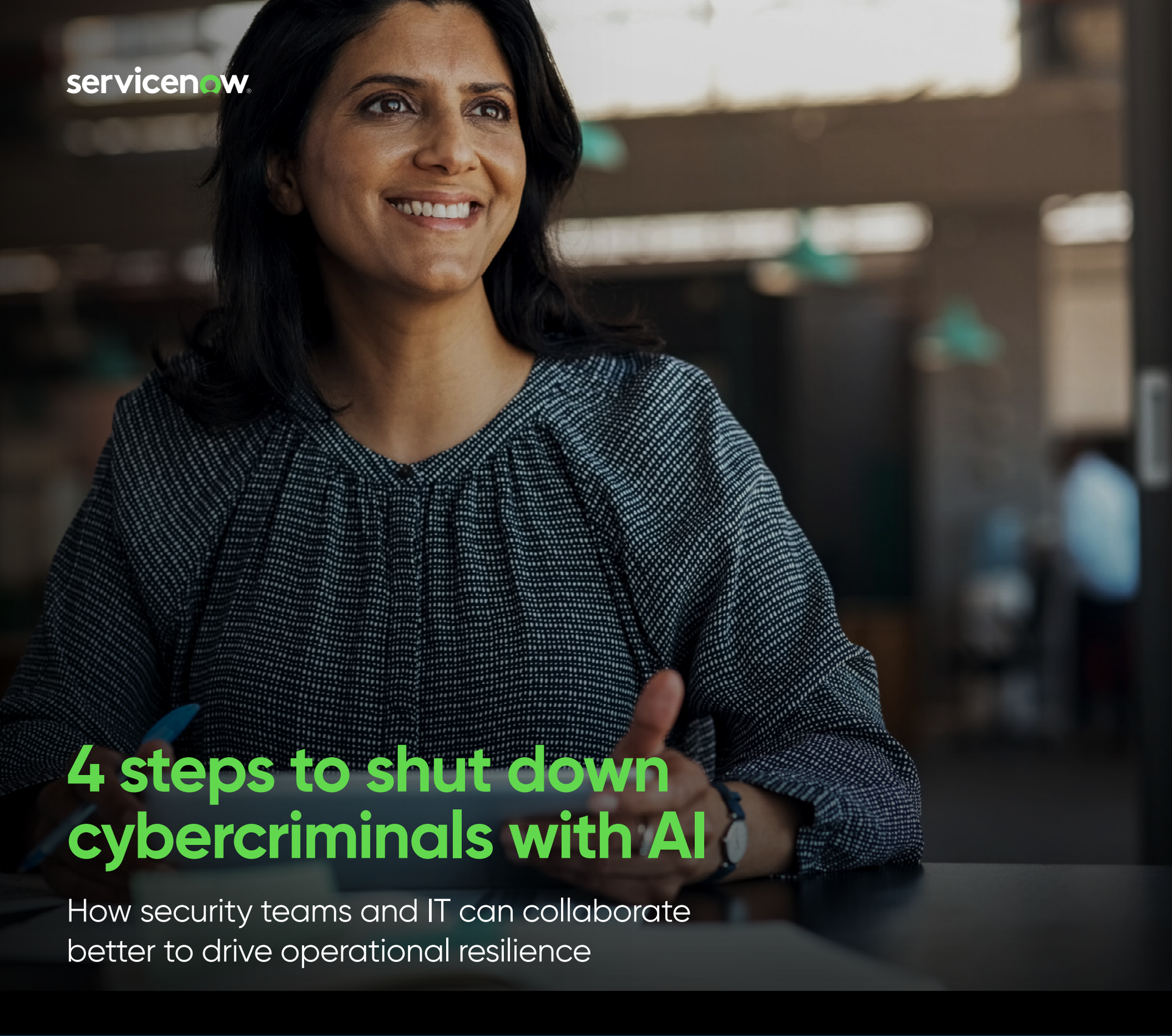
servicenow



4 steps to shut down cybercriminals with AI

How security teams and IT can collaborate better to drive operational resilience

servicenow

The perfect cybersecurity storm

Throughout the past decade, IT security has become increasingly more difficult to provide and manage. Cybercriminals have amplified their complexity and frequency of activity, eager to capitalize on confusion as well as profit from geo-political issues and unrest at home and abroad.

Phishing is the currently most common form of cybercrime, generating an estimated 3.4 billion spam emails sent every day. In 2022 alone, over 48% of emails that were sent included some form of phishing or spam. The massive volume of these threats creates an overwhelming task for security teams. And on top of this, ransomware attempts continue to explode with a 73% increase from 2022-2023.[1,2]

So not only have the threats increased in volume and velocity, but many organizations still allow many people to work from home, creating the "perfect storm." With a distributed workforce, the traditional network perimeter has all but vanished. This operational decision has created a much larger surface area to protect.

The need to act fast and respond to risks and threats has never been greater. Time is not a luxury security teams have, as they are spending over 130 hours a week just monitoring for threats. On average the breaches that occur are estimated to cost organizations more than $4 million a year.[1,3]

servicenow

You can't fix what you can't see

It's more critical than ever to secure and protect an organization's most important assets to reduce the risk of financial loss and reputational damage. In order to prioritize actions and respond effectively, IT and security teams need visibility into the incidents and the business context.

Many organizations are hindered by ongoing issues including:

- Siloed data
- A lack of resources
- Failure to patch known vulnerabilities
- Reliance on manual processes
- Minimal cooperation between security and IT teams.

These roadblocks reduce the speed of response to new threats that are emerging all the time, further compounding these problems:

- An incomplete understanding of the threat landscape
- An inability to prioritize threats quickly and accurately
- A response that's too siloed and slow to prevent impact on the business

Remove the roadblocks to resilience

As you start building a more resilient organization, you need confidence at every stage of the journey. This calls for closer collaboration between security and IT teams to maximize productivity and minimize risks.

That's where the closed loop approach comes in. It's a way to create a truly resilient organization that can protect itself, regardless of what's happening in the wider environment.

It's a four-step approach that lets you:

1. Plan and prioritize essential tasks by importance
2. Continuously monitor threats and vulnerabilities
3. Optimize and collaborate on responses to risks and threats
4. Enable smarter, repeatable response measures

We'll cover each of these four steps a bit later. But first, let's look at what ties them all together: automation.

AI-driven automation

Organizations rightly worry about the financial cost of a data breach. When you're stuck with manual processes and insular workflows, it's much harder to react fast, and it's harder to know what worked so you can repeat it the next time.

That's where automated security solutions that leverage artificial intelligence (AI) and machine learning can help. These AI-driven solutions expedite security analytics and streamline orchestrated incident response. They minimize the need for human intervention and are proven to reduce the costs associated with a security incident or data breach.

Automating workflows along with sharing data and tasks between security and IT teams, helps ensure that threats to your business are resolved before they can impact the business.

Automation that enables collaboration

Automation and collaboration drive efficiency of response and builds operational resilience: 80% of organizations with automation report that they can respond to vulnerabilities in a shorter timeframe.[3]

For organizations with no security automation, breach costs are dramatically higher than they are for organizations with fully- deployed automation. For instance, organizations with a fully deployed AI and automation program save on average $3.05 million during a breach.[1,3]

As the sophistication of threats and actors increase, costs will continue to rise. The average cost of a data breach rose from $9.44 million in 2022 to $9.48 million in 2023, with the global average cost at about $4.45 million.[1]

Breaches can be a huge financial drain on an organization, and without the proper systems and processes in place, the effects can often be irreversible. Deploying a program that utilizes both AI and automation can minimize the impact on an organization's employees and customers and even save it from potential ruin.

servicenow

Challenges	Solutions: steps to shut down cybercriminals	Tools
Siloed data 79% of organizations have no common view of assets and applications across security and IT.[3] Some of the biggest security threats exploit known vulnerabilities. But when the average security operations center (SOC) contains 75 different tools that all generate alerts, it's hard to distinguish the signals from the noise. And it's harder still to escalate issues to the right people to act quickly and reduce the risk of downtime.	**1. Plan and prioritize essential tasks by importance** With complete visibility, security teams know their security posture and gain the business context they need to identify high-impact threats among all the noise happening now. This enables them to keep operations running smoothly.	**Security Incident Response** Simplify identification of critical incidents and leverage automated workflows to speed up remediation. Connect the workflows and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. **Vulnerability Response** Efficiently prioritize patching efforts by linking them to business impact. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk.
Lack of resources 71% of security professionals are likely to quit, due to a combination of challenges in the SOC.[3] Manual processes are hinder IT security teams from continuously monitoring changes to threats and vulnerabilities and new ones as they arise. With security talent in high demand, many organizations don't even have the luxury of throwing more staff at the problem.	**2. Continuously monitor threats and vulnerabilities** By using AI and automation, you can identify security changes in real time and respond at machine speed. Your teams are empowered to prioritize the most pressing threats and vulnerabilities—making the best use of the resources you already have.	**Security Incident Response** Simplify identification of critical incidents and leverage automated workflows to speed up remediation. Connect the workflows and systems management capabilities of the Now Platform with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk. **Threat Intelligence Security Center** Enable your teams to perform advanced threat intelligence actions such as hunting, modeling, analysis, and monitoring. **Vulnerability Management** Automatically assess your assets to identify vulnerabilities, or weaknesses that can be exploited and potentially lead to a breach.
Cross-department collaboration 62% of breached organizations were unaware that they were vulnerable to a data breach.[3] With many teams now geographically dispersed due to today's remote working norm, the opportunity for closer collaboration is limited. The siloed nature of departments hinders efforts of security and IT to collaborate and share information.	**3. Optimize and collaborate on responses to risks and threats** Create open workflows across security and IT teams, enabling faster response. Reduce cumbersome processes and manual handoffs during response and remediation.	**Security Incident Response** Simplify identification of critical incidents and leverage automated workflows to speed up remediation. Connect the workflows and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. **Vulnerability Response** Efficiently prioritize patching efforts by linking them to business impact. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk and scalingteam capacity.
Over-reliance on manual processes 37% of security professionals identified advanced analytics, machine learning, and automation as key to alleviating their pain points.[3] Security teams struggle to identify the root cause of past events to improve controls, policies and strengthen operations. This results in the same risks and threats recurring, which means repetitive, manual work is required from security teams.	**4. Enable smarter, repeatable response measures** Automate cross-functional workflows and evidence collection and put an end to time-consuming and error-prone approaches such as email, spreadsheets, and phone calls.	**Security Incident Response** Simplify identification of critical incidents and leverage automated workflows to speed up remediation. Connect the workflows and systems management capabilities of the Now Platform™ with security data from leading vendors to give your teams a single platform for response that can be shared between security and IT. **Vulnerability Response** Efficiently prioritize patching efforts by linking them to business impact. With orchestration, automation, and better visibility, teams can respond more efficiently, reducing business risk and scaling team resources.

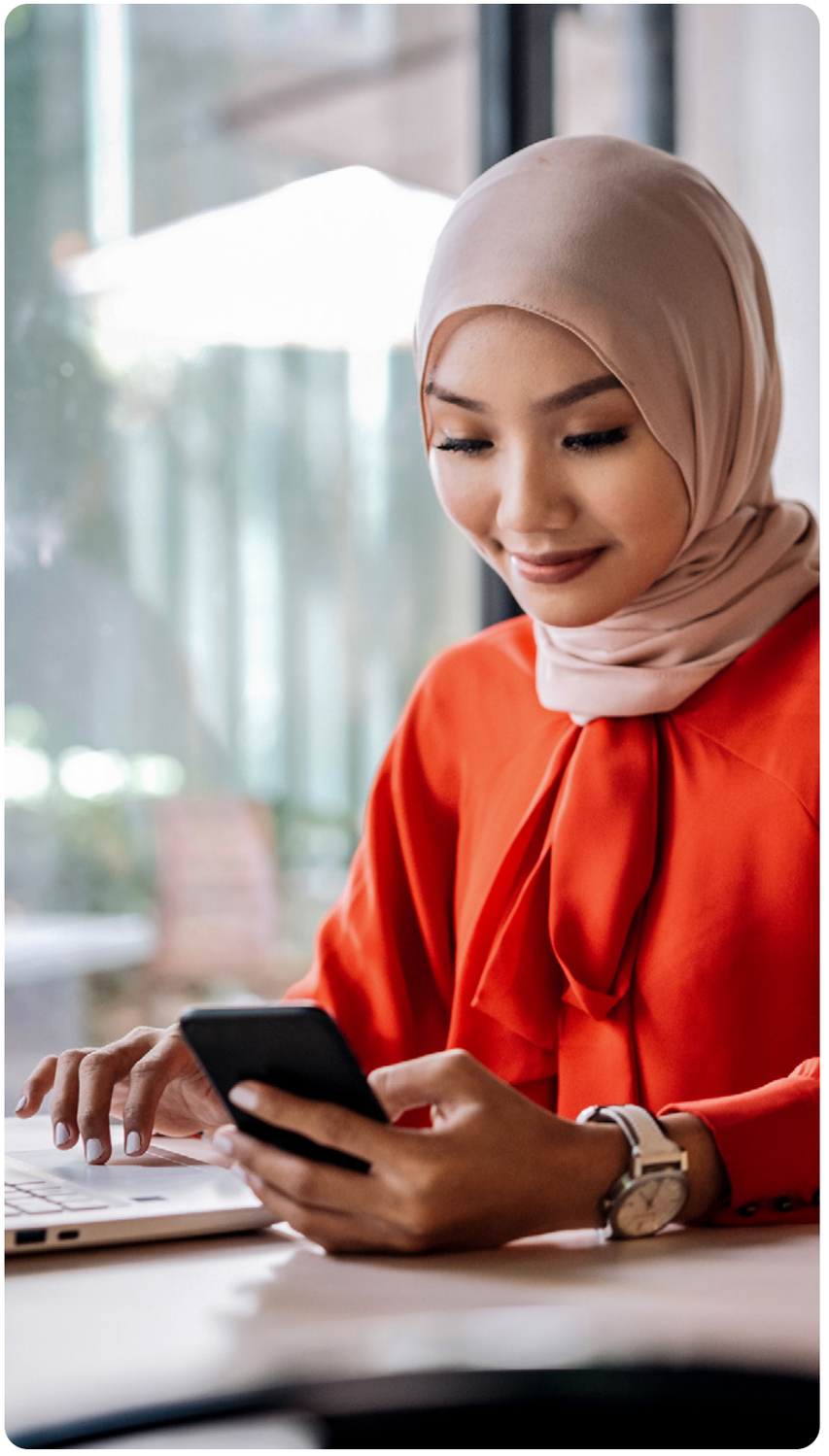
servicenow

Covering all the angles

When security and IT are working in harmony, they're able to drive continuous improvement so the business can always stay one step ahead of the latest threats.

Use accurate and repeatable processes to customize playbooks and policies for smarter, automated responses that unlock new efficiencies. This creates a culture that never stops learning, adapting and reporting, which ultimately leads to stronger, future-proofed security operations.

You can be secure in the knowledge that by pairing human action with AI and automation, you've got all angles covered, no matter what the threats are, or where your teams happen to be.



Automation in action: real-world success stories

Faster security investigations

Scandinavian Airlines (SAS) is a global, digital-first business – and a highly attractive target to cybercriminals. With ServiceNow Security Operations, SAS can easily understand security threats, spot trends, and vanquish attacks. It also monitors performance on all business-critical systems.

Read the full story

Reduced response 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%.

Read full story

Increased efficiency

Wellstar Health System 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.

Read full story

Getting better all the time

ServiceNow delivers business context and problem severity insights on a single platform, so you get a rapid, accurate assessment of the problem. **This helps you:**

- Focus your efforts on the incidents with the biggest potential impact
- Prioritize security incidents and vulnerabilities by business criticality
- Improve decision making for faster and more effective response efforts
- Align the right data with the right people
- Track incidents and assigns tasks to the correct responders
- Ensure tasks are completed on-time

ServiceNow Security Operations is an integrated solution on a single platform that enables your teams to quickly correlate security events and identify dependencies across systems, as well as automate tasks and system workflow interaction across the enterprise. Your teams are empowered to prioritize and align responses to threats and vulnerabilities before your business is impacted.

By leveraging the power of Security Operations and IT solutions together, teams can respond faster and more efficiently, reducing business risk.

Technology isn't about replacing humans in security; it's about empowering them to work better.

Learn More

1. Statista, The impact of cybercrime on companies in the U.S., 2023
2. SANS, Ransomware Cases Increased by 73% in 2023 showing our actions have not been enough to thwart the threat, 2024
3. AAG, The Latest 2024 Phishing Statistics, 2024

www.servicenow.com