TRUEFORT

ARTICLE

Why Security Needs An Application-Centric Lens

Forbes Technology Council

Sameer Malhotra
FORBES COUNCILS MEMBER

Sameer Malhotra is co-founder and CEO of TrueFort, a former Wall Street tech exec and an expert in IT infrastructure and cyber security.

During my time running IT infrastructure for several large Wall Street banks, my biggest challenge was securing systems from unauthorized access and protecting customer data. Because critical business assets are controlled and managed by applications, they represent the highest-value targets.

What became clear to me after any breach postmortem was that traditional "infrastructure-centric" methods we were using to secure applications and data were a poor fit for our needs. We were lacking, in my view, an additional application-centric lens into threats.

Infrastructure-centric tools are designed to protect component layers of the stack, like endpoints, VMs, containers, networks and servers. What these systems typically lack is observability and a contextual understanding of security-relevant behavior in the application layer of the IT environment. For example, network security tools don't understand if certain applications should be using specific ports when they're interacting with other applications.

As the co-founder and CEO of a company that provides an application and cloud workload protection platform, I believe a better approach would be to use security telemetry collected from existing infrastructure tools and supplement that with capabilities that are designed to protect the application layer. You can accomplish this by focusing on what constitutes the accepted, normal operational state of an application and the ability to detect any deviations from this baseline in real time.

This application-centric view of security should be based on four critical security capabilities:

The first is full security transparency and understanding the application environment. This comprises the ability to discover applications and understand their relationships and dependencies. It also includes the ability to observe and profile application behaviors to determine baseline normal security states, as well as the associated network and data path interactions within and between applications. This is critical information for securing increasingly complex application environments, which now include a collection of legacy, hybrid and more modern cloud-native applications. You should also be able to adapt to and reflect the dynamic nature of these environments where applications are continuously being added, patched and updated.

The second capability is a set of application-aware security controls that are purpose-built to protect application workloads and their data. They could provide application-layer hardening, segmentation, integrity assurance and allow listing, exploit prevention, and service identity protection capabilities. These refined controls should enable security teams to patch, scan and modify software host and network systems with an application context they don't have today.

The third set of capabilities involves empowering threat response teams with application-centric detection and response. The typical security operations center (SOC) is overloaded with threat-detection events and alerts from different tools. Correlating related security events specific to a given application, let alone prioritizing follow-up remediation actions, is often a time-consuming process that's slowed down by response teams trying to understand disparate detection events within the context of the application at risk. As a result, mean times to detection and response may be negatively impacted, while applications remain exposed or under active attack for long periods of time.

Application-centric detection and response, in contrast, should prioritize alerts based on anomalous behavior and its application impact. These would quickly lead SOC personnel to the source of a security event for investigation and remediation. What took my team weeks of analysis to understand and respond to could be done in minutes if alerts provided application-level context.

The final component is continuous assessment and reporting on an application environment's security posture. To be effective, CISOs need to be able to communicate the organization's current security risk profile and how it is being managed over time to the business team.

Currently, many CISOs are in the dark when it comes to understanding the risk posture of their application environment.

The complexity and manual work required to accurately summarize and report on application (and data) risk is far too great for most organizations. In addition, many operational security teams responsible for day-to-day protection of application environments also lack visibility into current risk levels needed to prioritize their activities. This lack of clarity at both the executive and operational levels creates a critical security blind spot.

Viewing security through the lens of the application, rather than the underlying infrastructure it runs on, provides new levels of visibility, control and reporting. Organizations can use this approach to gain the intelligence they need to harden their applications and data against cyberthreats, and to respond more quickly to shut down attacks when they do occur.

TO GET STARTED, CONSIDER THE FOLLOWING STEPS:

1. **Focus on the applications that matter most — in other words, your crown jewels.**
2. **Identify and prioritize the top security challenges you'd like to address, especially those that will have the greatest positive impact on the security team's productivity and the organization's security. For example, you could decide to improve microsegmentation, get a handle on system IDs or enhance security during the application development life cycle.**
3. **Define and set goals for your initiative and the team that will lead the effort. You should include a timeline for deploying new technology.**

Now you're ready to research vendors and solutions that can help you address the challenges and goals you've defined.

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM