ServiceNow Application Vulnerability Response

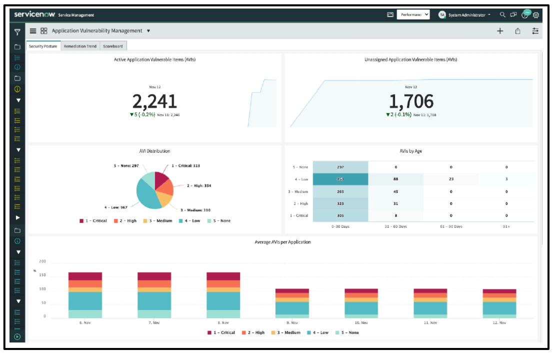
Applications present a rapidly growing attack vector

Application-based breaches are on the rise; according to the 2020 Verizon Data Breach Report, 43% of attacks in the past year targeted web-application vulnerabilities[1]. Increasingly, organizations have adopted agile application development practices, which can opened up potential security holes. For example, while open source code is commonly used to quickly develop applications, it is also a widely available resource for cyber criminals to study and exploit; in the past year, enterprises have seen a 50% increase in open source code vulnerabilities[2]. In spite of the growing nature of application-based attacks, it is often the case that organizations release applications knowing they could be vulnerable, in hopes that the vulnerability is relatively low risk. According to a Ponemon Survey, more than one-third of organizations knew they were susceptible to being breached before they experienced an attack[3].

To determine security flaws in deployment-stage applications, most organizations use multiple testing tools such as dynamic application security testing (DAST), Static Application Security Testing (SAST), and Software Composition Analysis (SCA). With disparate testing tools, this creates a new layer of complexity for security teams to access each of these tools individually, collect data points, identify relevant development teams, and determine next steps. Applications also can be developed in a variety of different languages and tools. This means that any remediation solution has to be customized to the application, which requires tight coordination between the software development owners and security analysts. Without a single pane of glass to understand priority and scope, drive remediation, and coordinate actions with development, it hampers the ability to swiftly address application vulnerabilities and reduce risk.

The ServiceNow solution

ServiceNow® Application Vulnerability Response assesses DAST results to track against vulnerable items and coordinate fixes. It offers a centralized view of all application vulnerabilities, determines their priority, and helps with coordinating the remediation process with relevant stakeholders across security, development, and risk.



	0-30 Days	31 - 60 Days	61 - 90 Days	91+
5 - None	297	0	0	0
4 - Low	[illegible]	88	23	3
3 - Medium	265	45	0	0
2 - High	323	31	0	0
1 - Critical	305	8	0	0

The Application Vulnerability Response dashboard summarizes active application vulnerabilities in your organization and criticality metrics.

Improve security and development collaboration

Centralize application vulnerability data and remediation tasks across teams. Coordinate workflows and track progress of issue resolution.

Drive faster, more efficient security response

Reduce the amount of time spent on basic tasks with orchestration tools. Automatically prioritize and respond to vulnerabilities with workflows and automation.

Pinpoint development issues proactively

Get actionable insight from remediation data and adapt policies accordingly. Leverage reporting insights to tune development practices and reduce organizational risk.

[1] *Source: 2020 Verizon Data Breach Investigations Report*

[2] *Source: 2020 Forrester State of Application Security Report*

[3] *Source: 2019 Ponemon ServiceNow-sponsored survey, "Costs and Consequences of Gaps in Vulnerability Response"*

Single pane of glass and coordinated actions

Having clear visibility into application vulnerabilities enables actionable insight for development and security teams. Application Vulnerability Response offers several important benefits that allow security analysts to coordinate the remediation path and shrink the vulnerability pipeline:

***Identification*:** With Application Vulnerability Response, we can centralize application vulnerability data (including CWE information, summary of issue), what is the affected application, and importantly, which release is impacted by this vulnerability. This not only provides valuable information to pinpoint problem scope, but by capturing release information, we can also understand software development deficiencies and proactively capture release issues that can be used to provide required customer awareness.

***Analyze*:** Building on centralized data points from DAST results and the contextualization offered by the Configuration Management Database (CMDB), we can provide a risk rating– the derivative of vulnerability severity and the criticality of IT assets and services which are related to the application affected. This prioritization leverages a configurable risk calculator, which accounts for these metrics, and is key to evaluating how critical the vulnerability is, and assigning work accordingly.

Respond: We leverage automated assignment rules to associate a set of remediation actions with the appropriate security and development owners for the application, as well as a means of tracking remediation progress. All of this is coordinated through a transparent workflow and facilitates swift closure of application issues to ensure security is not a development bottleneck. We can also measure policies impacted by these changes– which help in adapting long-term risk management for development practices. Finally, we can detect dependencies for the application in question, enabling analysts to make a determination on whether to remediate a given vulnerability.

Importantly, these benefits also work with the built-in features of the ServiceNow Vulnerability Response product to provide a holistic view of vulnerabilities across the IT estate. Vulnerabilities affecting applications, infrastructure, and misconfigured software can be centrally managed and remediated within ServiceNow Vulnerability Response.

Having clear visibility into application vulnerabilities enables actionable insight for development and security teams.

ServiceNow Security Operations

Application Vulnerability Response is part of ServiceNow Security Operations, a security orchestration, automation, and response engine built on the Now Platform. Designed to help security teams respond faster and more efficiently to incidents and vulnerabilities, Security Operations uses intelligent workflows, automation, and a deep connection with IT to streamline security response.

To learn more about ServiceNow Security Operations, please visit: **www.servicenow.com/sec-ops**

servicenow.