Red Hat

Next

Security spotlight: The cost of human error and the advantages of automation

Why government agencies are reconsidering manual approaches to managing security and how intelligent automation helps prevent potential threats from costly security gaps

In this e-book:

01 Introduction: The growing threat of cybercrime

Cybercrime is on the rise. In fact, the number of cybersecurity incidents increased by 15.5% in 2021, while the number of material breaches grew by 24.5%.[1] Even so, 34% of public sector organizations say they are not well prepared for the rapidly changing threat landscape.[1]

As government agencies embrace new technologies and adapt to hybrid models of work, cybercriminals are transforming their capabilities, too. Workforces and computing resources are becoming more distributed, and the fast-evolving landscape of IT infrastructure presents bad actors with new opportunities to exploit security gaps and vulnerabilities—causing the organizational cost of data breaches to grow. Even an organization that develops a strong security posture faces more risks in this environment.

Proactive security against cybercriminals

As cybercriminals devise new ways to breach protected systems and data, organizations are facing internal and external pressure to develop more strategic and proactive protections against cyberattacks. In fact, their data security and privacy measures must comply with more comprehensive rules and regulations.

And this trend of increasing security and privacy regulations applies across industries and regions. For example, the European Union's General Data Protection Regulation (GDPR) sets strict rules around how personal data is collected, used, and protected. Singapore's Cybersecurity Act establishes a framework that requires owners of critical information infrastructure to follow specific best practices for governance, access control, and incident detection and response, as well as other areas. Argentina's Dirección Nacional de Ciberseguridad also issues policies for protecting critical information infrastructure and improving security incident prevention, detection, response, and recovery at the national level. And U.S. government agencies must deploy zero trust architectures to meet federal cybersecurity objectives by the end of 2024.

Reinforcing your defenses

Organizations looking to improve their cybersecurity need to identify existing vulnerabilities first. Too often, human error and a lack of awareness can compromise security, even when comprehensive strategies are already in place. Left unchecked, small mistakes can introduce risk to your systems, compounding an already complex problem. As a result, organizations are adopting automation to increase reliability and reduce risk in their security strategy.

In this e-book, we'll explore how the risks introduced through human error affect the fight against cybercrime. We'll also discuss how automating key cybersecurity risk mitigation strategies can strengthen your security while reducing the volume of time-consuming tasks that burden your IT teams.

The global cost of cybercrime

24.5%

Growth in number of material breaches in 2021[1]

US$4.35 billion

Global average cost of a data breach[2]

60%

Percent of organizations that increased their service or product prices due to a data breach[2]

1. ThoughtLab. "Cybersecurity Solutions for a Riskier World." 2022
2. IBM. "Cost of a Data Breach Report 2022." July 2022.

02 Effective security strategies should involve everyone

Humans make mistakes

Even within IT teams, people often underestimate or misunderstand their systems' vulnerabilities and the resulting security risks. Our inability to accurately assess risk can result in significant costs to organizations.

For example, imagine this: A production outage occurs in a firewall, forcing a firewall engineer to manually update a policy under severe pressure. The change remedies the outage but also introduces a new attack vector that can be exploited by cybercriminals.

In this scenario, the manual, rushed firewall configuration change could result in various negative outcomes, including compromised data, violation of industry and government data security regulations, service interruptions, and system downtime—all at the organization's expense.

From patching applications and updating firewalls to setting and enforcing administrative privileges, so many elements of the security puzzle can go wrong when handled manually. And as cybercriminals get better at identifying and exploiting vulnerabilities, relying solely on manual operations for these tasks can have detrimental or irrecoverable consequences.

Talent shortages can worsen security gaps

Cybersecurity skills are in short supply, which only increases the likelihood of human error during manual tasks. There are simply not enough people with the skills and training to assess and address security risks. According to the (ISC)[2] Cybersecurity Workforce Study, 2.72 million more IT security workers are needed to close the global cybersecurity gap.[3]

This chronic shortage of cybersecurity experts makes it more difficult for organizations to adequately manage risk. Their IT teams are already stretched and don't have the time to enforce security processes across the organization—let alone establish them in the first place.

Equipping security teams with automation

Addressing how both manual security processes and skills shortages increase risk for organizations has become essential in the fight against cybercrime, and automation solutions offer a promising solution. As we will explore further, automating security processes provides much-needed consistency, accuracy, and scalability across the organization.

The risk of manual security measures

"Organizations with fully deployed security AI and automation were able to detect and contain a breach much more quickly than organizations with no security AI and automation deployed."[4]

3. (ISC)[2] Cybersecurity Workforce Study. "A Resilient Cybersecurity Profession Charts the Path Forward." 2021.
4. IBM. "Cost of a Data Breach Report 2022." July 2022.

03 Common challenges of risk management

Government agencies need better risk management

To ensure the confidentiality, integrity, and availability of official information, government agencies must be able to identify and manage risk, accurately and efficiently. Security threats are constantly evolving, which means an organization's risk profile and security posture should remain flexible. Automating operations is critical to be able to rapidly respond to these changes.

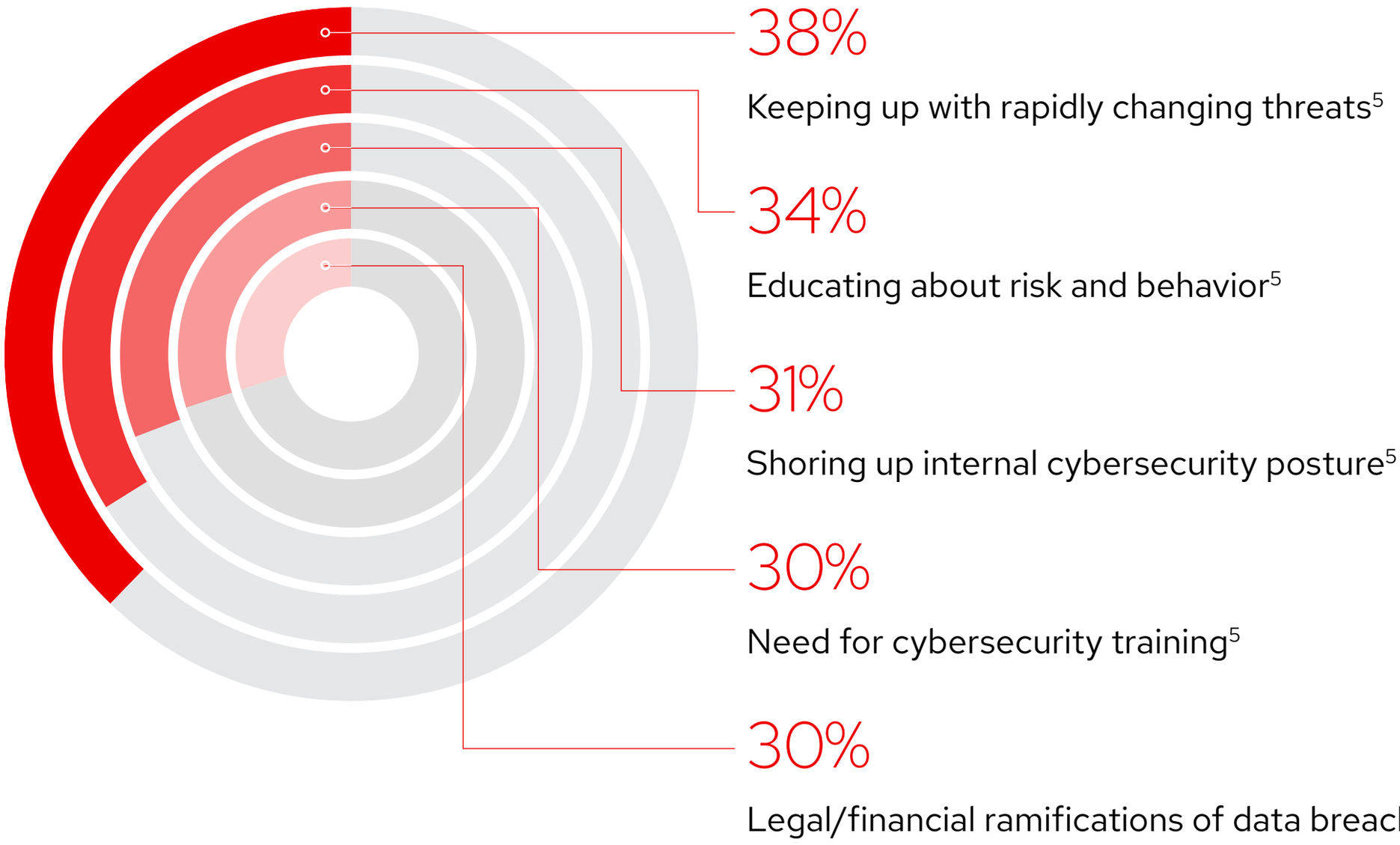
Obstacles to changing security practices

In their effort to enhance security, government agencies face several challenges—particularly related to managing change. Common questions include:

- How do we scale our team to implement a new cybersecurity initiative?
- How do we support different parts of the organization to ensure new security protocols are adhered to?
- What can we do to better secure our existing systems—which deliver critical services—while adopting modern security strategies that the organization needs?
- Can we implement strategies like zero trust on established architectures?

However, instead of seeing these considerations as a burden, organizations can view their changing security landscape as an opportunity to reassess their security practice and implement more rigorous protocols.

Common cybersecurity challenges



5. "State of the Channel 2021." CompTIA, Aug. 2021.

04 Strengthening your security posture with automation

Common themes in security regulations

Across all industries and regions, data privacy, access control, and incident protection, detection, and response are common themes throughout cybersecurity regulations and initiatives. While some regulations provide implementation details, many simply set guidelines and required outcomes, leaving organizations to figure out how best to comply based on their current situation, staffing levels, and infrastructure.

Security automation can help government agencies and organizations combat cybercrime and comply with regulations. By automating regular, repetitive work, cybersecurity teams can focus on more critical, strategic tasks. Additionally, automation helps avoid overburdening IT teams with tasks and work volume that make human error more likely and increase security risk.

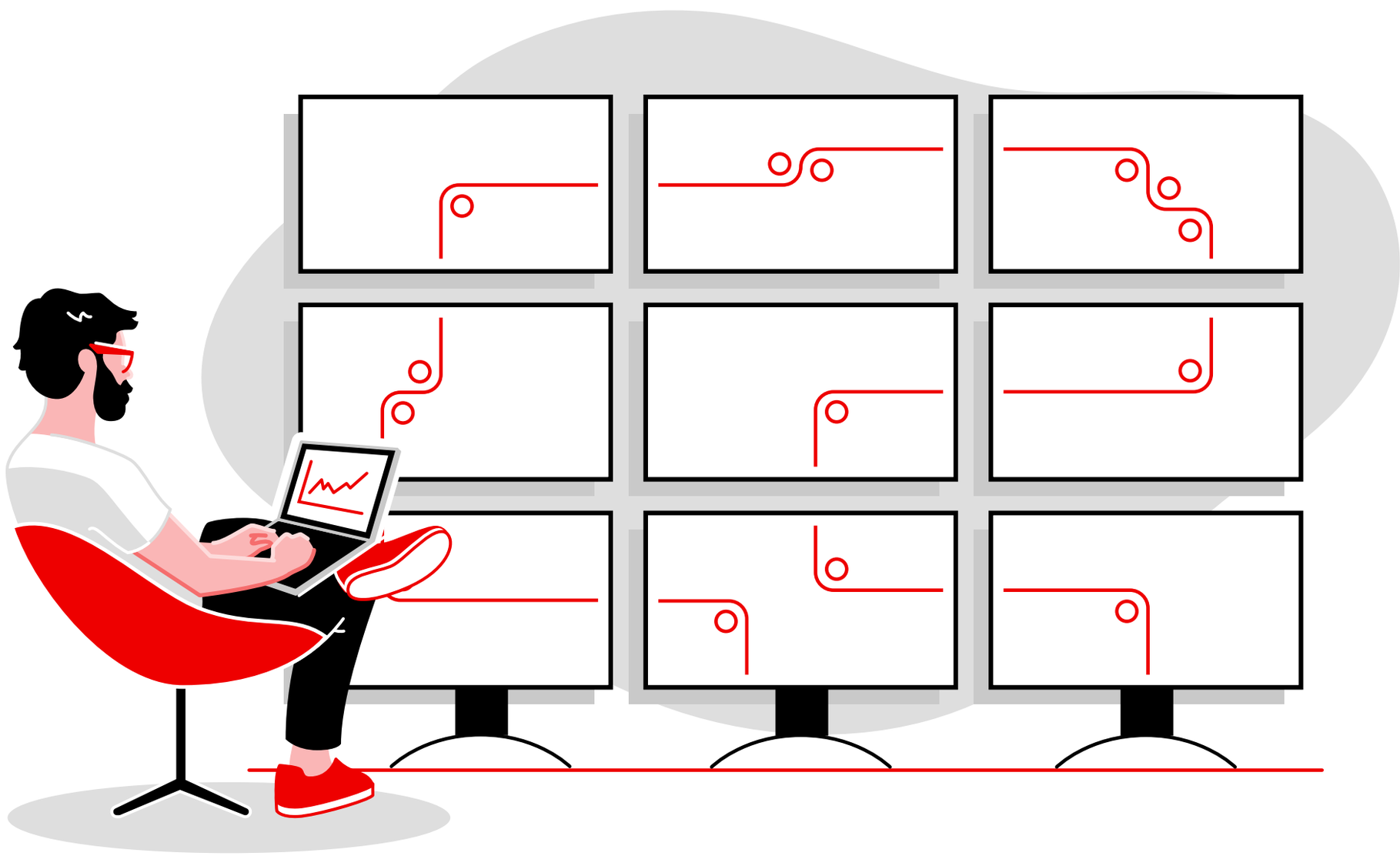
Security automation connects teams

Security automation consists of a variety of practices that connect teams and domains across your organization to better manage risk, defend against cyber threats, and mitigate incidents. For example, security analysts can apply automation to their incident response and remediation processes. IT operations teams can automatically patch systems and enforce compliance. Network administrators can set up and maintain network access controls.

Security automation can also help IT and security teams collaborate more effectively with other parts of you organization—like human resources, customer care, and legal teams—that are affected by security regulations. For instance, most organizations must verify their security controls and report cyber incidents to comply with legal requirements. Regulatory auditors need proof of compliance, but may not interact directly with an organization's security systems. Security automation can integrate external logging systems and record actions to provide the reports and evidence auditors need.

Apply automation to manage your risk

Automating key processes within your organization can help you strengthen your active and passive security posture. In the following sections, we will discuss several areas where security automation can help you comply with regulations and deliver real impact in your organization, no matter which region you are in.



Incident response and remediation

On average, it took 277 days to identify and contain a data breach in 2022.[6] Detecting and containing data breaches within 200 days or less can reduce the average cost of a breach by 26.5%.[6] Even so, breach detection and remediation across multiple platforms, tools, and environments can be complicated, time consuming, and error-prone when performed manually.

Incident response involves taking action to stop a breach from continuing. Once a breach is discovered, security staff must respond quickly and at scale to contain it. However, response actions often include multiple manual tasks performed across unconnected systems, slowing remediation time and leaving your organization vulnerable for longer.

By codifying remediation actions into repeatable, preapproved playbooks, security automation can help you respond to incidents faster. You can speed tasks like blocking attacking IP addresses or domains, allowing non-threatening traffic, freezing compromised credentials, and isolating suspicious workloads for further investigation to minimize the damage associated with the incident.

Patching and system updates

To help prevent attacks, many cybersecurity standards recommend that organizations regularly patch and update their systems and applications. That said, manual patching and updating are always vulnerable to human error, and it can be particularly time consuming in large organizations.

The importance of fast response

277 days

Average time to identify and contain a data breach in 2022[6]

26.5%

Cost reduction for data breaches detected and identified in 200 days or less[6]

Patching is a great use case for automated workflows. Instead of relying on manual testing, preflight checks, and patch deployment, organizations can automate verification and evaluation. Doing so ensures all these steps proceed smoothly and efficiently, with the proper security in place behind the scenes.

Privilege and credential management

Stolen or compromised credentials are the most common cause of data breaches.[6] Centralizing and controlling privileged access and credentials can help reduce your risk and comply with data privacy and security regulations.

Use the principle of least privilege to provide users with only the access they actually need. While you will need to audit and reassess current access rights for each user, this approach can help you minimize the impact of stolen or compromised credentials.

Storing access credentials centrally removes the need to inject them directly into applications, where they are more vulnerable. Automating privileged access management workflows makes the process more manageable, reliable, and consistent. It also lays the foundation for zero trust architectures and approaches.

Compliance and policy enforcement

Misconfigurations were the main cause of 44% of organizations' largest security breaches.[7] Improperly configured systems can be more vulnerable to attack. Systems that were configured properly at the time of provisioning can also become susceptible over time when organizations lack strong change controls.

By enforcing policies over the entire life cycle of your systems and applications, you can ensure that they are properly configured to start and maintained in that configuration over time. Automation can help you achieve this rapidly and at scale while increasing consistency across distributed systems and environments. You can also apply automation to change control processes to verify that change requests are approved, log change activities, and generate reports for audits.

6. IBM. "Cost of a Data Breach Report 2022." July 2022.
7. ThoughtLab. "Cybersecurity Solutions for a Riskier World." 2022

Zero trust architectures

As you automate each of the previous areas, your organization gains valuable experience and lays the foundation for zero trust architecture. Zero trust is an architectural pattern that applies security to each asset, rather than exclusively managing security at a network perimeter. No actor, system, network, or service operating inside or outside the security perimeter is implicitly trusted. In order for a user or subject to connect to a resource, the session must be both authenticated and authorized to establish explicit trust.

Identity and access management is at the core of zero trust architectures. Every subject that wants to interact with an asset must request access for that specific interaction and the risk of that interaction should be evaluated before allowing access. An understanding of the subject's identity and attributes are critical for this evaluation. You need to determine contextual information like who is requesting access, which assets they need to access, the purpose of the transaction, how their access should be constrained.

Once access decisions are made, you must store, manage, curate, and update identities and identity attributes in a protected and consistent manner. Most organizations use one or more identity and privilege access management systems to administer this information. You should also continually reassess these access decisions to ensure that they remain valid over time.

Because an assessment of risk is required for every interaction, zero trust approaches require a large amount of data and information to be collected from across your infrastructure and organization. This is where automation becomes critical. First, the number of interactions is simply too large for IT staff to handle manually—it would be impossible to grant access to any resource in a timely manner if each interaction had to be assessed manually.

Second, automation can help you gather data from disparate systems across your organization. For example, if an employee wants to access an internal application, you may need to collect and verify employment information from a human resource system, identity information from an IT system, and update status and location information from the employee's computer, at a minimum. Because an automation platform can connect systems and domains that usually do not or cannot interact with each other, you can easily and quickly gather, collate, and analyze information. You can even send this information on to security information event management (SIEM) and other centralized security systems as needed.

Finally, automation lets you respond dynamically to user events and status changes. If a user leaves or moves to a new role within your organization, you can use event-driven automation to update their access across all systems as soon as the change occurs, rather than waiting for manual action.

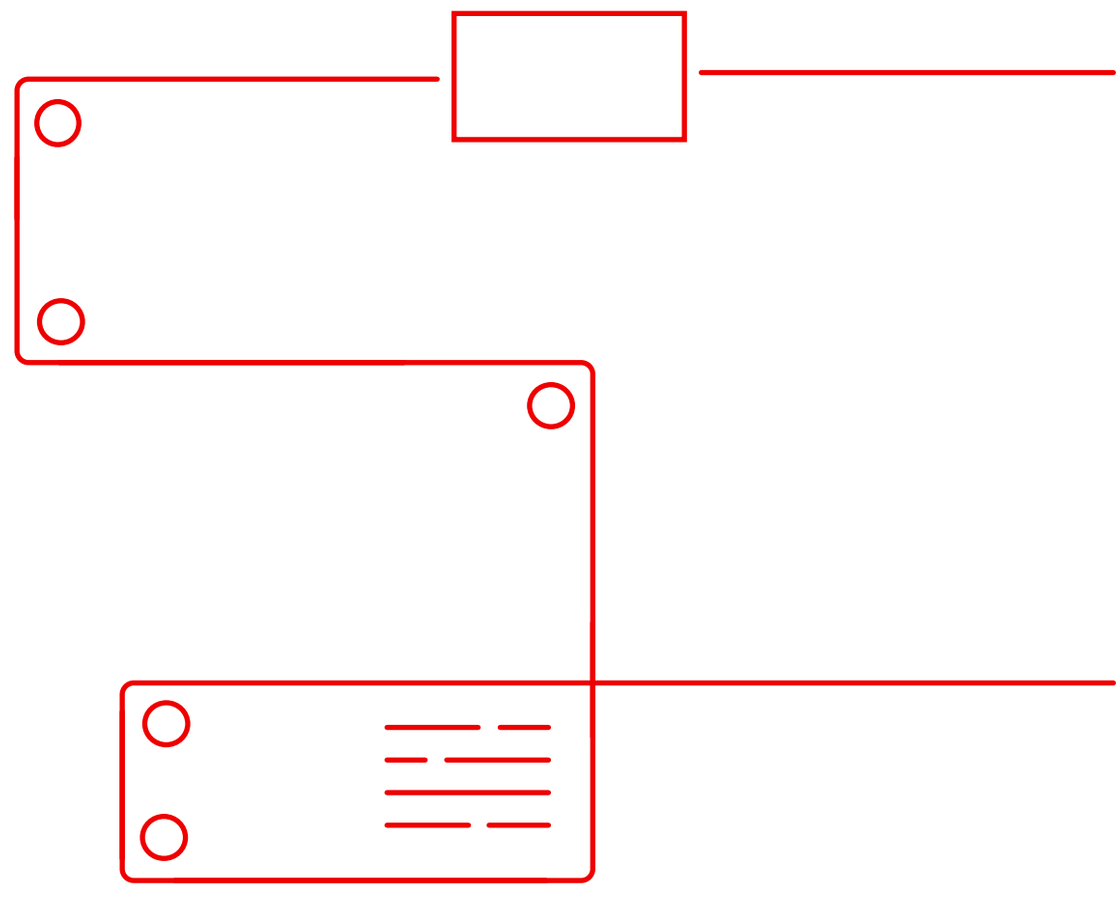
The benefits of zero trust approaches

20.5%

Percent savings in data breach costs for organizations that deploy zero trust[8]

US$1.65 million

Average data breach cost savings associated with a mature zero trust deployment versus no zero trust deployed[8]



8. IBM. "Cost of a Data Breach Report 2022." July 2022.

05 Red Hat's role in your cybersecurity approach

Building a future-ready cybersecurity practice

With automation at the foundation of your cybersecurity maturity model, you can take practical steps to quickly and iteratively replace manual processes, manage risk, and improve your security posture. Red Hat® solutions can help you automate your existing manual processes, allowing you to mitigate the risk of oversights due to overburdened, understaffed IT teams in your organization. Our open source products deliver flexibility and scalability across cloud environments and architectures, helping you boost security today and prepare for the uncertainty of the future.

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform is built with a human-readable automation language that turns complex manual processes into automated workflows. Ansible Automation Platform allows your IT teams to automate and integrate security protocols across your enterprise. Using this platform, your organization can investigate and respond to threats in a coordinated, unified way using curated, certified automation content. You can also automate:

- Updated and patching for common vulnerabilities and exposures (CVEs).
- Application control rollout.
- Backup, restore, and verification processes.

Ansible Automation Platform provides a security-focused, stable enterprise framework for building and operating IT automation at scale, from hybrid cloud to edge environments. This automation solution allows users across your organization—from developer and operations teams to security and network teams—to create, share, and manage automation content and playbooks. IT managers can set guidelines on how automation is applied to individual teams, and automation creators can write tasks that use existing knowledge.

Additionally, Ansible Automation Platform can serve as an integration point for security solutions using included content from certified partners like CyberArk, IBM, and Splunk, allowing you to automate the management and integration of security technologies.

Learn more about Red Hat Ansible Automation Platform ›

Red Hat Enterprise Linux

Red Hat Enterprise Linux® provides a foundation for scaling existing applications and rolling out emerging technologies across bare metal, virtualized, cloud, and edge footprints with consistent security.

Red Hat Enterprise Linux takes a practical, three-point approach to addressing security challenges:

- Mitigate: Manage security and reduce the risk of a breach before your data, systems, or reputation are exposed.
- Protect: Automate and maintain security controls over time, at scale, and with minimal downtime.
- Comply: Streamline compliance standards for organizations with highly regulated environments.

Red Hat Enterprise Linux also contains built-in security policies aligned with many regulations and standards—like Common Criteria (CC), Federal Information Processing Standard (FIPS) 140, and Secure Technical Implementation Guidelines (STIG)—to help you better manage risk by automatically and consistently applying security controls to new digital services.

Learn more about Red Hat Enterprise Linux ›

Red Hat

Previous

Strengthen your security with Red Hat

Red Hat is here to help improve the security of your digital services

Red Hat can help you automate regulatory standards and guidance and better manage risk with automated security integrations.

To learn more, get in touch today >