

42 Tips to Build a Resilient Cybersecurity Program

Securing Your Organization Is a Journey, Not a Destination.

The cybersecurity landscape is ever-changing, and a proactive approach can turn challenges into opportunities. While no organization can predict every threat, understanding which threats are most likely to impact your organization means you're always one step ahead—ready to respond and recover quickly. Even small, focused changes empower your team and fortify your defenses to minimize any potential impact.

Drawing on insights from our [Unit 42 Global Incident Response Report 2025](#), this guide offers practical, real-world recommendations to help you build a resilient, agile security program. Explore recommendations—divided into sections to help you focus your efforts—that protect your organization and pave the way for continued growth and confidence in your cybersecurity journey.

Comprehensive Recommendations to Make Your Organization More Secure

Identity and Access Management (IAM)

1. **Enforce strong, unique passwords and employ password managers** to maintain good password hygiene. Regular password changes are important, but requiring resets too frequently can create user fatigue, leading to weaker passwords over time.
2. **Use single sign-on (SSO) and multifactor authentication (MFA)** whenever possible, especially for critical systems, websites, and external-facing applications.
3. **Review Active Directory regularly for new accounts and configurations**, and disable unnecessary accounts, especially default and admin accounts. These services are a common initial attack vector.
4. **Quickly revoke access for terminated or voluntarily departing employees.** Also, enforce least-privileged access based on device type, geolocation, user role, and time of day.
5. **Implement an internal awareness campaign against sharing logins or accounts.** Promote good password hygiene, especially for accounts with admin or other privileged access.
6. **Be sure you implement these tips for partners and vendors** with access to your systems and data.

 **Weak or absent passwords and excessive permissions became more frequent contributing factors [in 2024].¹**

Risk, Vulnerability, and Patch Management

7. **Continuously monitor your internal and external attack surfaces for vulnerabilities** that an attacker could exploit. Where possible, segment your network and isolate critical systems to limit the potential impact of an attack.
8. **Conduct regular incident response (IR) plan reviews, tabletop simulations**, red team exercises, and penetration testing to ensure your people, processes, and technologies are optimized to identify and remediate threats quickly.
9. **Implement change control protocols and automated patch management** to prioritize fixes based on active attack trends and the threats most likely to impact your organization based on, for example, geography, industry and risk tolerance.
10. **Establish InfoSec policy guardrails** to regularly evaluate software and applications for vulnerabilities. Only use code your team has rigorously vetted and patched.

1. Global Incident Response Report 2025, Unit 42, February 25, 2025.

Data and Software Security

- 11. Enforce strong access controls aligned with zero trust best practices** to protect sensitive systems and data from both external and insider threats. Be sure policies include employees, partners, and vendors.
- 12. Protect data both in transit and at rest**, including email encryption and full-disk encryption for laptops, servers, and removable devices. Where possible, restrict the use of removable media to reduce the risk of data leakage.
- 13. Conduct regular secure code reviews**, vulnerability scans, and a robust patch management process for all software, including third-party libraries and open-source code.
- 14. Customize security approaches** to address the unique needs of on-premises versus cloud-based data and systems. Consider such factors as data storage, access controls, and potential misconfigurations specific to each setting.
- 15. Establish a data loss prevention (DLP) program** to classify, monitor, and protect sensitive data, ensuring that data is appropriately handled and protected from unauthorized disclosure.

Threat Detection and Response

- 16. Deploy endpoint detection and response (EDR)** or extended detection and response (XDR) solutions across the organization. Also, ensure your security operations team understands how to use this technology to maintain full visibility across the organization.
- 17. Strengthen your cybersecurity tools** with AI-driven behavioral analytics and threat intelligence. As cybercriminals increasingly use AI to enhance the speed and scope of their attacks, it's crucial to use AI-based defenses to stay ahead.
- 18. Adopt a SecOps platform with built-in automation** to centralize all security data into a single view. This way, you increase visibility across the enterprise and reduce manual log data correlation and analysis that slows down your detection and response.
- 19. Partner with trusted experts** to proactively assess and test your cybersecurity program and IR plans. Adjust your defenses as your environment and the threat landscape evolve.
- 20. Leverage 24/7/365 managed services** to augment your team as needed for threat hunting, detection, and response.

Additional Tips

- 21. Ensure employees can work safely** and simplify cybersecurity wherever possible. The more difficult it is to do their jobs, the more likely they are to find clever workarounds that often create security gaps.
- 22. Conduct regular disaster recovery exercises** and cyberattack simulations to develop resiliency against extortion and disruption attacks.
- 23. If you have cyber insurance (recommended)**, be sure to integrate the policy's key processes and contacts into your IR plans.
- 24. To reduce the risk of impersonation**, consider purchasing domains based on common spelling errors or variations of your organization's name.

Phishing has reclaimed its spot as the most common initial access vector in Unit 42 cases, accounting for 23% of incidents we investigated. In 76% of phishing incidents, the attacker compromised the victim's business email.²

Recommendations to Prevent Phishing Attacks

- 25. Create a security awareness culture with regular training.** Use trusted training vendors or platforms that allow for custom curricula tailored to the organization and employee roles. They should also take into account the fast-evolving nature of threat actor methodologies.
- 26. Gamify security training to better engage employees** by setting goals, rules for reaching them, rewards or incentives, feedback mechanisms, and leaderboards. Groups within your organization can compete against each other.
- 27. Make it easy for users to report suspected phishing** and other suspicious emails, as well as to visually alert users to emails from external sources, especially those with links and attachments. Make sure your SOC responds to submissions quickly to encourage continued vigilance.
- 28. Track leading performance indicators for your phishing tests** so you can adjust the content and difficulty based on the organization's needs and evolving cybercriminal tactics.
- 29. Use email security solutions** and consider blocking account logins based on geographic regions, time, and any unusual behavior.
- 30. Automate phishing response activities** to reduce the need for human touch.

² Global Incident Response Report 2025, Unit 42, February 25, 2025.

Recommendations to Keep Systems Secure and Up To Date

- 31. Inventory all IT assets (including storage, switches, laptops, and servers)** across the entire distributed organization through automated discovery tools to get a clear picture of what you have to manage.
- 32. Prioritize your patching needs**, beginning with critical systems and sensitive data. Based on your risk tolerance, determine which vulnerabilities represent high, medium, or low risk and their level of priority for the business.
- 33. Test patches in a development or QA environment** before moving them to your production environment. Then, deploy the patches broadly and monitor them for stability.
- 34. Implement a regular schedule for deploying patches.** Consider a minimum cadence of once a week, with the option to deploy high-priority patches out of cycle when necessary.
- 35. Isolate, remove, or update systems running unsupported operating systems** and applications, especially any that are no longer receiving security updates.

 **70% of incidents happened on three or more fronts – and nearly half (44%) involved a web browser.³**

Recommendations to Secure Your Cloud Environment

- 36. On-premises and cloud assets require distinct cybersecurity strategies.** While on-premises systems benefit from traditional defenses and physical security, cloud environments require a slightly different approach for each cloud provider.
- 37. Rogue cloud assets can create significant security blind spots.** To ensure comprehensive protection, establish a clear process for detecting and mitigating unauthorized cloud resources that fall outside of SecOps control.
- 38. Don't forget SaaS environments.** While SaaS providers secure their applications and infrastructure, businesses are responsible for securing the data and users within their environments.
- 39. Ensure your SOC includes cloud security expertise** and bring in third-party experts to augment these skills when needed.
- 40. Take advantage of cloud-native IAM solutions with MFA** and granular role-based access controls to protect access to your cloud assets and sensitive data.
- 41. Use automation to identify and remediate** overly permissive IAM policies and other cloud misconfigurations. Monitor for and delete unnecessary default accounts and unused admin accounts.
- 42. Encrypt sensitive data both at rest in cloud storage** and in transit between cloud services to maintain strong protection across your cloud ecosystem.

³ Global Incident Response Report 2025, Unit 42, February 25, 2025.

24/7 Expert-Led Defense with Unit 42 Managed Services

Today's cybersecurity operations are plagued by growing complexity, with 70% of attacks spanning across at least three attack surfaces⁴. The sheer volume of telemetry and siloed tools create noise rather than clarity, leaving organizations unable to connect fragmented events across endpoints, cloud, network, and identity systems. In addition to these challenges, many organizations struggle with staffing and skills shortages.

With **Unit 42 Managed Services**, you benefit from our years of experience protecting businesses, governments, and geographical regions from evolving threats. Our analysts use **Cortex XDR®** and **Cortex XSIAM®** to aggregate security telemetry across your endpoint, network, and cloud security tools. They also apply high-fidelity threat intelligence and AI-powered analytics to prevent, detect, and respond to the most advanced threats.

The Unit 42® Managed Services team uses a mix of proprietary processes, infrastructure, and enrichment to swiftly stop the malicious activity that might impact your organization. By using this mix, our team accelerates threat hunting, detection, and response to help you reduce risk and stay ahead of threats.

Initiate Your Response in Minutes with a Unit 42 Retainer

The clock starts immediately when you're under attack. But if you can't determine the root cause and contain the breach right away, your adversary will be back in no time.

With a **Unit 42 Retainer** in place, our experts become an extension of your team, on speed dial whenever you need help. Eliminate the unnecessary delays of negotiating costs and terms or scrambling to find help when time is of the essence. Instead, you will engage with an assigned point of contact at Unit 42—someone with an intimate understanding of your infrastructure, existing playbooks, and team—who can quickly support you. You also get SLA-driven response times that align to your existing SecOps and IR capabilities, budget, and strategy, bringing greater predictability. This helps minimize the impact of an attack so you can get back to business faster.

If you don't use all of your Retainer credits for IR, use them for Unit 42 proactive services to get ahead of threats and improve your cybersecurity readiness. These services include, for example, the **SOC Assessment**, **AI Security Assessment**, **Cloud Security Assessment**, and **Zero Trust Advisory**.

For an in-depth look at today's cyberthreat landscape and how you can defend your organization on all fronts, check out the **2025 Unit 42 Incident Response Report**.

4. *Global Incident Response Report 2025*, Unit 42, February 25, 2025.

About Unit 42

We believe no organization should face advanced cyberthreats alone. Unit 42® strengthens your team with the tools and expertise needed to stay ahead of threats and protect your business. With our proven strategies and insights from thousands of engagements, we'll help your team handle the toughest situations with confidence.

Learn more at paloaltonetworks.com/unit42.

Under attack? Get in touch.

If you think you may have been compromised or have an urgent matter, please contact the Unit 42 Incident Response team.

Contact us now



3000 Tannery Way
Santa Clara, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

42 Tips to Build a Resilient Cybersecurity Program | June 2025