ServiceNow Vulnerability Response

The vulnerability challenge

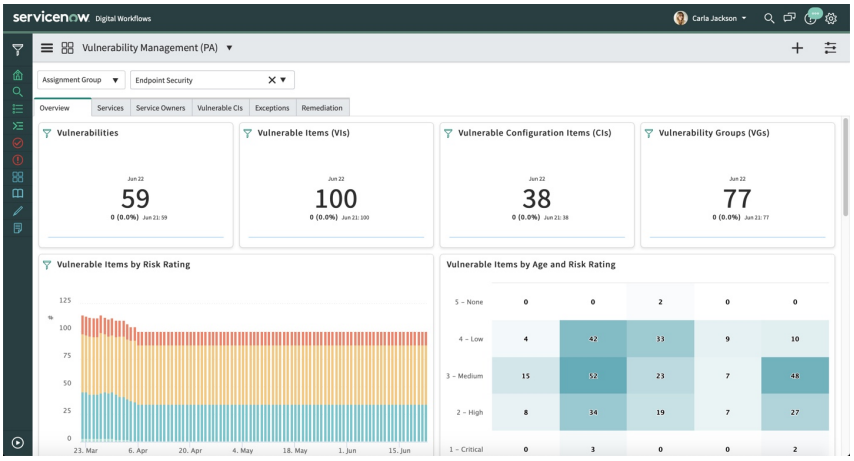
Critical vulnerabilities often hide under the radar of security challenges today. When exploited, lack of effective vulnerability response carries major impact to business reputation and data security. A study conducted by ServiceNow and the Ponemon Institute found that over a third of organizations who suffered a breach already knew they were vulnerable. In many cases, there was an existing patch for the vulnerability which was not applied due to reliance on manual processes, siloed information, and lack of visibility.[1]

Additionally, breaches are becoming more severe. Methods to exploit vulnerabilities are growing more sophisticated, with cybercriminals increasingly leveraging machine learning and artificial intelligence to thwart traditional vulnerability response mechanisms. Having a solution which interlocks all components —security, risk, and IT— is crucial to organizations staying ahead of these tactics and taking a holistic approach to vulnerability response.

The ServiceNow solution

ServiceNow® Vulnerability Response helps organizations respond faster and more efficiently to vulnerabilities, connect security and IT teams, and provide real-time visibility. It connects the workflow and automation capabilities of the Now Platform® with vulnerability scan data from leading vendors to give your teams a single platform for response that can be shared between security and IT.

Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given asset or service through integration with ServiceNow Configuration Management Database (CMDB), as well as the current state of all vulnerabilities affecting the organization. When used with the CMDB, Vulnerability Response can prioritize vulnerable assets by business impact, using a calculated risk score so teams can focus on what is most critical to your organization. The risk score can include multiple factors in its calculation, including the CVSS score of the vulnerability and whether the vulnerability can be easily exploited, using data from the vulnerability scanner and Shodan®.



The Vulnerability Response dashboard highlights the current status and associated risk of active vulnerabilities in your organization.

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

Connect security and IT

Coordinate response across teams for smoother task handoffs between groups and quicker resolution. Get accountability across the organization and know work is getting done with remediation targets.

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.

Know your security posture

View your current vulnerability status with customizable dashboards and reports backed by quantitative data. See which business services are impacted by critical vulnerabilities.

Importantly, Vulnerability Response centrally manages both infrastructure and application-level vulnerabilities. In addition to integrating vulnerability scanning data, Vulnerability Response can also assess Dynamic Application Security Testing (DAST) results to track against vulnerable items and coordinate fixes. Within the Now Platform, users can identify, prioritize, and remediate vulnerable misconfigured software in deployment-stage applications using ServiceNow Configuration Compliance. Finally, with Continuous Monitoring, security policies are connected into the vulnerability lifecycle by exchanging data collected from observables and workflows with ServiceNow Governance, Risk and Compliance. This ensures policies across application and infrastructure can be adaptive and stay up to date, and overall dramatically reduces organizational risk.

Respond automatically

When critical vulnerabilities are found, Vulnerability Response can automatically initiate an emergency response workflow that notifies stakeholders and creates a high-priority patch request for IT. To ensure accuracy in patching, Vulnerability Response recommends the most impactful remediation activities with Vulnerability Solutions Management. Analysts can monitor real-time status of patching progress and ensure process visibility across security and IT. It also optimizes remediation by using machine learning to identify the most appropriate teams for vulnerability findings and auto-assigning tasks. This results in a coordinated remediation strategy for vulnerabilities.

Not all vulnerabilities are urgent, however, so Vulnerability Response also includes exception handling. Groups of vulnerable items can be deferred until a selected date. When the deferment window expires, the group automatically becomes active again and team members are notified.

Vulnerability Response also improves visibility through reports and dashboards. With ServiceNow Performance Analytics you can easily see which services are impacted by critical vulnerabilities and which service owners are accountable to better understand your vulnerability risk in terms of your organization's operating structure. Dashboards for the vulnerability manager provide visibility into the organization's risk posture and team performance to quickly identify issues. Trending and predictive analytics can forecast future performance. For the remediation specialist, a separate dashboard displays task prioritization to work on the items that are critical or provide the greatest benefit first.

ServiceNow Security Operations

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

With better visibility, teams can respond more efficiently, reducing both the vulnerability backlog and your risk exposure.

servicenow