to detect suspicious file-sharing links or policy violations. Together, these modules provide a complete picture of the attack, allowing for precise and coordinated responses.

By connecting identity, email, and cloud security, Darktrace's platform removes silos that traditionally hinder security efforts.

It enables faster detection of identity-based threats, minimizes manual investigation time, and ensures a more robust security posture across the entire digital estate. This comprehensive approach is critical in defending against today's sophisticated cyber-attacks, where threats often move laterally across multiple systems before achieving their objectives.

Enhanced identity security for Microsoft 365 and Entra ID

The Darktrace / IDENTITY Microsoft 365 module provides visibility into several products including Sharepoint, OneDrive for Business, Dynamics, Teams, and other Microsoft 365 services. Depending on the service, this user activity can include user management, file creation and sharing, and administrative events. Data is retrieved directly from the Microsoft unified audit log.

Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Microsoft unified audit log. By default, one set of requests is made every minute. The data retrieved from Microsoft 365 is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation.

Microsoft 365 login activity is managed by Entra ID (formerly Azure AD). Events that will be retrieved include login and access activity, changes to recovery information, and changes to multi-factor authentication use. User administration changes including role assignment and removal, group membership, user creation, and user deletion will also be retrieved.

Response actions can either be automatic or manual and include forcing a user logout, disabling a user, and blocking access from an IP or IP range for a specific user.

Darktrace / IDENTITY

Real-time identity threat detection & response powered by Self-Learning AI.

Comprehensive visibility and monitoring for identity threat detection

Provides deep visibility across SaaS applications, establishing behavioral baselines for users to detect subtle anomalies like unusual login locations, unauthorized actions, or excessive file downloads. This unified view across platforms like Microsoft 365 and Salesforce ensures no vulnerabilities are overlooked, empowering organizations to identify and mitigate threats before they escalate.

Rapid investigation & response for full spectrum of identity attacks

Leverages AI-powered workflows to detect and respond to identity threats like account takeovers and insider threats within seconds, autonomously taking actions such as disabling compromised accounts. Cyber AI Analyst connects suspicious activities across platforms, providing actionable insights, and reducing response times, while alleviating operational burdens on security teams.

Expanding existing security controls with multi-platform coverage

Integrates seamlessly with SaaS applications like Microsoft 365 and Slack, supporting custom configurations and API-based connectivity for flexible coverage across SaaS environments. As part of the Darktrace ActiveAI Security Platform, it unifies identity, cloud, and email security, breaking down silos to detect and neutralize sophisticated attack patterns comprehensively.

Key capabilities of Darktrace / IDENTITY

Outsmart identity threats at machine speed.

Get complete identity coverage and uncover blind spots with precision threat detection.

At a glance:

- Comprehensive identity visibility and monitoring
- Detect known and novel identity threats across SaaS applications
- Uncover anomalous identity activity in real time
- Autonomous response at machine speed
- Streamline SecOps with Self-Learning AI

Comprehensive visibility and monitoring for identity threat detection

Darktrace / IDENTITY offers unmatched visibility and monitoring across SaaS applications, giving security teams deep insights into user behavior and the ability to detect early signs of credential theft, insider threats, and account takeovers.

By continuously analyzing identity activity, the platform establishes a unique behavioral baseline for each user, identifying subtle deviations that could indicate a threat. For example, unusual login locations, new device types, or out-of-character time-of-day access patterns are flagged in real time, allowing organizations to take proactive measures against potential attacks.

In addition to detecting anomalous activities, Darktrace / IDENTITY provides a unified view of identity activity across critical applications like Microsoft 365, Okta, Salesforce, and Slack. This holistic perspective ensures that no vulnerabilities are overlooked, even in fragmented, multi-cloud environments. The platform also extends its monitoring capabilities beyond authentication, analyzing post-login behaviors such as unauthorized administrative actions, excessive file downloads, or lateral movement within SaaS ecosystems.

This comprehensive approach empowers organizations to identify and mitigate vulnerabilities before they escalate into significant breaches, enhancing their overall security postures.

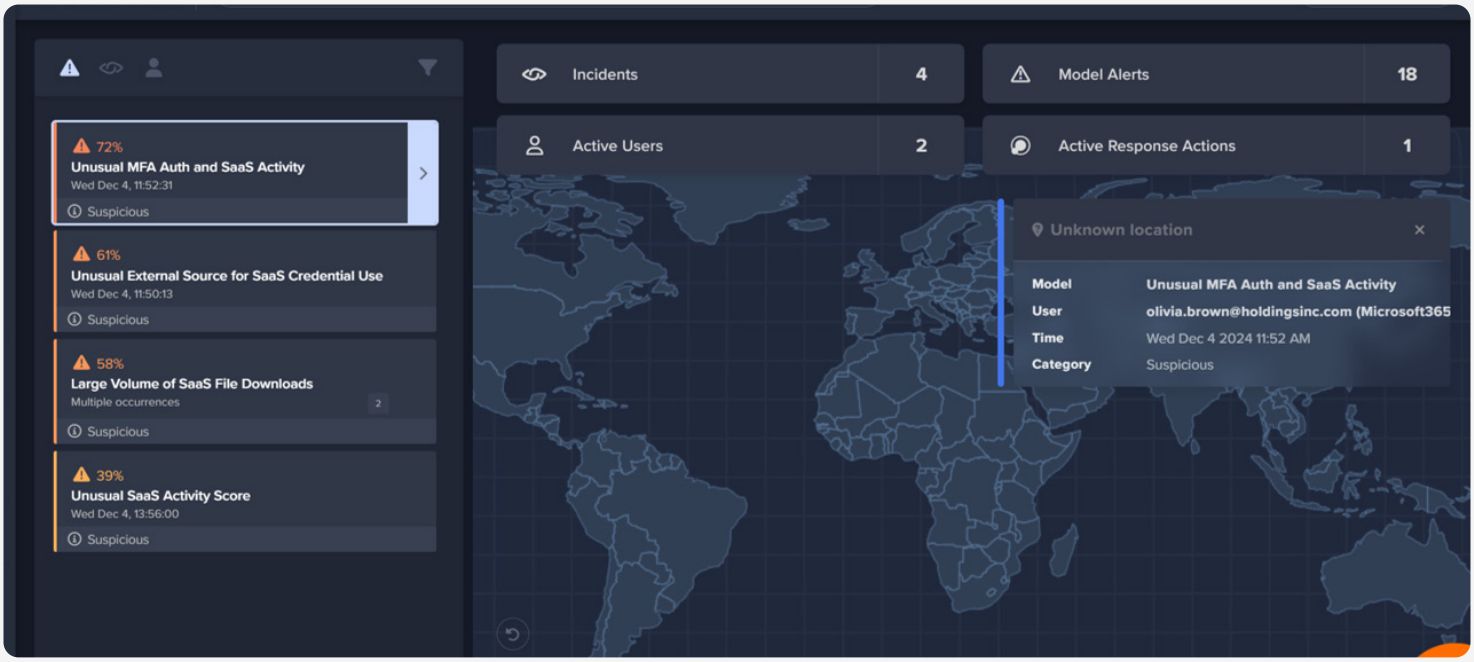

Figure 01: The Darktrace Threat Visualizer provides a unified view of identity activity across critical applications, analyzing authentication and post-login behaviors such as unauthorized administrative actions, excessive file downloads, or lateral movement within SaaS ecosystems.

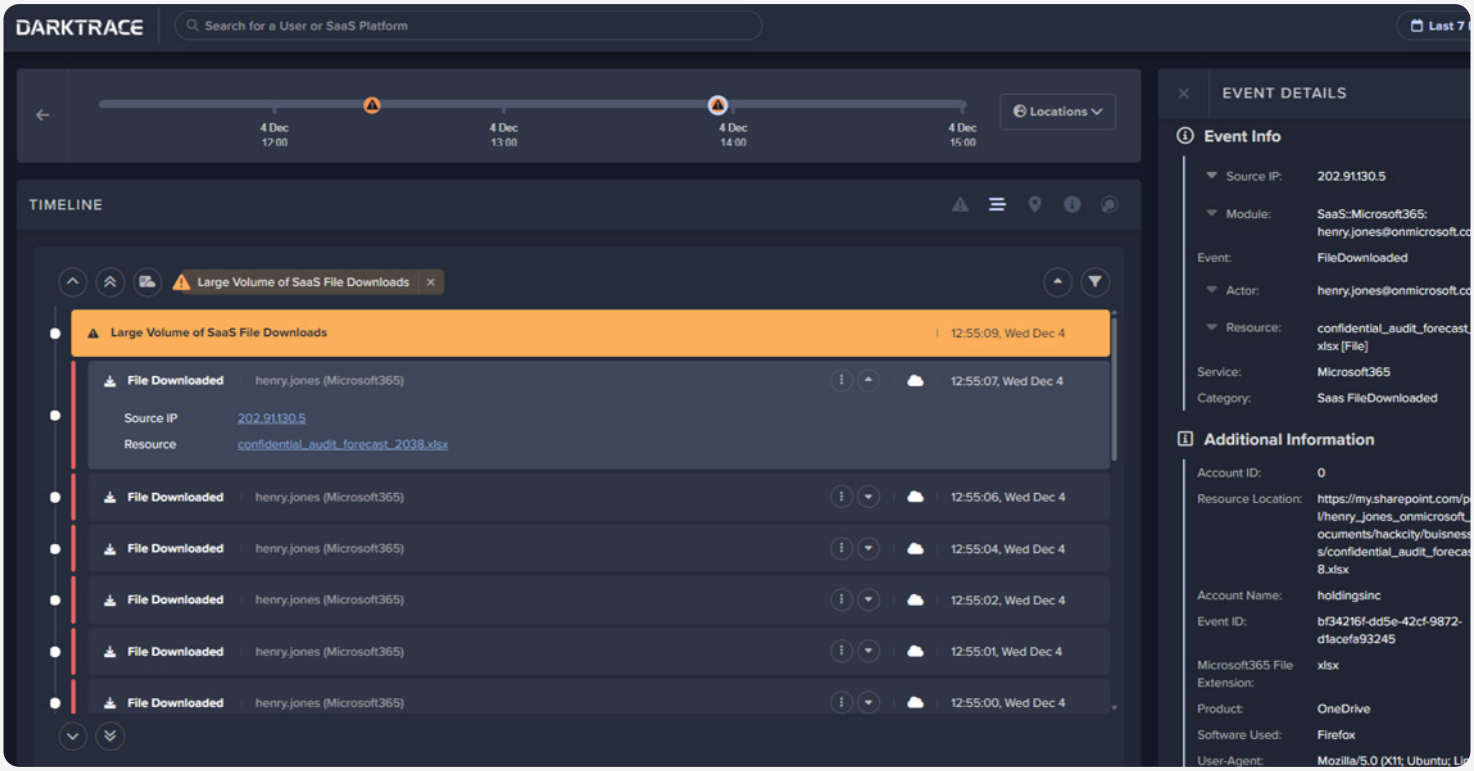

Figure 02: Darktrace's real-time detection and response capabilities ensure that attacks are contained before they can escalate, identifying threats such as account takeovers, credential stuffing, and insider threats, and takes immediate action by disabling compromised accounts, forcing logouts, or blocking suspicious IP addresses.

Rapid identity investigation & response for full spectrum of attacks

Darktrace / IDENTITY enables organizations to respond to identity threats with unprecedented speed and precision, leveraging AI-powered automated workflows that mitigate risks within seconds. Unlike traditional methods that rely on manual intervention and delayed alerts, Darktrace's real-time detection and response capabilities ensure that attacks are contained before they can escalate. The platform autonomously identifies threats such as account takeovers, credential stuffing, and insider threats, and takes immediate action by disabling compromised accounts, forcing logouts, or blocking suspicious IP addresses.

To further enhance incident management, Darktrace / IDENTITY integrates Cyber AI Analyst, which conducts enterprise-wide investigations into identity events.

By connecting seemingly unrelated activities across platforms, Cyber AI Analyst provides a comprehensive understanding of the threat, enabling teams to respond more effectively. Detailed logs, situational dashboards, and end-to-end visibility ensure that security teams can trace incidents to their root causes and take swift, informed actions.

These capabilities not only reduce response times from hours to seconds, but also alleviate the operational burden on security teams, allowing them to focus on higher-priority tasks while maintaining operational continuity.

Expand existing security controls with multi-platform coverage

Darktrace / IDENTITY seamlessly integrates with existing security tools, expanding protection to a wide range of SaaS applications and infrastructures. The platform connects directly with major SaaS applications such as Microsoft 365, Google Workspace, Salesforce, Slack, Zoom, and more, providing real-time monitoring of user activities, administrative changes, and file-sharing events.

Through its API-based architecture and modular configurations, Darktrace / IDENTITY also supports custom applications, enabling organizations to tailor their security measures to unique environments. With its REST API supporting JSON, OAUTH 2, and API key authentication, the solution ensures precise and flexible security coverage across SaaS environments.

As a key component of the Darktrace ActiveAI Security Platform, Darktrace / IDENTITY integrates seamlessly with other modules such as Darktrace / EMAIL, Darktrace / CLOUD, and Darktrace / NETWORK. This integration creates a unified, cross-platform security ecosystem that enhances threat detection and response across email, cloud, and identity layers. Organizations can scale their identity protection as they grow, maintaining consistent security while addressing complex threats without compromising performance.

By breaking down silos between identity, cloud, and email security, Darktrace / IDENTITY uncovers and neutralizes sophisticated attack patterns, empowering businesses to secure their digital environments comprehensively and efficiently.

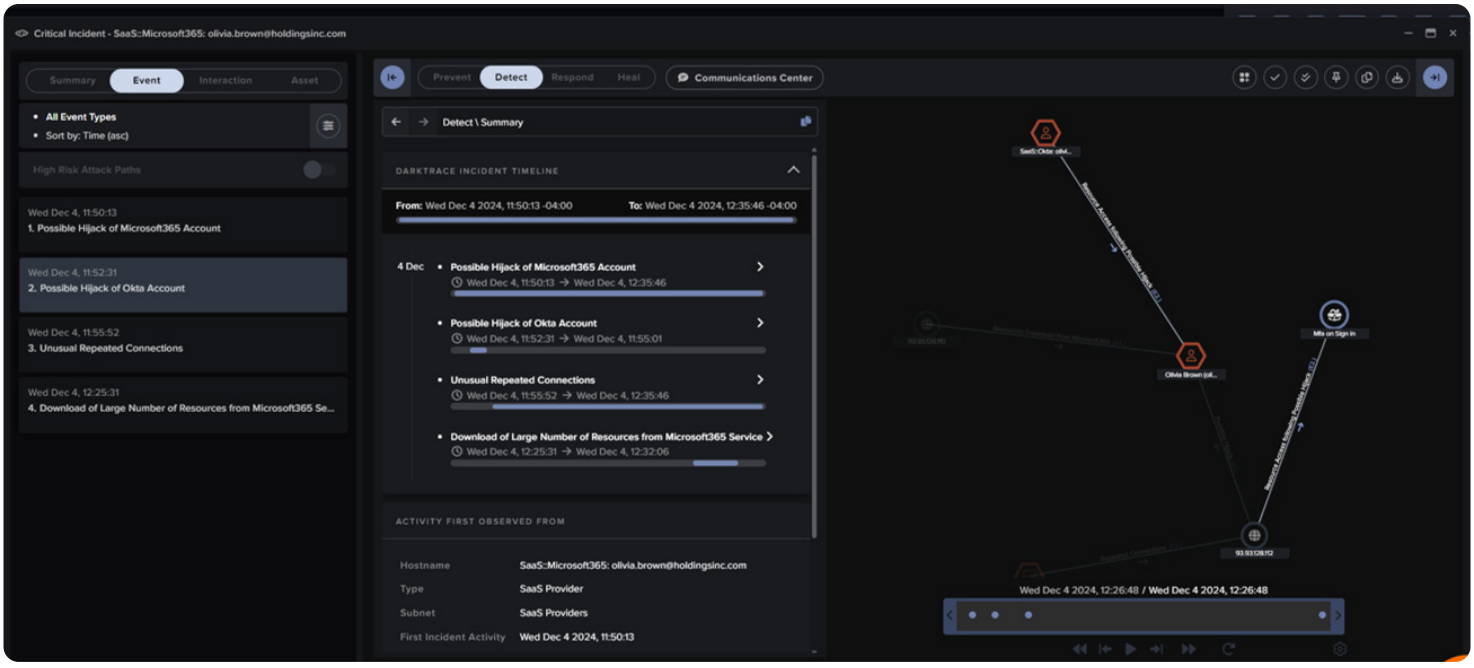

Figure 03: Darktrace connects directly with major SaaS applications such as Microsoft 365, Google Workspace, Okta, Salesforce, Slack, Zoom, and more, providing real-time monitoring of user activities, administrative changes, and file-sharing events.

Investigate all alerts in your environment with the industry's first AI analyst

Darktrace / IDENTITY leverages the power of Cyber AI Analyst, bringing cognitive automation to your data and accelerating SOC Level 2 analyses of incidents by 10x.

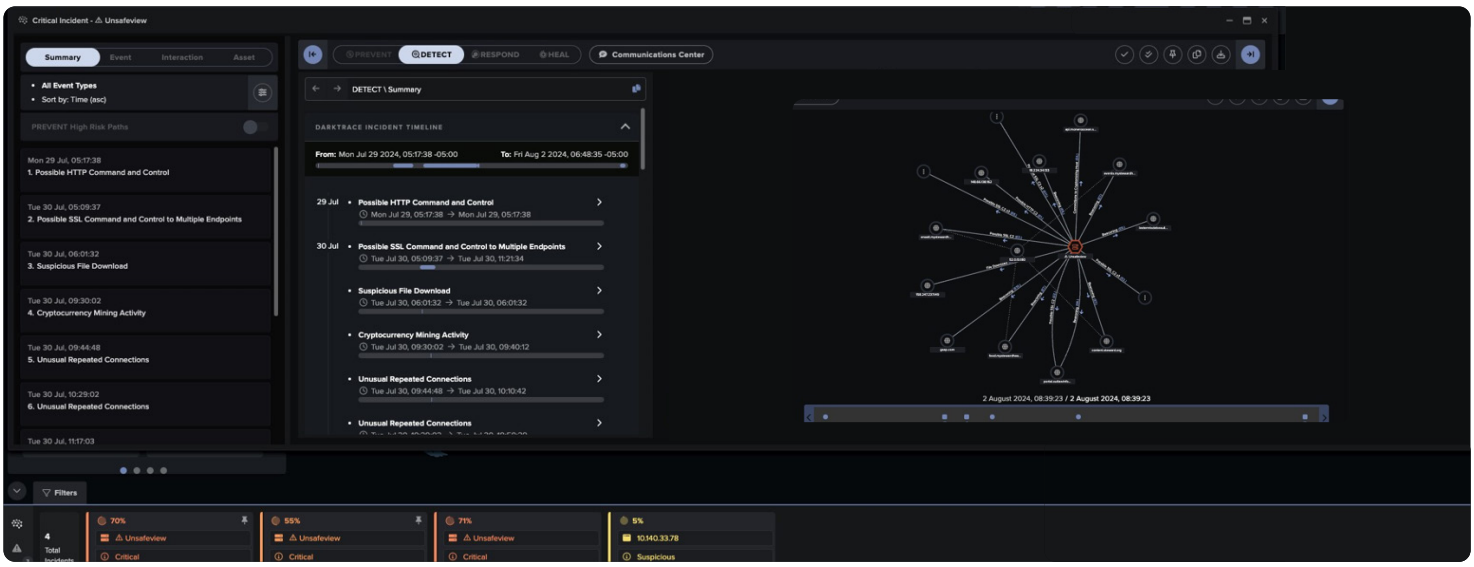

Figure 04: Cyber AI Analyst continuously analyzes and contextualizes all relevant alert in your identity landscape with an understanding of what is normal behavior for your organization. A detailed timeline of the incident and a full summary is provided to reduce time to meaning for your team.

At a glance:

- Harness the power of Cyber AI Analyst
- Augment your SOC team
- Automate alert triage and investigation
- Detailed cloud forensics
- Complete business context

Uncover sophisticated threats with detailed investigations

Our Cyber AI Analyst intelligently investigates alerts in your cloud, connecting seemingly benign events to uncover sophisticated threats and correlating related activities into a single incident.

By piecing together anomalies which may appear harmless, Cyber AI Analyst autonomously identifies subtle malicious actions and uncovers advanced network threats, tracking them across the entire kill chain in real time and at scale.

Augment your SOC team capabilities

Unlike prompt-based LLMs that just create incident summaries or other vendors with basic AI investigation capabilities, Cyber AI Analyst is the only technology on the market that can truly operate like an experienced human analyst. It helps your SOC team automate the investigation of security incidents at machine speed and drastically reduce triage times. Cyber AI Analyst continually analyzes and contextualizes all relevant alerts in your identity landscape with an understanding of what is normal behavior for your organization. It autonomously forms hypotheses and reaches conclusions just like a human analyst would, saving your team a significant amount of time and resources.

Get complete business context

Contextualize alerts from all areas of your environment in a single solution. Cyber AI Analyst tracks connections and events across network, endpoint, cloud, identity, OT, email, and remote devices, helping you detect and investigate modern threats that traverse your entire digital estate.

Neutralize cloud-based threats with the first Autonomous Response solution proven to work in the enterprise

Autonomously contain and respond to attacks in real-time without disrupting business operations.

At a glance:

- Autonomous response
- Pattern of life and behavioral context
- Targeted actions to avoid disruption
- Native response actions
- Fully customizable

Autonomous threat response

Darktrace / IDENTITY rapidly contains and disarms threats based on the overall context of the environment and a granular understanding of what is normal for a device or user – instead of relying on historical attack data. Darktrace / IDENTITY can autonomously enforce a pattern of life based on what is normal for a standalone identity or group of peers.

Darktrace / IDENTITY autonomously takes precise response actions in real time to contain threats without disrupting business operations – either natively or via third-party integrations. Actions can also be taken for remote user devices when combined with Darktrace / ENDPOINT, no matter where the endpoint is or whether they are off the corporate network.

Stay in full control

Darktrace / IDENTITY autonomously takes the most effective response to identity threats, so there's no need to spend time maintaining playbooks or manually tuning your deployment.

If you'd prefer to adjust response actions yourself, you can easily customize them with our intuitive model editor. Adjust every action and response logic in granular detail to fine-tune your deployment your way. Choose different response actions based on types of devices, IP ranges, office working hours, and countless other parameters.

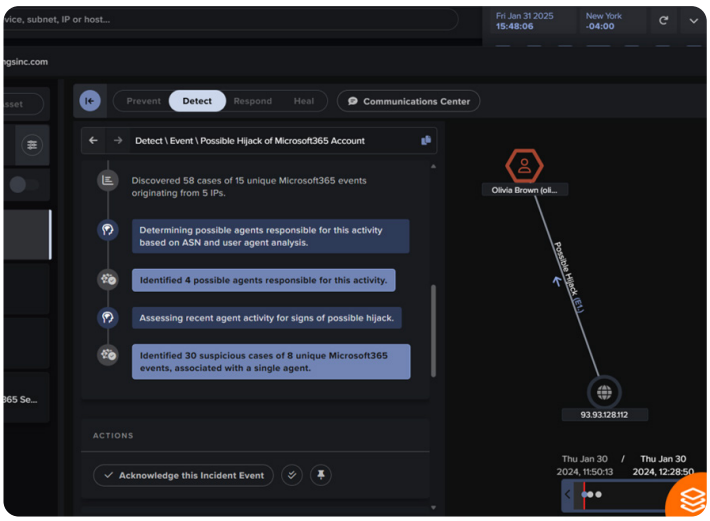

Figure 05: Get full visibility of the events leading up to an incident, including how our AI autonomously responds to protect your business.

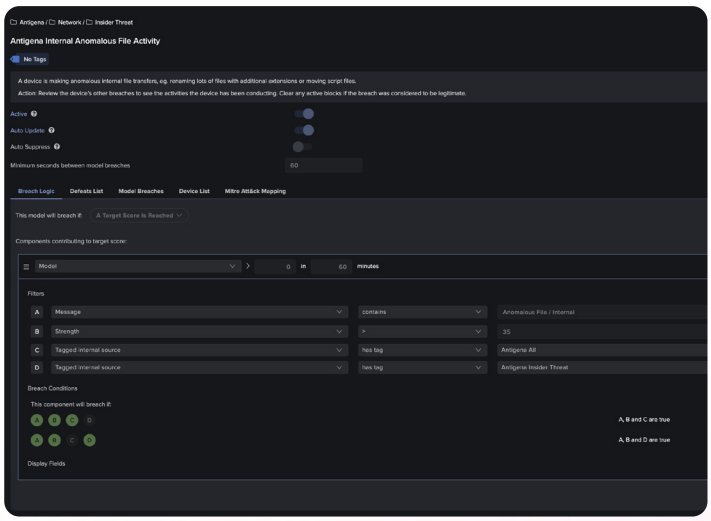

Figure 06: An example of the Darktrace Model Editor, which provides the ability to fine-tune response logic in granular detail if desired.

Extend identity visibility to your cloud and email

Darktrace / CLOUD

Extend real-time detection and response capabilities to your cloud and gain complete enterprise coverage with Darktrace / CLOUD. Disarm known and unknown novel cloud-based threats in seconds with platform-native autonomous response actions.

Darktrace / EMAIL

Enhance your native email security by leveraging business-centric behavioral anomaly detection across inbound, outbound, and lateral messages in both email and Teams.

Designed from the ground up to build on the benefits of your native email provider, Darktrace / EMAIL stops more threats and revolutionizes email security management to drastically decrease the load on security teams.

Achieve cyber resilience with the Darktrace ActiveAI Security Platform

Darktrace / IDENTITY is part of the Darktrace ActiveAI Security Platform, combining identity monitoring with the rest of your digital estate to enhance your security visibility and control across your cloud environments, endpoints, email, network, and OT devices. Darktrace / IDENTITY integrates with Darktrace / Attack Surface Management to deliver continuous, customized detection of externally exposed assets.

When combined with Darktrace / Proactive Exposure Management, your organization can take pre-emptive actions to identify, analyze ,and mitigate internal and external security risks. Darktrace / Incident Readiness & Recovery takes information from Darktrace / IDENTITY and all other areas of the Darktrace ActiveAI Security Platform to help you anticipate, detect, contain, recover, and learn from any cyber incident.

Tailored playbooks for effective recovery are based on a deep understanding of your identity and wider threat landscape, helping you to maintain operational continuity against modern adversaries. The Darktrace ActiveAI Security Platform revolutionizes your cyber defenses by helping you proactively prevent cyber-attacks, quickly recover from incidents, and continually strengthen your security posture, all within a single platform.

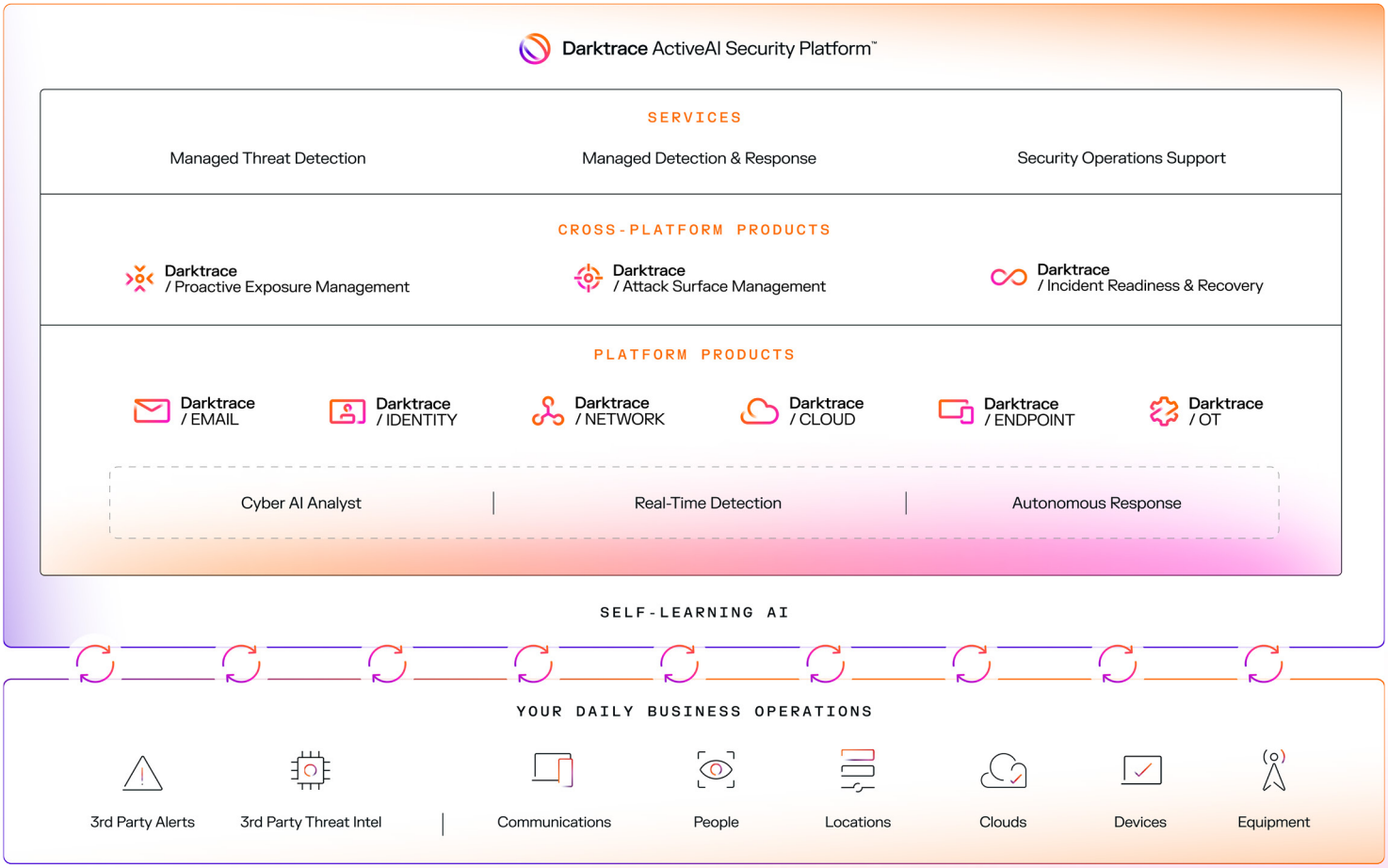

Figure 07: The Darktrace ActiveAI Security Platform.

Operational benefits

Real-time threat detection and response:
Automatically detects and mitigates identity-based threats such as credential theft, account takeovers, and insider threats, reducing response times from hours to seconds.

Unified visibility across SaaS environments:
Provides a holistic view of identity activity across platforms like Microsoft 365, Okta, Salesforce, and Slack, ensuring no blind spots in monitoring and analysis.

Enhanced security posture:
Continuously adapts to evolving threats with Self-Learning AI, enabling proactive risk management and prevention of incidents before they occur.

Reduced operational burden:
Automates detection, investigation, and response workflows, freeing security teams from manual, resource-intensive processes and enabling focus on higher-priority tasks.

Seamless integration:
Integrates effortlessly with existing security tools and infrastructures, including other Darktrace modules for a unified and cohesive security ecosystem.

Scalability and flexibility:
Rapidly deploys across growing infrastructures, supporting custom configurations via API for tailored security across diverse environments.

Comprehensive monitoring beyond authentication:
Extends monitoring to post-login behaviors, detecting suspicious actions such as unauthorized administrative changes, excessive file downloads, or lateral movements within SaaS platforms.

Operational continuity with Autonomous Response:
Minimizes disruption by autonomously disabling compromised accounts, blocking suspicious IPs, and terminating malicious sessions while allowing legitimate business operations to continue.

Streamlined investigation with Cyber AI Analyst:
Delivers high-level situational dashboards and detailed incident reports, enabling security teams to quickly understand and respond to complex attack patterns.

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

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