servicenow

6 steps to a stronger security posture through automation

Boost your cyber resilience to enable ongoing technology change with confidence

61%

of organizations surveyed said they understand the importance of security hygiene but find it difficult to prioritize the right actions that can have the biggest impact on risk reduction

So many tools, so little time

Remote work and the acceleration of digital transformation has pushed more companies to the cloud. This has expanded the attack surface of many organizations and has led to more expensive breaches according to the Ponemon Institute.[1] Preventable errors like misconfigurations are also expected to become a leading cause of cloud breaches. So how do you effectively protect your organization?

There's no limit to the number of security tools on the market to help you harden your attack surface and thwart attackers. But just adding more tools isn't enough. In fact, more tools often only create more alerts for staff to investigate—an additional challenge when security staff are in short supply. And many organizations are still using cumbersome spreadsheets to manage security hygiene.

With so much to keep track of, prioritization is critical to know where to start, but a recent study by ESG Research found many organizations struggle with this. About 60% of organizations surveyed said they understand the importance of security hygiene but find it difficult to prioritize the right actions that can have the biggest impact on risk reduction.[2]

As the attack surface continues to grow, it's not surprising that some teams are overwhelmed trying to keep up. To have a successful, proactive security program, you need to integrate the tools and teams involved to see the bigger picture and understand your risks. Workflows and automation can help you work effectively across teams to prioritize and remediate issues before they become a breach. Let's look at six steps you can take for more efficient and effective attack surface hardening.

1 Ponemon Institute, Cost of a Data Breach, 2022

2 ESG Research Study, Security Hygiene and Posture Management, January 2022

Step 1:

Know what you need to protect

Before you can get started, you need to know not just what you have, but what's important. That means understanding your assets, services, software exposure, and dependencies. With the attack surface constantly changing, this is an ongoing effort. Therefore, you need a way to build out your configuration management database (CMDB) and keep it consistently updated, whether assets are on-premises or in the cloud. This isn't practical for most organizations without automation, especially with dynamic cloud environments, as many are still using spreadsheets.

You need to discover and keep up to date with all types of assets in your environment, including virtual machines, servers, storage, databases, applications, and containers. This should also include your external attack surface, like public-facing assets outside of your firewall that could be compromised to reach your internal resources. In fact, 69% of organizations surveyed experienced a cyberattack that started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset.[3]

3 ESG Research Study, Security Hygiene and Posture Management, January 2022

69%

of organizations surveyed experienced a cyberattack that started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset

Assets then need to be classified to understand whether it's a laptop, cloud application, operational technology (OT) device, or something else. If data is coming from multiple sources, you also need to be able to reconcile conflicting data or duplicates for an accurate inventory. Both a horizontal and top-down approach are necessary to identify upstream and downstream dependencies to know if something supports a critical service. This mapping will assist with prioritization of any issues found, as will knowing if an asset is subject to regulatory requirements such as HIPAA and PCI DSS.

Software asset management can also help you know what's in your environment by tracking licenses and versions. Easily find all instances of a vulnerable version of software and prevent employees from installing unauthorized applications. This can help augment and update the asset database to ensure you have current, accurate information. You can even see when certain software will no longer be supported or patched and will pose an additional risk.

Top vulnerability management challenges

The biggest concerns according to an ESG Research survey:

1. Keeping up with the volume of open vulnerabilities
2. Coordinating processes across different tools (scanning, spreadsheets, etc.)
3. Automating the process of prioritization, owner assignment, and mitigation[5]

Step 2:

Find and prioritize vulnerabilities

Now that you know what you have, you can start searching for weaknesses. The challenge with vulnerabilities is often the sheer volume of them. If you're scanning infrastructure, cloud, and applications, it can easily become overwhelming for both security and IT, as multiple scanners and teams are involved. It's not possible or practical for patching to always be 100% up to date, so prioritizing what to patch is key.

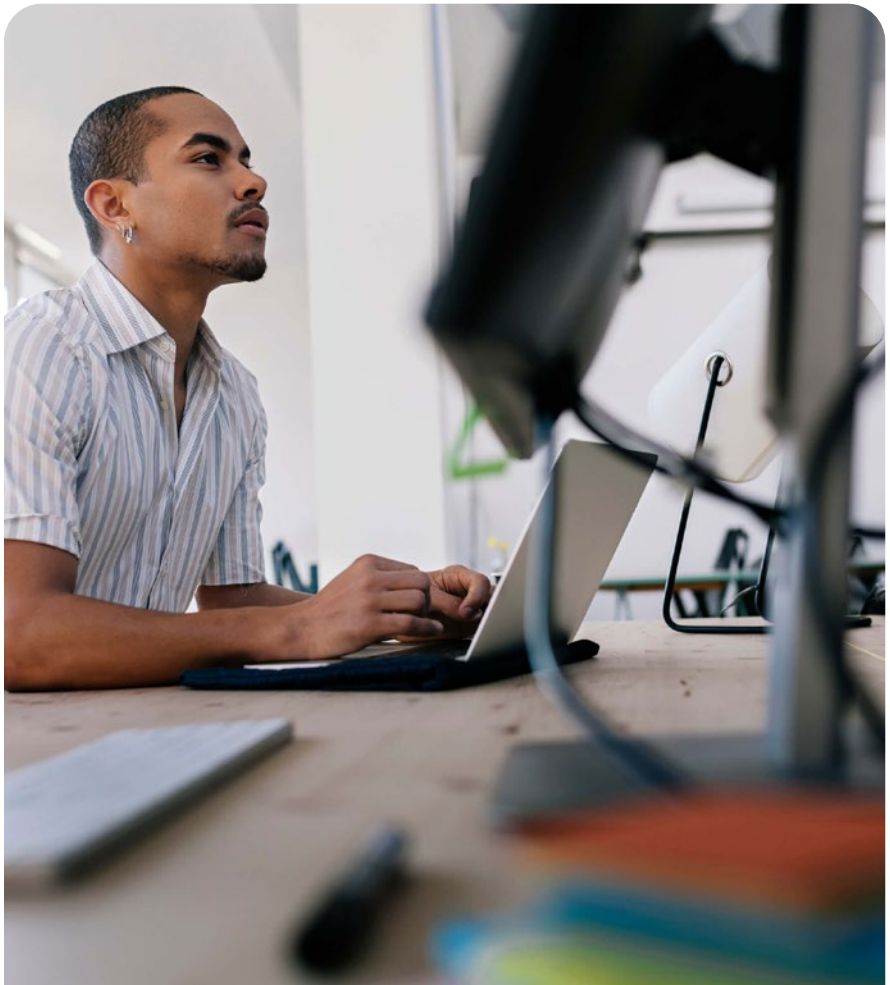
CVSS scores are still the most common means of prioritization, but threat intelligence should be included, too. Just 2%–7% of published vulnerabilities are ever observed to be exploited in the wild;[4] therefore, if you know an exploit exists for a vulnerability, that should be a higher priority. Knowing whether a specific CVE is related to potential attacks, as found in the MITRE ATT&CK framework, can also help prioritize vulnerabilities by risk.

Still, that's not detailed enough, and this is where the CMDB comes in. It can add business context, meaning how critical the particular asset is to your organization, to that prioritization score. Every organization is different, so you'll want to be able to configure your own prioritization calculator to ensure you're focused on what's most important.

Whether there are potential issues due to vulnerabilities on premises, in the cloud, in applications, or in OT devices, the general process is the same. Issues need to be prioritized and assigned to the right people for remediation. You'll want to manage all of those vulnerabilities, regardless of source, in a single system for easier tracking. In addition, automatically identifying the most impactful solution for a vulnerability can aid in decision making, speed up the resolution process, and help remediation teams work more efficiently.

4 Forum of Incident Response and Security Teams, 2023

Misconfigurations are the leading cause of error-related breaches



Step 3:

Address misconfigurations

Traditional vulnerability assessment usually focuses on infrastructure and application vulnerabilities to find flaws at the development level, but a holistic, risk-based approach to security hygiene also includes accounting for configuration vulnerabilities. These are flaws in deployment, such as open services for protocols, weak passwords, and misconfigured network shares, that create openings for attackers.

Misconfigurations pose a huge security risk, accounting for 35% of cyber incidents.[6] Just like other types of vulnerabilities, misconfigurations must be identified, prioritized, and remediated regularly.

It starts with a security configuration assessment tool to find misconfigured assets on premises or in the cloud. These failed configuration test results then need to be prioritized for remediation. The scoring should include whether the affected assets support critical services as determined by your CMDB. External authoritative sources like the Center for Internet Security (CIS) or compliance regulations can also assist in prioritization. Then automatically group together test failures based on the teams that will be involved in remediation.

6 SOCRadar, February 2023

Improve your security asset management

An ESG Research survey identified these top 3 actions:

1. Automate associated tasks and processes
2. Integrate security and IT tools
3. Establish metrics and reports to communicate importance to the business[8]

Step 4:

Remediate efficiently with IT

Security teams are often responsible for finding vulnerabilities and misconfigurations but not fixing them. About 30% of respondents in a survey by the Ponemon Institute[7] said IT operations is responsible for patching. Here's where connecting your security tools with IT and security teams via a single platform increases efficiency. You could have someone constantly cross-referencing your vulnerability or configuration assessment data against the CMDB for asset owners, or you could have automated workflows perform those tasks. Machine learning can group tasks and assign them to the right teams in IT.

Workflows can also help the IT team with patching. Use automation and orchestration to map solutions to assets, apply the patch, and initiate a rescan with the vulnerability assessment tool to ensure the fix is complete. This reduces the amount of work required for each patch. Integration with IT change management makes it easier for IT to track and complete the work using their established processes.

If IT and security work in the same platform, that also increases visibility across teams and ensures each group has the information they need. For example, security personnel likely want all data about an issue, but IT may prefer to see only what they need to know to accomplish the task, such as the asset and preferred solution. You don't need to worry about tasks slipping through the cracks when each one has a tracked service level agreement (SLA). Dashboards should include tracking patches versus SLAs to understand performance.

7 Ponemon Institute, Value of Vulnerability Response

8 ESG Research Study, Security Hygiene and Posture Management, January 2022

85%

of organizations' security hygiene and posture management activities are defined and executed based on regulatory compliance requirements[9]

Step 5:

Take a risk management approach to security

IT isn't the only team that needs to work closely with security in order to manage your attack surface. As many security requirements are also driven by regulatory compliance, hardening your attack surface must involve your risk and compliance teams. Combining risk, security, and IT together in a single platform makes it easier to monitor compliance.

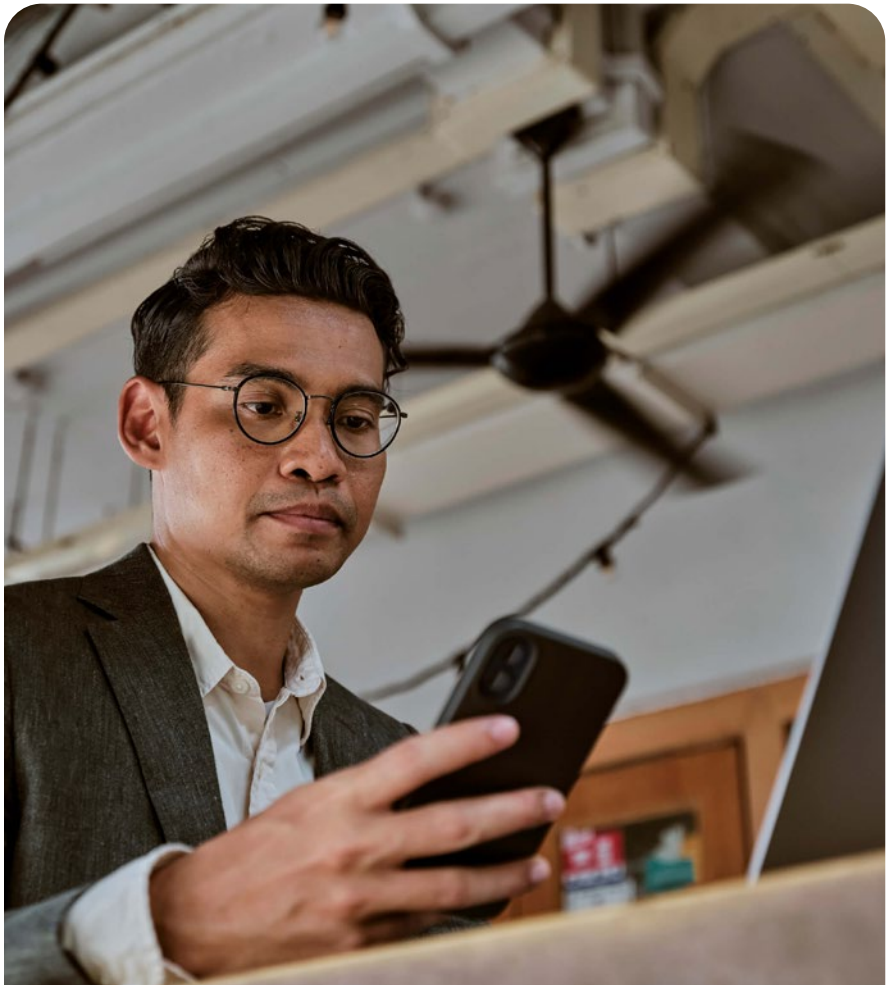
Harvesting and continuously monitoring key risk indicators from your vulnerabilities automatically allows you to track business risks due to vulnerabilities. For example, if a critical vulnerability's remediation SLA has lapsed, it poses an unnecessary risk that needs to be addressed.

Integrating vulnerability management and risk management is also useful for exception handling. Not all vulnerabilities can be patched immediately, whether due to resourcing or potential disruption. You need to be able to manage exceptions and track the risks and approvals associated with those exceptions. Understand tradeoffs and use robust governance for sound decision-making.

9 ESG Research Study, Security Hygiene and Posture Management, January 2022

51%

of respondents say their organizations are not assessing the security and privacy practices of all third parties before granting them access to sensitive and confidential information[10]



Step 6:

Go beyond your own ecosystem

Your attack surface can expand beyond your own infrastructure. Losing a vital supplier to ransomware could hurt just as much as if your own business had been attacked. There's also a direct risk to your organization if your vendors have access that can be compromised. Or they may have sensitive information that you are liable for due to privacy regulations. But monitoring risk of third parties adds an extra level of difficulty, and many breached organizations admit to not adequately assessing third party risk. That's unfortunate, because 13% of breaches in 2022 were caused by vulnerabilities in third-party software.[10]

This makes vendor risk management an important part of good security hygiene. Easily collect vendor assessments via a self-service portal to ensure vendors are compliant. Assessments are scored automatically based on a weighted scoring framework backed by a configurable scoring methodology and risk engine. You can associate issues to risks, controls, and risk ratings at a questionnaire and assessment level to track vendor risk alongside internal risks.

Thoroughly vetting your vendors before granting them access to sensitive information or systems is key to hardening your attack surface, though it's frequently overlooked. Self-service and automation simplify the process, allowing you to drive transparency and accountability with third-party stakeholders and align with overall enterprise risk management to create an integrated view of risk.

10 Ponemon Cost of Data Breach Report, 2022

Hardening your attack surface is easier than you think.

Good security hygiene requires ongoing effort, but workflows, automation, and a single platform for managing assets, vulnerabilities, 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.

The Now Platform® lets you bring together security, IT, and risk for a holistic approach to keeping your organization safe. From asset discovery to vulnerability management and integrated risk management, ServiceNow can make your people and processes more efficient. It will also inspire the confidence your organization needs to enable continual technology change for growth, even with economic challenges.

Learn more about ServiceNow Security Operations

About ServiceNow
ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud based platform and solutions help 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**.