ServiceNow Vulnerability Response

Harden the attack surface exploding across cloud, infrastructure, and applications

According to the Enterprise Strategy Group (ESG) Security Hygiene and Posture Management report, nearly 7 out of 10 respondents admitted to a cyber breach resulting from exploitation of unknown, unmanaged, or poorly-managed internet-facing assets.

Vulnerabilities pose a serious threat to business reputation and data security. Methods to exploit vulnerabilities are growing more sophisticated, with cybercriminals increasingly leveraging zero-day vulnerabilities and supply chain attacks.

One operational dilemma for security teams is the dependency on IT teams and tools for scanning and asset data, in addition to the actual patching and mitigation of issues. Almost every organization's security and IT teams struggle to keep up with the sheer volume of vulnerabilities in an ever-increasing, ever-diversifying attack surface.

As a result, the same ESG research found that the top recommendation for improving vulnerability management programs was integrating them with other security and IT technologies. These integrations facilitate visibility, prioritization, and collaboration, while directing the scarce human talent for the greatest impact.

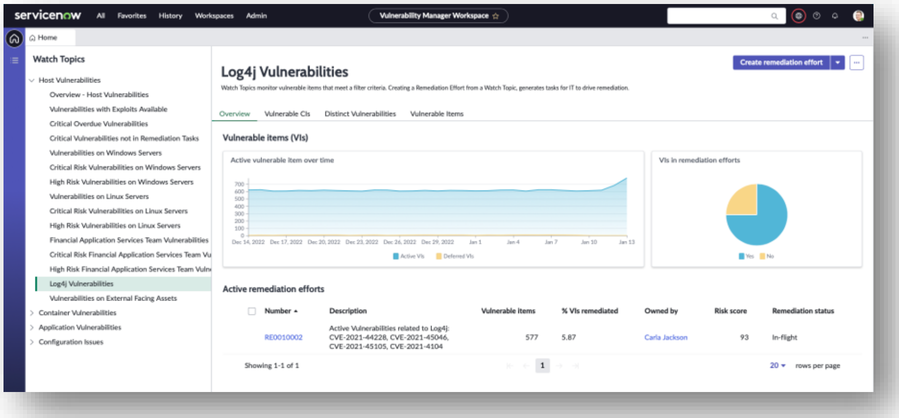
Transform operations with ServiceNow risk-based vulnerability management

ServiceNow Vulnerability Response synthesizes asset, severity, exploit, risk, and threat intelligence insights into automated workflows for fast, reliable prioritization and remediation. Integrations available on the App Store plug into multiple cloud, container, application testing, vulnerability assessment, OT/IT discovery, patch deployment, and asset management tools for fast time to visibility across your evolving attack surface.

This unified understanding helps both minimize blind spots and continuously calculate potential exposure based on threat intelligence and asset attributes. Native configuration compliance shows whether managed assets are deployed within policy and includes workflows to fix flaws and improve the security posture.

Turn visibility into closed cases and SLA compliance with the help of workflows

Vulnerabilities are grouped into Remediation Tasks according to business preferences to trim away repetitive and high-volume findings that typically overwhelm and delay processing. Tasks are automatically assigned, prioritized with risk score, and correlated with solution recommendations and patch deployments, so that authorized asset owners have the information they need to remediate the issue. Enterprises have reduced backlogs an order of magnitude with these features alone.


servicenow
All
Favorites
History
Workspaces
Admin
Vulnerability Manager Workspace
Home
Watch Topics
Host Vulnerabilities
Overview - Host Vulnerabilities
Vulnerabilities with Exploits Available
Critical Overdue Vulnerabilities
Critical Vulnerabilities not in Remediation Tasks
Vulnerabilities on Windows Servers
Critical Risk Vulnerabilities on Windows Servers
High Risk Vulnerabilities on Windows Servers
Vulnerabilities on Linux Servers
Critical Risk Vulnerabilities on Linux Servers
High Risk Vulnerabilities on Linux Servers
Financial Application Services Team Vulnerabilities
Critical Risk Financial Application Services Team Vu
High Risk Financial Application Services Team Vuln
Log4j Vulnerabilities
Vulnerabilities on External Facing Assets
Container Vulnerabilities
Application Vulnerabilities
Configuration Issues
Create remediation effort
Overview
Vulnerable CIs
Distinct Vulnerabilities
Vulnerable Items
Vulnerable items (VIs)
Active vulnerable item over time
700
600
500
400
300
200
100
0
Dec 14, 2022
Dec 17, 2022
Dec 20, 2022
Dec 23, 2022
Dec 26, 2022
Dec 29, 2022
Jan 1
Jan 4
Jan 7
Jan 10
Jan 13
Active VIs
Deferred VIs
VIs in remediation efforts
Yes
No
20
rows per page

Log4j Vulnerabilities

Watch Topics monitor vulnerable items that meet a filter criteria. Creating a Remediation Effort from a Watch Topic, generates tasks for IT to drive remediation.

Active remediation efforts

□	Number ▲	Description	Vulnerable items	% VIs remediated	Owned by	Risk score	Remediation status
	RE0010002	Active Vulnerabilities related to Log4j: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104	577	5.87	Carla Jackson	93	In-flight

Showing 1-1 of 1

Security and IT teams build trust with a collaboration space for vulnerability, risk, and remediation activities.

Key Features

Collaboration spaces

Expedite resolution across security and IT teams with shared data and integrated task management.

Expansive visibility

Cloud, containers, app, OT, IT, pen test, scanners, you name it: integrations on the store get you full coverage of your dynamic attack surface.

Automation

Replace your manual tasks and spreadsheets with AI-powered workflows that uplevel response, accuracy, and accountability across risk, security, and IT.

Prioritization your way

Flexible risk-based scoring and integrated asset and organizational data empower your team for effective action.

Vulnerability Solutions Management

Send fix suggestions with the ticket, view your organization's most high-impact remediation activities, and monitor their completion.

Performance analytics

Identify bottlenecks and areas for improvement. Consolidate scanning data to determine risk.

Say goodbye to the manual and mundane

And did we mention: no more spreadsheets! Instead, workspaces portray the relevant information according to role. ServiceNow even provides a specific workspace for security and IT teams to collaborate with consistent data, monitoring, and processes such as exception management! This emphasis on a great employee experience is one-way ServiceNow eases the cognitive burden and strain on your extended team.

Coordinate with application owners, developers, and the risk team

With broad DevOps and Agile adoption, internal software developers present a special challenge. The included ServiceNow Application Vulnerability Response unites your DevOps processes and Security teams to improve security at the speed of software development. You can schedule penetration testing, prioritize vulnerabilities from SAST/DAST/SCA scans, and coordinate fixes with developers in deployed applications. Organizations can also identify, prioritize, and remediate vulnerable container images for their cloud native applications with Container Vulnerability Response.

Use in-depth IT and asset insights to prioritize and build up an accurate CMDB

In the ESG survey, the top source of prioritization and patching data is vendor products in use, especially those with high-criticality. When used with the ServiceNow Configuration Management Database (CMDB), Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given asset or service, as well as the current state of all vulnerabilities across the organization.

Respond efficiently across security and IT when critical vulnerabilities appear

When critical vulnerabilities are found, Vulnerability Response can automatically initiate emergency response workflows that notify stakeholders and create high-priority patch requests for remediation owners.

Vulnerability managers can create watch topics to help them quickly visualize findings data and identify risky vulnerabilities based on parameters like exploitability, internet-facing, asset type, business services, and more, allowing for easier, more precise monitoring. Stakeholders can continuously monitor real-time status of patching progress and ensure process visibility across security and IT.

For maximum impact on vulnerability risk, vulnerability managers can also easily identify the most beneficial activities with Vulnerability Solution Management. It works by matching vulnerability scan data against Microsoft or Red Hat's solution databases to recommend which to deploy based on supersedence. If the preferred solution isn't practical, options are visible to help security and IT make the best choice. Once the best solution is found, use Patch Orchestration to complete the last mile of the vulnerability journey: automating the patching process via 3rd party patch tools.

ServiceNow Security Operations

Vulnerability Response is part of the ServiceNow Security Operations portfolio, which includes ServiceNow Security Incident Response, a security orchestration, automation, and response (SOAR) engine built on the Now Platform, and DLP Incident Response. To learn more, please visit: **www.servicenow.com/sec-ops**

Key Features

Configuration Compliance

Find and fix misconfigured software. Prioritize and remediate cloud configuration issues.

Patch Orchestration

Identify and recommend patches for critical vulnerabilities quickly, and schedule patch updates.

Cloud Container Security

Reduce risks from dynamic cloud deployments and container vulnerabilities.

Application Vulnerability Response

Drive faster, more efficient response across security and development teams. Offers a single location for application vulnerabilities from multiple sources and helps prioritize and coordinate the remediation process across security, development, and risk teams.

Reduce Open-source Vulnerability Risks

Software Bill of Materials (SBOM) Support in Vulnerability Response delivers Visibility into the risks of using open-source components, assess high-risk open-source software in your environment and respond with automated workflows.