The CISO's Guide to Cloud Security

Novel attack protection in a multi-cloud world

CONTENT

Abstract

Widespread use of the cloud continues to transform business, and cyber security systems are racing to keep up.

With the speed and scale of dynamic, multi-cloud environments creating unprecedented complexity, and the specter of multi-vector, AI-powered attacks on the horizon, enterprises cannot afford to rely solely on conventional security tools to protect their business.

The traditional approach to threat detection, analysis, prioritization, and response takes too much time and effort, and fails to spot and respond to more sophisticated novel and targeted attacks.

Disparate tools and point-in-time visibility leave dangerous visibility gaps that modern attackers use to target cloud-based assets, hiding and moving laterally through enterprise networks before launching attacks.

Security teams can no longer afford to rely on point-in-time visibility or systems trained with supervised machine learning (ML) to secure the cloud against cyber-attacks, vulnerabilities, and misconfigurations that lead to breaches.

New cloud security platforms, frameworks, and best practices such as Cloud Workload Protection Platforms (CWPPs), Cloud Infrastructure Entitlement Management (CIEM), Cloud Detection and Response (CDR), Cloud Security Posture Management (CSPM), and Cloud-Native Application Protection Platforms (CNAPPs) seek to balance the scales with unified visibility and smarter use of AI—but which approach is right for your business?

This guide overviews modern cloud security challenges, CISOs' options for managing risk, and how Darktrace/Cloud overcomes the limitations inherent in traditional approaches to protect your business from both known and novel attacks.

Are we still in the early stages of cloud adoption?

"

Looking at the bigger picture, it's clear that this market is enormous, is still largely untapped, and will likely outlast the current economic turmoil. By 2023, cloud spend is projected to reach nearly $600 billion, or about 12% of total IT spend.

FORBES

PART 1

Cloud Opens Doors to New Opportunities—and Risk

Enterprises have only just begun to tap the potential of cloud. While nearly nine in ten companies increased the scope of their cloud initiatives in recent years, Accenture Cloud Outcomes research shows just 42% are deriving the value they expected[1].

The mixed results can be partly attributed to the unexpected rate of digitalization since 2020. Complex environments grew quickly to span numerous clouds, networks, endpoints, and applications.

of companies report an increase in the volume and/or scope of their cloud initiatives since 2020

Accenture

Security slows adoption

Along with rapid transformation, concerns about security cause enterprises to rethink their migration strategies and defer disrupting their core business applications. Security infrastructures must protect the cloud to protect the business, but agility can no longer come at the expense of a robust cyber security deployment.

Dynamic cloud environments change constantly as workloads come and go and developers pivot without notice.

Let's look at some of the ways digitalization and cloud migration compromise cyber security:

Uncharted digital attack surface

Multi-cloud environments create a vastly expanded attack surface that extends beyond the enterprise's control.

A cloud-driven business model democratizes traditional IT—and security—as users spin up servers and instances at will, increasing the odds of misconfigurations and digital exposure from code exposed in public repositories.

Cloud gives rise to new attacks

Cyber-attacks targeting cloud architectures and known security weaknesses appear and progress at machine speed. Along with the sheer volume of threats, threat actors' use of AI and ML makes advanced cloud attacks easy to automate. Adversaries may even combine traditional "one on many" attacks with targeted "one on one" techniques and novel, hard-to-predict threats.

Proportion of security incidents that will be the customer's responsibility by 2025.

Gartner, "Is the Cloud Secure?" [2]

Modern challenges call for a modern approach

Challenges to securing today's dynamic, highly dispersed multi-cloud environments include:

- Unprecedented architectural complexity
- A worldwide scarcity of cloud security expertise
- Mounting pressure to comply with fast-changing federal, state, and industry mandates for protecting data privacy
- A lack of unified visibility across multi-cloud environments

A forward-looking approach to cloud security must also be dynamic and deliver three fundamental capabilities at all times:

1. Real-time visibility

Cloud compromises may occur even more quickly than most network events. The same attributes that make the cloud so useful to businesses — availability, speed, and scalability — also empower cyber adversaries to strike swiftly. Machine-speed attack techniques make it harder to maintain real-time awareness and build an accurate view of your environment and threat landscape.

Most traditional and easily deployed cloud security tools only offer "point-in-time" snapshots of risk, but not the unified, real-time visibility now vital to cloud security. A modern cloud security approach should achieve the dual goals of continuous, real-time views that surface security threats and easy deployment that supports dynamic DevOps pipelines.

2. Reduced complexity

Cloud environments do not exist in silos but are embedded deeply into the complex fabric of your business. Having one single, unified view of risk across diverse environments equips new tools to work smarter and faster, and promotes collaboration and knowledge-sharing across new domains. Having one "source of truth" reduces the chance for discrepancies and the need for redundant, siloed efforts by analysts to prioritize and take action.

3. Cloud-scale threat & exposure management

Amid perennial skills shortages, security teams must detect and respond to a broader range of known and unknown threats than ever before. Cyber defences can no longer rely on legacy, perimeter-focused security and basic "detect and respond" approaches to spot and prevent novel, business-specific and AI-powered threats from leading to breaches. Cloud-based threats need cloud-driven security. Fortunately—and perhaps unfortunately—CISOs can choose from a growing arsenal of best practices, platforms, and point tools designed from the ground up to secure the cloud.

[1] https://www.accenture.com/gb-en/insights/technology/maximize-cloud-value
[2] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

PART 2

Breaking Down Market Segments

As they develop a long-term vision for their cloud security journey, enterprises need assurance that every investment – every step they take along the way – will make their cloud security infrastructure faster, smarter, and more scalable. Several new frameworks, platforms, and programs aim to uplevel cloud security by consolidating or connecting the dots between controls within one holistic, streamlined approach.

The vast cloud security market consists of various – often overlapping – market segments as defined by Gartner and other analyst firms.

Cloud Security Posture Management (CSPM) to harden cyber defenses

CSPM goes beyond protecting workloads—and beyond basic detection and response—to improve your cloud security posture. Cloud security posture management encompasses threat intelligence, detection, and remediation of risk across today's complex cloud environments.

CSPM connects the dots between CWPP, CIEM, and CDR with a unified approach designed to hasten responses, guide remediation, prevent configuration drift, streamline compliance, and promote smarter, faster DevOps integration over time.

CSPM leverages sophisticated automation and AI to identify, visualize, and assess risk from malicious activity, insider threats, vulnerabilities, and misconfigurations across all Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) environments.

Cloud Workload Protection Platforms (CWPPs) to protect workloads

As the name suggests, CWPPs protect all types of cloud workloads—physical servers, containers, virtual machines (VMs), and serverless—across on-premises systems and multi-cloud environments. The CWPP's charter includes container protection, vulnerability scanning, configuration management, and other capabilities aimed at promoting faster detection and investigation of active threats and exploits.

Cloud-based CWPPs provide a consistent and unified framework for securing applications, prioritizing patching, and detecting external threats. CWPPs continually scan environments for activity that violates corporate security policies and for improperly configured settings that put assets and regulatory compliance at risk.

Cloud Infrastructure Entitlement Management (CIEM) to bolster identity management

CIEM outlines a comprehensive, centralized approach to managing permissions that governs user access to corporate resources in the cloud. CIEM improves internal policy enforcement and compliance across the entire cloud infrastructure with unified visibility of user entitlements, permissions, and access privileges.

CIEM strengthens identity and access management (IAM) by visualizing which users can take which actions, so cloud security teams and business leaders can refine permissions based on roles and responsibilities and minimize privilege misuse. CIEM systems also automate the provisioning and deprovisioning of entitlements to mitigate third-party and non-employee risk and generate data used in audit trails to demonstrate compliance.

Cloud Detection and Response (CDR) to shut down cloud risk faster

CDR expands and tailors classic "detect and respond" security to the dynamic nature of cloud. Like endpoint, network, and managed detection and response (EDR, NDR, MDR), cloud-native CDR processes include monitoring, detection, analysis, threat prioritization, and prescribing or performing automated steps to contain or remediate threats.

Designed from the ground up for highly distributed cloud architectures, CDR delivers visibility and automation across workloads, APIs, and complex multi-cloud services and environments. CDR finds risk inherent to cloud like vulnerabilities stemming from misconfigurations and the lack of unified visibility across complex multi-cloud environments. Solutions may employ both agent and agentless data collection to perform continuous real-time monitoring and analysis of the entire ecosystem.

CDR can detect both known and novel threats as well as suspicious telltale activity like lateral movement and privilege escalation. CDR goes beyond detection to aid in prioritizing cloud events based on severity, reducing false positives, simulating threats, and understanding threat actor behavior. Upon identifying risk, the system triggers automated responses such as quarantining workloads and creating isolation zones.

Cloud-Native Application Protection Platform (CNAPP) to pull the pieces together

CNAPPs are defined by analyst firm Gartner as a unified and tightly integrated set of security and compliance capabilities that protect cloud-native applications in development and production.

To this end, a CNAPP combines various elements and benefits of CWPP, CDR, CSPM, and CSPM.

With an ambitious vision for consolidation, Gartner outlines a continuous process for identifying, prioritizing, and addressing risk in cloud-native apps and infrastructure.

CNAPP consolidates runtime protection, visibility, and vulnerability management within a single platform that gives SecOps and DevOps teams unified visibility to respond and avoid threats.

Like CSPM, building a CNAPP moves enterprises forward on their journeys to enforce least-privilege access and adopt zero trust security postures.

Other valuable features of an end-to-end CNAPP include automated detection of vulnerabilities within containers, VMs, and serverless functions as well as scanning for exposure, malware, and infrastructure as code (IaC).

Ultimately, the acronym soup and puzzle pieces may culminate within CNAPP but enterprises will get there in stages. Throughout the journey, CISOs must continue to prioritize based on their business's unique threat environment, tolerance for risk, and mandatory data privacy requirements.

CNAPP promises the ultimate whole that is greater than the sum of its parts: a platform approach to cloud security in which a single tool or solution reduces swivel-chair analysis, alert fatigue, redundant investigations, and the time and effort taken to correlate and remediate or avoid risk.

> By 2025, Gartner expects 75% of new cloud security posture management purchases will be part of an integrated CNAPP[3]
>
> **FORBES**

$3.32B **Projected value of CSPM market by 2027.**

The CSPM market is projected to reach in 2027, growing at a 25.7% CAGR.

Gartner, "Is the Cloud Secure?"

Which to use when?

All of these approaches aim to:

- Leverage AI to improve detection & response to find and stop threats faster
- Automatically avoid and shut down novel attacks
- Make security practices more proactive
- Improve utilization and retention of cyber skills and expertise

Budget, skills, and cyber insurance requ irements all factor into CISOs' investment decisions, along with evolving challenges to securing the cloud.

Challenges include applying the right AI in the right way at the right time to stop AI-led novel attacks that elude today's security infrastructures[3].

	CSPM	CWPP	CIEM	CDR	CNAPP
Focus	Hardening security posture	Events/Incidents	Identity	Events/Incidents	Maintaining a unified approach
Strengths	/ Actionable context around threats / Automatically identifies risk / Guides remediation	Unified view of workloads	/ Promotes least-privilege access and authorization policies	/ Reduces alerts, false positives / Speeds detection / Automates response	/ Actionable context around threats / Automatically identifies risk / Guides remediation
Limitations	Unable to detect or action on in-progress threats	Limited focus on workloads	Focus limited to identity	Limited focus on detecting and responding to incidents	Takes time and expertise to implement in phases
Impact on security posture	/ Delivers unified cloud visibility / Provides continuous monitoring and detection / Promotes faster response / Improves compliance / Automates L1 SOC tasks and automates SecOps / Advances journey toward Zero Trust / Stands to reduce cyber insurance liability premiums				

A summary of the major cloud security categories available to CISOs

[3] https://www.gartner.com/en/documents/4295099

PART 3

Traditional Cloud Security Has Reached Its Limits

Traditional cloud security doesn't tell IAM and security leaders what they really need to know—which users can access which cloud resources—in real time.

Let's look at some of the limits of existing solutions:

Static insights in a dynamic world

Dynamic cloud environments allow servers and containers to be spun up and architectural changes made by virtually anyone with the mere push of a button. Unfortunately, that means DevOps engineers may not engage the security team until the last minute, or until something goes wrong, and by then it's too late.

Today's static cloud security solutions provide snapshots of your threat environment prior to integration and installation. Static insights help validate and set up controls before deployment, but the real risks related to cloud migration appear later. How can security teams know when everything isn't OK?

Solutions built around "point in time" insights into security incidents lack the ability to analyze and correlate threats in real time. Alerts are abstracted from the environment, leaving cloud security professionals at a disadvantage in diagnosing incidents and understanding what's most critical.

Static approaches aid in demonstrating compliance but do little to improve detection, particularly of novel, unpredictable attacks. After applying rules based on "if/then" scenarios, static tools may prescribe basic response actions such as quarantining segments or containers while analysts investigate incidents. In applying preset rules, analysts need to know which threats represent the greatest risk to your business before they actually happen.

Lack of genuine response

The same attributes that make the cloud so useful and attractive to organizations – speed, agility, availability, and scale – hold a symmetrical appeal for attackers. When cyber-attacks in the cloud unfold rapidly, it's not enough to simply detect attacks.

Most cloud security products today products may be able to alert analysts when something goes wrong, but lack the ability to mount a genuine response. Even newer solutions claiming to provide automated response are generally referring to the ability to automate the creation of a ticket.

Genuine response requires an understanding of your complete cloud architecture, including what cloud-native mechanisms are available to initiate a real response.

Inability to fend off novel attacks

Innovative cyber-criminals will naturally look toward AI to make the attack process faster and more efficient. Generative AI and large language model (LLM) tools lower the barriers to entry, empowering novice threat actors to mount sophisticated automated attacks.

With these developments, Darktrace expects to see – and in some cases is already seeing – a sharp rise in novel attacks.

To level the playing field, cyber security leaders must also apply AI in the right way, using traditional supervised AI capabilities where necessary, and combining this with AI that understands the business in order to stop novel threats.

In the next section we'll see how Darktrace's self-learning technology is unique in its ability to understand your business and offer defenders a powerful advantage against known and unknown attacks.

Increase in novel social engineering attacks during Q1 2023*

Darktrace

Failure to fully leverage leading-edge AI

Many traditional approaches and vendor solutions rely on super- vised machine learning (ML) to train the security system. Supervised ML involves shipping a company's data out to a large data lake stored in the cloud, combining it with data from thousands of other organizations data, and training an AI system to look for attacker patterns and profiles based on the homogenous data set.

This approach works perfectly well for detecting future cyber-attacks that in some way resemble previous attacks, but that's not always the case. The growth of novel attacks stands to outpace that of known attacks, particularly as attackers innovate to leverage AI tools in their own design efforts.

Self-Learning AI works in a completely different way than supervised ML. As the term itself indicates, Self-Learning AI-based solutions train themselves and develop an evolving understanding of 'patterns of life' for each unique business environment in which they get dropped.

Systems trained with Self-Learning AI can spot anomalous behavior behind cyber-threats, regardless of whether a particular threat has been spotted before. Investments in Supervised ML continue to serve their purpose, but the dawning era of novel and AI-augmented attacks requires a newer approach to cloud security – one designed from the ground up that uses Self-Learning AI to advance your security stack.

*Based on the average change in email attacks between January and February 2023 detected across Darktrace/Email deployments with control of outliers.

PART 4

Harnessing AI to Protect Cloud Environments from Novel Threats

Static, "one size fits all," and point-in-time solutions cannot adequately protect today's multi-cloud environments. To address these concerns, Darktrace has created a dynamic, unified, lifecycle approach based on deep understanding of your unique cloud environments and challenges.

Darktrace/Cloud™ modernizes your security posture from prevention to proactive hardening of defenses by making smarter use of AI at every stage. The system trains itself on your business to identify patterns, prioritize threats, and remediate anomalous behaviors as or before they happen.

Real-time visibility illuminates risk

Darktrace/Cloud delivers unified, real-time visibility into every user, workload, container, and asset across dynamic public and multi-cloud environments.

Using a single AI-powered solution, Darktrace can provide comprehensive coverage to surface and investigate threats unfolding anywhere in a progressive multi-cloud environment.

Darktrace/Cloud visualizes your entire cloud architecture to graphically depict entitlements and curtail misuse and misconfigurations.

Self-Learning AI gets to know your business

Using Self-Learning AI, Darktrace/Cloud can provide comprehensive cyber resilience for multi-cloud environments. Built for the dynamic nature of cloud, the platform establishes patterns of life for your cloud resources, identities, and services, and uses these insights to model and understand who has access to what and how.

Darktrace/Cloud learns an organization's unique cloud environment at the cloud network layer, the architectural layer, and the manage- ment layer.

A deep understanding of privileges highlights excessive rights, inactive roles and users, and overly permissive policies.

Smarter use of AI can also decrease misconfigurations, improve vulnerability management, and speed up response while maintaining compliance with security policies and industry standards.

Our Self-Learning AI:

- Learns 'on the job' and from scratch, without preconceptions or a massive upfront effort by your team to train the system
- Uses probabilistic mathematics to revise assumptions about behavior on a constant basis
- Stays up to date without relying on human input

Darktrace/Cloud includes our Cyber AI Analyst™ which continuously conducts investigations behind the scenes, operating at machine speed and scale to generate actionable reports of complex, multi-stage incidents that present the greatest risk to your business.

	Signature-Based, Leveraging Known Attacks	DARKTRACE
AI Type	Supervised Learning	Self-Learning Cyber AI
Data Source	Large data lake	Your business data
Speed	Processing results in latency	Real time - No latency

Darktrace/Cloud trains in real-time on your organization's unique business data to understand how every user, account, device, and type of cluster normally behaves.

A better understanding of "you" helps to identify and fix weak points in your security posture as they occur.

Benefits Unlocked with Darktrace/Cloud

Cloud-native response

By understanding your unique cloud footprint within the context of your own business, Darktrace/Cloud uniquely detects when something unusual is occurring that requires a response right now. The use of AI to understand your environment enables a truly autonomous and precise cloud-native response. An understanding of 'normal' unlocks the ability to initiate a precise response, allowing regular business activity to continue while targeted only the unusual activity.

Because the platform understands your complete cloud architecture, it knows what cloud-native mechanisms are at its disposal to initiate a real response. Automated real-time responses include cloud-native actions like detaching EC2 instances and applying security groups to contain risky assets.

Detect and shut down novel attacks

Used in combination with other AI methods such as LLMs, generative AI, and supervised ML, Darktrace/Cloud's Self-Learning AI identifies emerging cyber-attacks in real-time, regardless of whether the threat has been seen before. Darktrace/Cloud's approach of understanding a business' unique cloud footprint at every layer unlocks the ability to shine a light on a wide range of security risks – not only misconfigurations and vulnerabilities, but insider threats and unexpected data loss.

Prioritize and seal off dangerous attack paths

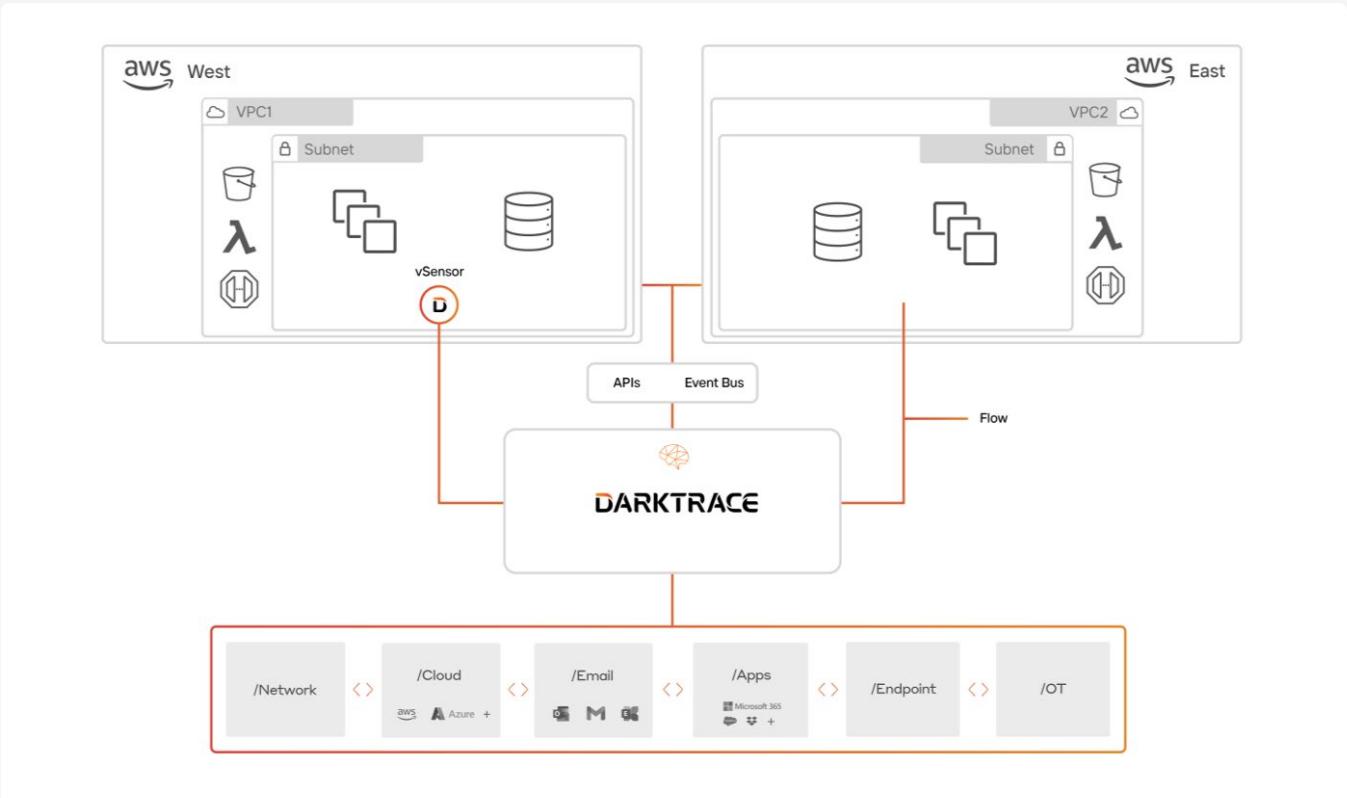
Darktrace/Cloud enables universal attack path modeling with real attacker methodologies. Where traditional modeling focuses on cloud-to-cloud attack paths, Darktrace identifies potentially risky paths and where assets may be under attack.

Working together with anomaly and threat detection, proac- tive attack path modelling lets defenders see and prioritize avenues through which attackers might move laterally and where compromise may initially take place.

Make the right decisions faster with Cyber AI Analyst™

Darktrace's Cyber AI Analyst™ goes beyond detection to automatically investigate and summarize incidents for your security team and systems.

Rather than bombard analysts with data and alerts, Cyber AI Analyst uses AI to automate L1 SOC workflows, prioritize risk, and generate incident summaries even non-technical responders understand.



Darktrace deploys in minutes through an agentless approach, or lightweight agents can be deployed where necessary.

Streamline and consolidate on tools and vendors

Cloud infrastructures can no longer be compartmentalized and neither can cloud security. Darktrace/Cloud combines with other Darktrace products, allowing you to consolidate the functionality of disparate point solutions to better protect your applications, email systems, endpoints, Operational Technology (OT), and other assets on-premises and across hybrid and multi-cloud environments.

Darktrace/Cloud integrates with other tools across your security stack, allowing investigations to be initiated by third-party sources like CrowdStrike or Carbon Black.

Insights into incidents can also be exported directly to SIEM, SOAR, and ticketing systems.

Architectural modeling

Darktrace/Cloud gives users a near-immediate understanding of their cloud footprint, including real-time visibility into cloud assets and architectures, as well as users and permissions.

Cost insights give you a better understanding of resource allocation, helping teams contextualize resources.

See what attackers see

Effective security doesn't start or stop with detection or an internal view of risk. Darktrace/Cloud includes attack surface management (ASM) that adds the critical external view of your organization—the vantage point from which threat actors build attacks.

Combining internal and external views creates a complete, actionable picture of exposure that helps your team prioritize threats and seal off attack paths. When threats find their way into your environment, Darktrace/Cloud's AI-generated playbooks can help speed triage, remediation, and recovery.

Unified solution optimizes use of cloud

Leverage deployment flexibility

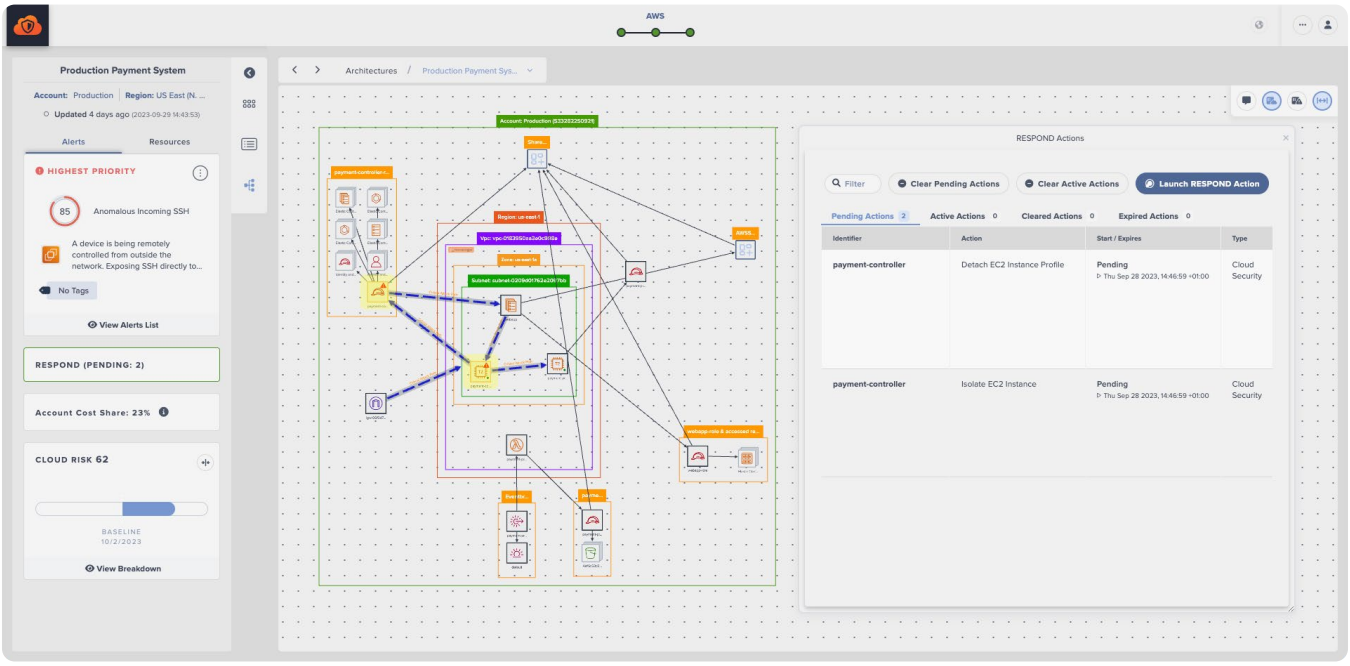
Darktrace/Cloud is agentless by default enabling swift installation. In more complex environments, analysts can also leverage dynamic architectural overview and risk context to elect to deploy real-time agents.

Improve cloud resource allocation

Darktrace analytics provide insight to optimize your use and allocation of cloud resources. Insightful dashboards and reports show where you have under-utilized cloud compute power with a common language, promoting knowledge-sharing and tighter alignment between DevOps and security teams.

Streamline security workflows

Darktrace/Cloud facilitates communication between security and DevOps teams via messaging platforms and offers on-demand ticket creation using your connected tools such as Jira and ServiceNow. Alerting and anomaly detections can be sent to SIEM or SOAR products or the Darktrace Mobile app.



PART 4

A Guide to Choosing the Right Solution

Cloud security should embody the best of cloud:

Dynamic agility, ease of use, and complete deployment flexibility based on your organization's goals for cloud environments.

The ideal approach reduces risk, cost, and complexity at the same time, and scales to accommodate the changing nature of business – vendor consolidation, mergers and acquisitions, remote work, completing digitalization, and whatever comes next.

To improve readiness and resilience, cloud security strategies must include:

- Real-time visibility to see who's doing what in the cloud to reduce risk and maintain compliance
- Continuous monitoring and analysis to detect anomalies at cloud speed and scale
- Self-Learning AI to prioritize risk, automate detection and response to known and novel attacks, and reduce the volume of alerts security analysts must investigate
- A unified, lifecycle approach to reduce risk, complexity, and cost

A 10-Point Checklist for Evaluating Cloud Security Platforms

1. Can the solution learn your business or would a massive upfront effort be required to train the system?
2. Does the solution deliver 100% real-time, end-to-end visibility to detect and prioritize risk across multi-cloud environments?
3. Are insights limited to static, point-in-time views of risk?
4. Does visibility combine internal and external views of your attack surface? Can your team see what hackers see?
5. Does the tool allow defenders to model attack paths and lateral movement?
6. Can the solution recognize novel attacks? Does it include playbooks to guide your response to novel attacks?
7. Do flexible deployment options include both agent and agentless monitoring?
8. Does the solution leverage the right AI for the right purpose at the right time?
9. Does this approach consolidate the benefits of CWPP, CSPM, and CNAPP into a single solution?
10. Will this approach streamline compliance and the journey to least privilege and zero trust?

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 over 145 patent applications filed. Darktrace employs over 2,200 people around the world and protects c.8,800 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