Observability speeds zero trust and application security

Using AI-driven observability throughout the software life cycle ensures the ongoing performance and security of applications

Willie Hicks
Dynatrace

EVERY SINGLE AGENCY IS being attacked thousands of times a day. If even 1% of these breaches are successful, that's a major problem. In response to increasing cyberthreats, the government is speeding up the move to zero trust. This security model assumes that every user, request, application and non-human entity is not to be trusted until its identity can be verified.

Zero trust principles require a layered defense that is more effective when rooted in observability. To develop an architecture that validates and revalidates every entity on the network, it is necessary to know what those entities are, how they're communicating and how they typically behave so we can recognize deviations. Zero trust and observability technologies work together to create a more secure and resilient network environment by assuming that all requests for access are untrusted and continuously monitoring the network to detect and respond to potential threats.

Developing applications with security in mind is critical for a strong zero trust model; applications are a significant threat vector and susceptible to various attacks such as SQL injection, cross-site scripting and malware injection. Therefore, implementing observability early in the software development life cycle helps agencies identify and remediate vulnerabilities, creating a more secure and resilient network environment that supports the zero trust approach.

> "In today's highly complex digital landscape, **troubleshooting application issues can be an incredibly challenging task that requires aid from artificial intelligence."**

USING AI TO TROUBLESHOOT COMPLEX SYSTEMS

Accurate and timely insight into the security and performance of applications helps agencies answer simple questions such as: Is the application ready to deploy? Are all known vulnerabilities remediated? And after an application has been deployed, are we continuously monitoring? Something that might not have been a vulnerability when an application was built can become an exploit later, so it's important to always have an eye on the application.

In today's highly complex digital landscape, troubleshooting application issues can be an incredibly challenging task that requires aid from artificial intelligence. This is where Dynatrace comes in. As a platform designed to optimize application performance, Dynatrace unifies data from various sources — observability, business and security data — with continually updated mapping of relationships among these data points, providing valuable data context.

Consider this real-world example of Dynatrace's effectiveness. At a government agency, a team spent considerable time in a "war room" attempting to isolate an issue with an application. After the team members falsely concluded that they had identified the root cause, Dynatrace revealed that they had actually identified the wrong problem and were about to head down a time-consuming remediation path. By identifying the actual root cause of the issue, Dynatrace saved the team countless hours and enabled it to focus on resolving the problem efficiently.

INNOVATION AND INTELLIGENCE TO STAY AHEAD OF ATTACKERS

Dynatrace has access to a massive database of vulnerabilities and how they affect an application so we can help agencies triage remediation priorities. For example, Dynatrace can

Source: iStock

tell if the application is exposed to the internet, if it carries sensitive data, what it's talking to, where its dependencies are, and whether it performs back-end processes or interacts directly with external users.

When the Log4Shell vulnerability in Apache Log4j 2, a popular Java library for logging error messages in applications, was revealed, agencies used Dynatrace to detect hundreds of entities that were using Log4j. The platform also helped agencies prioritize remediation efforts.

Attackers are continually innovating, using AI and other capabilities as part of their strategy. Agencies must do the same. AI-driven observability is a crucial part of building a strong zero trust architecture throughout the software life cycle to ensure the ongoing performance and security of applications. ■

Willie Hicks is public-sector chief technologist at Dynatrace.