FEBRUARY 2025

Enhance AWS Cyber Resilience With Darktrace / CLOUD

Justin Boyer, Technical Validation Analyst

Cloud Security Challenges

Cloud technology has grown in adoption and sophistication throughout the last decade. Organizations want to use the cloud to achieve business goals. According to research from Informa TechTarget's Enterprise Strategy Group, 83% of survey respondents have moved existing production applications to run on cloud infrastructure.[1]

While there are benefits to deploying new or existing applications to the cloud, it presents unique challenges for security teams. Enterprise Strategy Group research respondents reported several factors that make security operations more difficult in this environment, including a constantly changing and evolving attack surface, gaps in monitoring tools and processes, and difficulty in developing detection rules that keep up with new attacks.

Lack of visibility into cloud infrastructure, along with the increasing complexity and scale of these environments, leads to gaps in security coverage. Additionally, many cloud security tools are siloed and pertain to a specific provider or a particular part of the whole, making it difficult to build a complete view of an organization's security posture.

Having a complete view of security posture across a cloud environment leads to challenges in preventing attacks and defending against them. Disparate tools, manual processes, and environmental complexity make defending against active attacks even more difficult. According to Enterprise Strategy Group research, 28% of respondents directly named the increasing use of public cloud services as the primary reason their security operations are more challenging than two years prior.[2]

Organizations need automated solutions built to handle the unique challenges that public cloud usage presents. Companies see attacks against these assets and struggle to protect themselves. When asked what led to successful attacks against their cloud infrastructure in the past 12 months, respondents indicated several factors that exemplify the challenges of a cloud environment, including exploitation of misconfigured assets, the use of stolen privileged credentials, malware moving laterally to cloud workloads, and novel "zero-day" exploits on previously unknown vulnerabilities (see Figure 1).

[1] Source: Enterprise Strategy Group Research Report, *Cloud Detection and Response*, December 2023. All Enterprise Strategy Group research references and charts in this Technical First Look are from this report unless otherwise noted.
[2] Source: Enterprise Strategy Group Research Report, *The Triad of Security Operations Infrastructure: XDR, SIEM, and MDR*, June 2024.

Figure 1. Recent Attacks Against Cloud-hosted Infrastructure

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Darktrace / CLOUD

Darktrace / CLOUD is an AI-driven cloud security solution that uses multilayered self-learning AI to deliver unified visibility and security for hybrid, multi-cloud environments. Darktrace continuously learns from day-to-day cloud operations to help organizations visualize and monitor cloud assets, automate the investigation process, and disarm cloud-based threats in seconds. Darktrace / CLOUD supports multi-tenant, hybrid, and serverless environments and is agentless by default—with optional agents for organizations desiring enhanced real-time response and deep inspection.

Darktrace was built to detect anomalies instead of trying to predict threats based on threat intelligence or other means. Darktrace learns the organization's network, cloud architecture, and users, and creates a baseline of normal behavior. It then detects anomalous behavior and alerts security staff of such behavior or activity. This anomaly detection is precise down to specific and narrow use cases—for example, detecting potential account takeover by seeing such as an administrator account accessing resources from an unrecognized location or device.

Darktrace / CLOUD takes the powerful foundation of anomaly detection and extends it to public cloud environments such as AWS. It provides complete visibility and architectural awareness, along with proactive responses against threats.

Darktrace provides real-time cloud detection and response against threats such as:

- Data exfiltration and destruction.
- Critical misconfigurations.
- Compromised credentials.
- Insider threats and admin abuse.

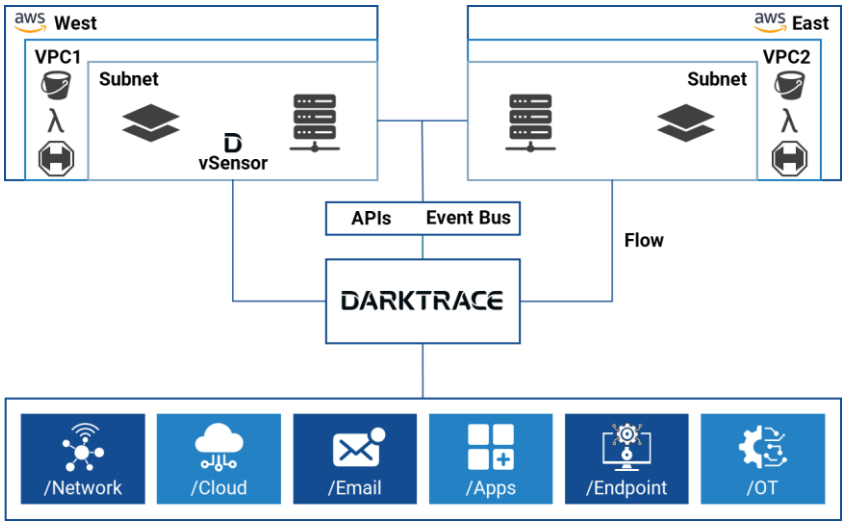
First Look

Enterprise Strategy Group reviewed how Darktrace / CLOUD helps organizations using AWS to build a comprehensive view and understanding of their architecture, along with potential problems and real-time detection and response.

Darktrace defaults to an agentless architecture, monitoring network flow logs, APIs, containers, and users to learn what is "normal" for an organization. Many solutions aggregate data across customers and attempt to use a "big data" approach to finding potential threats based on the threats others have faced. Darktrace instead learns the organization's unique environment and is, thus, able to detect anomalies based on what is typical for them. Darktrace's deep visibility into cloud traffic allows for an understanding of normal patterns for users, devices, and applications. Atypical behavior from any of these prompts an alert or an automated response. This approach is especially useful in detecting novel threats and never-before-seen attacks, instead of relying on known attack data.

Darktrace's agentless architecture can be deployed to a cloud in minutes. However, Darktrace can also collect data from vSensors, lightweight virtual probes that can be deployed as a standalone VM. Darktrace probes perform deep packet inspection on ingested data, providing a continuous stream of data to the master appliance at a fraction of the bandwidth of the original traffic. While not required to take advantage of Darktrace's capabilities, this architecture can be useful depending on the organization's needs. Figure 2 shows both possibilities, with the sensor deployed in the AWS West environment and the agentless model deployed in the AWS East environment.

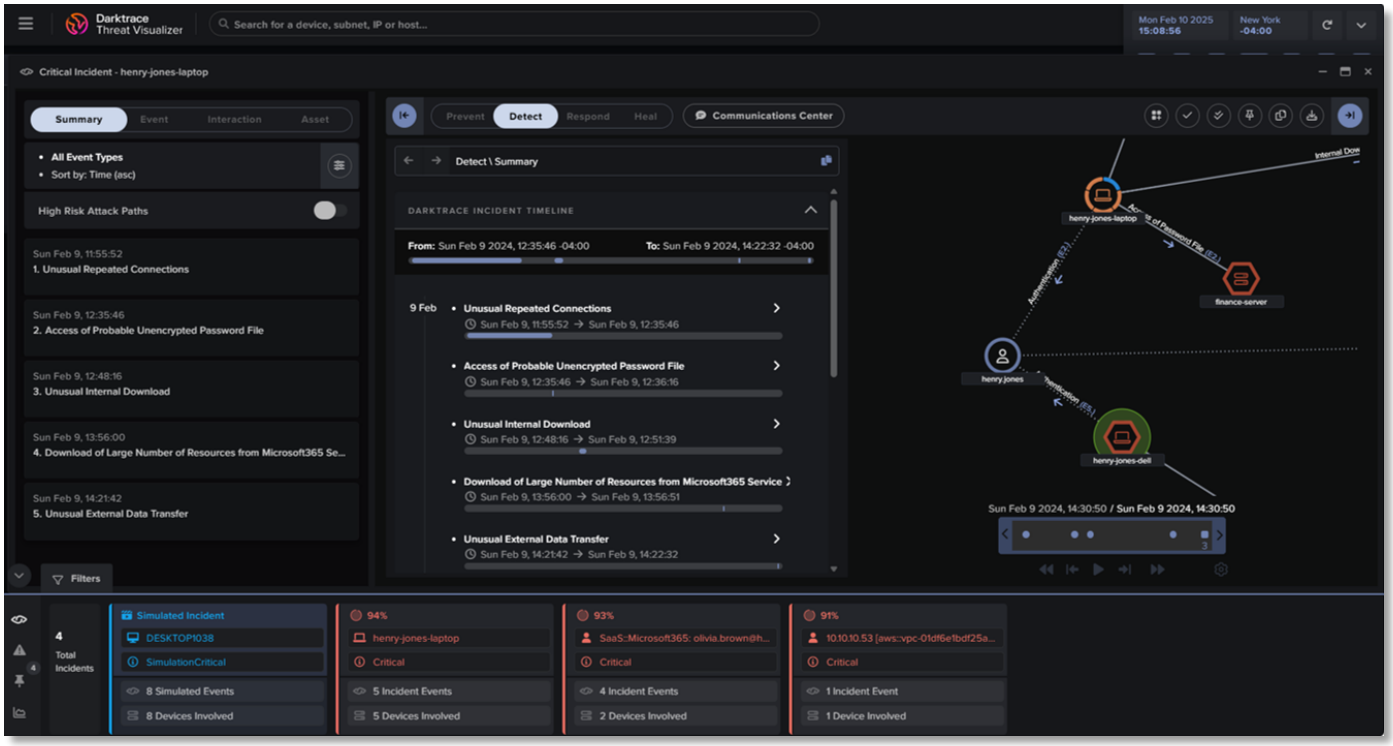
Figure 2. Darktrace / CLOUD Architecture



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

We saw how the Darktrace Threat Visualizer alerts security teams of potential incidents (see Figure 3). It creates a visualization of the incident, including the series of events that occurred to trigger the alert. Security teams can view the details of these events, such as the individual anomaly detections. Darktrace Cyber AI Analyst™ augments security teams by gathering thousands of data points and using these to automatically investigate and triage alerts. Darktrace Cyber AI Analyst is trained using advanced AI techniques to mimic human security analysts' investigative process at machine speed and scale, leveraging three years of incident response decisions from Darktrace's internal security team. Using the sum of their experience, Cyber AI Analyst aims to make the same decisions as a human analyst would.

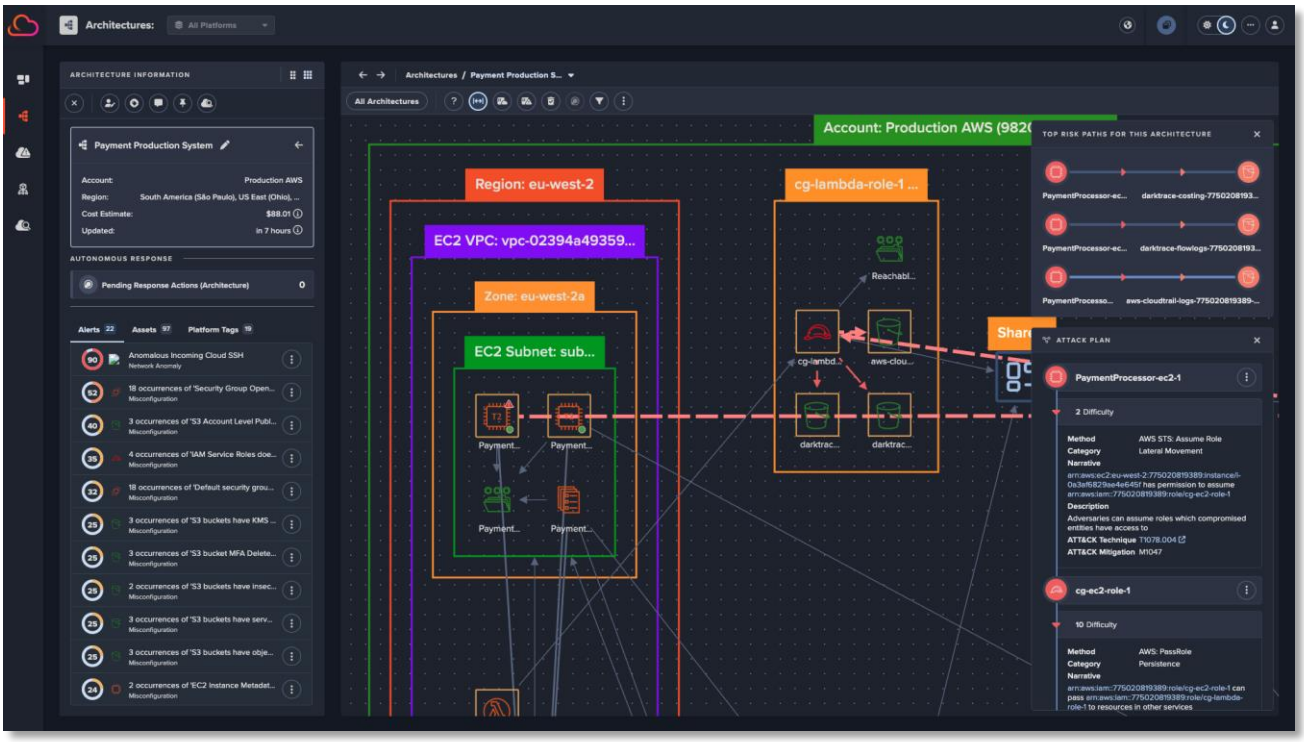
Figure 3. Darktrace Threat Visualizer



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Darktrace's deep knowledge of network traffic and cloud audit logs enables it to create real-time architecture diagrams to visualize the AWS environment (see Figure 4). As new assets are created in the cloud, Darktrace updates the diagram immediately based on audit log data. From here, analysts and DevOps teams can visualize their architecture and view misconfigurations and potential attack paths. Darktrace accounts for each organization's unique environment and constraints to find the most probable attack paths. Through these tools, security teams can have complete visibility into their AWS environment while proactively protecting against novel threats and taking steps to improve their cloud security posture.

Figure 4. AWS Environment Diagram With Attack Paths



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Darktrace's visibility into cloud audit logs unlocks the ability to find identity-based threats in addition to network compromise. By applying Darktrace's proprietary techniques to cloud-based monitoring tools, it can detect compromised keys and credentials by identifying unusual behavior at the identity level. Doing so enables Darktrace to detect insider threats and novel attacks previously unseen or for which no known signature exists.

Identifying potential threats, misconfigurations, and vulnerabilities isn't always enough. When an attacker is actively exploiting these vulnerabilities, it's critical to stop it and prevent further damage. Partnering Cyber AI Analyst with optional Autonomous Response, Darktrace intelligently contains threats with an instant, precise, and proportional response, without interrupting cloud infrastructure or services.

Conclusion

As businesses continue to move their workloads to public cloud providers such as AWS, they have to acknowledge and plan for the challenges that brings. Fast changes to architecture and a potentially large and ever-changing attack surface can easily put security teams in a precarious position. Security teams indicated that lack of automation, an increasing attack surface, gaps in security monitoring, too many manual processes, and an inability to tune security controls effectively and in a timely manner contributed to making their job harder over the past two years. Without a clear picture of their risk and an automated way to deal with threats and active attacks, organizations will continue to struggle in defending their cloud assets from attackers.

Darktrace / CLOUD is a solution built to provide AI-powered autonomous detection and response in the cloud. While many solutions combine all of the data from their customers into a large database for analysis, using the combined whole to find potential threats, Darktrace takes another approach, instead continuously monitoring and learning each customer's unique environment and patterns. Using flow logs, APIs, and cloud audit logs, Darktrace finds anomalous behavior happening in the environment and alerts the security team or precisely takes nondisruptive measures to contain and stop the incident.

Enterprise Strategy Group research showed that, while 83% of organizations have lifted and shifted production workloads to the public cloud, lack of visibility, combined with the overhead of using and tuning separate security tools that depend on signatures and policies, stands in the way of organizations feeling comfortable with their security posture. Darktrace / CLOUD enables organizations to clearly see and understand their cloud architecture with real-time architecture diagrams built from audit logs. Security teams can view probable attack paths throughout the environment, helping them to prioritize strategic initiatives that will demonstrably improve their security posture. Additionally, Darktrace Cyber AI Analyst and Autonomous Response alert security teams to abnormal behaviors based on known patterns and take intelligent, precise action to contain potential attacks without disruption to cloud applications and services.

Securing public cloud environments is challenging and requires the right tools and absolute visibility to keep up with rapid changes and a growing attack surface. It's also necessary to respond to potential incidents quickly, without disrupting business operations. If your organization uses AWS services to deploy critical business applications, Enterprise Strategy Group recommends you consider Darktrace / CLOUD to help secure them.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com