dynatrace

Dynatrace Application Security automatically detects and blocks attacks in real time

Best Practices

Overview

Dynatrace adds real-time attack protection to the Dynatrace Application Security module. Based on code-level insights and transaction analysis, attacks can be detected and blocked without configuration, achieving a perfect OWASP benchmark score for injection attacks—100% accuracy and zero false positives.

In today's world, the speed of innovation is key to business success. Cloud-native technologies, including Kubernetes and OpenShift, help organizations accelerate innovation and drive agility. Unfortunately, they also introduce risk.

One key element for securing applications in modern environments is vulnerability management. Static Application Security Testing (SAST) solutions are a traditional way of addressing this. They are part of continuous delivery pipelines and examine code to find vulnerabilities. But this approach doesn't work in new environments and **today's container security scanners fail to provide comprehensive answers to new security threats.** That's why Dynatrace added Application Security to its platform, powered by full production insights and enabling automatic vulnerability management.

Gerhard Byrne is Senior Product Manager for Dynatrace Application Security. His focus is on identifying and driving security use cases at Dynatrace. Prior to joining Dynatrace, Gerhard worked in various security and development functions including founding a security product company. When not working on security topics, Gerhard can be found climbing boulders and playing board games with family and friends.

Real-time attack protection needs precision to fix security problems

There is another critical aspect that needs to be addressed: **how do you protect applications against attacks that exploit vulnerabilities while DevSecOps teams** simultaneously **work to resolve those issues in the code**?

Without real-time attack protection in place, the only possible next step is forensics after the attack to investigate what happened. In the worst case, you have to inform customers and the public about security breaches and stolen data. As important as this is, current approaches to attack detection also leave gaps:

WAFs (web application firewalls) generate massive continuous configuration efforts, create false positives, and they don't cover unknown attacks.

WAFs protect the network perimeter. They monitor, filter, or block HTTP traffic. Compared to intrusion detection systems (IDS/IPS), WAFs are focused on the application traffic. While WAFs work great for some scenarios, they have significant weaknesses for others:

- WAFs are rule-based. Configuring rules and potential permutations requires significant effort and makes it nearly impossible for teams to keep up with new threats and highly dynamic application landscapes.
- WAF rules produce false positives that can potentially block valid requests. So they need to be continuously improved.
- WAFs are often managed by dedicated teams, which creates complexity in end-to-end DevSecOps collaboration.
- As WAFs are rule-based, they are not able to detect unanticipated attacks.

Current Runtime Application Self Protection (RASP) solutions don't live up to their promise or work in enterprise environments.

RASP solutions sit in or near applications and analyze application behavior and traffic. When issues are detected, RASP solutions can identify and block individual requests. While the promise of RASP is compelling, existing solutions don't live up to expectations:

- RASP solutions rely on agent technology, which introduces deployment challenges across large-scale, heterogenous, and highly dynamic environments.
- For most enterprises, using a RASP solution means running multiple agents on their production systems, potentially creating risk due to incompatibilities.
- A key requirement for agent technology is avoiding a negative impact on performance. Existing RASP solutions often introduce significant overhead, which negatively impacts application performance and customer experience.
- RASP solutions may lack the precision required to confidently apply automatic blocking of attacks.

Dynatrace Application Security adds real-time attack detection and protection

Our customers know that Dynatrace resolves the challenges associated with RASP solutions. Our platform and OneAgent® technology support highly automatic deployments and the lowest overhead. They provide intelligence and automation for the world's largest applications and environments every day.

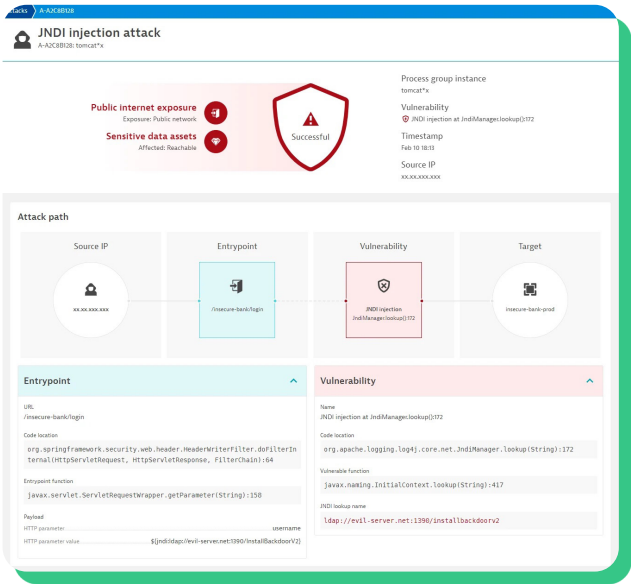
We're happy to announce that Dynatrace has added real-time attack detection and protection to our Application Security module.

To explain this new capability, let's look at an example you may have stumbled upon: **Log4Shell.**

When Log4Shell became public, Dynatrace Application Security customers already had an advantage: literally **10 minutes** after information about this vulnerability hit the wire, **Dynatrace customers were notified** if they had an issue, how severe the issue was, and where to start remediation most effectively.

Of course, as with all vulnerability management solutions, there was and is the risk that vulnerabilities can be exploited while DevSecOps teams are working to fix them.

With the new ability to identify and block attacks, Dynatrace Application Security can protect your applications from the very beginning. Dynatrace now detects **attacks like Log4Shell automatically in real-time, with no configuration required.**



100% accuracy and zero false positives

With transaction analysis and code-level insights, Dynatrace detects whenever user-generated inputs are sent to vulnerable application components without sanitization. With this approach, you can identify SQL injection attacks, command injection attacks, and JDNI attacks like log4shell or the H2 vulnerability.

This means that Dynatrace doesn't rely on vulnerability databases but is rather able to identify and block such attacks automatically even if they are exploiting unknown weaknesses.

A perfect OWASP benchmark score for injection attacks—100% accuracy and zero false positives—impressively proves the precision of our approach.

This is one step towards delivering the promise of runtime application self-protection. We will further enhance the detection and blocking capability of Dynatrace to cover additional attack types, so stay tuned for updates!

How to get started

Real-time attack detection and blocking for Java will be available in the next 120 days.

- If you're already a Dynatrace customer and want to start using the Application Security module, just select Application Security from the main menu in the Dynatrace web UI.
- If you're not using Dynatrace yet, it's easy to get started in under 5 minutes with the Dynatrace free trial.

For more information, visit our website to watch the demo or read our previous Application Security blog posts. To learn more, see Application Security in Dynatrace Documentation.