ServiceNow Configuration Compliance

Monitor, prioritize, and respond to configuration drift, errors, & vulnerabilities

Traditional vulnerability assessment focuses on determining and tracking flaws in both infrastructure installations and software development. However, holistic, risk-based vulnerability management also includes accounting for errors in configurations during deployment and maintenance. Configuration issues take many forms, such as unauthorized open ports for services, weak passwords, and misconfigured network shares. These flaws enable security breaches and business disruptions. As systems get more complex, the management backlog builds.

Many organizations track configuration issues manually via spreadsheets, leveraging data from a security configuration assessment (SCA) tool to scan for anomalies. They also use golden images—hardened images that are certified for OS vulnerabilities, security policies, and operational frameworks—to achieve a degree of configuration compliance.

Golden images can keep infrastructure and applications up to date in accordance with tools like CIS benchmarks, but they are only a snapshot in time. Activities of users, administrators, and software can make systems drift into an exploitable state.

IT teams struggle to keep up. They deserve a way to monitor deviations, prioritize vulnerable assets, assess security posture automatically, and report their findings and updates in real time.

The ServiceNow solution

Instead of wading through outdated data in massive spreadsheets, now security and IT analysts can use integrated workflows to proactively monitor and resolve configuration vulnerabilities.

ServiceNow® Configuration Compliance aggregates data from scanning systems and uses workflows to identify, prioritize, and respond to vulnerable misconfigured software. Configuration Compliance uses the same processes as ServiceNow Vulnerability Response for end-to-end assessment, management, remediation, and reporting.

Through automated triage, service-aware risk scoring, and integrated change management, Configuration Compliance can help protect your business from service outages and data loss.

Easily monitor test results, risk criticality, and outcomes of configuration scanning.

Reduce backlogs through automation

- Centralize configuration data and remediation tasks across teams.
- Group test results and assignments to consolidate tasks.
- Coordinate workflows and track progress of issue resolution.

Improve your risk posture

- Ingest scan and test data automatically, every day.
- Automatically prioritize based on risk.
- Use analysts for higher value activities.

Mature your vulnerability management program

- Use actionable, accurate insight from remediation data to adapt policies.
- Leverage reporting insights to tune security and IT practices and reduce organizational risk.
- Use with ServiceNow Vulnerability Response to manage your infrastructure, applications, and configuration attack surface.
- Use with ServiceNow risk solutions to better report and manage exposure.

Automated triage

You determine the profile you want to validate using external authoritative sources, such as PCI regulations or CIS Benchmarks. Configuration compliance automatically imports policies, tests, authoritative sources, and technologies from your third-party scanner, and automatically correlates test results to configuration items. These configuration tests are grouped into policies that can be modified to meet the needs of every organization, which improves scale and eases management, showing how internal controls such as password length impact compliance obligations like PCI.

Risk-based prioritization

Daily, the solution imports scan test results and severities from secure configuration assessment applications. When tests are run, the solution can match any failed configuration test results against assets in the ServiceNow Configuration Management Database (CMDB) to gauge business criticality and identify owners. A risk score calculator can be customized to include additional criteria, such as test criticality, or to give greater weight to specific factors such as failures on external-facing assets and critical manufacturing application servers.

Rules-driven grouping and assignment

The system automatically groups test results and assigns them to groups or individuals based on conditions you define, such as specified results, technologies, risk scores, and any other data related to the test results. This bulk group expedites remediation management and lets automation help move test results, prioritize based on risk, mark changing state, or defer them. Test results can belong to more than one test result group giving you the flexibility to actively work with one group and monitor another.

Flexible and automated remediation

The security analyst can easily create IT change tickets associated with the configuration items or groups, including priority, timeframes, and target rules. Pre-populated vulnerability information and automated reminders encourage cooperation. Non-critical failures can be deferred to the next standard change window. Once failures are addressed, updated test results close out the issue.

Exception management helps juggle business requirements and risk. Remediation owners can request an exception, and a workflow guides the process to approve, track, and expire the exception.

Visibility for Overall Risk Management

The Configuration Compliance dashboard provides an executive view into policies, CIs, tests, and test results, helping security staff and stakeholders pinpoint areas of concern quickly. Test results from Configuration Compliance can also feed into the separate ServiceNow Governance, Risk, and Compliance (GRC) solution for continuous monitoring of compliance against key indicators and policies.

Get started today

Download the latest release from the ServiceNow store. Configuration Compliance is available with ServiceNow Vulnerability Response, a risk-based vulnerability management solution in the ServiceNow Security Operations portfolio. Designed to help security teams respond faster and more efficiently to incidents and vulnerabilities, Security Operations also features Security Orchestration, Automation, and Response (SOAR). These solutions streamline security incident and vulnerability management through intelligent workflows, automation, and a deep connection with IT.

www.servicenow.com/sec-ops

Driving resolution of configuration issues is crucial to risk-based vulnerability management.

servicenow

SN-DataSheet-ConfigurationCompliance-040121