SEACOAST CYBERSECURITY GROUP (CSSCG) WHITE PAPER

Modern Cloud Detection and Response (CDR) for Breach Containment and Cyber-resilience

By Jon Oltsik, Principal Security Researcher

July 2025

This White Paper was commissioned by Illumio and is distributed under license from SCCSG.

Contents

Executive Summary

The recent onslaught of cloud-based applications and infrastructure has fundamentally reshaped modern enterprise IT, offering unparalleled agility, scalability, and cost efficiencies. However, this transformative shift has simultaneously exposed organizations to increasing numbers of cyber threats, making robust cloud security an imperative, not an option. The sheer volume and nature of these threats—ranging from misconfigurations and insecure APIs to costly data breaches and ransomware, pose a significant and growing risk to business processes, financial stability, and reputational integrity.

In this heightened threat landscape, a comprehensive and proactive approach to cloud threat prevention, detection, and response is no longer merely a best practice; it is a critical business necessity. This white paper concludes that organizations must prioritize:

- **Proactive threat prevention:** Implementing rigorous zero trust and microsegmentation controls is paramount. This involves adopting a "never trust, always verify" mindset, denying all communication by default, and allowing only explicitly authorized traffic between workloads. The goal should be to continuously minimize the attack surface.
- **Real-time threat detection:** Robust security requires ongoing**,** AI-driven visibility into all infrastructure and application activities and network traffic flows. Ingesting large amounts of observability and security data requires a security graph database to classify resources, identify anomalous behaviors, pinpoint sophisticated lateral movement, and uncover cyber-attacks in progress. The goal? Contain breaches, reduces the Mean Time to Detect (MTTD), and create a cyber-resilient hybrid IT and multi-cloud environment.
- **Rapid Threat Response:** Beyond detection, organizations need to contain and remediate security as quickly as possible. Rather than rely on cross-departmental workflows and incongruent IT and security tools, security teams need automated response capabilities to contain breaches, limit an attack's "blast radius," minimize damage, and promote cyber-resilience.

Achieving an enhanced level of threat prevention, detection, and response will require a new type of platform specifically built for breach containment and cyber-resilience. Since cloud-based infrastructure and application have become the center of the IT universe, CISOs should think about anchoring their security operations with a modern CDR platform architecture capable of real-time threat prevention, detection, and response across hybrid IT and multi-cloud environments.

The Cybersecurity Paradox

According to Gartner, worldwide spending on information security is expected to reach $212 billion in 2025, marking a 15.1% increase from $183.9 billion in 2024. This increase is driven by a multitude of factors, including application/workload proliferation, increasing use of security services, and as a countermeasure to increasingly sophisticated threats. Despite this massive investment, however, nearly all organizations still face constant cybersecurity incidents, including breaches, ransomware, and data exfiltration. For example:

- Among large enterprises (revenue over $1 billion), 40% reported a recent cyberattack resulting in a security breach. (source: KPMG)
- 44% of organizations have experienced a cloud data breach due to factors like human error, exploitation of known vulnerabilities, and a failure to implement MFA (source: Thales Cloud Security Study)
- According to the FBI Internet Crime Complaint Center, cybercrime losses reached a record $16.6 billion in 2024, marking a 33% increase from 2023. This surge was primarily driven by low-tech scams such as investment frauds and phishing attacks.

Numerous research studies also indicate that cyber-attacks have become particularly focused on cloud infrastructure and cloud-based applications. For example, 81% of organizations experienced at least one cloud security incident over the past year (source: TechMagic 2025 Cybersecurity Statistics), and 80% report an increase in the frequency of cloud attacks (source: SentinelOne 2025 Cloud Security Statistics). Since organizations are accelerating development and deployment of cloud-based business-critical applications, CISOs should be particularly concerned about these alarming trends.

Security Challenges Remain Pervasive

Why are organizations spending more while still suffering from a never-ending stream of cybersecurity events and data breaches? Industry research indicates that despite massive investment, enterprises still face numerous cybersecurity challenges including:

- **Limited visibility and blind spots.** According to DuploCloud, 67% struggle with limited visibility into their cloud infrastructure, hindering threat detection and response.
- **Tools sprawl.** A 2024 CDW survey found that 68% of organizations manage between 10 to 49 security tools, with 40% reporting difficulties in integrating these tools effectively. Tool sprawl is especially pronounced in areas like security operations and cloud security, causing a disconnect between threat prevention, detection, and response processes and actions. These tools that were purpose-built for either cloud or on-premises security are contributing to the security blind spots.
- **Cybersecurity resilience issues.** In the World Economic Forum's Global Cybersecurity Outlook 2024, only 19% of executives felt their cyber resilience "exceeds our requirements," while 36% felt it "meets minimum requirements" and 51% felt it was "insufficient." This reflects low confidence in current capabilities.

While these challenges are pervasive across all IT infrastructure, they are pronounced in the cloud due to the rapidly changing nature of cloud-based applications and workloads, leading to issues like misconfiguration**,** vulnerabilities**,** overly permissive administrator accounts, and exposed data. This is yet another reason cloud-based infrastructure and applications are such an attractive target.

Cloud Detection and Response (CDR) to the rescue?

Since cloud-based infrastructure and applications remain a cybersecurity weak link, many organizations have adopted or plan to adopt CDR and cloud security posture management (CSPM) tools to bridge this gap. This seems like a sound decision. CSPM tools can help organizations enhance visibility, improve regulatory compliance, and identify vulnerable assets. CDR systems can complement CSPM by detecting unauthorized changes, integrating with threat intelligence, and using detection rules or artificial intelligence (AI) to spot anomalous, suspicious, or malicious behavior. This is especially useful when monitoring for things like crypto mining/jacking, lateral movement between cloud and on-premises environments, cloud identities, and Kubernetes/container security.

At first glance, CDR seems to address many of the security challenges described above. Unfortunately, existing CDR tools also have some limitations. Security professionals complain that CDRs:

- **Minimize application-level monitoring.** CDR tools tend to focus on cloud infrastructure, like virtual servers, APIs, and cloud identities. While cloud infrastructure monitoring is important, CDR tools may suffer from application blind spots, missing threats like code injection and zero-day exploits. This omission provides a wide-open door for adversaries to attack cloud-based applications directly.

- **Can be extremely noisy.** CDR tools rely on agents or logs which tend to generate a lot of data. Thus, CDR relies on AI or static rules to filter data, but many CDR tools remain immature in this area. The result? Alert storms that make it difficult for analysts to find critical signals within the overwhelming volume of noise.

- **Ignore on-premises applications and infrastructure.** While many CDRs claim to have multi-cloud support, some tools struggle to attain consistent monitoring from different logging formats, APIs, and security controls across disparate cloud service providers (CSPs). Given this, threat detection and policy management can be difficult at best. CDR traditionally lacked any visibility within on-premises applications and assets, forcing organizations to have multiple tools across hybrid infrastructure. This makes it especially difficult to detect ‘cloud-to-ground’ attacks that begin with cloud footing with the exploitation of a cloud asset (ex. vulnerable software, misconfiguration, open storage repository, etc.), establish cloud persistence, move laterally to on-premises assets (the ground shift), perform on-premises reconnaissance, and finally, achieve an operational breach objective.

- **Offer limited response capabilities.** Once an attack is detected, CDR responses are extremely limited with actions like isolating a VM or blocking an IP address. These actions may miss ongoing malicious activities at the application layer, or complex multi-staged attacks that anticipate and circumvent minor CDR countermeasures.

Aside from these shortcomings, some CDR tools miss the bigger picture of a cyber-attack. In other words, they may detect individual malicious tactics but cannot link individual actions to an entire attack path or multi-staged cyber-attack in progress to reduce alerts and prioritize risks. Finally, some CDRs are designed with an assumption that security teams have advanced cloud knowledge. This makes them complicated for security teams to deploy or administer.

Toward Cyber-resilience and Breach Containment

Given the current limitations of CDR tools, CISOs must adhere to time-tested advice – Caveat Emptor. Organizations must do more to prepare themselves for inevitable incidents by prioritizing threat prevention, improving management of the attack surface, accelerating threat and exposure detection, and decreasing the mean time to remediate discovered issues. Rather than relying on CDR functionality alone, organizations should make actions part of a comprehensive breach containment strategy.

Accomplishing these goals demands a more comprehensive CDR platform architecture with contextual visibility across cloud and on-premises applications and infrastructure. Modern CDR should span prevention, detection, and response, and include:

- **A comprehensive real-time view of multi-cloud and hybrid applications and infrastructure.** Rather than continue to have application, cloud, or on-premises blind spots, a modern CDR platform architecture must have 'north/south' (i.e., across clouds and between cloud and on-premises infrastructure and applications) and 'east/west' (i.e., infrastructure and applications) visibility. This demands monitoring and interpreting a full understanding of identities, assets, flows, connections, and application behavior at all times. Technical views must be enriched with third-party inputs (i.e., from IT and security systems) and supplemented with an appropriate level of business context (i.e., who owns each asset, asset business value, asset location, etc.). Of course, understanding the relationship between assets and asset characteristics in real-time requires a highly scalable graph database capable of modeling the environment, benchmarking normal behavior, and then detecting anomalous, suspicious, or malicious behavior. Note that the best CDR platform architectures will have active 'hooks' into on-premises applications and infrastructure for rapid detection and response to 'cloud-to-ground' attacks.

- **Continuous security controls management**. Complementing policy management described above, modern CDR solutions should provide continuous security controls management as well (i.e., modifying security controls based on emerging threats, configuration changes, etc.). This should enable a zero trust model for managing the attack surface, setting up trust relationships between assets, and creating an environment in support of the least privilege principle. Security controls must be continuously monitored and then adjusted in response to new types of vulnerabilities, threats, or business requirements. If a breach occurs in one segment, (i.e., within a network segment dedicated to business application resource such as a database, storage resource, or container), it should be limited to that specific area, preventing lateral movement of threats (like ransomware) across the entire network.

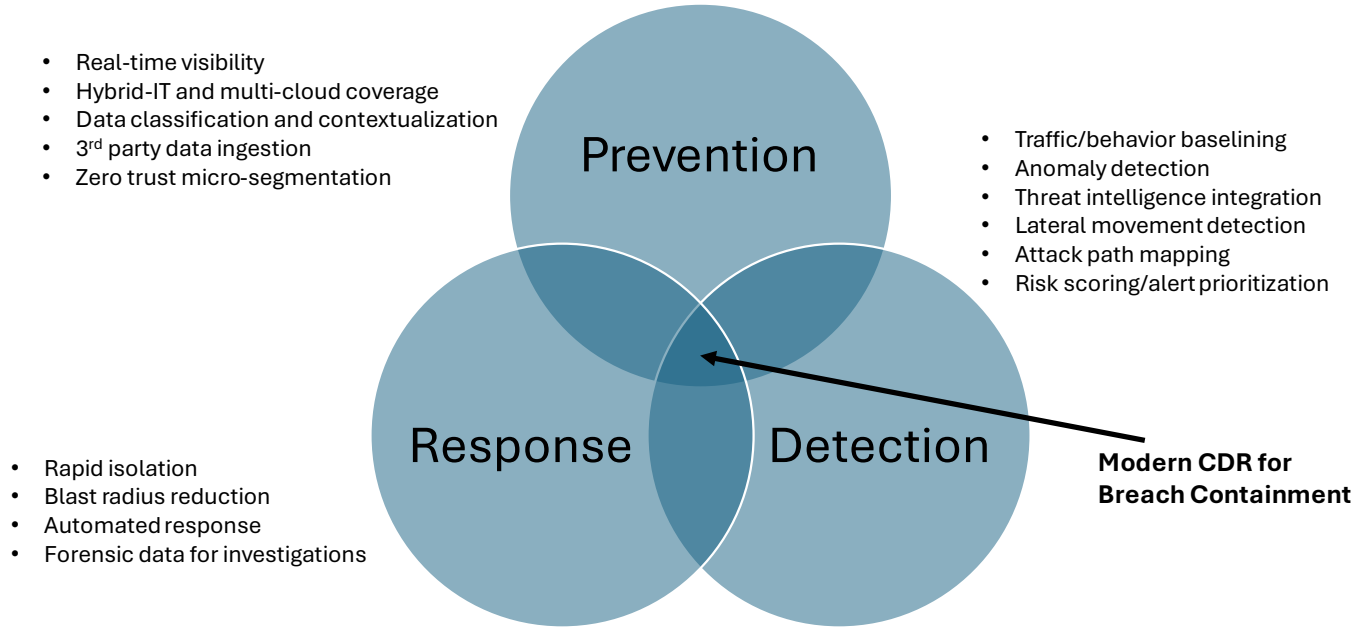
- **Vigilant monitoring and enhanced analysis for threat detection.** Beyond threat prevention, modern threat detection and response must bring together and monitor network traffic and asset activities to quickly detect anomalous/malicious/suspicious behavior and generate synthesized and accurate alerts (rather than alert storms and false positives). Threats must then be analyzed and enriched with appropriate threat intelligence to assess whether they are consistent with known adversaries, campaigns, or adversary tactics, techniques, and procedures (TTPs). Upon threat detection, leading CDR solutions will also provide thorough threat details, including timelines, attack path mapping, TTP alignment with the

MITRE ATT&CK framework, all the Indicators of Compromise (IoC) that created the contextualized alert, and risk scoring/prioritization. This will require advanced technical capabilities like stream processing, as well as strong AI capabilities in areas like machine learning and behavior analysis for detecting anomalous traffic patterns that could indicate an attack in progress.

- **Simple but thorough breach containment capabilities, including automation.** Cyber-resilience and breach containment depend upon a rapid transition from accurate incident detection to urgent response. As previously stated, this is where traditional detection-and-response limitations may block specific adversary tactics but lack the intelligence to piece together all the components of a cyber-attack in progress. Once a threat or risky behavior is identified, modern CDR should provide for dynamic quarantine of affected workloads, including across different cloud and on-premises environments – either with simple human-in-the-loop or automated capabilities. In this way, modern CDR can be used to quickly quarantine compromised resources, thus reducing the "blast radius" of a breach – or stopping it in its tracks.

- **Easy policy visibility and management.** Beyond cloud detection and response, organizations should complement CDR by mapping policies to application behavior, facilitating micro-segmentation that blocks all malicious and unauthorized traffic. This function should highlight ease-of-use with visual representations of what traffic is allowed and where policies may be fragile or conflict with business processes. Policy management should also enable organizations to model and test policies before they are put into enforcement mode. In this way, security teams can improve security while reducing the risk of disrupting business operations or breaking applications. These capabilities are especially useful when they can map policies across hybrid IT and multi-cloud environments.

Figure 1. Modern CDR Spans Prevention, Detection, and Response



Source: Seacoast Cybersecurity Group.

To ease deployment and accelerate time-to-value, modern breach containment solutions should be able to discover all elements of hybrid IT without the need for agent deployment or architectural changes. In other words, modern threat detection and response should deploy and deliver results in hours – not days or weeks. Beyond core prevention, detection, and response, modern tools should also support diverse security use cases like assessing risky traffic, enabling threat hunting, and identifying potential data exfiltration.

The Illumio Platform for Breach Containment and Modern CDR

While lots of security point tools can be used to address some of the tactical breach containment requirements defined above, few if any offer a true platform offering comprehensive coverage for prevention, detection, and response. Illumio is an exception to this limitation. The Illumio Platform is designed to achieve cyber resilience by stopping the spread of breaches across hybrid and multi-cloud environments. In this way, the Illumio Platform is built with an “assume breach” mindset, focusing on breach containment.

Aligning with cyber-resilience, Illumio spans:

- **Threat prevention.** Illumio’s primary prevention mechanism is Illumio Segmentation which is used for continuous and granular microsegmentation. Segmentation models are based on things like application dependency mapping, consistent policy mapping across hybrid IT and multi-cloud environments, and specific policy enforcement. Through microsegmentation, Illumio can help organizations reduce the attack surface and mitigate cyber-risk.

- **Threat detection.** Illumio recently extended its platform with the introduction of Illumio Insights – a modern AI CDR. Insights ingests network flow and resource data from all managed workloads, classifies and contextualizes this data, and adds the data to its AI security graph database. By using AI, Illumio Insights can then identify risky traffic, anomalous behavior, lateral movement, and other activities that could indicate a cyber-attack in progress. To help organizations prioritize and address their highest risks, Insights delivers context-rich alerts and attack path mapping.

- **Threat response.** With its integrated microsegmentation engine, Insights can isolate compromised workloads, drastically reducing the blast radius of an attack, even across different environments. Complex actions can be executed by security analysts while simple risk mitigation remediation can be programmed as automated responses.

In summary, the Illumio Platform offers a broad solution for breach containment across hybrid IT and multi-cloud visibility, AI-powered threat detection, and granular segmentation for cyber-risk management and incident response.

Summary

When it comes to cybersecurity, it is not hyperbole to suggest that the world grows more dangerous every day. Several studies suggest that if cyber-crime were measured as a country's GDP, it would represent the world's third largest economy. Aside from cyber-criminals, organizations must also defend against state-sponsored adversaries, hacktivists, and even malicious insiders.

Unfortunately, cybersecurity seems like it is often 'one step forward, two steps back' for defenders. CISOs spend on new security technology countermeasures to thwart the latest threats, only to face the complexity of point tool solutions, difficult technical integration, manual processes, and staffing/skills shortages.

What is needed? Comprehensive breach containment solutions that span threat prevention, detection, and response across hybrid IT and multi-cloud environments. Through breach containment solutions like those described above, organizations can enforce zero trust policies to reduce their attack surface, rapidly detect anomalous/suspicious/malicious behavior, and respond quickly to minimize business disruption. CISOs should seek out vendors that cover all these requirements.