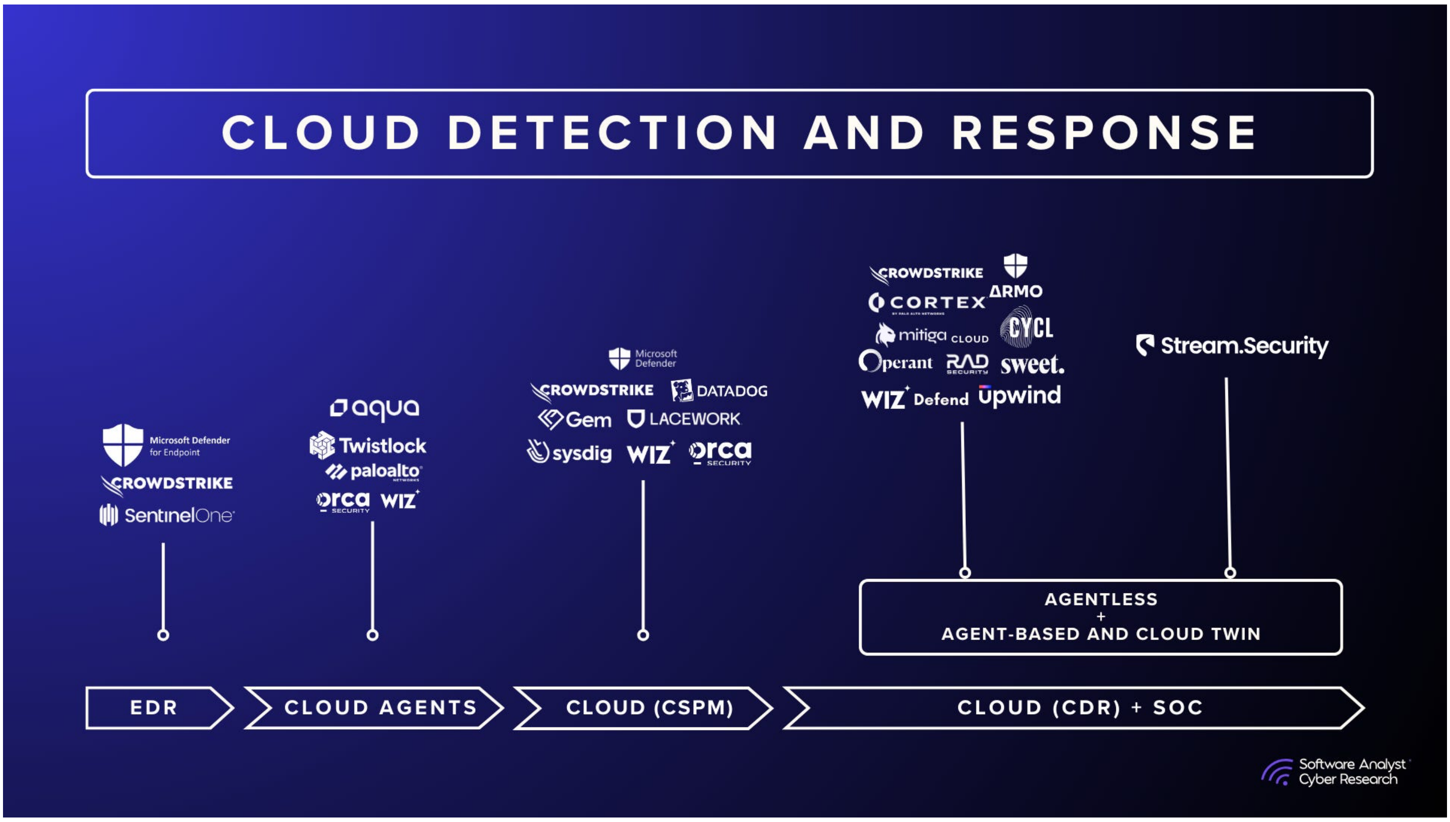
Case Study: Closing the State Gap in Cloud Detection and Response with Cloud Twin Architecture

January 13, 2026

Author

- **Aqsa Taylor** (https://www.linkedin.com/in/aqsa-taylor/) is the Chief Research Officer at Software Analyst Cyber Research, where she leads research initiatives and the CISO Arm (security leaders community). She is a published author with over a decade of experience building cloud security platforms and consulting more than 44% of Fortune 100 organizations on their security posture.



Readers,

Today, we are going to dive deep into the concept of a digital twin for cloud security, an architecture that brings real-time stateful awareness of the cloud to CDR. Once rooted in posture and compliance, cloud security is now moving closer to the SOC, where speed, context, and precision are important for effectiveness.

This report examines how stateful modeling reshapes detection and response workflows, from faster triage to impact-aware remediation. One way to implement such stateful detection is through a digital twin architecture of the cloud, known as a Cloud Twin.

A Cloud Twin introduces a stateful, continuously updated model of the cloud environment that enables real-time, context-aware threat detection with full awareness of configuration, identity, and exposure. The result is not a replacement for the existing technology stack but a complementary layer to SIEM, EDR, and emerging AI SOC solutions, providing the missing real-time, stateful understanding of the cloud.

We deep dive into practical implications of such an architecture with a case study on Stream Security, whose Cloud Twin implementation demonstrates how stateful cloud context enhances SOC visibility, reduces mean time to respond, and enables a more intelligent form of detection rooted in live risk rather than static findings.

Through this lens, we assess how the architecture differs from traditional solutions, and what its adoption signals for the future of SOC in 2025 and beyond.

Executive Summary: The Rise of the Cloud Twin in Cloud Detection and Response

Cloud security has reached a point where static visibility and periodic scanning no longer meet the operational demands of the SOC. Traditional CNAPP and CSPM platforms deliver posture and compliance, but they operate on snapshots that fail to capture the point-in-time, dynamic nature of modern cloud environments. At the same time, SIEM and EDR systems, while critical, remain focused on workload and event telemetry, often missing the broader context of how identities, configurations, and network paths shape real exposure.

A Cloud Twin architecture introduces the missing stateful layer which acts as a bridge between both. By continuously modeling the live state of cloud infrastructure, including configurations, identities, and connectivity, it enables SOC teams to detect, triage, and respond based on what is true right now, not what was true hours ago. This turns the cloud from a static data source into an interactive model that reasons about risk in real time.

For security operations, the benefits of such as stateful model are:

- **Improved detection:** By maintaining near real-time context on alerts with actual exploitability and cloud context.
- **Faster investigations:** through automatic mapping of attack paths and impact in dynamic state.
- **Reduced operational risk:** by simulating response actions before execution.
- **Greater efficiency:** in SIEM and SOAR workflows through enriched, high-context alerts rather than unfiltered log streams.

The Cloud Twin does not replace the existing tech stack. It complements them by connecting vulnerability data from CNAPP, workload visibility from EDR, and telemetry from SIEM into a unified, stateful model of the environment. In doing so, it shifts SOC workflows from reactive triage to proactive containment, enabling teams to get full defense coverage by triaging every alert and mapping it to the right risk, based on their own environment, replicated by the CloudTwin.

A Shifting Threat Landscape

Cloud adoption has become universal, but confidence in detection has not kept pace.

- **78%** of organizations use two or more cloud providers.
- **61%** cite security and compliance as barriers to further adoption.
- **64%** lack confidence in real-time threat detection.

Meanwhile, adversaries have shortened their timelines dramatically. **Breakout times** are under an hour, and **median dwell times** average just **7 days**. With cloud configurations changing by the minute, posture data captured once a day no longer reflects the environment defenders must protect.

These pressures have exposed a core limitation of traditional cloud security: it operates on stale, stateless data in a world that changes every second.

Challenges with Existing Approaches to Cloud Detection and Response

Despite advances in posture and runtime security, existing methods remain insufficient for modern SOC operations.

1. Scan Frequency Gaps: Most posture management platforms scan once or twice daily. Any configuration change between scans creates blind spots. Attackers exploit these windows to escalate privileges or move laterally before detection.

2. Static Context: Posture tools evaluate risk based on outdated snapshots. They lack the ability to reflect real-time reachability or new attack paths that form instantly when permissions or network rules change.

3. Runtime Isolation: Runtime agents offer deep process visibility but little understanding of the cloud control plane. They detect commands but not the permission changes that made those commands possible.

4. Fragmented SOC Workflows: SIEM and EDR platforms remain event-driven and log-centric. They surface what happened but not how it changed the cloud state. Analysts spend time reconstructing stories from disconnected signals, increasing mean time to respond and reducing confidence in triage.

The result is a SOC buried in alerts without context, forced to operate on data that is either outdated or incomplete.

Introducing Cloud Twin

Effective cloud detection must align with each organization’s unique architecture and risk profile. A context-aware policy engine enables teams to define custom rules that reflect their threat models, business logic, and operational priorities. By correlating identity reachability, asset criticality, connectivity, and security posture, detections become both organization-specific and risk-driven.

The **Cloud Twin** represents the next stage of CDR evolution. It continuously models an organization’s entire cloud environment: identities, configurations, and network reachability in real time. By ingesting cloud logs and recalculating only the affected portions of the graph with every change, it keeps an always-current view of risk and exposure.

Key capabilities include:

- **Real-time visibility** into configuration and identity changes without agents.
- **Impact modeling** that shows how each event reshapes attack paths.
- **Anomaly-based detection:** Baselines normal behavior across cloud resources, identities, and services to identify real-time deviations tied to actual exploitability rather than static, rule-based SIEM logic.
- **Configuration change detection:** Monitors and correlates control-plane modifications such as role, permission, and configuration changes to uncover how environment drift contributes to privilege escalation or lateral movement.
- **Predictive response simulation** that tests the effect of proposed actions before implementation.
- **AI-driven triage** that prioritizes real risks and reduces noise.

The Cloud Twin bridges the gap between posture management and runtime defense, bringing real-time, stateful context to a space long dominated by static snapshots.

Stream Security: The Case Study

Stream Security, founded in 2021, pioneered this concept with its **Cloud Twin** architecture. After 2.5 years of R&D, Stream launched a model that continuously synchronizes cloud configuration changes and instantly recalculates security impact.

How Stream's Cloud Twin Works

- Begins with a one-time scan, then streams write events to maintain a live graph.
- Highlights new attack paths created by permission or network changes.
- Detects anomalies by learning normal behavior and the unique properties of an environment
- Automatically triages every alert based on real risk in your environment.
- Integrates with identity providers and vulnerability feeds for complete risk context.
- Includes **deception canaries** to boost detection fidelity.
- Allows response **simulation** to predict operational impact before execution.

Customer Outcomes

- **Gap Closure:** Eliminates visibility delays between scans, catching threats in real time.
- **Reduced SIEM Overload:** SOCs rely on Stream's stateful AI triage, forwarding fewer raw logs.
- **Precision Response:** Enables surgical containment, revoking credentials or reverting risky changes without disrupting production.

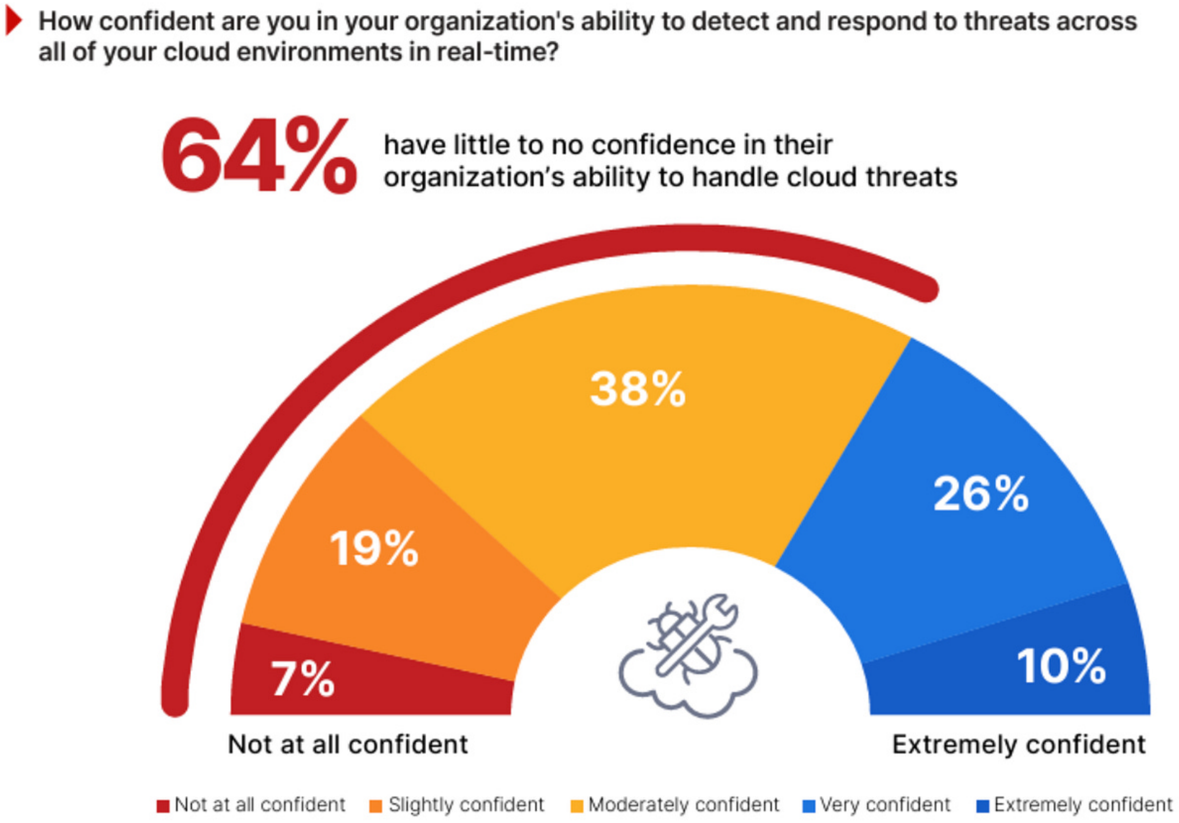
The Analyst View

The transition to stateful cloud modeling marks a defining moment in SOC modernization. As security operations evolve beyond log correlation toward real-time reasoning, architectures such as the Cloud Twin will become the backbone of effective detection and response. The future of cloud security lies not in collecting more data, but in understanding the state behind it.

For SOC and cloud detection engineers, the Cloud Twin is a **living model** that transforms the question from *what happened* to *what matters **now***.

State of Threat Landscape in 2025

Before we dive into the digital twin concept, it's important to understand the context on "why this now".



Source: https://www.cybersecurity-insiders.com/state-of-cloud-security-report-2025/ (https://www.cybersecurity-insiders.com/state-of-cloud-security-report-2025/)

According to a survey from cybersecurity insiders, Cloud environments are now the default rather than the exception: over **78% of organizations** report using two or more cloud providers, and **54%** have adopted a hybrid (on-premises + public cloud) model. Yet despite this broad deployment, security and compliance remain major roadblocks: **61%** of respondents cite security/compliance as the top barrier to further cloud adoption.

Confidence in real-time threat detection is also low, **64%** of respondents say they don't feel confident in their ability to detect threats as they occur. To counter these gaps, nearly all respondents (**97%**) favour unified cloud security platforms offering centralised visibility and policy control.

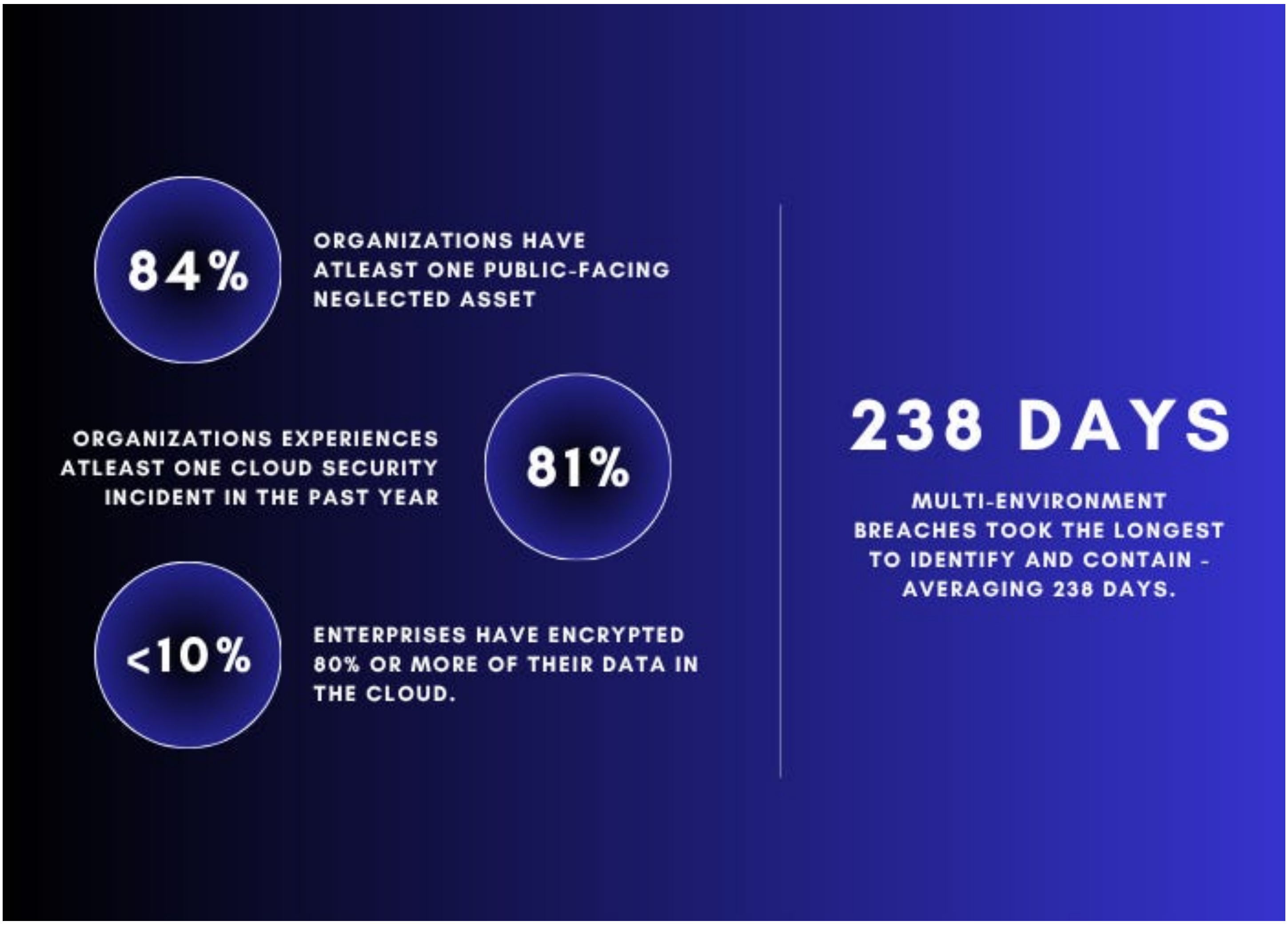
This data underscores a central tension: cloud scale has outpaced security maturity. The shift toward consolidated, context-rich platforms is less about chasing tool coverage and more about closing threat attack surface blind spots. As organisations embrace multi-cloud complexity, security teams are now under pressure to translate visibility into assurance and not just more dashboards.This demands the need for easy deployment, visibility at scale and real-time threat detection and coverage.

Faster Dwell and Breakout Times

According to CrowdStrike in their 2025 Global Threat Report, the average "e-crime breakout time" (how fast threat actors pivot after initial access) is **48 minutes.** In the same report, the fastest recorded e-crime breakout time was **51 seconds**.

Per Sophos's *2025 Active Adversary Report*, (https://news.sophos.com/wp-content/uploads/2025/04/It-Takes-Two-2025-Sophos-Active-Adversary-Report.pdf) the overall median "dwell time" (time from initial compromise to detection) is **7 days**, with ransomware cases often at **4 days**, and non-ransomware cases at **11.5 days**. According to LevelBlue in their *2025 Threat Trends Report (Edition Two)*, adversaries once inside moved laterally with an average breakout time of "**under 60 minutes**, and in some cases **less than 15 minutes**.

Signaling the necessity for defenders to react, contain and respond to these attacks within minutes not hours.



Reference: https://www.techmagic.co/blog/cloud-security-statistics (https://www.techmagic.co/blog/cloud-security-statistics)

Cloud remains the most targeted terrain

Cloud remains the most targeted terrain. According to **Fortinet's 2025 Threat Report** (https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf), exposures like open storage buckets, over-permissioned identities, and misconfigured services continue to be the fastest route to compromise

Sensitive Data is leaking through the cracks

Tenable's 2025 Cloud Security Risk Report (https://www.tenable.com/blog/cybersecurity-snapshot-cloud-data-secrets-exposure-cyber-risks-06-20-2025) reports that 9% of publicly accessible cloud storage contains sensitive data, and a stunning 97% of that is labeled restricted or confidential. Even more concerning: secrets left in services by design, not oversight. This shows an increasing need for not only good posture management but also quick insights on blast radius.

Siloes between Cloud Security and SOC

Organizational silos hinder collaboration, especially between SOC, cloud security, and platform teams. This fragmentation leads to blind spots and inefficiencies, with 44% of organizations citing fragmented visibility due to too many separate tools as a major challenge.

The Evolution of Cloud Security: From Posture to Runtime to CDR

In modern cloud attacks, the control plane is often the first target. Adversaries modify roles, permissions, and network rules to expand their reach. Stateful detection elevates these changes as primary attack indicators rather than secondary audit findings. Each modification is mapped to potential new attack paths and linked to high-value assets, enabling SOC teams to visualize how environment drift becomes an active part of the attack chain.

Before the shift to cloud, enterprise security lived in a world of clear perimeters. Firewalls and endpoint protection defined control. Visibility ended at the datacenter edge. Security tools were built for static infrastructure, predictable workloads, and long patch cycles. When workloads began moving to public clouds, organizations tried to lift those same models into a new environment built on APIs, ephemeral resources, and shared responsibility. It didn't work. Security teams needed context, scale, and automation, not signatures and rules.

The past decade of cloud security has been defined by a loop between visibility and control -from the rise of agentless scanning to the reemergence of runtime defense. Over the past decade, agentless technology moved from an innovation to a mainstream approach for securing large-scale cloud environments. But the need for real time visibility brought back light weight, ebpf agents into center stage again.

Posture Security and The Agentless Scanning Advantage

Then came a wave of cloud-native tools focused on using cloud provider APIs to monitor configurations and detect misconfigurations. Companies such as Dome9 and Evident.io (acquired by Palo Alto Networks) introduced solutions that scanned cloud resources without installing any agents. This approach gave rise to Cloud Security Posture Management (CSPM), marking a significant step in cloud visibility and compliance.

By 2019, companies like Orca Security and Wiz Security demonstrated that it was possible to achieve similar results for workload visibility without deploying agents or modifying workloads. This architecture was quickly adopted as it gave an easy way of gaining visibility without the complexity of deploying agents. This milestone redefined cloud visibility and made agentless scanning the default choice for many organizations.

These systems create snapshots of the workloads and perform daily or periodic scans of the environment to identify misconfigurations and exposures. However, this model had inherent constraints. CSPM tools are typically scanned once or twice a day. Any configuration change between scans created a blind spot that attackers could exploit. Posture data represented static snapshots rather than real-time states. Attack paths changed faster than posture graphs could update.

Key Industry Challenges:

1. **Scan Frequency Gaps:** With scans occurring once or twice per day, any configuration change between scans creates blind spots. Attackers can exploit these gaps to escalate privileges or move laterally before detection.
2. **Static Context:** Posture management tools evaluate risks based on outdated states of the cloud, failing to reflect real-time reachability or newly created attack paths.
3. **Agent-Based Tradeoffs:** Runtime agents increase visibility but introduce operational complexity, scalability issues, and security overhead. They have visibility on the workload level but not on the cloud posture.
4. **Blast Radius Blindness:** Posture data reflected a point-in-time assumption about blast radius that could shift quickly with new connections or privileges.

Runtime Revisited

The resurgence of runtime tooling driven by eBPF and container-native agents has given security teams deeper behavioral insight into workloads. But runtime alone doesn’t solve the problem either. Traditional EDR-style telemetry is rich in process data but blind to cloud identity, network configuration, or IAM transitions. You can detect the command that ran, but not the permission change that made it possible.

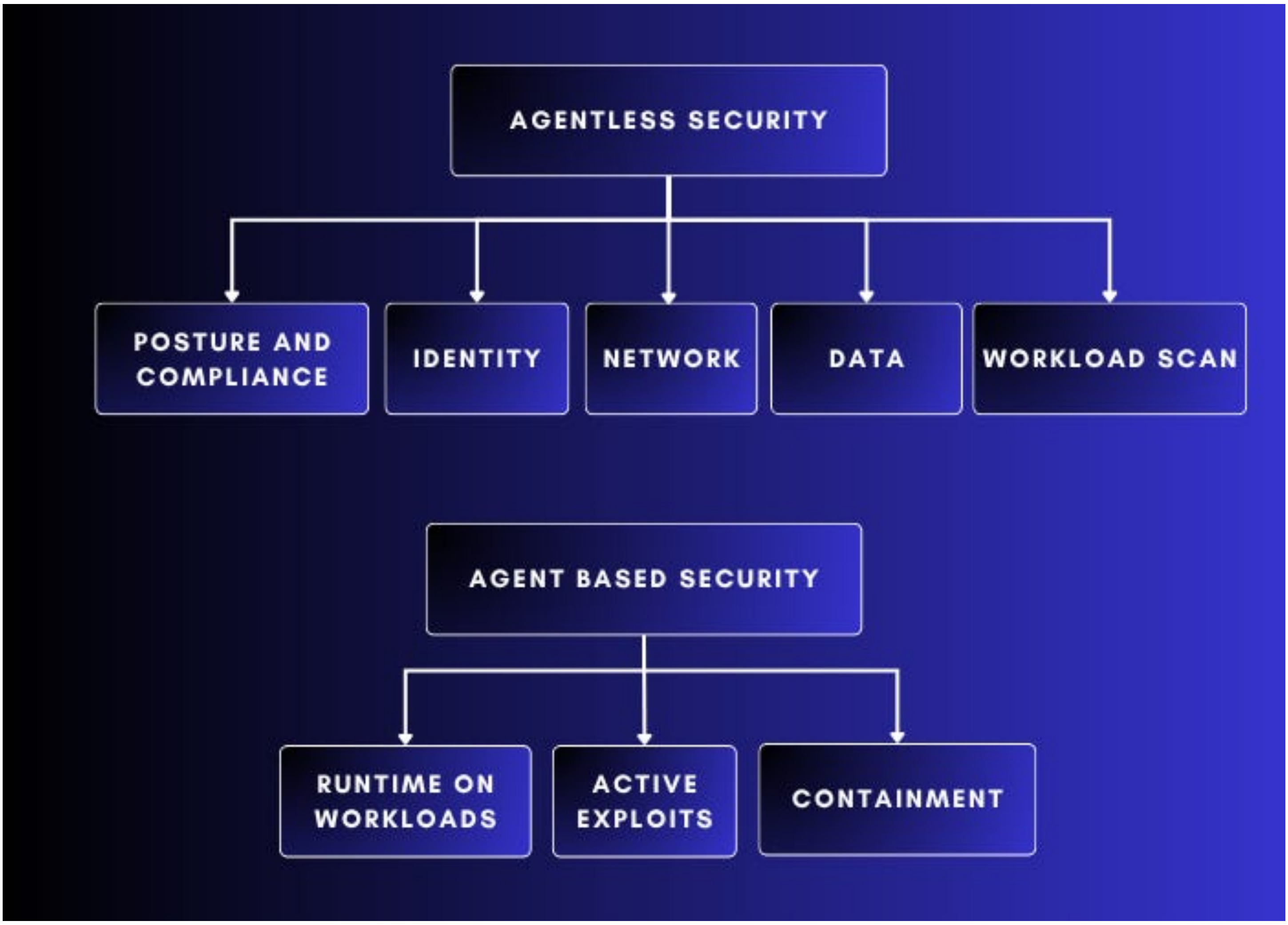
Why runtime matters

- **Rapid change:** Workloads in the cloud spin up and down, scale dynamically, use ephemeral containers and serverless functions. A configuration snapshot from last night may no longer reflect what a live attacker sees. The report from ARMO Sec (https://www.armosec.io/wp-content/uploads/2025/05/Survey-Report_Final_May_25.pdf) found that runtime-oriented tools are increasingly essential for Kubernetes and container environments.
- **Behavioral visibility:** Runtime agents capture process, file, network, kernel, identity activity, not just configuration state. That visibility is necessary to detect lateral movement, in-memory attacks, anomalous network flows or privilege misuse.
- **Reducing dwell time:** Detecting an attacker while they’re “in the house” is vastly more valuable than finding misconfigurations after an incident. Runtime security narrows the window between compromise and detection.
- **Market push:** The “cloud workload protection” market is expected to grow from USD 7.33 billion in 2024 to USD 9.0 billion in 2025 (CAGR ~22.8 %) according to Business research (https://www.thebusinessresearchcompany.com/report/cloud-workload-protection-global-market-report). This growth reflects the rising importance of runtime controls.

Key Industry Challenges:

- **Data Overload:** Runtime telemetry generates massive event volumes, creating alert fatigue and requiring intelligent prioritization to maintain analyst efficiency.

- **Limited Context Correlation:** Many runtime systems lack seamless integration with configuration and identity data, making it harder to determine the root cause or exposure path of detected activity.
- **Operational Complexity:** Security and DevOps teams often face challenges deploying and maintaining agents across diverse environments, leading to increased management overhead.
- **Latency in Response:** Without automated orchestration, runtime detections may not translate into immediate containment, extending mean time to respond (MTTR).



Evolving SOC Operations: The Rise of Cloud Detection and Response

With posture and runtime in place, the question becomes: how do we *detect, investigate and respond* to real threats across cloud infrastructure? That is precisely where CDR comes in. Cloud Detection and Response, or CDR, represents the next stage of full defense. It unifies posture visibility and runtime telemetry into an operational detection and response model. CDR continuously analyzes identity behavior, workload activity, configuration drift, and network traffic to identify threats in real time. In simple words, Cloud Detection and Response (CDR) is designed for the SOC runtime by integrating data from cloud posture and runtime defense sources to SIEMs and security operations platforms.

What CDR Should Deliver

- **Real-Time Monitoring:** Continuous data collection from workloads, APIs, and identities.
- **Behavioral Correlation:** Connecting anomalies in runtime with identity misuse and configuration changes.
- **Investigation and Response:** SOC-ready workflows to isolate workloads, revoke credentials, and orchestrate containment.
- **Automation:** Integrating detection with remediation to shorten mean time to detect (MTTD) and mean time to respond (MTTR). According to research from cybersecurity insiders, 61% of (https://www.cybersecurity-insiders.com/2024-cloud-security-report-trend-micro/) cybersecurity professionals advocate for automated response mechanisms to ensure quick and effective action against threats, highlighting the need for systems that can autonomously react to and mitigate potential breaches immediately.

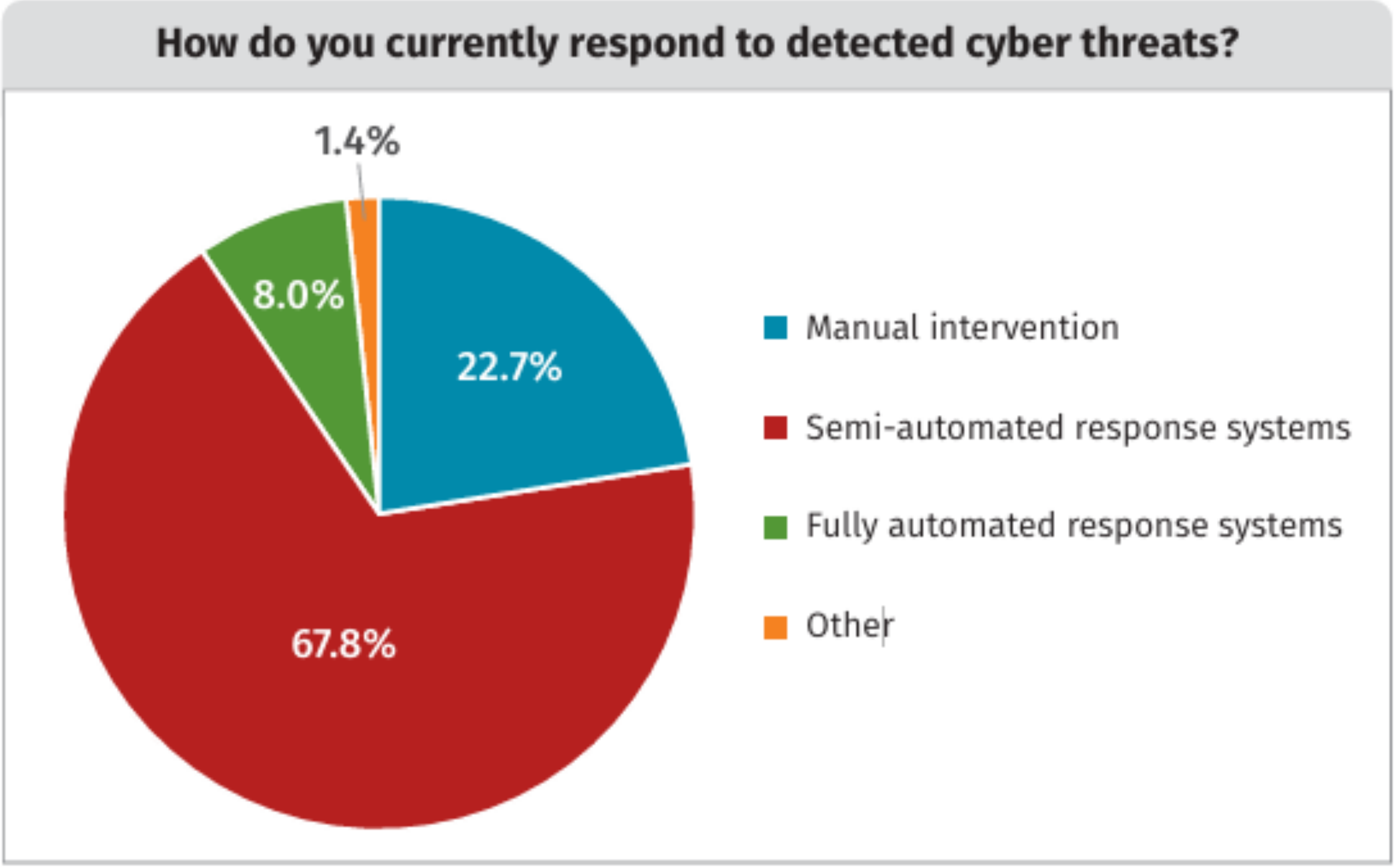
A developer unintentionally grants broad permissions to a serverless function. A posture scan flags it later. A runtime agent detects outbound data activity. A CDR platform correlates both with an identity event, alerts the SOC, and triggers an automated fix. The attack path is cut off before exfiltration. That is the value of full-loop defense.

What Makes Cloud Detection and Response Different

Cloud detection and response presents different challenges and opportunities compared to traditional endpoint detection and response platforms, due to cloud environments’ dynamic nature and scale. Static telemetry and periodic scans cannot keep pace with environments that shift every second. The result is predictable: teams are overwhelmed with alerts and underinformed on context.

More than half of security leaders from a survey conducted on (Detection and Response conducted by SANS (https://www.sans.org/white-papers/sans-2024-detection-response-survey)) 56 percent, report that their teams lack the expertise to manage cloud threats effectively. The operational strain appears elsewhere too. Integrating controls across multiple cloud providers is difficult for 51 percent of organizations, and almost as many struggle to align cloud telemetry with existing tools.

The data shows a shift in confidence but also in expectations. Cloud-native detection tools are viewed as capable yet incomplete. Two-thirds of respondents find these tools effective, while 13 percent consider them ineffective. That gap reflects a deeper issue where the threat surface evolves faster than detection logic. Manual monitoring remains in place for many teams, with 59 percent calling it effective, but it cannot scale in dynamic environments. Its continued use signals how much human intuition still compensates for missing visibility.



Refr: SANS 2024 Survey on Detection and Response

As a result, SOC teams face detections detached from reality. They triage alerts about compromised resources without knowing whether the exposure still exists or has already been remediated.

This visibility lag carries immeasurable consequences. In a 2025 Global Cloud Detection and Response report (https://www.illumio.com/blog/global-cloud-detection-and-response-report-q-a-on-the-human-side-of-cloud-security-gaps) by Illumio, analysts found that the problem is that almost 40% of data lacks enough context to be useful. Security teams don't have the information behind that visibility to prioritize or address risk.

In reality, the cloud demands detection that understands state, not just events.

Challenges that SOC teams currently face

Modern SOCs are facing three major challenges in cloud defense.

- **Stateless visibility creates blind spots:** Most CNAPP and CSPM tools still rely on periodic snapshots. Adversarial control-plane changes or short-lived workloads can appear and vanish between scans, leaving analysts with partial point in time visibility.
- **Log-centric detections lack cloud context:** SIEM rules focus on raw events rather than live reachability, identity relationships, or toxic combinations. This produces high false positives and slows triage as analysts reconstruct what the logs cannot show.
- **Fragmented signals delay response:** Without a unified, real-time view of identities, configurations, and network

paths, SOC teams struggle to piece together attack storylines and act confidently at the right control point.

The implications for security leaders are clear: mean time to respond keeps rising, SIEM platforms are overloaded with low-fidelity alerts, and teams take “shot-in-the-dark” actions based on stateless context that risk disrupting production.

A stateful, real-time model of the cloud detection and response system closes these gaps. It continuously contextualizes every activity and configuration change, mapping exploitability and blast radius at the moment of detection. This allows SOC teams to reason about what matters most and to respond with precision rather than noise.

The Need for Stateful, Real-Time Context for Cloud Threats in SOC

Effective detection in the cloud is not just about collecting logs or scanning assets; it is about understanding the **state.** What the cloud looks like at the precise moment of an event. Without state, detections are guesses. With it, security teams can reconstruct attack paths, validate blast radius, and respond with precision.

True CDR demands a paradigm that treats the cloud as a living system. It requires continuous synchronization between configuration data, identity context, and workload runtime events, what can be described as the evolution from **stateless scanning to stateful modeling**.

SIEM, EDR, and emerging AI-driven SOC platforms still lack a real-time, stateful understanding of the cloud. Traditional telemetry captures what happened but not the state of the environment when it occurred. A stateful detection layer closes this gap by continuously modeling the live cloud environment, linking every event to its actual risk and context. This bridge between raw data and meaningful detection enables faster, more confident response in complex cloud ecosystems.

Introducing Cloud Twin: The Missing Stateful Context for Modern SOCs

A Cloud Twin introduces a stateful, continuously updated model of an organization’s cloud environment that reflects configuration, identity, network reachability, and exposure in real time. It converts stateless events into a living graph of access and risk. For modern SOCs, this model represents the connective tissue between prevention and response, closing a critical gap left by existing SIEM, EDR, and even emerging AI-SOC platforms that still operate on static or log-centric data.

Architecture and Role in the SOC Stack

A Cloud Twin ingests existing cloud telemetry including configuration logs, identity data, and vulnerability intelligence, and continuously recalculates how each change reshapes the environment within a digital twin. Rather than deploying new agents, it builds its real-time model by streaming cloud configuration events as they occur and updating only the affected portion of the graph. This creates an always-current representation of exposure, reachability, and trust relationships across cloud services, users, and workloads.

For the SOC, the Cloud Twin acts as a stateful reasoning layer. It associates every alert or event with its surrounding context about the attack vectors and not just discreet events: What changed, who made the change, and what that change enabled. Analysts can visualize how an IAM update, security group modification, or network route adjustment alters attack paths in real time. The model also supports response simulation, allowing teams to preview the operational impact of an action such as revoking credentials or rolling back a configuration before applying it in production.

This architecture complements the existing SOC technology stack rather than replacing it. SIEM and EDR continue to serve as log collectors and workload sensors, while the Cloud Twin provides the missing stateful cloud layer that turns raw telemetry into meaningful detection and response. It enriches SIEM alerts with cloud semantics, improves prioritization through exploitability context, and orchestrates precise response through SOAR or native integrations.

Advancing Detection: Bringing Stateful Cloud Context to the SOC

Behavioral analytics in the cloud must extend beyond user actions to include how services, resources, and configurations behave under normal conditions. Stateful detection systems based on cloud twin, baseline these elements with full cloud semantics, surfacing deviations that matter because they tie directly to real exploitability within the current environment graph. This moves beyond static rules built on raw logs to dynamic detections informed by live context and relationships.

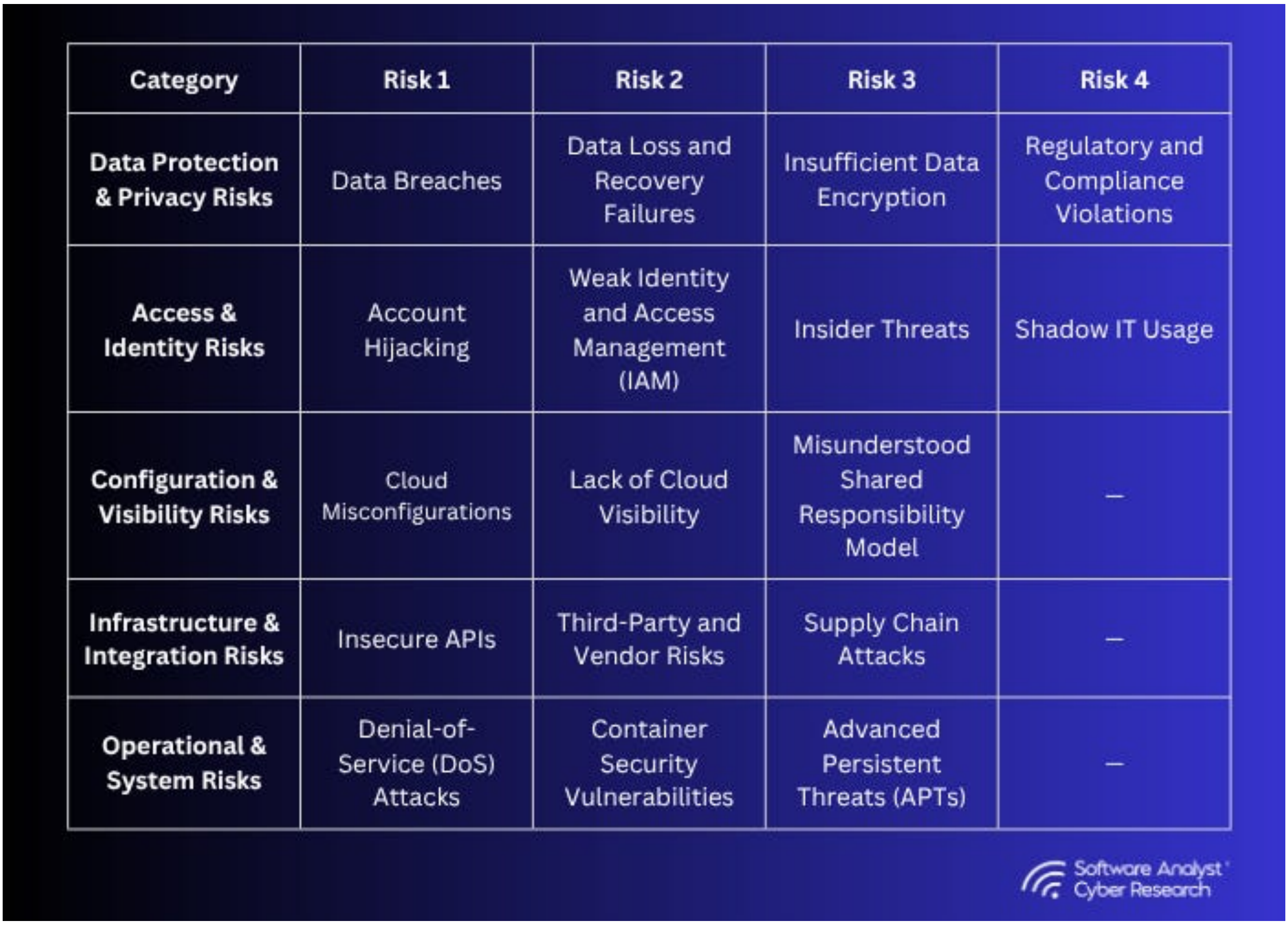
Core Advantages of Stateful Detection

Stateful models allow SOC teams to see attacks as evolving stories rather than isolated alerts. They combine identity, configuration, and workload context into a single operational view, revealing how risk propagates across the cloud environment in a near real-time lens. This continuous context provides several advantages: it reduces alert fatigue by eliminating false positives, shortens investigation time by surfacing impact automatically, and improves response precision by showing where to intervene without disrupting production. In practice, this shifts SOC workflows from reactive triage toward proactive containment.

Real-time Configuration Change Detection with Impact Analysis

In modern cloud attacks, the control plane is rarely collateral damage, it’s the entry point. Attackers don’t just exploit workloads, they reshape roles, permissions, and network rules to quietly expand their reach. Stateful detection treats these changes as attack progress, not background noise. Every modification is evaluated for the access it creates, the paths it unlocks, and the critical assets it exposes so SOC teams can see how configuration drift becomes a deliberate step in the attack.

The figure below shows example risks across each category of cloud surface. Delayed detection or remediation increases the likelihood of exploitation.



Category	Risk 1	Risk 2	Risk 3	Risk 4
Data Protection & Privacy Risks	Data Breaches	Data Loss and Recovery Failures	Insufficient Data Encryption	Regulatory and Compliance Violations
Access & Identity Risks	Account Hijacking	Weak Identity and Access Management (IAM)	Insider Threats	Shadow IT Usage
Configuration & Visibility Risks	Cloud Misconfigurations	Lack of Cloud Visibility	Misunderstood Shared Responsibility Model	–
Infrastructure & Integration Risks	Insecure APIs	Third-Party and Vendor Risks	Supply Chain Attacks	–
Operational & System Risks	Denial-of-Service (DoS) Attacks	Container Security Vulnerabilities	Advanced Persistent Threats (APTs)	–

Environment-Tuned Policy Engine

Effective detection in the cloud must adapt to each organization's architecture and risk model. A policy engine tuned to environmental context allows teams to define custom rules that visualize their own threat models, business logic, and operational priorities. By combining identity reachability, asset criticality, connectivity, and posture context, detections become both organization-specific and risk-aware.

Detection Depth

For teams that need deeper visibility, stateful detection can integrate workload-level telemetry without forcing an additional agent deployment. Where runtime coverage is already in place, SOC teams can simply ingest that data into the same stateful graph.

Contextualization across all planes

Identity signals, SaaS context, and vulnerability intelligence enrich the twin so detections incorporate who can do what, from where, and with which software liabilities. Some implementations add deception canaries to raise fidelity and slow adversaries, and apply automatic AI triage on the stateful graph.

Because the twin mirrors real state, proposed actions can be simulated to forecast the butterfly effect before execution, enabling precise controls like revoking the right credential or rolling back a risky Security Group (SG) change instead of terminating production workloads.

Together, these capabilities redefine how SOC teams approach detection in the cloud. They provide a living model of the environment that interprets activity in context, turning what was once raw signal into actionable understanding.

Why This Matters

A stateful graph lets detections and triage operate on “actual risk” rather than theoretical findings. Analysts can see when an innocuous policy tweak created a live path to a sensitive system and can prioritize accordingly.

Role in the stack: Working alongside what you already have

Cloud Twin based CDR does not displace existing layers in the security stack. It strengthens them.

- **Prevent and Posture:** CNAPP and CSPM remain the foundation for governance, misconfiguration management, and preventive controls. They define the baseline of cloud hygiene but stop short of showing how attacks unfold in real time. This model continuously baselines normal behavior across every cloud resource, identity, and service to detect deviations and remediation impact in real time.
- **Detect and Respond:** Cloud Twin extends this foundation into the SOC. It enriches SIEM alerts with stateful context, ranks detections by real exploitability, and enables tailored, context-aware detections that reflect the unique patterns and risk profile of each environment
- **Endpoint and Workload:** EDR and XDR continue to provide deep telemetry inside machines and containers. Stream complements these layers by exposing what they cannot see: the control plane, identity relationships, and service interconnections that determine how an incident actually propagates.

Together, these systems form a continuous chain from prevention to response, giving SOC teams a unified understanding of both the workload and the cloud fabric around it.

Case study: Stream Security

Founded in **2021**, Stream Security spent 2.5 years building its proprietary CloudTwin architecture before going to market. The company now serves large scale enterprise customers, including **RingCentral, New American Funding and CrossRiver**.

Stream operates primarily in the **enterprise segment**, often complementing rather than replacing existing CNAPP platforms. This positioning shows that many organizations recognize the value of Stream’s *real-time context layer* on top of their existing posture management tools.

Voice of the Customer

We were able to connect with a customer of Stream Security. Here are the answers from the security leader’s perspective –

What did your organization struggle with prior to Stream?

- Attribution of cloud activity to users and resources. CSPM would show us the problem, but it didn’t show us how it happened.

- Cloud architecture validation and blast radius assessment – Stream is special in the CDR space because it also operates on network data. That allows us to get a complete picture of a systems architecture, upstream and downstream dependencies, and attack paths to critical assets.
- Network detection and response – legacy NDR vendors are not built for AWS data. Stream is cloud-native and provides the easiest AND most complete network monitoring we found in our extensive search.
- Cloud native deceptions – Our deceptions platform before Stream was from the on-prem days and did not scale well with cloud. Stream's deceptions were more effective and easier to manage.

Why didn't other solutions like CNAPP platforms or other solutions address these needs? Or why Stream in particular?

Other CNAPPs were constrained by either not having enough sources to track network traffic or were focused mainly on containers and kubernetes environments. Stream provided the best overall value for our diverse environment.

Any missing capabilities that you would like to see on Stream's roadmap?

The product team has stayed ahead of us in this space. They continue to surprise us with great new capabilities to drive new value in our security stack.

How it Works

- Starts with an initial scan, then streams cloud write events to keep a real-time graph.
- Calculates the security impact of each change and shows emergent attack paths instantly.
- Integrates identity, SaaS, and vulnerability knowledge for actual risk scoring.
- Includes deception canaries to raise signal quality, with automatic AI triage over stateful data.
- Simulates response actions to predict operational impact before execution.

Target User: The primary beneficiary is the SOC and cloud detection engineering team who need accurate, current state to hunt, triage, and respond.

Stream Security: Technical Capabilities

Here's a glimpse of what Stream Security provides with its proprietary Cloud Twin model –

- **CloudTwin Model:** Maintains a live, continuous view of your environment with full state awareness across every change.
- **Risk-based Detection:** Identifies meaningful signals across identity, network, configuration, runtime, and data layers. Provides real-time insight by ingesting cloud logs and identity data, with optional runtime sensors for K8s.
- **Anomaly-based detection:** Stream continuously baselines normal behavior across every cloud resource, identity, and service to detect deviations in real time. This enables tailored, context-aware detections that reflect the unique patterns and risk profile of each environment, unlike static, manually written SIEM rules based on raw telemetry that lack cloud context and exploitability awareness.
- **Cloud configuration change detection:** Attackers frequently manipulate the cloud environment itself, modifying

configurations, roles, or permissions, as part of their TTPs for privilege escalation and lateral movement. Stream identifies and correlates these control plane changes as part of an evolving attack chain, revealing how environment drift can be weaponized.

- **AI-driven Triage and Investigation:** Cuts through noise, enriches alerts with context, and speeds investigation and response.
- **Stateful Attack Storylines:** Connects entities and events into a visual narrative for root-cause and lateral-movement analysis. Detects new attack paths instantly as configuration or identity changes occur.
- **Predictive Analytics and Response Simulation:** Models potential impact before action to prevent over-remediation.
- **Automated, Environment-aware Response:** Executes targeted actions such as credential revocation, group rollback, quarantine, and perimeter controls.
- **Dynamic Deception:** Deploys adaptive traps and decoys to raise signal fidelity and disrupt attackers.
- **Seamless Integration:** Enhances existing CNAPP, SIEM, XDR, and EDR stacks with real-time cloud context.
- **StreamLine Automations:** Expands orchestration across EDR, SIEM, SOAR, and multi-cloud (AWS, Azure; GCP in progress).
- **Business Impact Mapping:** Links risks to affected services and owners to prioritize response based on operational impact.

Customer Outcomes

- **Reduced MTTD and MTTR:** Continuous context and automation shorten the time from alert to action.
- **Gap Closure:** Real-time streaming fills the visibility gaps between CNAPP scans, allowing SOCs to spot and stop cloud-layer pivots immediately.
- **Better Triage at Lower Cost:** Stream's AI triage reduces manual analysis and event volume, with customers forwarding fewer raw logs to the SIEM.
- **Precise Response:** Teams can safely roll back risky security group edits or revoke the exact credential behind lateral movement instead of over-remediating.
- **Optimized SIEM Load:** High-fidelity alerts lower storage and processing overhead across security systems.
- **Improved SOC Efficiency:** Analysts spend less time chasing noise and more time resolving high-impact threats.
- **Higher Operational Resilience:** Real-time impact mapping aligns security actions with uptime and business priorities.

Analyst Take: Why SOC Modernization Requires Stateful Cloud Context

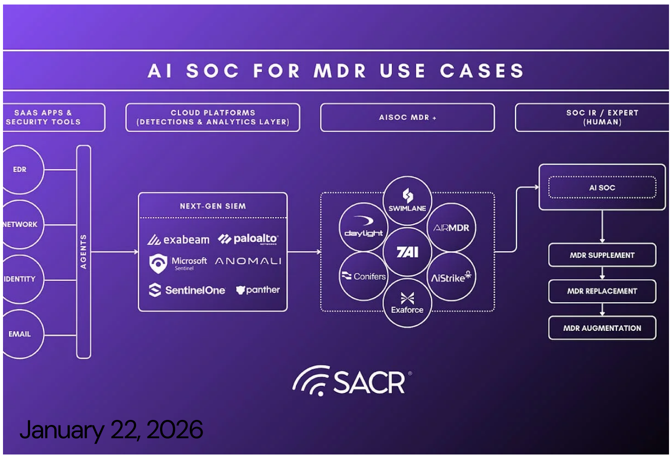
The SOC has become the convergence point for cloud risk. As enterprises adopt multi-cloud architectures, the number of signals has multiplied while the context behind them hasn't matured. Analysts now face an ecosystem of partial truths: SIEM shows what happened, CNAPP shows what is misconfigured, and EDR shows what executed, but none can explain how these layers interact in real time.

Stateful cloud modeling changes that equation. It gives detection and response teams a live system of record that brings together posture, identity, and activity into a single operational view. Instead of querying logs, analysts can query state: who made a change, what that change enabled, and whether it opened a new path to critical exposure. In addition, be able to simulate a response and measure it's impact, without affecting the real environment. This level of reasoning transforms the SOC from a reactive function into an intelligence-driven center that understands its environment as a living system, not a list of alerts.

In 2025 and beyond, the most effective SOCs will be those that can interpret the cloud in context. Stateful architectures such as the Cloud Twin signal this transition away from volume-driven monitoring toward state-driven understanding. The winners in this evolution will not be the teams with the most data, but those with the clearest picture of what that data means in the moment it matters.

←(https://softwareanalyst.io/reports/disruptive-technolo ne-evolution-of-1password-identity-security-solutions/)→

RELATED POSTS

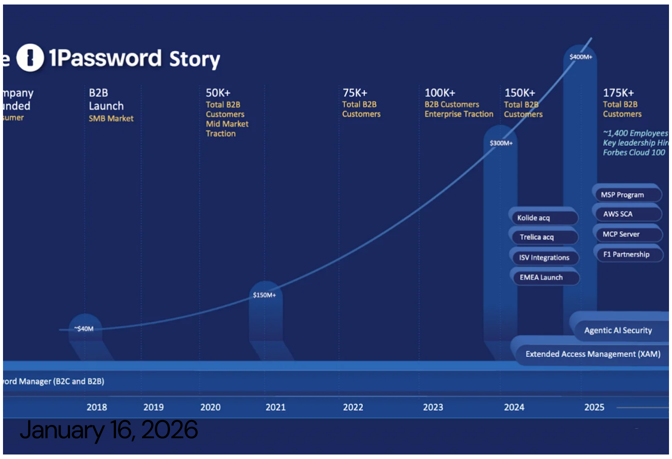


January 22, 2026

Security Operations, SOAR / AI-SecOps, TIP / MDR

AISOC for MDR: The Structural Evolution of Managed Detection and Response

Read More (Https://Softwareanalyst.io/Reports/Aisoc-For-Mdr-The-Structural-Evolution-Of-Managed-Detection-And-Response/)



January 16, 2026

AM, Identity & Network Security

Inside 1Password's Enterprise Identity Transformation

Read More (Https://Softwareanalyst.io/Reports/1password-The-Evolution-Of-1password-Identity-Security-Solutions/)

NO COMMENTS

Stay up to date!

Sign up to our newsletter and receive every new report in your inbox.

(https://softwareanalyst.io)

We deliver clear, concise, and in-depth analysis of the rapidly evolving cybersecurity landscape, built for cyber leaders, operators, and investors.

About

What We Do

Our Unique Approach

Careers

Testimonials

More

All Reports

Market Maps

Privacy policy

Terms of use

Get In Touch

Contact

Subscribe

(https://ca.linkedin.com/compa

(https:// [illegible]

analyst)