ServiceNow Security Posture Control (SPC)

Gain visibility and management of your growing attack surface

One question every cybersecurity team needs to answer is: what assets are we responsible for protecting and where are our coverage gaps? According to the *Randori State of Attack Surface Management report 2023*, 69% of organizations have been compromised via an unknown, unmanaged, or poorly managed internet-facing asset in the preceding year. It is critical to monitor which assets are protected or managed by security tools, such as endpoint protection, anti-malware, endpoint management, encryption etc. When these assets are deployed in public cloud infrastructure, any accidental configuration errors risk exposing assets to the internet and should be strictly monitored.

Although there are vendors offering products in the category of 'Cyber Asset Attack Surface Management', some things to consider include:

- Whether or not the product provides an end-to-end solution covering detection of security gaps as well as response workflows
- For large enterprises using a centralized CMDB to track asset inventory and ownership, it takes huge investment and ongoing maintenance to integrate with and benefit form the insights generated by the products that maintain their own asset database
- Can the solution be integrated seamlessly into existing vulnerability management programs
- Does the solution require your teams to build their own custom solutions to map the alerts from these products with the control objectives in their Governance, Risk, and Compliance (GRC) initiatives or is it integrated

Introducing ServiceNow Security Posture Control

Security Posture Control (SPC) provides an end-to-end solution offering asset security detection, response, and compliance that unifies attack surface coverage data, and helps to identify the highest risk gaps.

Detection

Security Posture Control provides visibility into asset security coverage gaps, such as missing endpoint protection agent or missing configuration & patch management agent (and more) on enterprise assets, including on-prem devices and cloud-based virtual machines. This also includes assets with high-risk combinations involving missing security tools, vulnerabilities, internet exposure etc.

Security Posture Control leverages the vulnerability data gathered from third-party vulnerability assessment tools, including Qualys, Rapid7, Tenable and more, to identify high-risk assets.

Key Highlights

Frictionless Approach
Security Posture Control uses API-connectors (Service Graph Connectors) to collect asset data from multiple security and IT tools to generate the insights.

CMDB maturity
Operationalizing Security Posture Control by using Service Graph Connectors integrating with various tools helps with maturing the asset data in CMDB.

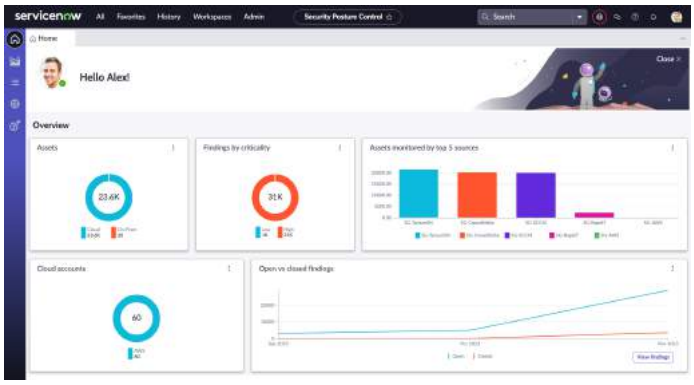
Asset risk engine
Security Posture Control can be used as a central risk calculator for the assets by creating policies based on security tool configuration (e.g., version/profile of endpoint protection agent), core asset data, vulnerability data, and IRM exception data to identify risky assets.

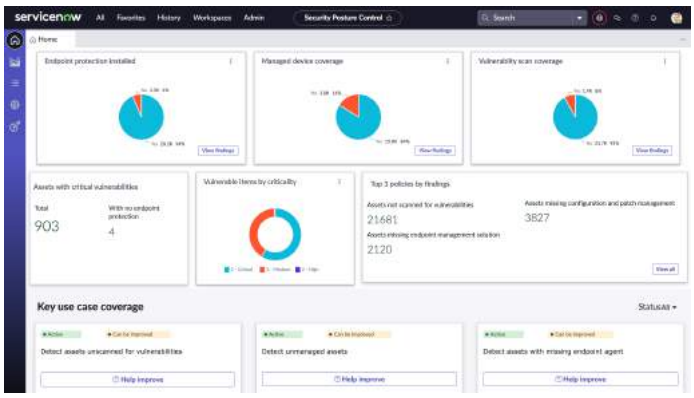
Integrated platform
Security Posture Control comes with built-in better together use cases with CMDB, Integrated Risk Management (IRM), and Vulnerability Response.

ServiceNow includes out-of-the-box policies to detect assets with the following security gaps:

- Assets missing security tools (e.g. endpoint protection, antimalware, etc.)
- Unmanaged assets (assets missing configuration and patch management agent or endpoint management solution)
- Assets missed by vulnerability scanners
- Assets missing security tools and having critical vulnerabilities
- Cloud assets exposed to internet and having critical vulnerabilities and/or security tool coverage gaps

Customers can also create their own policies and custom insights based on asset metadata, security tool configuration data, and vulnerability data to monitor assets violating internal security standards.





Better together with Vulnerability Response

Customers using ServiceNow Security Posture Control and Vulnerability Response together can benefit from the built-in capabilities that allow vulnerability managers to define remediation targets and risk scores for vulnerabilities, based on policy violation data from Security Posture Control. For example, assets missing endpoint protection or cloud assets facing internet with critical security tools missing can be prioritized for remediation/patching of vulnerabilities.

Response

ServiceNow captures any findings related to asset and/or cloud security into Configuration Compliance. This allows automation of response workflows to run, including automated assignment, grouping of issues into remediation tasks, remediation target setting, exception management, and more. As the findings from Security Posture Control are directly tied to Configuration Items (CIs) in the CMDB, identifying the owners for remediating these issues, as well as the ability to manage change requests, is included out-of-the-box.

Compliance

By using the built-in integration between Configuration Compliance and integrated Risk Management (IRM) in ServiceNow, compliance managers can always see the latest compliance status of various control objectives based on policy evaluation outcomes from Security Posture Control.