Prepared for

ALLUVIO IQ

From Complexity to Clarity: Resolving Challenges in Cybersecurity Observability

May 2023 EMA White Paper

By **Ken Buckler, CASP**, Research Analyst
Information Security, Risk and Compliance Management

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Challenges Today's Enterprises Face

Network Complexity

Network complexity presents significant challenges for observability in cybersecurity. With the increasing number of devices, endpoints, and applications connected to networks, it becomes difficult to gain comprehensive visibility into network activities. Complex networks often lack standardized monitoring practices, making it challenging to observe and detect security threats consistently. Additionally, the dynamic nature of modern networks—with devices joining and leaving the network frequently—as well as remote devices and multiple distributed sites further complicate the observability process. Network administrators and security teams face the daunting task of managing and correlating vast amounts of data these networks generate to identify potential threats accurately. Achieving effective observability in complex networks requires robust monitoring solutions, advanced analytics, and automation to ensure timely threat detection and response. This complexity further compounds the other challenges today's large, distributed enterprises already face.

Volume of Data

Upcoming EMA research found that, due to the volume of data observability solutions process, 48% of organizations are forced to only store a subset of their data for analysis and 37% of organizations had to discard most of their observability data due to the volume of that data.[1] The exponential growth of data poses significant challenges for observability in cybersecurity. Networks generate vast amounts of data from various sources, including network devices, applications, and logs. Analyzing and processing this large amount of data in real time to detect security threats is a daunting task. It requires powerful computational resources, advanced analytics, and efficient data storage and retrieval mechanisms. Additionally, data overload can lead to information overload, making it challenging to extract meaningful insights and identify potential threats. Implementing effective observability strategies involves leveraging scalable data collection and analysis techniques, leveraging machine learning and artificial intelligence algorithms, and deploying efficient data management systems to handle the ever-increasing data volume that networks generate.

[1] EMA, "Observability in Today's Hybrid Multi-Cloud Environment" Q3 2023.

Lack of Visibility

Even with the tremendous volume of data being generated, the lack of full visibility poses significant challenges for observability in cybersecurity. This challenge was especially highlighted in 2023 EMA research, in which 75% of organizations responded that they only have full visibility into 40% or less of their technology stack, creating huge gaps in observability.[2] In many cases, devices and applications may not have sufficient logging or monitoring capabilities, making it difficult to observe their behavior and detect security threats. Without proper visibility, network administrators and security teams are unable to gain comprehensive insights into network activities, leaving blind spots that attackers can exploit. Addressing this challenge requires implementing better monitoring practices across the network, deploying robust logging mechanisms, and leveraging network visibility tools and technologies. Enhancing observability by improving visibility allows for timely detection of anomalies, faster incident response, and better overall network security posture.

Building Business Resiliency Through Integration With Existing Security Tools

Building business resiliency requires the integration of observability with existing security tools. By doing this, organizations can gain a comprehensive view of their systems and networks, enabling proactive threat detection and response. Integrating observability with security tools allows for the correlation of monitoring data, logs, and events across various systems, providing a holistic perspective on security incidents. This integration enhances incident investigation and response by enabling security teams to identify the root cause of issues quickly and take appropriate action.

Moreover, the integration of observability and security tools facilitates automation and orchestration of security processes. By leveraging observability data, organizations can develop automated incident response workflows and playbooks, streamlining incident handling and reducing response times. This integration also allows for real-time threat intelligence sharing, enabling security tools to leverage observability data to identify and block emerging threats effectively.

[2] EMA, “Observability in Today’s Hybrid Multi-Cloud Environment” Q3 2023.

Security Tools Need Observability Data

Availability – The Forgotten Pillar of Cybersecurity

Availability is an often-overlooked pillar of cybersecurity, overshadowed by the more commonly recognized principles of confidentiality and integrity. While confidentiality ensures data privacy and integrity focuses on data accuracy and consistency, availability ensures that systems and resources are accessible and operational when needed. It ensures that critical services and data are consistently available to authorized users, preventing disruption to business operations.

Unfortunately, availability and performance are often considered the sole responsibility of IT operations teams. However, this mindset is misguided. Availability and performance are integral to the overall cybersecurity posture of an organization. Downtime or degraded performance can lead to significant financial losses, reputational damage, and legal implications. Cyberattacks targeting availability, such as distributed denial of service (DDoS) attacks or ransomware, can cripple businesses by rendering services inaccessible or holding critical data hostage. These attacks highlight the importance of ensuring resilient systems and networks that can withstand such threats and quickly recover.

In today's interconnected enterprises, availability now intersects with user experience, customer satisfaction, and revenue generation. In an increasingly interconnected world, organizations rely on digital platforms to deliver services and products. If these platforms suffer from performance issues or downtime, customers may seek alternative solutions, leading to revenue loss and damage to brand reputation. To address the availability challenge, organizations must adopt a holistic approach that integrates cybersecurity, IT operations, and business objectives.

The Advantages of Tool Consolidation

EMA found that 46% of organizations have between six and 10 observability/monitoring solutions in their environment.[3] Not only are each of these tools expensive, with continuing maintenance costs and infrastructure, but switching between tools can be extremely time-consuming for analysts. Cybersecurity and IT operations tool consolidation offers significant advantages for observability, resulting in labor cost and time savings—but beyond cost savings, by consolidating various tools into a unified platform, organizations can also streamline data collection, storage, and analysis, eliminating the need to duplicate efforts and collect data separately for different purposes.

[3] EMA, "Observability in Today's Hybrid Multi-Cloud Environment" Q3 2023.

Tool consolidation reduces complexity. Having multiple disparate tools for cybersecurity and IT operations can create a fragmented view of the environment. Consolidation provides a centralized and holistic view, enabling better correlation and analysis of data. It eliminates silos, enhances data sharing and collaboration between teams, and promotes a more efficient incident response process. Furthermore, consolidating observability tools minimizes duplication of data collection efforts. Instead of collecting and storing data separately for cybersecurity and IT operations, a single integrated platform can gather and store data once, making it available for multiple purposes. This not only saves time and effort, but also reduces the storage requirements and associated costs.

Consolidation also enables better data analysis and cross-domain insights. When cybersecurity and IT operations data are combined in a single platform, not only can tools with duplicate coverage be eliminated, but it also becomes easier to identify correlations and patterns that might indicate security threats or performance issues. These insights enable proactive measures to prevent potential incidents and optimize system performance. Moreover, consolidated tools often provide advanced analytics capabilities by leveraging machine learning and artificial intelligence techniques. These technologies can process large volumes of data more effectively, identify anomalies, and provide real-time alerts for potential security breaches or operational abnormalities.

How Alluvio IQ Delivers Unified Observability

Scalable Access to Full-Fidelity Data

One of the most important features of Alluvio IQ is its ability to provide access to full-fidelity data at scale. Having scalable access to full-fidelity data is crucial for observability in cybersecurity and performance monitoring. Full-fidelity data refers to comprehensive, unaltered data that captures all relevant information about network activities, system behavior, and security events. Scalable access to such data ensures that organizations can effectively monitor, analyze, and detect anomalies or security and performance threats across their systems. It allows for in-depth visibility into network traffic, application logs, user behavior, and system performance, enabling proactive identification of potential issues.

By having full-fidelity data at scale, organizations can perform detailed forensic investigations, better trace the root causes of incidents, and analyze the complete context of security events. This comprehensive understanding is essential for effective incident response and accurate threat detection. Furthermore, scalable access to full-fidelity data enables the application of advanced analytics techniques, such as machine learning and anomaly detection, to detect patterns, correlations, and irregularities that may indicate malicious activity or system irregularities.

Machine Learning & Correlation for Easier Identification of Events

Machine learning (ML) plays a vital role in Alluvio IQ's correlation and identification of events to enhance observability in cybersecurity. ML algorithms can analyze large volumes of data, identify patterns, and establish correlations between events that may not be apparent through manual analysis. This automated correlation enables the identification of complex attack sequences or suspicious behaviors that may indicate security threats. Moreover, ML-based approaches consider the context of events, considering various factors such as user behavior, system configurations, and historical data. Understanding the context helps in distinguishing between legitimate activities and potential threats, reducing false positives and false negatives.

This correlation and contextual analysis addresses alert fatigue, a significant challenge security analysts face when overwhelmed by a high volume of alerts. ML-based event correlation allows for the prioritization of alerts based on their relevance and potential impact. Filtering and consolidating alerts reduces noise and enables analysts to focus on critical incidents, improving response times and resource allocation. The combination of ML and event context provides a more accurate and efficient approach to observability, enabling organizations to detect and respond to security threats effectively while minimizing alert fatigue and optimizing the use of valuable security resources.

Automating the Collection of Diagnostic Insights

Alluvio IQ's collection of diagnostic insights is crucial for effective observability in cybersecurity. By automating the process, organizations can efficiently gather information on key aspects, such as availability, latency/performance, and misconfigurations and routing issues. Automated collection of availability data enables continuous monitoring of systems and services to ensure they are accessible and operational. It allows for immediate detection of downtime or service disruptions, supporting prompt remediation and minimizing business impact.

Collecting data on latency and performance metrics helps identify bottlenecks, network congestion, and/or application performance issues. Automated collection of such data facilitates the identification of performance degradation, allowing organizations to proactively optimize their systems and enhance user experience. Additionally, automating the collection of data related to misconfigurations and routing issues helps organizations to swiftly identify and rectify configuration errors, network misalignments, or vulnerabilities. It enhances security posture by reducing the window of exposure to potential attacks and improving overall network reliability.

By automating the collection of these diagnostic insights, organizations can achieve real-time visibility into the health and performance of their systems. This proactive approach allows for quicker issue identification and resolution, enhancing overall observability and assisting with more effective incident response.

Working Within the Customer Ecosystem

Flexible APIs Facilitate Integration

Working within the customer ecosystem requires seamless integration with various tools and systems. Flexible application programming interfaces (APIs) play a vital role in enabling this integration, facilitating smooth communication and data exchange between different platforms and applications. Flexible APIs allow organizations to connect their cybersecurity solutions with existing customer systems, such as network infrastructure, security information and event management (SIEM) platforms, or incident response systems. These APIs provide a standardized and programmable interface that facilitates data sharing, event correlation, and coordinated incident response.

By leveraging flexible APIs, organizations can easily integrate their cybersecurity solutions into the customer ecosystem, enhancing overall observability and threat detection capabilities. It aids in the aggregation of data from multiple sources, such as logs, alerts, or network traffic, into a centralized platform, providing a holistic view of the security landscape. Flexible APIs also support customization and extensibility, allowing organizations to tailor the integration to specific customer requirements. It generates a seamless exchange of information, contextual data, and automated workflows between different systems, promoting efficient collaboration and incident response.

Pull Data From Security and Other Third-Party Solutions

By pulling data through APIs from endpoint protection, firewall logs, intrusion detection systems, or vulnerability scanners, aggregated data provides a comprehensive view of the security landscape, enhancing proactive threat detection capabilities. Furthermore, pulling data from third-party solutions beyond security, such as cloud infrastructure, network monitoring, or application performance management tools enriches observability capabilities. This broader scope enables organizations to correlate security events with network performance, system health, or application behavior, facilitating the identification of potential security vulnerabilities or anomalies.

Through this data collection, organizations can centralize and analyze diverse datasets, gain cross-domain insights, and establish comprehensive situational awareness. Such an integrated approach to observability empowers security teams to make informed decisions, prioritize incidents, and respond effectively to emerging threats.

Push Actionable Insights to Security and Other Third-Party Solutions

Pushing actionable insights through APIs to security and other third-party solutions is crucial for enabling better observability and automated forensics. By utilizing APIs, organizations can empower proactive actions and improve overall security effectiveness. These actionable insights can be pushed to security solutions, such as SIEM platforms, endpoint protection systems, or incident response tools, improving incident response capabilities through real-time alerting.

Furthermore, pushing actionable insights to third-party solutions beyond security, such as IT service management tools or ticketing systems, facilitates the integration of security incidents into broader organizational workflows. It streamlines incident response processes, enhances collaboration between security and IT teams, and accelerates the resolution of security issues. Pushing insights to cybersecurity tools also empowers automated forensics through relevant data for forensic analysis tools or incident investigation platforms. This streamlines the ability of organizations to understand root causes and impact of security and performance incidents more effectively.

EMA Perspective

Overcoming Challenges in Today's Environment

Modern cybersecurity faces a range of challenges that IT leaders must overcome to ensure effective observability and threat detection. One such challenge is the complexity of networks, which feature numerous devices, endpoints, and applications. This complexity hinders consistent monitoring and threat detection, necessitating standardized practices, advanced analytics, and automation.

The exponential growth of data volume that network devices and applications generate presents another hurdle. Analyzing and processing this data in real time is a formidable task, demanding scalable data collection, storage, and analysis techniques and advanced technologies, like machine learning.

Insufficient logging and monitoring capabilities in certain devices and applications contribute to a lack of visibility, resulting in blind spots for threat detection. Addressing this challenge involves implementing standardized monitoring practices and utilizing network visibility tools to enhance observability.

Integrating observability with existing security tools is vital for a comprehensive security posture. However, the complexity and diversity of security technologies pose integration challenges. Overcoming this obstacle requires careful planning, ensuring interoperability, and leveraging automation and orchestration capabilities.

To tackle these challenges, organizations must invest in comprehensive observability solutions, such as Alluvio IQ, that encompass real-time monitoring, advanced analytics, and automation. By implementing standardized monitoring practices, utilizing efficient data processing technologies, enhancing visibility through logging and monitoring, and integrating observability with existing security tools, organizations can bolster threat detection, incident response, and overall cybersecurity resilience.

Benefits of Riverbed's Approach

Alluvio IQ offers a comprehensive set of features that effectively address today's challenges of observability in cybersecurity. Its scalable access to full-fidelity data ensures organizations can efficiently collect, store, and analyze comprehensive and unaltered data. By having access to complete data sets, organizations can achieve a holistic view of their network activities, system behavior, and security events, enabling effective threat detection and incident response.

Leveraging machine learning (ML) and correlation techniques to facilitate the identification of events allows Alluvio IQ to analyze large volumes of data, detecting patterns and establishing correlations between events that might be challenging to identify manually. This automated correlation improves the accuracy of threat detection, enabling organizations to pinpoint complex attack sequences or suspicious behaviors that may indicate security threats.

By automating the collection process of diagnostic insights, Alluvio IQ allows organizations to gather crucial information on availability, latency/performance, and misconfigurations/routing issues. This data gathering streamlines monitoring and troubleshooting processes, enabling proactive identification of issues, efficient incident response, and optimized system performance.

Finally, Alluvio IQ's flexible APIs allow the push or pull of data to/from other systems, such as SIEM platforms, incident response tools, or IT service management systems. This integration facilitates the exchange of actionable insights, streamlines incident response workflows, and enables efficient collaboration across different teams and tools. Combined, these powerful features enable organizations to achieve comprehensive observability, enhance threat detection capabilities, streamline incident response processes, and optimize their cybersecurity resilience.

About Riverbed

Riverbed is the only company with the collective richness of telemetry from network to app to end user. Such telemetry illuminates, then accelerates, every interaction so organizations can deliver a seamless digital experience and drive enterprise performance. Riverbed offers two industry-leading portfolios: Alluvio by Riverbed, a differentiated unified observability portfolio that unifies data, insights, and actions across IT so customers can deliver seamless, secure digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app over any network to users anywhere. Together with our thousands of partners and market-leading customers globally – including 95% of the Fortune 100 – we empower every click, every digital experience. Learn more at **riverbed.com**

Riverbed, Alluvio, and certain other terms used herein are trademarks of Riverbed Technology LLC. All other trademarks used herein belong to their respective owners.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com** 4290.053023