ServiceNow Configuration Compliance

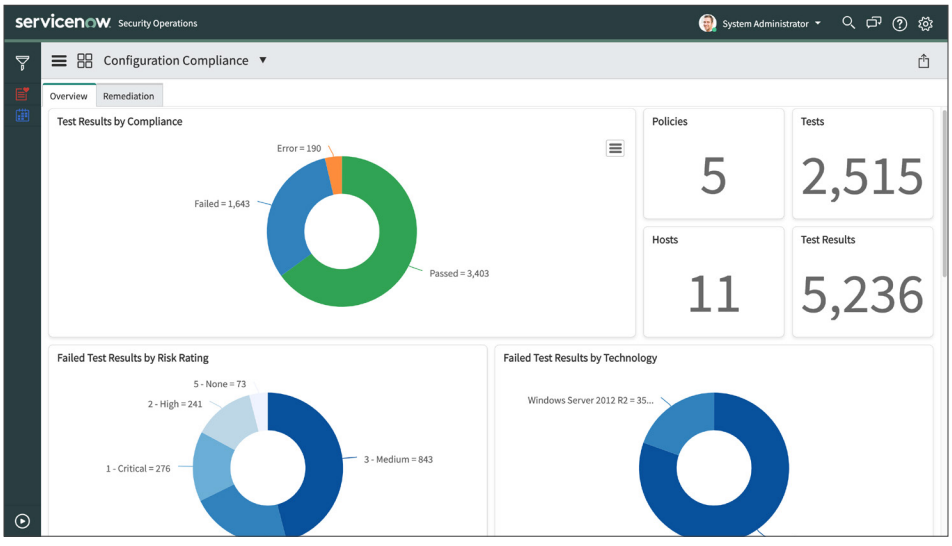
Prioritize and remediate misconfigurations to reduce your attack surface

Traditional vulnerability assessment usually focuses on infrastructure and application vulnerabilities to find flaws at the development level, but a holistic, risk-based vulnerability management approach also includes accounting for configuration vulnerabilities. These are flaws in deployment, such as open services for protocols, weak passwords, and misconfigured network shares, that create openings for attackers. Misconfigurations accounted for 10% of all breaches in 2020, according to the Verizon Data Breach Investigations Report.

Many organizations track configuration issues manually via spreadsheets, leveraging data from a security configuration assessment (SCA) tool to scan for anomalies. They also use gold images – hardened images that are certified for OS vulnerabilities, security policies, and operational frameworks – to achieve a degree of configuration compliance. Gold imaging is a useful way to keep infrastructure and applications up to date in accordance with Center for Internet Security (CIS) benchmarks, but they are only a snapshot in time. For many organizations, IT and security still continuously struggle to keep up with re-certifying their images and conducting compliance checks on a regular basis. They want a way to monitor deviations, prioritize vulnerable assets, and assess security posture automatically, and they need a way to report their findings and updates in real-time.

The ServiceNow solution

ServiceNow® Configuration Compliance allows you to identify, prioritize, and remediate vulnerable misconfigured software in deployment-stage assets. By leveraging automated triage, service-aware risk scoring, and integrated change management, Configuration Compliance can help mature your vulnerability management journey.



The Configuration Compliance dashboard summarizes test results, risk criticality, and outcomes of configuration scanning.

Reduce backlogs and improve visibility

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

Drive faster, more efficient response

Prioritize and respond to misconfigurations quickly with workflows and automation. Reduce the amount of time spent on basic tasks with orchestration tools.

Mature your vulnerability management program

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

It starts with integrating your SCA tool with ServiceNow® Security Operations. Pre-built integrations for Qualys and Tenable make setup easier. Data is imported from your SCA tool into ServiceNow, including tests, authoritative sources, and test results.

Configuration tests: settings or controls that a user enforces on assets (such as password length). These configuration tests are grouped into policies that can be modified to meet the needs of every organization. Tests can also be organized by technology, with different versions of configuration tests based on the specific technology.

Authoritative sources: these are industry-standard regulations that define known software and hardware configurations. For example, this could encompass security policies and procedures like PCI DSS. Authoritative sources can also report on compliance to prepare for an audit.

Test results: the results of the configuration tests are imported into ServiceNow. When import is complete, calculations are run to prioritize the results.

Prioritize automatically

Failed configuration test results are matched against assets in the ServiceNow® Configuration Management Database (CMDB) to help prioritize using business context. A customizable calculator uses both the severity of the misconfiguration and the criticality of the affected asset to prioritize test results. With a prioritized list of configuration test failures, you can pinpoint which configuration issues to address first. Then group together failures based on the teams that will address them.

Remediate quickly with workflows

If remediation requires action from IT, the security analyst can easily create IT change tickets directly from a test result group or associate test results with existing change requests in ServiceNow® IT Service Management. Remediation target rules define the expected time frame for remediation to see when dates are approaching or past due and ensure all failures are addressed. Alternately, when there are non-critical failures, exceptions can be requested and approved to defer remediation to a future date. Once failures are addressed, a follow-up scan confirms the fix and closes the issue.

Gain insights and manage risk

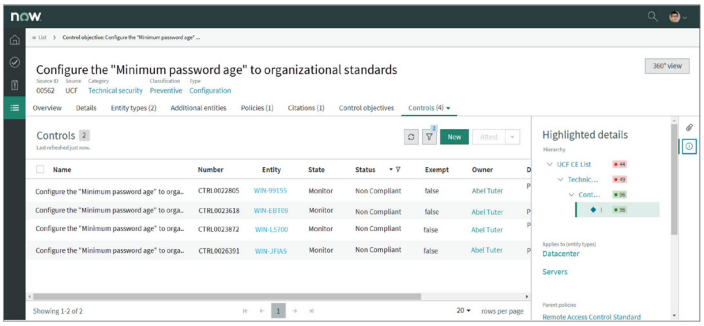
Quickly see the status of configuration issues with the Configuration Compliance dashboard. Test results from Configuration Compliance can also feed into ServiceNow® Governance, Risk, and Compliance to monitor risk. Configuration tests can be associated with a GRC policy to generate controls, profiles, and indicators. A test failure means the control is non-compliant, generating a risk issue. When the misconfiguration is remediated, the risk issue is closed automatically.

This enables real-time visibility into configuration issues and allows organizations to take a proactive, risk-driven approach. Configuration Compliance also works with ServiceNow® Vulnerability Response for end-to-end assessment, management, and remediation of infrastructure, application, and configuration vulnerabilities.

ServiceNow Security Operations

Configuration Compliance 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**



Continuous monitoring of controls shows the entities affected by misconfiguration and identifies any policy exceptions.

servicenow