Vulnerability Scanning

A single Static Application Security Testing (SAST) report could identify hundreds — if not thousands — of instances for each vulnerability, but running SAST and Dynamic Application Security Testing (DAST) tools only identify the vulnerabilities, they do not fix them.

Vulnerabilities also occur throughout the rest of the code in the underlying frameworks, libraries, transient dependencies, servers, services and even the runtime platform itself (JVM, .NET, etc.).

Critical Patch Updates

Routine critical patches that come from Oracle and Microsoft represent a significant part of the burden teams face. Microsoft’s Patch Tuesday is an institutional event and Oracle’s quarterly Critical Patch Updates (CPU) have more than doubled in size since April 2016 – from the 130s to the 300s per CPU in July 2017. The July 2017 CPU reflected finding a new vulnerability every 68 hours (on average) based on the Java-related CVEs patched – 2/3rds of which had a High Severity CVSS score and 87 percent of which could be remotely exploited without authentication.

Waratek Patch allows you to apply custom security rules as well as current and historical virtual patches for instant protection.

Benefits

• **No false positives.** Waratek Patch will never produce a false positive and we are so confident in that feature that we back it up with a $10,000 USD financial guarantee.

• **Ultra-low performance overhead.** Waratek Patch is built on the ARMR Application Security Management Platform, which means that if your applications experience any performance impact, it should be less than 3 percent. Some of our clients have even reported performance improvements in certain conditions.

• **No code changes required.** Security is risky. Patches and security updates often mean adjusting source code and taking an application down for maintenance. Waratek Patch will safeguard your applications without the need to worry about application failure or financial impacts from downtime.

• Compensating Controls for Compliance. Ensure compliance with the PCI, SOX, HIPAA, federal, state, and other regulations using virtual patches to remediate applications on your risk register.
“WE WERE UNDER ACTIVE ATTACK AND UNSURE WHAT TO DO. OUR THIRD-PARTY SUPPORT PROVIDER SUGGESTED WARATEK. WE WERE ABLE TO PURCHASE AND DEPLOY IN THE SAME DAY AND STOP THE ATTACKS ON OUR WEBSITE.”

DAN SMITH, CTO
CARETECH