servicenow. | Microsoft

SOLUTION BRIEF

ServiceNow Security Operations platform and Microsoft: Cutting through security chaos

By integrating Microsoft's rich insights with ServiceNow's centralized point of security incident response, you deliver network-wide visibility and incident context, analyst scalability, and the confidence to act.

The Challenge

Pinpointing and prioritizing threats to IT networks has become a daunting task. Increasing cyber-attacks and an expanding number of vulnerable end points have driven IT and security teams to deploy multiple siloed point solutions. These disparate solutions detect intrusions and threats, but together they also send up an overwhelming volume of alerts and inconclusive information. As a result, critical issues can be missed simply because they are hidden amid the noise. Add to that manual processes and cross-team handoffs that often hinder the security team's effective response and may lead to errors—a problem made worse by a lack of available experts to efficiently deal with security issues. The result: Breaches continue to impact enterprises and take too long to contain and resolve, and costs to the business continue to increase.

The Solution: ServiceNow Security Operations with Azure Sentinel

ServiceNow® has solved this transparency challenge by enabling security teams to natively integrate Microsoft security technology like Azure Sentinel, Microsoft Defender Advanced Threat Protection, Azure Security Center, and more via Microsoft Graph with the ServiceNow® Security Operations platform. This creates the best of both worlds: ServiceNow's system-wide visibility, workflow efficiencies, and automation with all the visibility and rich insights from Microsoft solutions. The combination enables you to respond quickly to security incidents, ensuring business and operations are protected, and to meet ongoing spikes in threats and incidents— all accomplished with the team you have today.

ServiceNow Security Operations ingests alerts from Microsoft's solutions and automatically creates security incidents in ServiceNow® Security Incident Response, enabling security teams to manage, prioritize, and respond to all security incidents from within the Now Platform®. The Now Platform Configuration Management Database (CMDB) maps threats, security incidents, and vulnerabilities to business services and IT infrastructure, creating prioritization based on business impact and risk scoring.

Drawing on the data from Microsoft Sentinel, ServiceNow Security Incident Response tracks the progress of security incidents from discovery and initial analysis through containment, remediation, and recovery. Built-in workflows automatically route incidents to the correct personnel or response tools to contain, mitigate, or resolve threats. Response teams can access post-incident reporting, customizable dashboards, and metrics to gain performance insights for driving continuous improvement of the enterprise's overall security posture.

Solutions

- ServiceNow Security Incidence Response
- Microsoft Azure Sentinel
- Microsoft Azure Security Center
- Microsoft Defender ATP
- Microsoft Graph Security API

Challenges

- Too many disparate endpoints
- Multiple siloed security solutions
- Too much noise and chaos

Results

- Single source for all security alerts and information
- Faster response to security threats
- Simplified security management
- Reduced burden on IT teams

How It Works

ServiceNow Security Operations with Microsoft delivers several key benefits for your organization.

Visibility

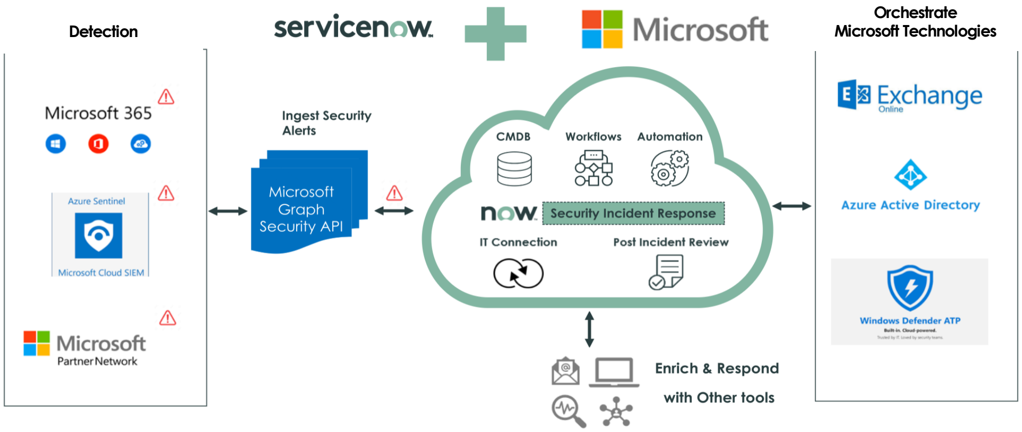
Security Incident Response—Use the data gathered by Microsoft's security technology solutions to quickly identify, prioritize, and respond to security threats. Easily view and track response tasks that run in parallel from a single console. Speed up remediation and ensure company best practices are followed with customizable workflow and automation.

Vulnerability Response—Discover, prioritize, and respond to vulnerabilities based on business impact. The CMDB identifies dependencies across systems and quickly assesses the business impact of changes, enabling response teams to use the workflow and automation tools in the Now Platform to shore up vulnerabilities faster.

Configuration Compliance—Identify and fix misconfigured software centrally from the Now Platform. Workflows and automation enable quick action against individual items or in bulk. Easily coordinate between security and IT in a single platform to address changes and updates, and Configuration Compliance data can be fed into the continuous monitoring feature of ServiceNow governance, risk, and compliance solutions to further mitigate risk.

Playbooks—Accelerate security incident investigations by automating complex and mundane tasks. A comprehensive library of configurable and repeatable playbooks, sub-flows, and actions enables you to quickly automate step-by-step workflows for faster response. Playbooks can be launched and customized easily without writing complicated code. The drag-and-drop feature provides flexibility in moving objects, condition checks, parallel branching, decision tables, and more.

ServiceNow Security Operations and Microsoft Security Solution Architecture



Click here to view the eight Microsoft products that Graph Security API supports.

Workflow and Automation

Threat Intelligence—Add context and threat analysis to security incidents. Find Indicators of Compromise (IoC) and hunt for low-lying attacks and threats. Automatically search threat feeds for relevant information when an IoC is connected to a security incident and send IoCs to integrated Microsoft solutions for additional analysis. Analyze threats posed by targeted campaigns or state actors with the Security Case Management application; case-related records, such as security incidents, observables, CIs, and affected users can be added to cases to accommodate broad and specific analysis. The ability to easily pivot through the records and related information enables analysts to assess whether they are facing a targeted campaign, advanced persistent threat, or other serious threats to the enterprise.

Confidence

Performance Analytics for Security Operations—Create or use out-of-the-box real-time dashboards and reports with 60+ security-specific KPIs for monitoring security operations processes. Organizational objectives and metrics are automatically tracked in Analytics Hub, an immersive studio for analyzing, comparing, and predicting progress toward defined targets. Access real-time trends, overall team and individual analyst performance results, and answer questions in real-time. Make better-informed decisions with embedded and contextual analytics and empower employees with self-service intelligence based on secure, real-time data—while retaining the business context needed to turn insights into action. Get end-to-end transparency within each process, reduce response times, and reveal areas in need of automation and analyst training via the unique visualization library.

Key Benefits

ServiceNow Security Operations with Microsoft integration delivers a number of key benefits to enterprises:

- Cut through the noise to get an enhanced view of all point solutions, creating even more transparency
- Gain critical information needed to prioritize and act on incidents
- Simplify management and response to security issues by deploying a central platform for IT and security teams
- Reduce burden on the security and IT teams and eliminate potential errors by automating incident response processes
- Easily customize security workflows to allow for scaling teams as needed
- Gain greater confidence that you're making the correct decisions in planning, management, and incident response
- Get even deeper knowledge of your security posture and current security status, with the data needed to improve processes and team performances

About ServiceNow Security Operations

ServiceNow Security Operations is a security orchestration, automation, and response engine built on the Now Platform. It brings in security and vulnerability data from your existing tools and uses intelligent workflows, automation, and a deep connection with IT to streamline security response. Learn more.

About Microsoft Azure Sentinel

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across your enterprise. Learn more.

About Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. It is a unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection. Learn more.

About Microsoft Defender ATP

Microsoft Defender ATP provides a centralized security operations experience. Users can see alerts from various supported operating systems in Microsoft Defender Security Center and better protect your organization's network. Learn more.

servicenow. | Microsoft