servicenow™

BUSINESS VALUE OF SERVICENOW SECURITY OPERATIONS

Experience transformational gains from automating workflows and data-sharing among IT, security, and risk teams to rapidly remediate threats.

Why there's a need for solutions that drive agility, collaboration, and scalability

With a rapidly expanding attack surface and an ever-growing volume of costly threats, the road to transforming security operations for technology leaders like you is paved with challenges. You have to figure out how to share siloed data, prioritize vulnerabilities, respond quickly despite manual processes, and do it all while not burning out your teams.

You also face growing threat vectors and increasingly complex environments as you rely more on the cloud, new devices, and transformative services. Today, 280 days is the average time to identify and contain a cyberbreach and each breach leads to an average loss to organizations of $4M.

Top three issues:

1. **Inefficiencies in assessing and protecting your entire attack surface** - Almost 60% of organizations say that things slip through the cracks because emails and spreadsheets are used to manage security response processes.
2. **Lack of optimization and orchestration between IT and security** - A heavy and unmanageable workload is the #1 reason for IT security staff burnout and turnover.
3. **Inability to respond quickly to minimize impact of evolving cyberthreats** - It's hard to believe, but 87% of organizations have experienced an attempted exploit of a vulnerability that was already known.

280 days

is the average time to identify and contain a cyberbreach

$4M

is the average loss in revenue to enterprises of each breach

60%

of organizations say that things slip through the cracks due to manual processes

87%

of organizations experience vulnerability exploit that is already known

A single platform for AI-driven, automated workflows and intra-departmental collaboration

Only ServiceNow enables you to bring together multiple IT functions on a unified cloud platform to deliver a single source of truth. With ServiceNow, your security, risk and IT teams can gain unprecedented visibility of threats and drive continual cyber resilience. They'll be able to rapidly mitigate ever-changing security risks, despite increasingly complex vulnerabilities, threat volumes, and skills shortages. You can empower them to:

Systematically harden the digital attack surface with integrated, AI-driven processes – Automated workflows unite security, risk, IT, and asset management – because threats don't care about business silos. Such an approach can improve the mean time to contain breaches by 85%.

Optimize and orchestrate enterprise security operations to improve investigations, decisions, and threat responses – Digital processes streamline cyberthreat remediation and boost security analyst efficiency by 3x. Start by using automated, best practice playbooks connected to IT and third-party data, tools, and teams.

Respond with agility and minimize impact of evolving cyberthreats – Besides automated playbooks, your teams can integrate a myriad of vendor solutions for orchestrated actions. With these resources, you can reduce delays in response as well as the attacker's ability to succeed.

With these capabilities, you can take the burden off your often overworked and limited staff, as well as free up 8,700 hours annually that you can redirect toward other critical business areas. And that enables you to lead your organization confidently and boldly into a secure future in which the enterprise can thrive even with constant technology change..

A closer look at how you can transform security operations

Systematically harden the digital attack surface with integrated, AI-driven processes.

Readily access data on severity, business context, risk levels, true exposure, and external threat intelligence for a scoring system to prioritize and drive response.

Tap into AI-powered intelligence to assign mitigations and remediations to the right teams for the most efficient and effective response.

Gain visibility across your digital infrastructure—including applications, cloud, OT, and services—to uncover assets and their vulnerabilities.

Automate patch orchestration that works with change management systems and the CMDB to avoid disruption and continuously harden the attack surface.

Optimize and orchestrate enterprise security operations to improve investigations, decisions, and threat responses.

Use security orchestration, automation, and response (the SOAR approach) to scale resources as well as reduce errors and friction from handoffs across tools and responsibilities.

Connect the security operations center (SOC), network operations center (NOC), and data protection teams for seamless management, extraordinary efficiency, and close collaboration that will become critical for major incident management.

Respond with agility and minimize impact of evolving cyberthreats.

Use real-time, adversarial insights to skillfully beat back evolving attack techniques, predict attacker behavior, and guide your responses to high-profile incidents like ransomware and data breaches.

Monitor performance of processes and analysts for continuous improvement as well as reduced risk and exposure.

Take advantage of integrations, playbooks, dashboards, and a common data model to speed investigations and responses across IT, security, and risk teams and minimize impact on the organization (including data loss and reputational damage).

CUSTOMER OUTCOMES

How companies like yours thrive from automating and orchestrating security operations

SAS Scandinavian Airlines

SAS shows how to secure a digital first airline
SAS, one of the world's largest airlines, is a global, digital-first business – and a highly attractive target to cybercriminals. Its main priority is safeguarding company and passenger data. With ServiceNow Security Operations, SAS can easily understand security threats, spot trends, and vanquish attacks. It also monitors performance on all business-critical systems.

RESULTS
- <1 minute to identify a threat
- <10 minutes to contain it
- <1 hour to analyze future risk

> We're a digital-first airline. Cybersecurity is foundational for our business.

Thomas Widen
Head of cybersecurity and compliance for SAS

LEARN MORE ➔

YOKOGAWA

Yokogawa Electric significantly shortens threat response and recovery times
Yokogawa Electric develops and manufactures measurement and control equipment for oil, gas, and chemical industries, to name a few. Inconsistent IT security management put the company's global operations at risk. With ServiceNow, the company streamlined its security workflows to shorten incident response times by 30%.

RESULTS
- 35K global IT assets visible
- 30% efficiency gain by prioritizing incidents
- 1 minute from threat detection to response, vs. 1 to 3 weeks previously

> ServiceNow ITOM and Security Operations provide visibility of global IT asset management statuses, and automate security breach prevention from serious threats.

Tetsuo Shiozaki
Deputy head of digital strategy

LEARN MORE ➔

servicenow

CUSTOMER OUTCOMES

How companies like yours thrive from automating and orchestrating security operations

Wellstar
HEALTH SYSTEM

Wellstar delivers patient care with quality and confidence
Wellstar Health System is a regional – but nationally ranked – U.S. healthcare network. To ensure it could continue providing excellent patient care, the company established an efficient vulnerability management system built on the ServiceNow platform. With a clear plan for prioritization, assignment, and grouping, remediation of vulnerabilities is executed efficiently.

RESULTS
- 99% of vulnerability groups are assigned correctly
- 92.5% of all vulnerability items are remediated within SLA targets
- 100% of critical vulnerabilities are effectively remediated

> “
>
> Wading through laborious spreadsheets to provide data to meet compliance is now a challenge of the past. Senior leadership has access to performance analytics through one intuitive dashboard with customized reporting.
>
> **ITS Partners,** which helped implement the vulnerability management system

LEARN MORE ➔

Accelerating security operations with automation
To avoid manual, spreadsheet-driven processes, ServiceNow leverages its automated, integrated tools for visibility, alert processing, handling phishing email reports, and authentication failure checks. This allows security analysts to focus on investigating and prioritizing issues for fast, then orchestrate remediations. It also creates a more fulfilling experience for the team, allowing the company to attract and retain the best security talent.

RESULTS
- 6X faster alert processing
- 50% increase in number of incidents handled per analyst
- $5.7M hours saved annually

> “
>
> We can’t just hire more people. We need to get the most out of our existing team and automation lets us do that.
>
> **Security Incident Response team leader at ServiceNow**

LEARN MORE ➔

Business value certified by Forrester Consulting

Forrester Consulting can validate the business value of ServiceNow Security Operations solutions via Total Economic Impact™ (TEI) assessment data. TEI is a methodology developed by Forrester Research that improves a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. It helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. All figures calculated below are based on metrics collected from ServiceNow customers as part of Forrester TEI studies as well as customer surveys and interviews, as a commissioned validation on behalf of ServiceNow.

Productivity benefits

Vulnerability response staff function:	% productivity improvement
Exceptions	23%
Reporting	75%
Remediation and tracking	50%
Triage and assignment	55%
Incident response staff function:	**% productivity improvement**
False positives	60%
Duplicates	60%
Triage and escalation	30%
Reporting	30%
Resolution	35%

- Source: The Total Economic Impact™ Of ServiceNow –Validated Financial Model Data: Validated default inputs and benefit metrics for ServiceNow solutions, February 2022.

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Calculations of savings you could achieve

Below are estimates of how much organizations of various sizes could save using ServiceNow Security Operations.

Financial benefits

# of employees in company	# of unaddressed critical vulnerabilities	# of security incidents	Expected annual savings
10,000	350	15,000	$3,974,701
50,000	500	25,000	$23,994,493
150,000	1,000	50,000	$108,839,732

Use our free Value Calculator to see how much your organization could save based on its unique circumstances, then download an insightful business value brief for additional background and details.

Next steps:

Access our Security Operations Use Case Guide

Visit our website

servicenow.com