The Road To Supply Chain Security

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.

Supply chain attacks have become ubiquitous recently. One study by Nokia (via Mimecast) concluded that "2021 has become known as the year of the supply chain attack."

The use of third-party code in enterprise software has made all sorts of products vulnerable to attack. In the last year, a number of large cyber incidents were due to vulnerable or compromised software components that have either gone undetected or have no patch to mitigate them. Security teams had to drop everything to analyze both the products they use and the supply chain software within their own code.

We have seen a number of examples of these. Sunburst, a bit of malware that exploits a vulnerability in business software, opened a backdoor to the systems of thousands of organizations worldwide. Log4Shell took advantage of a vulnerability in Log4J2, a common open source piece of code used globally by Java developers.

In March, the identity authentication company Okta disclosed that more than 300 of its clients had been breached in a ransomware attack where two supply chain issues converged. First, its customer service contractor, Sitel, was targeted by attackers, but Okta had little visibility into its security; it took two months for Okta to announce which customers were affected. Second, the environment was complicated because Sitel had just acquired a rival customer experience vendor, Sykes, whose legacy network was the target of the breach.

Traditional security controls come up short in defending against these attacks. In the Sunburst attack, compromised certificates were used to avoid detection by traditional or "next-gen" antivirus tools and other malware detection products. It took security analysts recognizing that a second multifactor authentication device was being registered without the user's knowledge to ultimately uncover one of the largest-scale attacks against our infrastructure in recent history.

Since we need to detect zero-day attacks as they are occurring, we can no longer rely on traditional safeguards such as code-signing certificates and "known-bad" detection methods like indicators of attack (IOA) and indicators of compromise (IOC).

Service accounts with non-expiring passwords and unchecked activity between workloads are being used to move laterally across systems and reach the crown jewels much more rapidly than in previous years. CrowdStrike noted in 2021 that many adversaries had decreased breakout time to under 30 minutes, over an hour faster than the average speed from initial infiltration to performing lateral movement into other systems and workloads.

Like nesting Russian dolls, supply chain vulnerabilities can hide inside software updates signed by legitimate vendors, which makes them even harder to detect and mitigate. What can be done to detect insider threats, credential misuse, supply chain compromises and zero-day vulnerabilities that may be targeting our core infrastructure and workloads?

One approach is to focus on workloads themselves by limiting their behavior to only what is needed while blocking anomalous or malicious activity. It requires segmentation of workloads, continuous monitoring and dynamic enforcement of policies to adapt to changes in the environment.

With these shorter breakout times now being observed, organizations are frequently being forced by their cyber-insurers to show they have implemented effective segmentation policies. This approach makes sense since it limits the impact of a supply chain attack, ensuring that even a trusted workload cannot change its behavior—for example, by connecting to external applications unexpectedly or to a new database server containing critical data.

Continuously analyzing changing behaviors of workloads against a positive baseline is an effective approach for detecting threats that bypass traditional cloud security methods that use point-in-time, rearview-mirror assessments. By establishing what constitutes normal and acceptable workload activity and enforcing this behavior, companies with complex supply chains can defend against previously unpreventable security breaches.

> Continuously analyzing changing behaviors of workloads against a positive baseline is an effective approach for detecting threats that bypass traditional cloud security methods that use point-in-time, rearview-mirror assessments.

CONSIDER THESE RECOMMENDATIONS FOR SECURING WORKLOADS:

- Catalog all applications running in both the data center and the cloud, including who the application owner is and what its criticality to the business is.
- Develop a shared risk mitigation plan between the security team and application owners that lays out where any sensitive data is stored and processed as well as the most critical assets for the resiliency needed to avoid any downtime.
- Go beyond network-based segmentation and implement dynamic policies using identity, workload, network and process-level or runtime protections across complex, hybrid cloud workload environments.
- Implement a continuous monitoring system that adapts to dynamic workload environments and does not only perform point-in-time scans against past, known vulnerabilities or configuration benchmarks.
- Make sure the workload protection enforces dynamic segmentation policies to take that action in real time before the next intrusion becomes a breach. Since applications change over time, potentially causing new vulnerabilities, you need the ability to shut down suspicious or high-risk workload activity before damage occurs.

ABOUT TRUEFORT

TrueFort is an advanced approach to protecting data center and cloud workloads that makes zero-trust architectures possible. Our platform uses continuous monitoring to deliver real-time detection and response as soon as noisy workload behavior strays from known, understood activity. By absorbing telemetry from multiple agents, we decipher all intra-application communications and trigger suspicious activity alerts. The TrueFort Platform is the only solution instilling the confidence to protect workloads across all production environments. By reducing the impact of security incidents, we increase your overall business resilience, shrink your exploitable attack surface, and enable you to take immediate action against live attacks. We bring the single truth security and application owners need to effectively protect workloads of all forms.

For more information, visit truefort.com and follow us on Twitter and LinkedIn.

TRUEFORT™

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

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM