servicenow

Top 10 ways to anticipate, eliminate, and defeat cyberthreats like a boss

Improve your cyber-resilience and vulnerability management while speeding up response times

Introduction

Cyberthreats are constantly evolving. Inefficient processes, human error, new initiatives like digital transformation, and unforeseen delays will all increase your risk. At the same time, complexity keeps growing with each new process, application, and piece of hardware. Despite the best intentions, critical items keep falling through the cracks—and most organizations can't even identify what fell through, let alone the potential impact if left unchecked.

The fact is, defending against potential and actual cyberbreaches is an ongoing process, and the collection of legacy point solutions you might be using don't enable you to prepare for risks adequately—let alone react to incidents.

In this ebook, we'll reveal the top 10 ways you can manage risk and cybersecurity with a modern, cloud-based platform approach that equips you to continuously monitor activities, improve decision-making, and accelerate performance when vulnerabilities or breaches occur. Following these best practices will allow you to confidently support ongoing technology change and bolster your reputation as a leader.

servicenow

1

Combine IT, risk management, and security operations workflows on one platform

Good cybersecurity hygiene requires ongoing effort, but workflows on a single platform for managing assets, vulnerabilities, security incidents, and risk can make the process easier. By integrating the tools and teams involved, you can better understand your risks and work efficiently to prioritize and remediate issues before they become a breach. Bringing together IT, security operations and risk management gives you a holistic strategy for keeping your organization safe. From asset discovery and vulnerability management, to integrated governance, risk and compliance management, you can make your people and processes more efficient.

Your security operations must be able to leverage your Configuration Management Database (CMDB) to map threats, security incidents, and vulnerabilities to business services along with IT infrastructure, like servers, computers, and users. This mapping enables prioritization and risk scoring based on business impact, ensuring your security teams are focused on what is most critical to your business.

Working in a single platform also enables efficient collaboration with IT for remediation of risks and incidents, plus delivers the benefits of visibility and service level agreement tracking to ensure nothing is missed. It also allows you to connect security and risk together by aligning with regulatory compliance and ensuring correct business processes are followed. This provides the context needed for ongoing updates to cyberpolicy and processes.

Bringing together IT, security operations and risk management gives you a holistic strategy for keeping your organization safe. From asset discovery and vulnerability management, to integrated governance, risk and compliance management, you can make your people and processes more efficient.

servicenow

2

Automate and orchestrate to save time for security and risk management professionals

Resourcing is an ongoing issue for both risk management and IT security organizations. A 2021 study from the Information Systems Security Association (ISSA) and ESG1 found that 57% of organizations are impacted by the lack of cybersecurity resources, and 44% said the problem is getting worse. One way to mitigate this is by employing automation and orchestration wherever possible to ease the burden on skilled personnel.

Some organizations are reticent to relinquish too much control to their security platform, but there are plenty of ways automation can help you scale while still allowing your skilled analysts to handle decision making. A great starting point for this is threat enrichment. Most organizations already use threat intelligence feeds as part of their incident response process. Automatically integrating and correlating threat enrichment sources, as well as threat context from other security tools, can dramatically reduce the time spent on analysis and incident prioritization.

A 2021 study from the Information Systems Security Association (ISSA) and ESG1 found that 57% of organizations are impacted by the lack of cybersecurity resources, and 44% said the problem is getting worse.

servicenow

3

Use your compliance program as part of your security and risk management foundation

Your organization is required to regularly show that it adheres to a host of mandates that are related to security and risk management, such as:

- Managing access, including creation, change, and termination (tasks include retrieving a laptop and badge and removing an employee from Active Directory)
- Preventing unauthorized access to an asset holding data that's mission-critical to an organization or PII
- Tracking unpatched systems and provide evidence that patches are applied
- Preventing changes to hardware or software without approval or a backout plan as well as documenting emergency changes
- Ensuring and proving that sensitive customer data isn't compromised by indentifying vulnerablities associated with applications that touch it
- Addressing the business risk of misconfigured software, older protocols, and weak passwords (based on regulatory standards such as SOX, PCI, and ISO)

You should use the orchestrated risk management and security operations solutions on the same platform to both maintain compliance and safeguard your organization—easily and confidently.

44% of breaches included personal data—the most expensive to remediate.

– IBM/Ponemon

servicenow

4

Maintain continuous reporting for real-time insights on security posture and security operations center (SOC) performance

Visibility can be an elusive topic in security operations. You know you need it, but what exactly do you need to see to be successful? With the vast number of security tools used in modern enterprises—more than 75 on average—understanding the big picture when it comes to security has become increasingly difficult. But it's more than just the big picture—you also need to tailor visibility to the viewer and their goals. A 2021 report from the SANS Institute4 looked at three key stakeholders and their expectations. With shared data from IT, security and risk management on the same platform, you can provide visibility for:

- Senior management (data on industry trends in security and risk, security preparedness, organizational risk exposure, and SOC performance over time)
- Operational security teams (a near real-time view of vulnerabilities, events, and threats, plus signs of malware, misuse, or compliance failures)
- Analysts (insight on baseline behavior, device communication, the latest threat, and how similar incidents are resolved)

With modern enterprises using an average of 75 security tools, understanding the big picture when it comes to security has become increasingly difficult.

servicenow

5

Proactively monitor and resolve misconfigurations

It's not unusual for IT teams to maintain thousands of different software packages, systems, and devices. While most teams have processes in place to verify configurations, mistakes still happen. Misconfigured software leaves an organization open to attackers and can be responsible for at least 10% of breaches. A newly installed router may have a password entered in clear text which leaves it visible. Maybe an access control for a new firewall isn't set up properly, leaving an opening for intruders. Or the user of a device has admin privileges and can install unauthorized software or change important security settings, which could leave an opening for an attacker to gain unrestricted access to your network. Too often, organizations identify misconfigurations only after an attack. A better approach is to identify the misconfigurations before they put your business at risk.

With risk management and security operations working together, these are easily preventable issues that you can find and remediate to reduce your attack surface. The process starts with setting policies to define secure configurations (for example, minimum password length requirements), and you can monitor data from security configuration assessment tools. But you also want to use risk management to extend continuous monitoring to the configuration hardening policies. This will allow you to identify a failed configuration test result, assess the potential business impact, automatically create an issue, and proactively engage the responsible party to address the weakness before it is exploited. You can also leverage risk management for ongoing oversight to ensure lingering misconfigurations are flagged until they are addressed, and audit trails are created for the business.

Misconfigured software leaves an organization open to attackers and can be responsible for at least 10% of breaches.

– Source: Verizon Data Breach Investigations Report, 2021

servicenow

6

Find and remediate application vulnerabilities

Organizations are increasingly developing their own custom software applications, but these can unfortunately lead to new security risks. About 40% of data breaches stem from web application compromise, according to the Verizon Data Breach Investigations Report. One cause is using open-source code for faster application development, as this code is also readily available for cyber criminals to study and exploit.

To determine security flaws in deployment-stage applications, most organizations use testing tools such as Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), and Software Composition Analysis (SCA). These provide different ways to find weaknesses, whether in a running application or by examining source code. Using multiple testing tools creates a new layer of complexity for security teams to collect data points, identify relevant development teams, and determine next steps.

When you use an automated vulnerability response tool in conjunction with a risk management framework, you can drastically streamline the remediation process. Ideally, the vulnerability response tool should work with application vulnerability scanners and the Common Weakness Enumeration (CWE) to assesses DAST and SAST results, identify vulnerable items, and coordinate fixes. Dynamic (DAST) scans can then assess a running service, and results would come with a URL location of the discovered vulnerability. Static (SAST) scans can use the source code of the application and return a file and line number location of the vulnerability. The scan data should be pulled into the vulnerability response tool to see which applications and their releases are impacted. And of course, your risk management tool should continually report on any unresolved vulnerabilities to ensure they're taken care of.

About 40% of data breaches in 2020 stemmed from web application compromise, according to the Verizon Data Breach Investigations Report.

servicenow

7

Manage and resolve risks from high-profile vulnerabilities

Many organizations find they're overwhelmed with the number of vulnerabilities they need to deal with across multiple departments and functions. A recent survey from the Enterprise Strategy Group found 61% of organizations understand the importance of security hygiene but find it difficult to prioritize the right actions that can have the biggest impact on risk reduction.3 That means when a critical vulnerability hits, it can be hard to tell what's important.

Someone on the security team may be able to spot a vulnerability due to a missing application patch—but it takes an integrated risk platform to tell you that the vulnerability affects the point-of-sale system with the potential for millions in lost revenue. An integrated risk management program can help you gauge the associated risk in relation to all others and track it through to resolution. You can also easily communicate the risk status and potential business impact to upper management as well as identify and enforce the needed security.

You can prioritize and track vulnerabilities with an automated vulnerability response tool A tool like this should be able to connect security and IT teams, and provide real-time visibility into all vulnerabilities affecting a given asset or service. When used with the CMDB, it should be able to prioritize vulnerable assets by business impact using a calculated risk score so teams can focus on what is most critical to their organization. And that means they can respond faster and more efficiently to vulnerabilities,

61% of organizations understand the importance of security hygiene but find it difficult to prioritize the right actions.

servicenow

8

Know an attacker's next move by mapping incidents to MITRE ATT&CK®

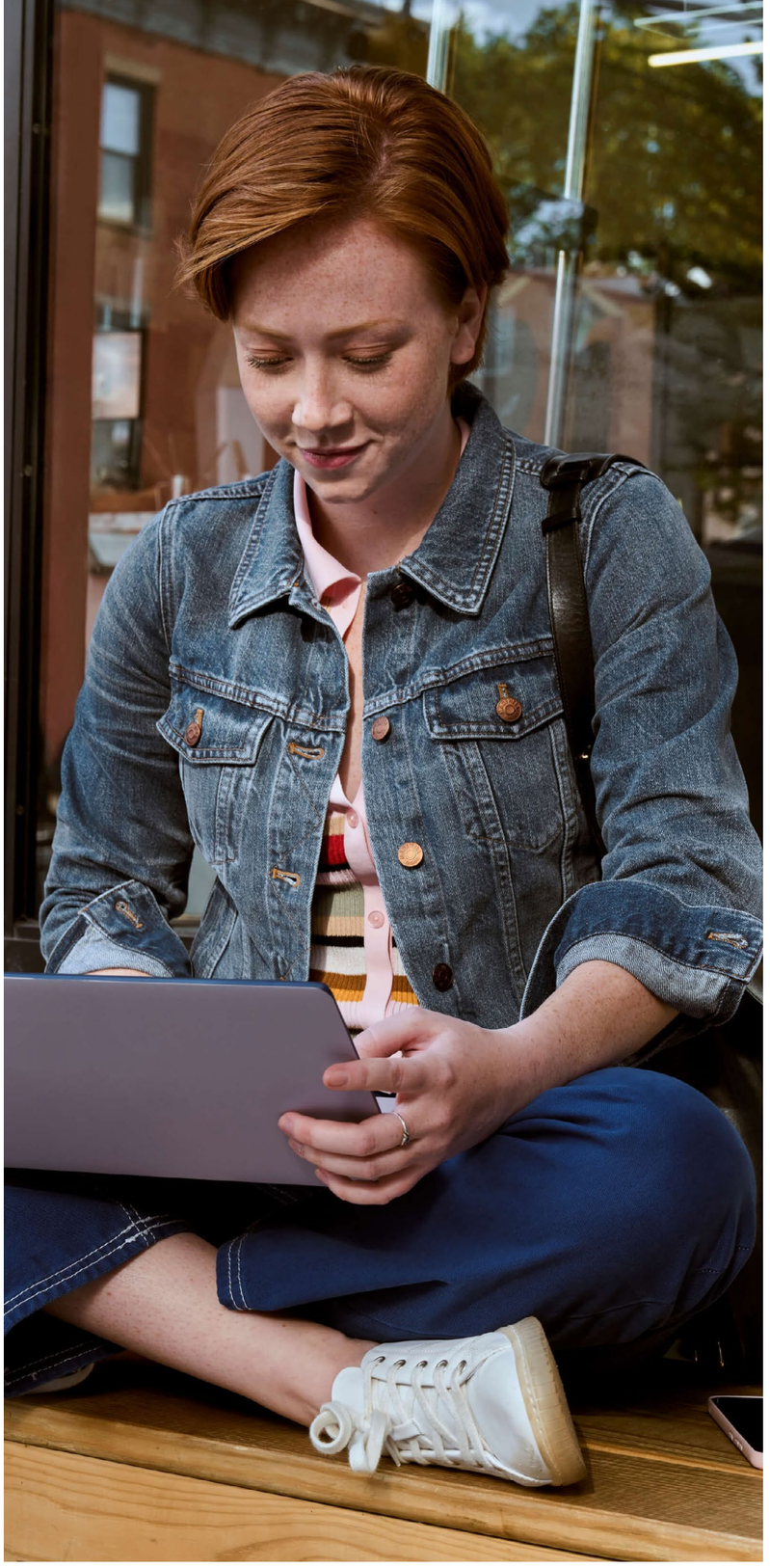
Security teams have historically found internalizing an adversary's intent a challenge when dealing with security incidents and may incorrectly prioritize security incidents without this insight. MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) documents and tracks various adversarial techniques that are used during different stages of a cyberattack. By integrating the MITRE ATT&CK knowledge base with your security incident response tool, you can more quickly identify threats and anticipate cyberattack responses. This framework helps security analysts align events and indicators of compromise (IoCs) with the tactics and techniques used by adversaries and attack campaigns.

servicenow

9

Use playbooks and integrations to accelerate security incident response

Speed is critical when it comes to security incidents. We've covered how automation can help reduce the amount of work security analysts need to do while also driving efficiencies and helping them respond faster. Security incident playbooks are another tool to help increase the effectiveness of your security analysts, especially those who are newer to the organization or early in their career. Playbooks provide step-by-step guidance to remediate common security threats.



servicenow

10

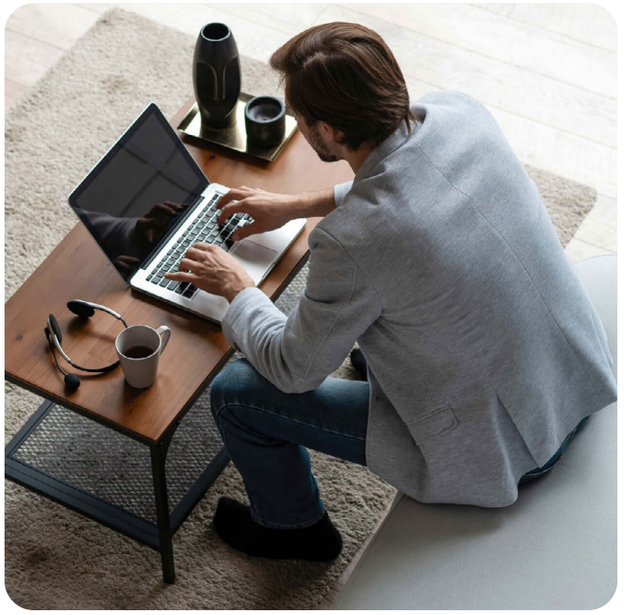
Defend against high-profile cyberattacks and reduce your attack surface

High-profile cyberattacks such as ransomware have become big news, causing major disruption to business, government, and the general public. The total cost of ransomware was more than $20 billion USD in 2021 and will be as much as $265 billion annually by 2031. Between expanding attack surfaces and the rise of ransomware-as-a-service, the risk will only continue to grow.

Adequately defending against these high-profile attacks requires organizational resilience, defined as "the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper." This final best practice is all about applying all of the other ones we've covered in this ebook. We can't emphasize enough how important the first two steps of resilience are (anticipate and prepare). In essence, best practices one through eight are all about these two steps—and having continuously monitored controls established to eliminate the chaos of cyberattacks. Following these practices gives your organization a proactive posture instead of a reactive one, ensuring you stay ahead of whatever comes your way.

70% of all system intrusion breaches involved malware, with ransomware making up 99% of those cases.

– Source: Verizon Data Breach Investigations Report, 2021



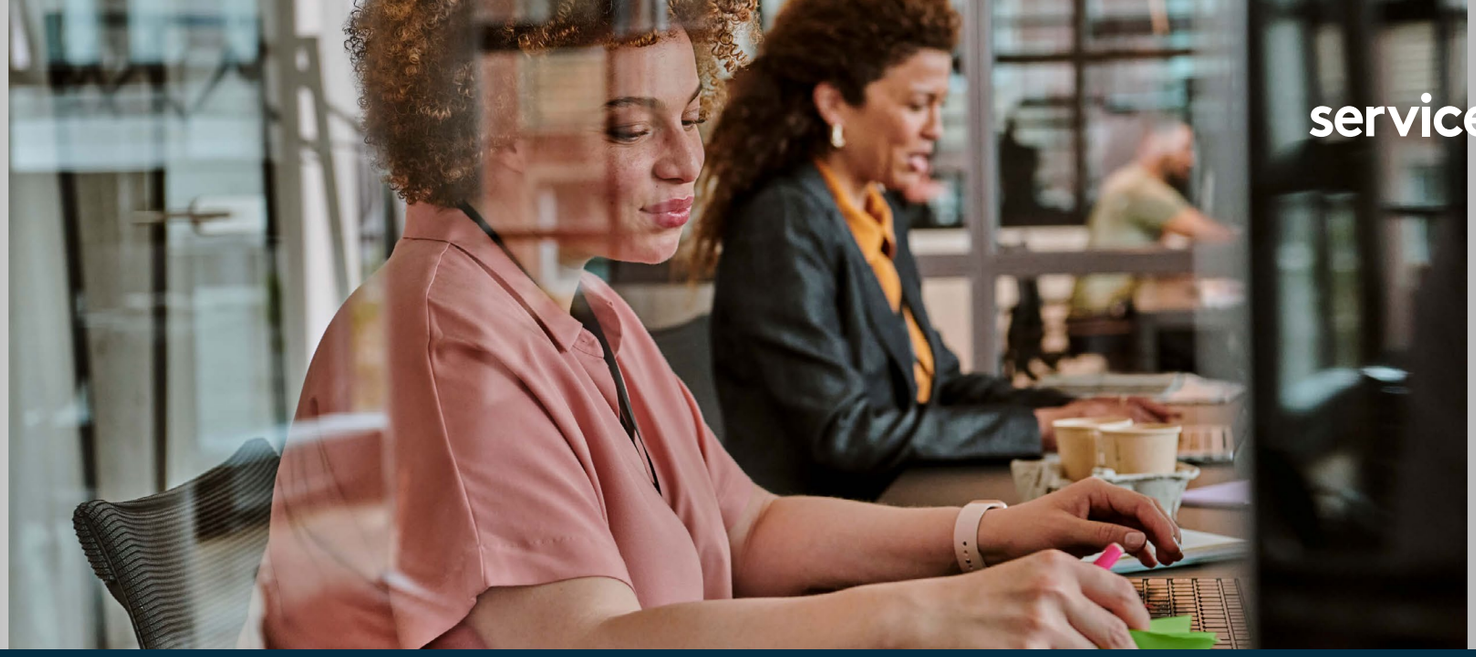
Conclusion: Elevate the maturity of your security and risk management posture

The scope and potential impact of cybersecurity threats will continue to expand. And any organization pursuing a digital transformation faces new challenges every day. To anticipate and counter these greater risks and increased pressures, you must embed IT operations, IT asset management, security, and risk management into new digital workflows and ensure these functional areas think and act as one. They must share information more effectively to—first and foremost—prepare for the worst with controls in place that are continuously monitored. This ensures you can identify breaches and disruptions before they wreak significant damage.

Only an integrated solution on a common platform can solve this challenge, allowing you to:

- Continuously monitor for risk and cyberthreats across the extended enterprise
- Holistically prioritize risks, vulnerabilities and incidents based on business impact to improve decision making
- Automate repetitive and redundant manual tasks to increase performance

ServiceNow offers such a solution. It helps your IT, security, and risk management teams to scale faster, smarter and more efficiently—automating critical data collection and remediation processes across these teams to effectively respond to threats and incidents. Plus, it brings in security and vulnerability data from your existing tools and uses intelligent workflows to streamline security response. ServiceNow helps you use the power of the Now Platform® to reduce cybersecurity risk and drive cyber-reslilience.



Learn more

Ebook: Same cyberthreat, different story

See how security, risk, and technology asset management teams collaborate to easily manage vulnerabilities—within a workday

Governance, Risk, and Compliance use case guide

Discover how to continuously monitor activities, improve decision making, and increase performance through automation.

Security Operations use case guide

See how to improve your cyber resilience and vulnerability management while speeding up response times.

About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help to digitize and unify organizations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNow®. For more information, visit: www.servicenow.com.