Dynatrace augments observability with runtime application security

JANUARY 8 2021

By Daniel Kennedy

A provider that shows up more frequently in 451’s research on observability, Dynatrace announced entry into the application security market on December 8 with the release of its Application Security Module, a runtime application self-protection offering.
Introduction
A provider that shows up more frequently in 451’s research on observability, Dynatrace announced entry into the application security market on December 8 with the release of its Application Security Module, a runtime application self-protection (RASP) offering already live with customers.

451 TAKE
Historically, a level of distrust has existed on the part of developers around security tools that act on the runtime; as a result, the RASP space has been one of fits and starts. For a time, it appeared the RASP space would become largely thought of as an implementation option for a web application firewall (WAF), but microservices architectures and the shift away from monolithic application stacks may be changing the conversation; resistance on the part of maintainers to layers of third-party controls within the application seems to be eroding. Implementing additional security controls using an already instrumented application performance monitoring agent – in this case Dynatrace’s OneAgent offering – should overcome objections to the addition of a new runtime agent.

Details
RASP forms a part of the ‘shift right’ paradigm in application security alongside other technologies, such as WAFs and bot detection and mitigation tools, by providing application protection for production applications. This plays opposite ‘shift left,’ where many aspects of application security testing (AST) have moved into pre-production development and testing, with the goal of pushing mostly security-vulnerability-free – or at least security-vulnerability-aware – code changes into production. That second part, having an awareness of the overall risk of an application, is important. Some vulnerabilities identified by AST programs will nonetheless go into production as accepted risks. That doesn’t account for missed defects or vulnerabilities that become known – for example, a new vulnerability in a popular open source component – after an application is already in production. For those reasons, even the best application security testing programs will still need an application protection – or shift-right ‘strategy’ – for production.

The example of an open source vulnerability above is relevant here because that’s where the new Dynatrace module is starting, using an agent-based instrumentation approach that leverages existing components in its product stack, including real-time dependency detection via Smartscape and distributed tracing at the code level via PurePath. A partnership with software composition analysis provider Snyk provides open source vulnerability data. Service flow analysis allows for prioritizing high-impact fixes. This new offering targets large customers with a predicted 20% uplift in cost based on existing licensing modules that consider an environment’s RAM footprint. In a nod to being able to test pre-production what exists in production, pricing is the same across environments.

The new module differs from traditional RASP in that it concentrates on the open source vulnerability piece and is alerting rather than blocking (or preventing) requests. The prevention piece is perceived as highly valuable in application protection, when it works. The legacy of the space, however, is littered with, for example, WAF implementations where prevention rules were reduced to the most basic protections at the first false-positive results that blocked legitimate application traffic, so care in implementation is required. To that end, implementing both prevention and extending into the evaluation of custom code beyond open source – for example, input validation vulnerabilities – is on the horizon.
Application Security Testing Tools Implemented by Enterprises

Which application security tools has your organization implemented? Please select all that apply.

WAF 67.8%
SAST 61.2%
DAST 47.9%
SCA 29.8%
IAST 20.7%
RASP 18.2%

Other (please specify) 3.3%

Sample Size: 121
Base: Respondents currently using application security