Enterprise Strategy Group by TechTarget

SHOWCASE

MARCH 2024

Closing the Gap Between CNAPP and XDR

Dave Gruber, Principal Analyst

Abstract: While organizations have invested in solutions to reduce the cloud attack surface and prevent attacks, using tools such as security information and event management (SIEM), security orchestration and automation response (SOAR), cloud-native application protection platforms (CNAPP), and extended detection and response (XDR) technologies, security teams continue to struggle to investigate and respond effectively to cloud threats. Cloud investigations are taking too long, enabling attacks to progress further and resulting in more disruption and damage. New strategies and solutions are needed.

Overview – The Problem

For decades, the security operations center (SOC) has been at the foundation of organizational security and risk mitigation. SOC analysts perform critical operations, helping to keep systems updated and handling the day-to-day monitoring of operational IT. In recent years, their responsibilities and mandates have expanded to support the rapid pace of cloud transformation. SOC teams must manage IT and business assets dispersed across multiple public cloud service providers (CSPs) and software-as-a-service (SaaS) applications.

Poor Cloud Threat Investigation

Security teams continue to struggle to investigate and respond effectively to cloud threats. 42% report that the complexity of the attack surface and the ephemeral nature of modern cloud workloads is not well supported by existing technologies.[1]

A series of new security solutions have emerged to address cloud security, including cloud security and posture management (CSPM) and, now, the broader category of CNAPP. Despite the rapid adoption of these solutions and the importance of the security problems they are addressing, there remains a gap in detection and response support within them.

Highlighting this gap is the concurrent growth of the XDR movement, which is addressing the broader complexity in the detection and response of advanced attacks across all facets of the attack surface. Recent research by TechTarget's Enterprise Strategy Group shows that a top-three use case for XDR tools selection is to improve cloud threat detection and response, illustrating the struggle that security operations teams are having with this new responsibility.[2]

Further compounding this challenge is the growing adoption of multi-cloud operating strategies. A recent Enterprise Strategy Group research study highlighted that most organizations are using three or more public cloud service providers and over 250 business applications.[3] The territory SOC teams now need to cover is vast.

[1] Source: Enterprise Strategy Group Research Report, *Cloud Detection and Response*, December 2023.
[2] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.
[3] Source: Enterprise Strategy Group Complete Survey Results, *2023 Technology Spending Intentions Survey*, November 2022.

Cloud Security Challenges

Pre-cloud, the use of on-premises identity and access management controls made it much easier for the SOC team to keep track of who was accessing what and where. Microsoft Active Directory and similar on-premises systems provided an easy pathway to track and investigate access within the on-premises enterprise. And since on-premises Microsoft Active Directory services have existed since 1999, the security world has spent multiple decades improving the process of monitoring and responding to on-premises incidents and security issues. Maintaining, monitoring, and analyzing local, on-premises application logs is both well understood and highly operationalized.

Cloud operating infrastructure changed all this. Applications no longer rely on on-premises controls. Cloud operating logs are now managed across individual cloud vendors and cloud application providers. Most SOC teams lack the access and visibility into the cloud forensic data needed for effective incident response.

Beyond access challenges, the volume and variety of cloud data is challenging to ingest and analyze. Further exacerbating the issue is the lack of standards across cloud providers, resulting in the need for additional manual effort to normalize and correlate data. And while many are ingesting some amount of cloud logs, identifying and locating which logs can provide the necessary level of detail is challenging across multiple CSPs. Adding further complexity, security teams must configure and operationalize custom alerts for individual CSPs and SaaS applications, requiring the teams to understand and keep up with each providers' formats and data structures over time.

So, despite ongoing investment in tools such as SIEM, SOAR, and XDR technologies, security teams are still struggling to capture the signals needed to investigate and respond to cloud threats. Adding to the challenge, many SOC workflows still depend heavily on manual investigation, which is not scalable in cloud environments. A lack of automation and orchestration creates delays and gaps.

Summarizing the Five Gaps in Cloud Security

As security teams strive to detect and respond to threats across multiple public CSPs and SaaS applications, they must overcome five key challenges:

1. **Lack of visibility into cloud forensics and logs.** There is limited visibility into cloud infrastructure as compared with that of on-premises environments. Critical logs, such as S3 bucket access logs, are not enabled by default and are often not collected. And even if they are collected, they aren't maintained for long enough periods to support investigations.
2. **Integration challenges across fragmented logging.** Logs from different cloud providers and SaaS platforms are stored in different formats. Integrating and normalizing this data is difficult.
3. **Limited detection capabilities for cloud threats.** Many security tools are focused on prevention and lack real-time detection and response capabilities tailored for cloud environments, which is compounded by limitations in log recording and streaming.
4. **Identity management challenges.** With the move to cloud, identity has become the new perimeter, enabling attackers to move from "breaking into" to "logging in." Many SOC teams lack the identity visibility that on-premises Active Directory provides. Further complicating this issue is that different identity providers offer different log coverage and different event reporting. And while the on-premises identity was mostly through Microsoft Active Directory, the cloud identity realm offers multiple vendors with various solutions.

Gaps Continue in Cloud Security

Despite investments made in SIEM, SOAR, and XDR, cloud investigation and response capabilities are still lacking.

5. **Gaps in cloud security skills and experience.** Many teams lack experience responding to cloud attacks and analyzing logs from various cloud services. While today's security professionals have decades of materials and experiences using on-prem technology to learn from, cloud technology is still in its infancy. This lack of experience slows down incident investigation and response.

Are CSPM and CNAPP Enough?

Reducing the time to cloud detection and remediation can dramatically reduce risk. Investigation requires a detailed understanding of what happened. Any gaps in visibility translate into delays in containment and remediation.

Forensic investigations in the cloud require the collection and analysis of cloud logs to understand attacker activity, including what files were accessed and how attackers got in. Security data across multi-cloud infrastructure must be both available and normalized for analysis.

CSPM tools have become increasingly popular—and with good reason. The posture management capabilities a CSPM provides can help an organization better understand cloud configuration to prevent potential security incidents. The basic idea is that a CSPM will monitor how secure an organization's cloud environment is so that breaches won't happen. CNAPP solutions are subsuming CSPM, consolidating additional cloud security functions.

CSPMs Aren't Enough

CSPM and CNAPP platforms are designed to highlight problems, errors, and security risks related to an enterprise's current cloud configurations or workloads. But when something happens, a CSPM can't investigate the whole cloud attack lifecycle or help determine the blast radius.

CSPM and CNAPP platforms are designed to highlight problems, errors, and security risks related to an enterprise's current cloud configurations or workloads. But when something happens, a CSPM can't investigate the whole cloud attack lifecycle or help determine the blast radius. Further, CSPM lacks the ability to secure SaaS application use.

In today's escalating cloud threat landscape, it's not enough to fix misconfiguration. Security teams must be able to fully investigate the threat and quickly get answers to questions such as, "Did an incident take place?" "If so, how did the attacker get in?" "Where did the attacker go while inside?" "What did they take?"

Despite organizations deploying CSPM or CNAPP technologies, cloud and SaaS security breaches are still happening. It's a situation that is somewhat reminiscent of the earliest era of internet security, when everyone had antivirus technology but systems still got malware and were breached. No preventative system, no matter how robust, can fully eliminate cloud breaches, so it is important to catch them quickly and contain them in order to minimize impacts.

Is XDR the Answer?

XDR solutions are quickly being adopted to help security teams improve the detection of advanced attacks, speed up investigations, and respond faster. Recent Enterprise Strategy Group research shows that closing cloud visibility gaps is a top-five requirement when selecting an XDR solution,[4] demonstrating both the need for and belief in XDR to help organizations better secure cloud resources.

[4] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

Yet, while XDR solutions have been adopted by nearly two-thirds of organizations, Enterprise Strategy Group research shows that closing specific gaps in cloud detection and response capabilities is still a top-five challenge,[5] demonstrating that, for many, XDR solutions are falling short in meeting the needs for this growing part of the attack surface.

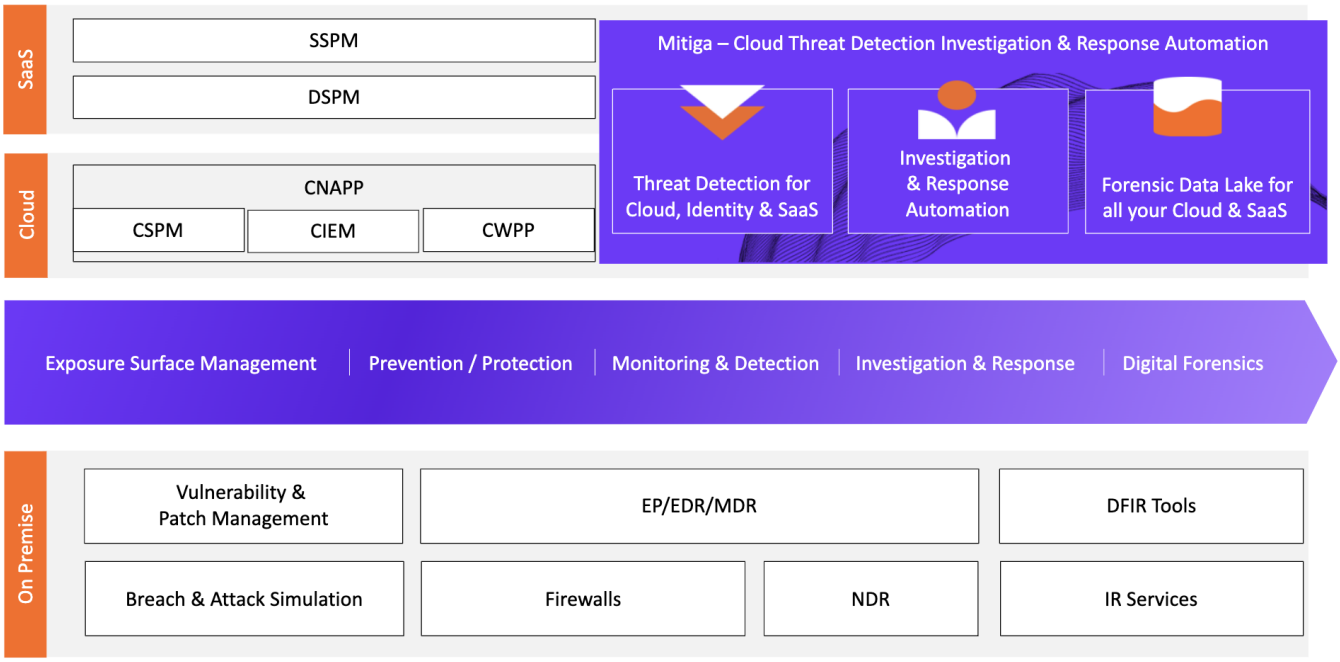
Closing the Cloud Security Gap – Introducing Mitiga

Mitiga provides the industry's only cloud investigation and response automation (CIRA) solution, which was built to help security teams speed up SOC decision-making, minimize breach impact, and enhance enterprise cyber resilience (see Figure 1). Mitiga proactively and continually gathers, retains, and analyzes all cloud application log data required for investigation, providing critical context, including the full scope of compromise. By using advanced techniques such as anomaly detection, behavioral analysis, and threat intelligence, Mitiga helps identify and eliminate threats that evade existing security controls.

Mitiga further supports threat hunting, helping security teams proactively search for signs of malicious activity within cloud environments—before damage or data loss occurs. By empowering teams with knowledge of the tactics, techniques, and procedures used by attackers, this context-informed threat analysis enables and dramatically accelerates incident response, lowering breach impact.

New solutions that close the CSPM, CNAPP, and XDR gaps and that can provide teams with deep cloud investigation and response capabilities are needed. And these solutions need to do this without requiring deep cloud incident response knowledge. To close the cloud security gap, SOC teams need solutions that provide unified visibility, focus on detection and response, automate cloud data ingestion and analysis, and augment staff with cloud security expertise.

Figure 1. Mitiga Closes the Cloud Security Gap



Source: Mitiga Security.

[5] Ibid.

Conclusion

Defending cloud infrastructure and applications is a top priority for security operations teams. Despite investments in upgrading detection and response tools infrastructure, security teams continue to struggle to gain the visibility and security data needed to investigate and respond to threats involving cloud resources.

The cloud operating model is fundamentally different than traditional on-prem operating models, making it difficult for traditional security operations tools to support investigation and response. Modern SOC teams that gain the understanding and tooling to fully manage their organization's cloud and SaaS security set themselves up for greater success and set their enterprises up for a higher level of risk mitigation and resilience.

New security solutions have emerged that capture and analyze the cloud telemetry necessary to support raid cloud incident investigation and response. Enterprise Strategy Group recommends that security and cloud technology leaders investigate solutions from vendors like Mitiga that provide technologies and services to help security teams operationalize effective cloud security operations.

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