SANS

Analyst Program

Spotlight

Shining a Light in the Dark: Observability and Security

Written by **Matt Bromiley**

March 2024

elastic

Introduction

Today's enterprises deal with sprawling, intricate environments with potential vulnerabilities, rapid development cycles, and hidden dangers. The traditional security approach, often isolated from other practices, is struggling to keep pace with the latest threat(s) on the horizon. Adversaries, who can switch up their tactics at a moment's notice, exploit fragmented defenses while organizations remain oblivious to the hidden shadows in their environment.

There is an opportunity within this issue, however: the convergence of security and observability. When organizations operate in silos, critical blind spots can be left exposed. Uniting security and observability unlocks a holistic view of environmental health and behavior, providing security teams the broader insight they need to detect and deter threats proactively. Simultaneously, this shift allows organizations to service their customers effectively. Catching security issues early reduces downtime and loss of revenue while increasing customer satisfaction.

This convergence of security and observability can also:

- Streamline data, tools, and workflows
- Empower both the observability and security teams
- Introduce the power of generative AI insights

Within this Spotlight paper, we cover high-level strategies for combining security and observability data. This is not a unique, niche problem. It will grow alongside the complexity and size of enterprise footprints, which now comprise hybrid and multi-cloud. As you read this paper, we recommend comparing what is described here with the challenges in your environment to determine whether a combined approach would benefit your operations and security teams.

Security + Observability

It's easy to state the issue from a security perspective—things simply aren't working because adversaries are still finding success. Gone are the days of static perimeters and somewhat predictable attacks. Today's adversaries are sophisticated, adaptive, and armed with ever-changing tactics. The only way to combat adversarial versatility is with as much visibility as possible into the entire environment.

The only way to combat adversarial versatility is with as much visibility as possible into the entire environment.

Let's examine some of the security issues that face enterprises today. Security teams are charged with protecting environments that are growing in terms of both complexity and the rate of changing business development needs. Complexity challenges include:

- Enterprises are vast and distributed environments, spanning multiple clouds, data centers, applications, and endpoints. This sheer size and complexity create inherent challenges for legacy security approaches.
- Security operations centers (SOCs) are often overwhelmed with alerts and data points from disparate sources. Siloed tools and processes make it difficult to correlate events, prioritize threats, and respond swiftly and efficiently.

Conversely, software development moves rapidly when led by DevSecOps methodologies that emphasize integrating security considerations throughout the software development lifecycle. However, this "shift-left" approach can leave gaps in monitoring and vulnerability detection.

Fortunately, observability offers a powerful solution and increased visibility to the above issues. By providing real-time insights into application behavior, runtime health, and infrastructure performance, organizations (and security teams in particular) are empowered to:

- **Detect security anomalies** such as deviations from normal application behavior and resource usage. They may not be bona fide security incidents but likely warrant a follow-up investigation.
- **Uncover vulnerabilities** by highlighting potential vulnerabilities and configuration errors introduced during the development or deployment phases.
- **Profile attack vectors** with careful analysis of application behavior and attack surfaces, gaining a more comprehensive understanding of how adversaries might target their environment.

More holistic and deeper insights help teams detect and identify threats much faster than before, minimizing damage and disruption to their organization.

We want to see a recognition that the security team can benefit from observability data to help uncover anomalies across the environment. We want developers—and their associated telemetry—to become an integral part of an organization's security posture. Holistic visibility empowers teams with:

- **Proactive maintenance**—By analyzing historical trends and patterns within security and observability data, organizations can recognize potential issues before they occur, enabling proactive maintenance with minimal disruptions.
- **Comprehensive visibility and resource optimization—**A single vantage point allows for a deeper understanding of resource utilization across the environment, helping teams optimize resources and identify potential issues that could impact security or performance.
- **Enhanced collaboration**—One of our favorite features of a combined approach is the collaboration fostered between security and operations teams, which accelerates problem detection and resolution.

A great way to break down barriers between these siloed tools and teams is to foster collaboration. A converged approach fosters and builds these relationships, combining the operations and security teams on a common mission.

Converged Tools and Data Platforms

We can hear the questions now: "Security and observability? Is this something new or two new things I need to buy?" Many organizations already embrace both and wonder if they need to deploy *yet another thing*. Quite the opposite—we are calling for a convergence among tools.

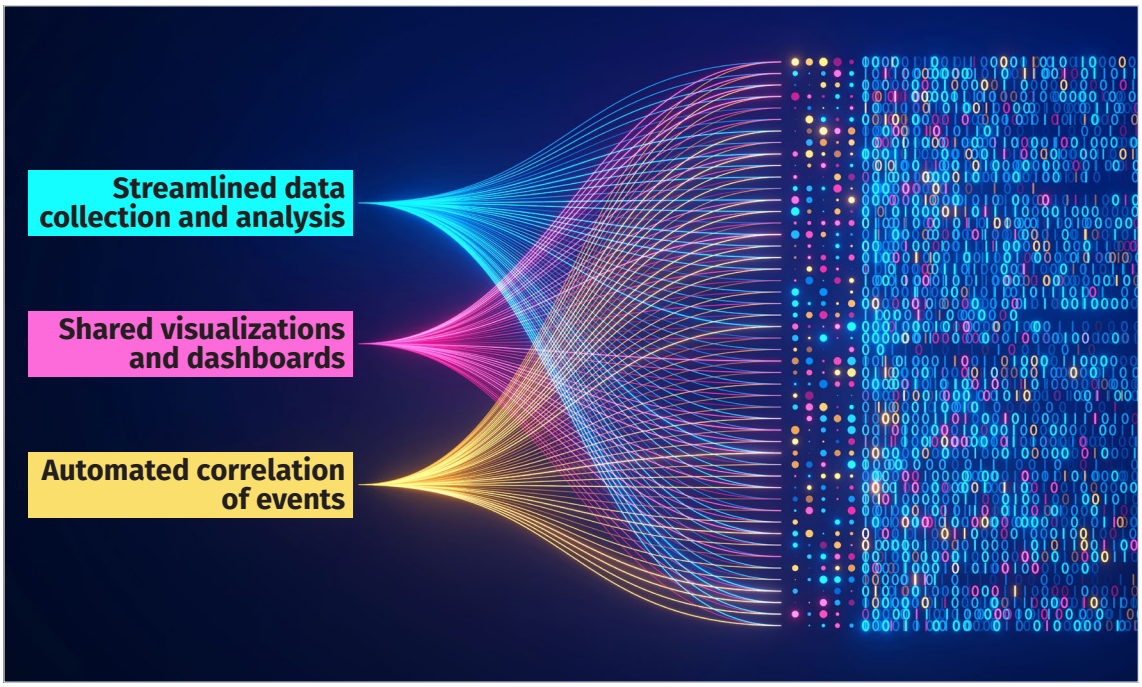

Figure 1. Benefits of Converged Solutions

As shown in Figure 1, converged solutions offer:

- **Streamlined data collection and analysis**, helping eliminate redundant data collection and silos of information. Converged platforms allow for the gathering and analysis of data holistically, providing insights for operational efficiency and security monitoring.
- **Shared visualizations and dashboards** continue to foster collaboration and break down communication barriers between security and operations teams. All teams work from a unified platform with the same set(s) of data, enabling faster decision making, anomaly detection, and threat response.
- **Automated correlation of events** can reveal hidden patterns and potential threats that might otherwise be missed in isolated analysis.

Convergence also helps promote frameworks and standards to find and define optimal telemetry. For example, OpenTelemetry (OTel) is critical in enhancing observability effectiveness, which can benefit security teams. Let's look at the overarching benefits to both *teams*:

- **Enhanced observability—**OTel defines tool- and vendor-agnostic specifications, ensuring *consistent* data formats across different services and applications. In short, this simplifies data collection and analysis while making it vendor-agnostic.
- **Unified telemetry streams—**OTel ingests and exports in a standard format, enabling easy correlation of security events, metrics, logs, and traces from diverse sources.
- **Improved visibility—**With a single, unified platform approach, OTel enables a comprehensive view of an organization's IT landscape and minimizes blind spots.

We feature OpenTelemetry as an example of how a framework in observability can benefit security teams. Given your environment's niches or requirements, you may have other examples in mind. Regardless, establishing telemetry consistency is the key to empowering the security team.

How does a framework like OpenTelemetry assist security teams? Oddly enough, it begins with the standardization of telemetry. Many security teams are used to vast, disparate, and incompatible telemetry sources. Given the size of the modern enterprise sprawl mentioned previously, visibility gaps are often found when data sets "don't play nice."

OTel works wonders for security teams for the following reasons:

- **It empowers security teams** to detect anomalies and potential threats by focusing on different data types (metrics, logs, traces) in a common schema—before they become incidents.
- **Faster investigations** result from a unified view and ease of navigating metrics, logs, and traces.
- **Reduced mean time to resolution (MTTR)** can be had with faster detection and investigation capabilities. OTel helps security teams resolve security incidents quickly.
- **Better governance** can result from managing fewer technologies and reducing the threat surface by working with fewer vendors who have access to your agents.
- **Budgetary savings** are likely when tools are consolidated.

These benefits and more show how a convergence of tools and telemetry frameworks can help security and observability functions to thrive together.

Case Study

To help paint the picture of observability and security convergence, we'll look at Enterprise customer.

The Problem

Enterprise has struggled with siloed operations between security and IT operations teams, which led to multiple operational inefficiencies. The security team relied on disparate tools and alerts, leading to missed threats and alert fatigue. IT ops grappled with limited visibility into system behavior, preventing issue identification and resolution. This impeded efficient incident response and increased security risks.

The Implementation

Enterprise needs both observability and security solutions. However, to acquire those solutions piecemeal simply makes no sense. Both teams require access to and insight from the same telemetry. The best answer is a solution that combines observability and security functionality in one.

- **Security teams** require access to logs, endpoint detection and response/network detection and response (EDR/NDR) alerts and telemetry, vulnerability scans, and other SaaS platform audit logs and alerts.
- **IT ops** require infrastructure monitoring data, application performance metrics, server logs, and configuration data (among others)

By combining these needs into a single platform, the organization can realize benefits such as cost optimization, unified tooling, and a central point of analysis. Furthermore, it should come as no surprise that in today's enterprises, each team can benefit from insight into the other's data. The security team, for example, can utilize metrics to identify oddly performing systems or misconfigurations. IT ops teams, on the other hand, would benefit from security logs to help identify user activity or OS-specific performance issues.

Generative artificial intelligence can also play an important role in this implementation. AI is useful at scaling across all data types to:

- **Correlate events and behavior** across combined telemetry, identifying hidden patterns and anomalies across security and operational datasets.
- **Predict incidents** by leveraging historical data and real-time trends. AI can potentially identify misconfigurations, infrastructure disruptions, or other potential issues before they can be exploited by adversaries.
- **Generate insights and visualizations** that lead to comprehensive dashboards, providing both teams with shared, context-rich visibility into system health and potential threats.

Closing Thoughts

The convergence of security and observability is not some futuristic hypothetical. It's a necessity for today's security teams. By embracing a combination of technologies and telemetry, organizations can focus on building a resilient security posture, achieving operational efficiency, and gaining a much-needed edge against threat actors. The future of security is not in siloed solutions—it's in unified data platforms that empower the organization.

Consider the size of your organization, its digital footprint, and the complexities your security team is combatting. Consider also the various applications, platforms, and tools that operations, developer, and security teams utilize to complete their jobs.

Is there an overlap in data or functionality? Are these teams siloed or are they working together? You know the answer, and we encourage you to find ways to break down the barriers and empower each team to defend the organization with the best tools and telemetry at their fingertips.

Sponsor

SANS would like to thank this paper's sponsor: