CHECKLIST

MAKE VULNERABILITY MANAGEMENT FAST AND EASY:

KICK SOME AST WITH AUTOMATION

Modern DevOps demands velocity and agility. That means breaking free from manual vulnerability identification and remediation verification and letting security teams kick some serious AST by using instrumentation to automate application security (AppSec). Software instrumentation is already widely applied across the software development life cycle (SDLC). Now, Contrast extends it to security through its DevOps-Native AppSec Platform.

MEET BOTH SECURITY AND RELEASE TARGETS WITH CONTRAST

All three elements of the Contrast DevOps-Native AppSec Platform are critical in relieving the burden of vulnerability management, both in development environments and in production runtime:

UNLOCK AUTOMATION USING INSTRUMENTATION

Contrast Assess uses instrumentation to perform vulnerability analysis while an application is running. Sensors are placed within the code that monitor how the code is operating. This runtime analysis automates vulnerability testing that is integrated into the continuous integration/continuous deployment (CI/CD) pipeline and processes. Continuous runtime testing occurs when code is committed to the repository, minimizing technical debt incurred from correcting vulnerabilities. Additionally, continuous test execution ensures that new vulnerabilities can be identified and corrected as soon as they are made public.

FACILITATE RISK PRIORITIZATION WITH INTEGRATED, AUTOMATED VULNERABILITY MANAGEMENT

Embedded sensors within application code also enable Contrast Assess to integrate into the development team's CI/CD pipeline and automate vulnerability management. Vulnerabilities are mapped to routes (runtime code paths) within an application. Contrast Assess reveals the full extent of an application attack surface, how much of it was security tested, and the areas where additional test coverage is needed. This enables developers to prioritize remediation of identified issues based upon their potential impact to the application. Route Intelligence also enables developers to learn more about their identified vulnerabilities, providing code-level advice on how to reduce vulnerabilities in the future. In addition, Contrast Assess can be integrated into issue tracking and project management systems used by the development team, which improves visibility into outstanding issues and their current remediation status.

AUTOMATE VERIFICATION OF VULNERABILITY REMEDIATION

After a development team identifies and remediates vulnerabilities, it is necessary to verify that the corrected code actually fixes the vulnerability and did not introduce any new issues. By performing continuous vulnerability testing, Contrast Assess detects and diagnoses vulnerabilities that exist in the current version of the code. These are then correlated with previous detections to determine if a previously detected vulnerability has been successfully remediated.

OBTAIN FULL VISIBILITY OF VULNERABILITIES FOR RISK MANAGEMENT AND COMPLIANCE

Contrast Assess maps URLs to code path and uses the internal visibility provided by instrumentation to identify all potential entry points and execution paths within an application. This provides developers and security teams with full visibility of execution paths, and thus a complete and accurate view of all vulnerabilities in an application—including application programming interfaces (APIs).

Visibility of application vulnerabilities is extended to open-source software (OSS) libraries and frameworks using Contrast OSS. It allows developers to create a complete software

bill of materials that includes third-party libraries and dependencies, which are often overlooked by legacy AppSec solutions. Using the bill of materials generated by Contrast OSS, developers can identify and remediate inherited vulnerabilities that pose security and licensing risk or noncompliance with regulations and standards such as the National Institute of Standards and Technology (NIST) and the Payment Card Industry Data Security Standard (PCI DSS).

VIRTUALLY ELIMINATE FALSE ALERTS WITH RUNTIME PROTECTION

Despite the best efforts in development, some vulnerabilities may make their way into production code. Historically, organizations protected—or purportedly did so—applications in production runtime with perimeter defenses (viz., web application firewalls [WAFs]). But this outside-in approach is fraught with challenges—from unending false positives that consume substantial time to triage to false negatives that put applications at risk.

Contrast Protect takes an inside-out approach by embedding security monitoring within the running software. Residing alongside vulnerabilities, Contrast's binary runtime application self-protection (RASP) detects attacks and prevents them from exploiting vulnerabilities. Contrast Protect also differentiates between attacks that are simply probes versus those that are vulnerability exploits. This virtually eliminates false positives that are endemic with perimeter defenses, which are unable to differentiate between probes and exploits, lumping all of them together in noisy alert feeds.

CONTRAST SECURITY
240 3rd Street
Los Altos, CA 94022
888.371.1333