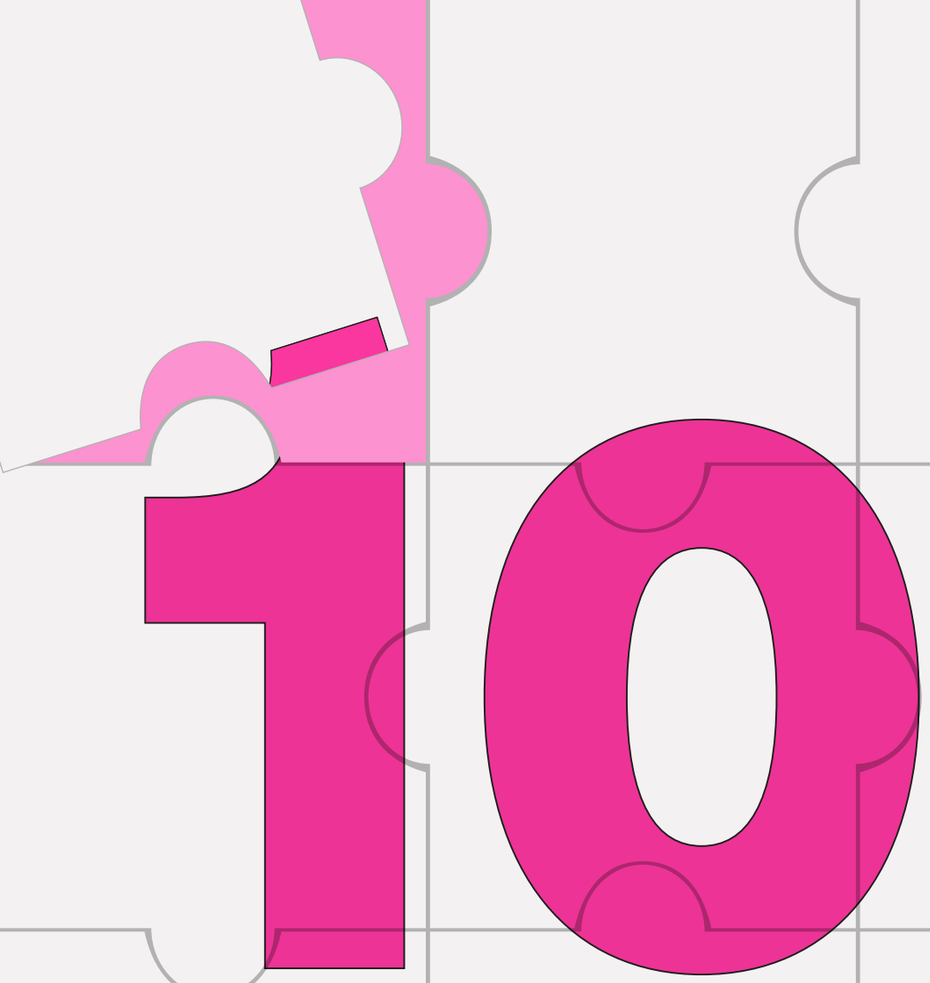


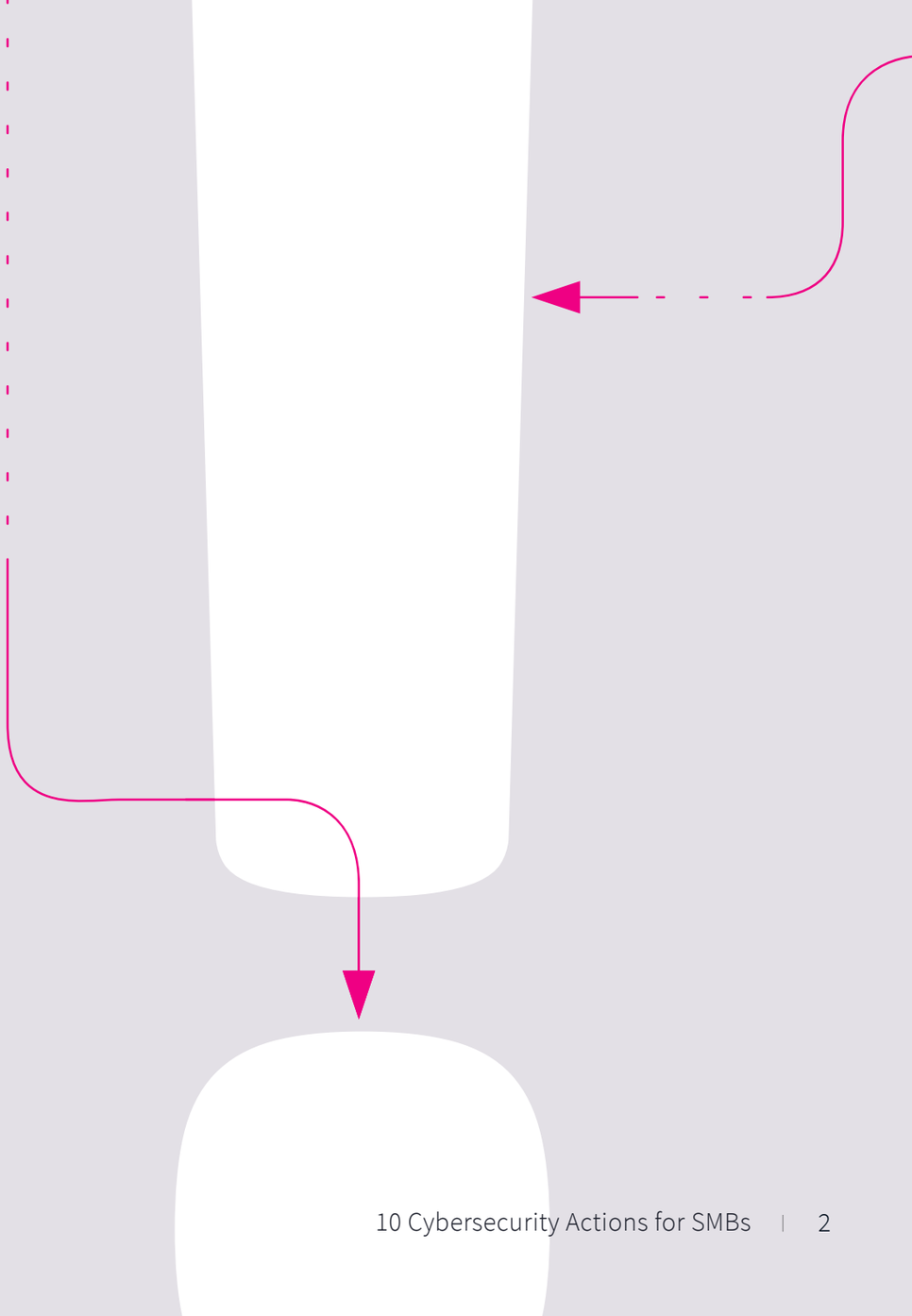
10 Cyber Security Actions for SMBs

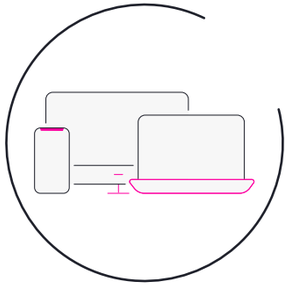
Introduction.

In today's interconnected digital world, organizations of all sizes face an ever-growing array of cybersecurity threats. The evolving tactics and techniques employed by cybercriminals require a proactive and comprehensive approach to protect sensitive data, maintain business continuity, and safeguard customer trust. Cybersecurity is no longer a luxury but a necessity for any organization seeking to thrive in the digital age.

While cybersecurity can appear complex and daunting, the principles and best practices outlined in this ebook are designed to provide actionable steps that any organization can implement to bolster their defenses, even organizations with limited budgets, staff, and security expertise. By selecting the right cybersecurity providers, leveraging technology solutions, and establishing a culture of security awareness, organizations can greatly enhance their resilience against cyber threats. Whether you are a small business or a larger enterprise, the insights shared here will help you navigate the cybersecurity landscape and protect your valuable assets.

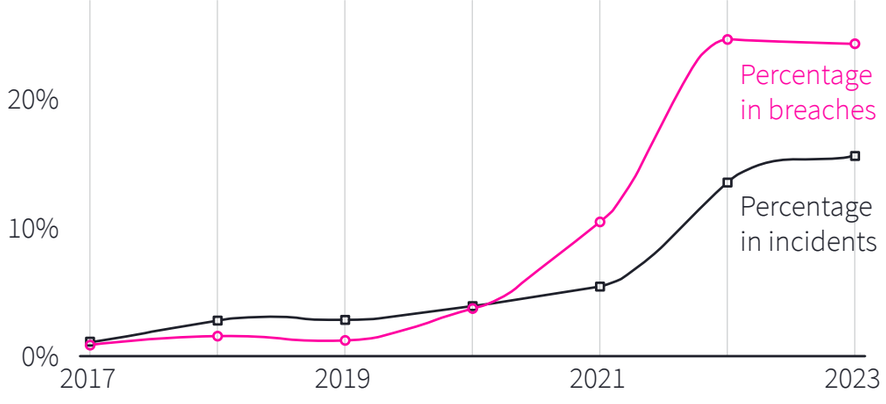
The following pages outline ten key steps that organizations can take to enhance their cybersecurity posture and mitigate today’s most prevalent threats.





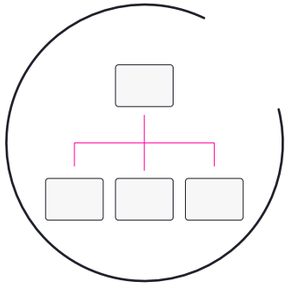
Action 1
Protect your Endpoints

Criminals use various malware to access valuable corporate data on endpoints and servers. Ransomware is used to lock endpoint and file access until payments are made. According to the Verizon 2023 Data Breach Investigation Report, ransomware is involved in 24% of all breaches analyzed (see figure below). Endpoint protection is the foundation of a strong cybersecurity program, as it guards against malware and ransomware that can compromise sensitive data on devices and servers.



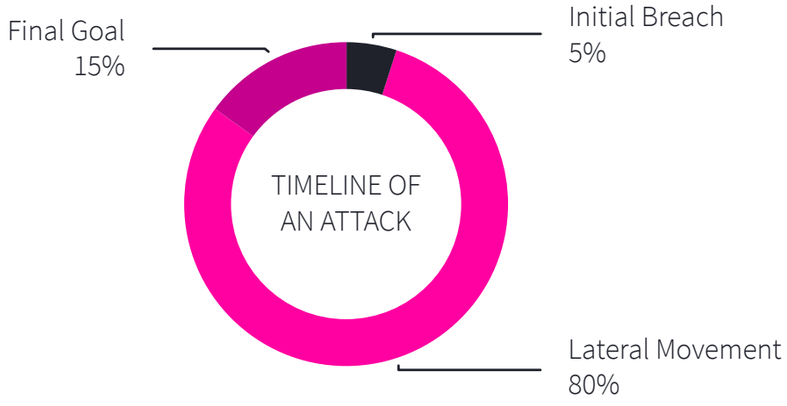
Ransomware over time

- Evaluate endpoint solution providers based on factors such as detection rates, response capabilities, ease of use, and ease of deployment to ensure you choose the most effective solution for your organization. Endpoint tools vary greatly in how complex they are to configure, operate and manage.
- Better endpoint detection and response (EDR) solutions include Endpoint Protection Platform (EPP) and Next Generation Antivirus (NGAV) capabilities seamlessly integrated into a single platform. The MITRE ATT&CK Evaluation is a great resource to help evaluate endpoint solution providers.
- Regularly update and patch endpoints to address vulnerabilities and minimize the risk of exploitation by cybercriminals.
- Implement behavior-based endpoint protection solutions that utilize machine learning and artificial intelligence algorithms to detect and block emerging threats, even those with no known signatures.
- Regularly educate employees about the importance of safe browsing habits (and also consider domain filtering tools), avoiding suspicious downloads (and also consider email filtering tools), and reporting any unusual system behavior to the IT or security team.

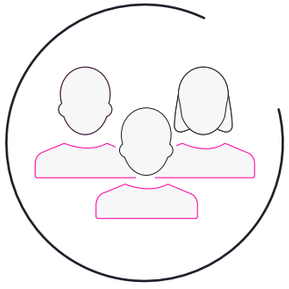


Action 2
Keep your Network Safe

Maintaining a secure network environment is crucial for detecting and preventing unauthorized access, ensuring that cybercriminals cannot infiltrate your systems undetected. According to Smokescreen's Top Lateral Movement Techniques Guide, attackers spend 80% of their time on lateral movement during an attack. Moreover, they found that 54% of lateral movement techniques went undetected..

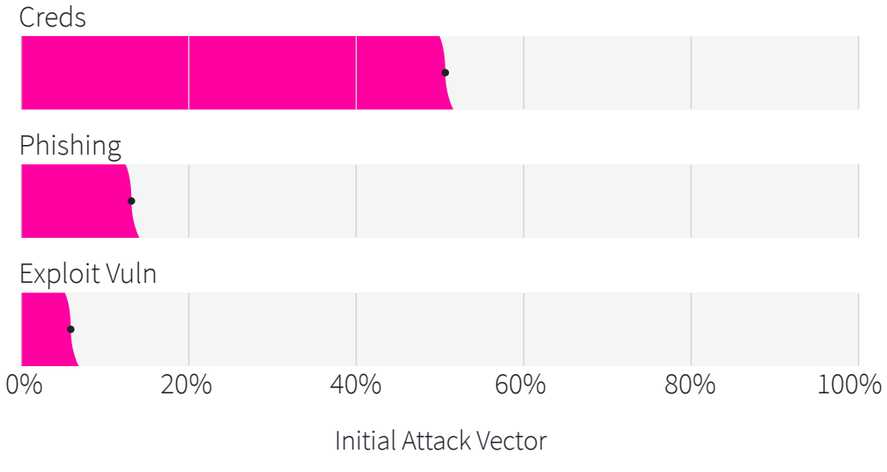


- Network monitoring and detection mechanisms are essential to identify potential threats, such as port scanning and lateral movement, that may indicate the presence of malicious actors within your environment.
- Deception technologies can enhance network security by deploying decoy files, users, and devices that divert cybercriminals' attention and provide early warning signs of a breach.
- Regularly conduct network assessments and penetration testing to identify and address vulnerabilities before they are exploited by attackers.
- Implement network segmentation to isolate critical systems and sensitive data, reducing the potential impact of a breach and limiting lateral movement by attackers within the network.
- Conduct red teaming exercises or penetration testing to simulate real-world attack scenarios and identify any vulnerabilities or weaknesses in your network defenses.

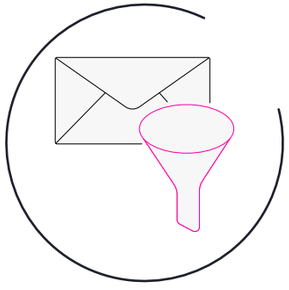


Action 3
Protect your Users

Your users are both the first line of defense and typically the weakest point in your cybersecurity defenses, making it essential to implement robust measures that safeguard their identities and prevent account compromise. According to the Verizon 2023 Data Breach Investigation Report, stolen credentials were used as the initial attack vector in 45% of all reported breaches.

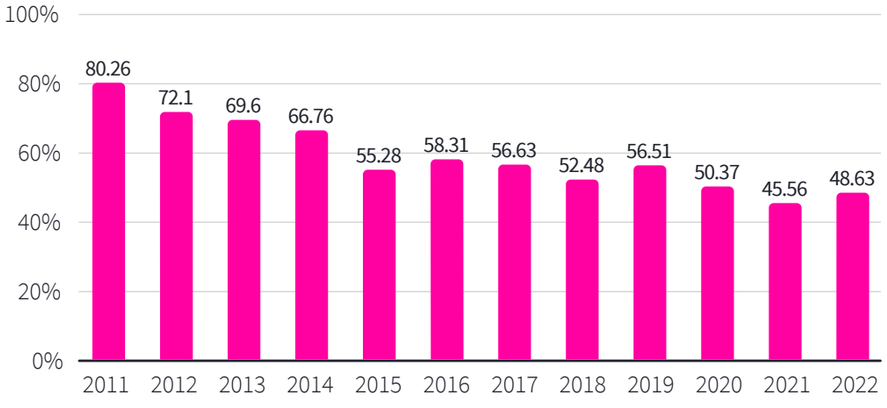


- Multifactor authentication adds an extra layer of security by requiring users to provide multiple forms of identification, making it more challenging for attackers to gain unauthorized access.
- Monitor user behavior patterns and activities to detect anomalies that may be indicative of account takeover or an insider threat.
- Implement continuous monitoring of user entitlements and access privileges, using automated tools to promptly identify and remediate any discrepancies or unauthorized access.
- Develop comprehensive offboarding procedures to promptly revoke all access for users who leave the organization, minimizing the potential for account misuse.
- Conduct regular security awareness training sessions for employees, focusing on identifying social engineering techniques, recognizing phishing emails, and maintaining strong password hygiene.



Action 4
Filter your Email

As one of the most common entry points for cyber-attacks, implementing a strong email security solution is helpful for defending against phishing attacks, malware infections, and credential theft. Statista estimates that while we continue to see a steady reduction, close to half of all email traffic was spam in 2022.



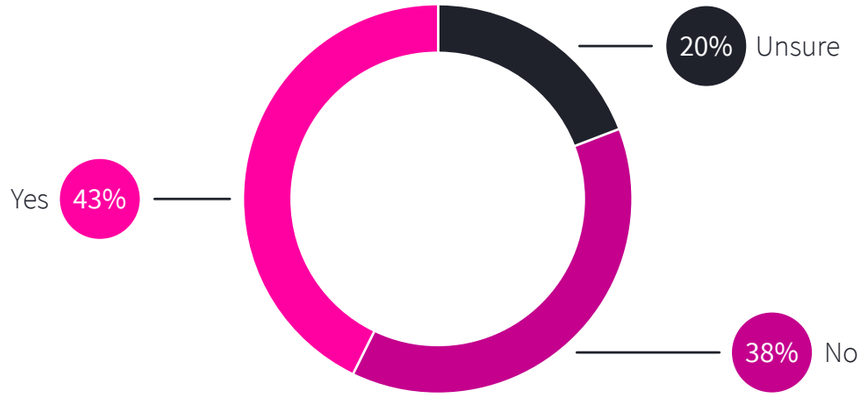
Global spam volume as a percentage of total email traffic

- A robust email security solution can proactively detect and block malicious emails, reducing the chances of successful phishing attacks and the subsequent compromise of sensitive information.
- Implement email authentication protocols like SPF, DKIM, and DMARC to verify the authenticity of incoming emails and prevent domain spoofing.
- Regularly educate employees about email best practices, such as identifying suspicious senders, avoiding clicking on unknown links, and reporting suspicious emails to the IT or security team.
- Implement advanced threat intelligence and machine learning algorithms to analyze incoming emails for potential indicators of compromise, such as suspicious attachments or phishing URLs.
- Enable email encryption to protect sensitive information shared via email and ensure that only authorized recipients can access the encrypted content.

Action 5

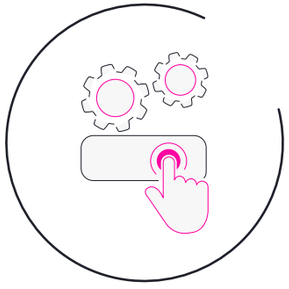
Eliminate Risks with SaaS and Cloud Applications

As organizations increasingly rely on cloud and SaaS applications, ensuring their proper configuration and security is crucial for protecting sensitive data and minimizing the risk of unauthorized access. The Cloud Security Alliance 2022 SaaS Security Survey Report indicates that up to 63% of organizations have dealt with a security incident due to SaaS misconfigurations.



Percent of organizations that say a SaaS misconfiguration led to a security event

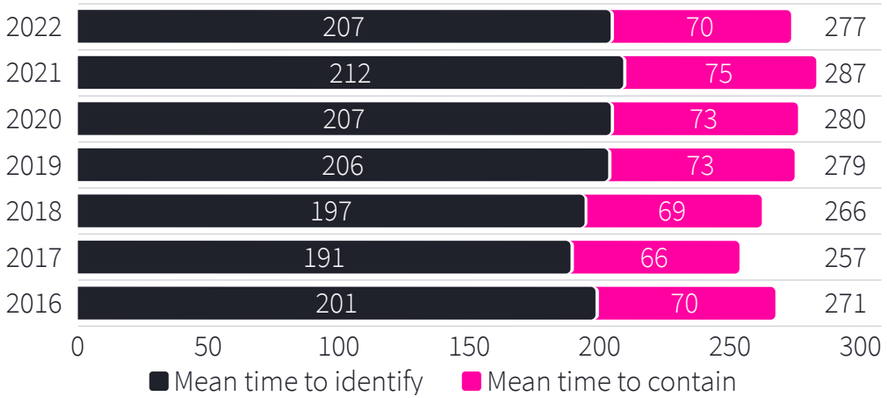
- Misconfigured cloud and SaaS applications can inadvertently expose sensitive data to unauthorized access. Implement regular configuration reviews and leverage automated tools to detect and remediate misconfigurations promptly.
- Use identity and access management (IAM) solutions to enforce strong access controls, ensuring that users only have access to the data and functions necessary for their roles.
- Establish a cloud governance framework that includes policies, procedures, and training to ensure employees understand their responsibilities for securely using cloud services.
- Regularly review access logs and audit trails of cloud and SaaS applications to detect and investigate any unauthorized access attempts or suspicious activities. Centralized log Management (CLM) and security information and event management (SIEM) tools greatly simplify log collection and analysis.
- Employ data loss prevention (DLP) solutions to monitor and control the movement of sensitive data within cloud environments, preventing unauthorized sharing or exfiltration.



Action 6

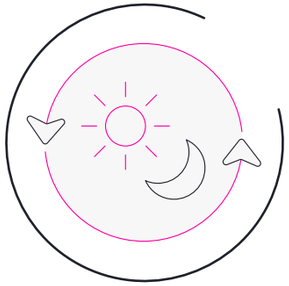
Put Your Response Actions on Autopilot

In the face of a growing number of threats and limited resources, automating your incident response processes can streamline workflows, improve efficiency, and ensure proper and consistent handling of security incidents. IBM Security Cost of a Data Breach Report 2022 found that it took an average of 207 days to identify a breach and then 70 days to contain the breach. Unfortunately, these times have not meaningfully improved for the past 7 years.



Average time to identify and contain a security event

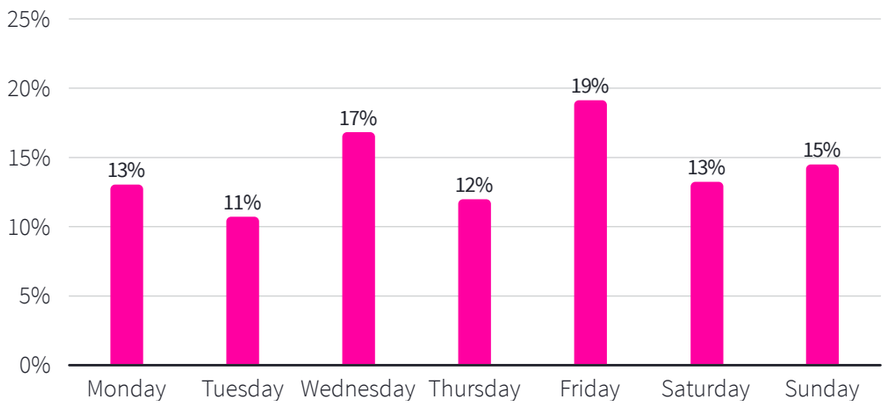
- Response automation can help alleviate the burden on security teams by automatically analyzing and responding to security incidents, ensuring appropriate, consistent and timely actions to mitigate potential threats.
- Implement security orchestration and automation response (SOAR) platforms to streamline incident response workflows, integrate with security tools, and provide real-time visibility into security incidents.
- Continuously refine and update automated response playbooks based on lessons learned from previous incidents, industry best practices, and evolving threat intelligence.
- Leverage threat intelligence feeds and security automation platforms to enrich incident data and enhance the accuracy of automated response actions.
- Regularly test and refine automated response playbooks to ensure they align with your organization's evolving security landscape and emerging threats.



Action 7

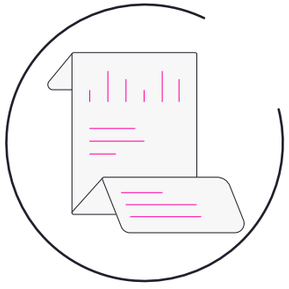
Ensure 24/7 Security Coverage

Cyber threats don't rest, and neither should your organization's security. By leveraging managed detection and response services, you can maintain round-the-clock security coverage and access expert guidance when needed. Research by RiskRecon showed that 28% of ransomware detonation events occurred on weekends.



Distribution of Ransomware Detonation Events by Day of Week

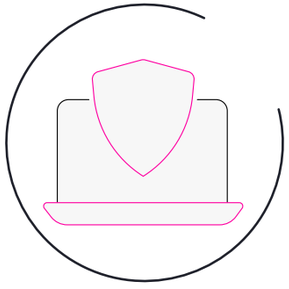
- Managed detection and response (MDR) services provide round-the-clock monitoring, threat detection, and incident response capabilities, leveraging specialized expertise and advanced technologies.
- Partner with an MDR service provider that aligns with your organization's specific needs, ensuring they can provide timely incident response and proactive security recommendations.
- Regularly communicate and collaborate with your MDR provider to share threat intelligence, adjust security strategies, and stay informed about emerging threats and industry best practices.
- Implement threat hunting practices alongside MDR services to proactively search for signs of advanced persistent threats (APTs) or sophisticated attack techniques that may bypass traditional security controls.
- Ensure your MDR service provider has a strong track record quickly and successfully responding to and resolving security incidents.



Action 8
Leverage Your Log Data

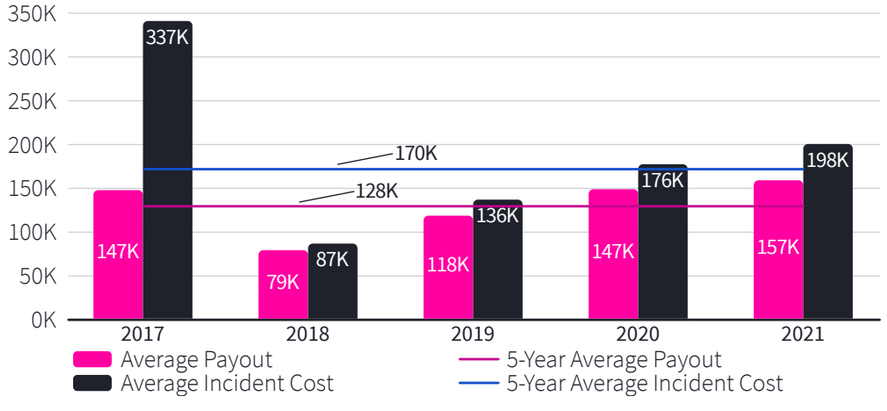
Logs hold a wealth of information about your systems' activities, and effectively leveraging that data through centralized log management can provide critical insights for threat detection, incident response, and regulatory compliance.

- Centralized log management (CLM) solutions enable the efficient collection, storage, and analysis of log data from various systems and devices, facilitating threat hunting and compliance reporting.
- Security information and event management (SIEM) solutions correlate and analyze log data in real-time, enabling early detection of suspicious activities and timely incident response.
- Develop log retention policies that align with regulatory requirements and consider leveraging log analysis tools to identify patterns and anomalies that may indicate potential security incidents.
- Employ machine learning and analytics tools to perform advanced log analysis, identifying patterns and anomalies that may indicate insider threats or targeted attacks.
- Integrate threat intelligence feeds with your CLM and SIEM solutions to enhance log analysis capabilities and proactively detect indicators of compromise.



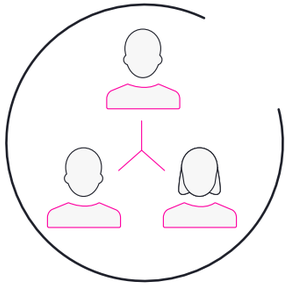
Action 9
Get Cyber Insurance

While investing in robust cybersecurity measures is crucial, cyber insurance serves as an additional layer of protection, offering financial assistance and peace of mind in the event of a significant cyber incident. According to the NetDiligence Cyber Claims Study 2022 Report, the average incident cost in 2021was $198,000 and the average insurance payout was $157,000, covering approximately 80% of costs.



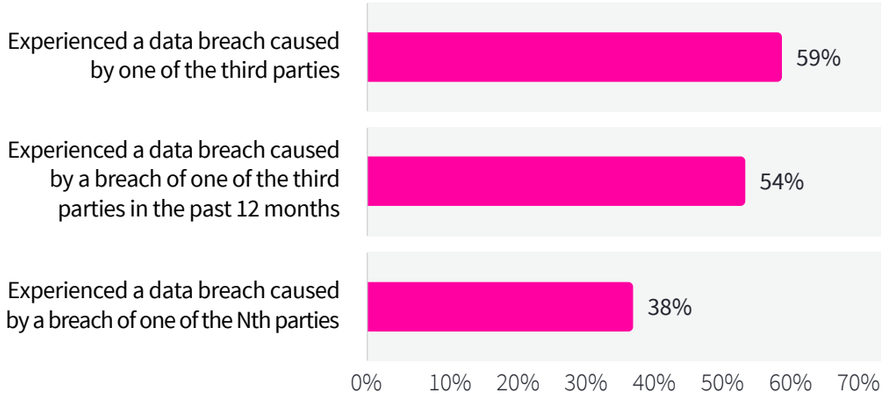
Average Payouts and Incident Costs SMEs

- Cyber insurance provides financial protection and support in the event of a cybersecurity incident, including the costs associated with data breaches, legal expenses, and reputational damage.
- Conduct a thorough risk assessment to determine the appropriate coverage needed for your organization, considering factors such as potential financial losses, business interruption, and reputational damage.
- Work closely with insurance providers to assess your organization's specific risks, policy coverage, and exclusions, ensuring that the insurance policy aligns with your cybersecurity program and business objectives.
- Maintain accurate and up-to-date documentation of your cybersecurity program, risk assessments, incident response plans, and other relevant information to support insurance claims if needed.
- Regularly review and update your cyber insurance policy to align with your evolving cybersecurity program, ensuring that new risks and emerging threats are adequately covered.



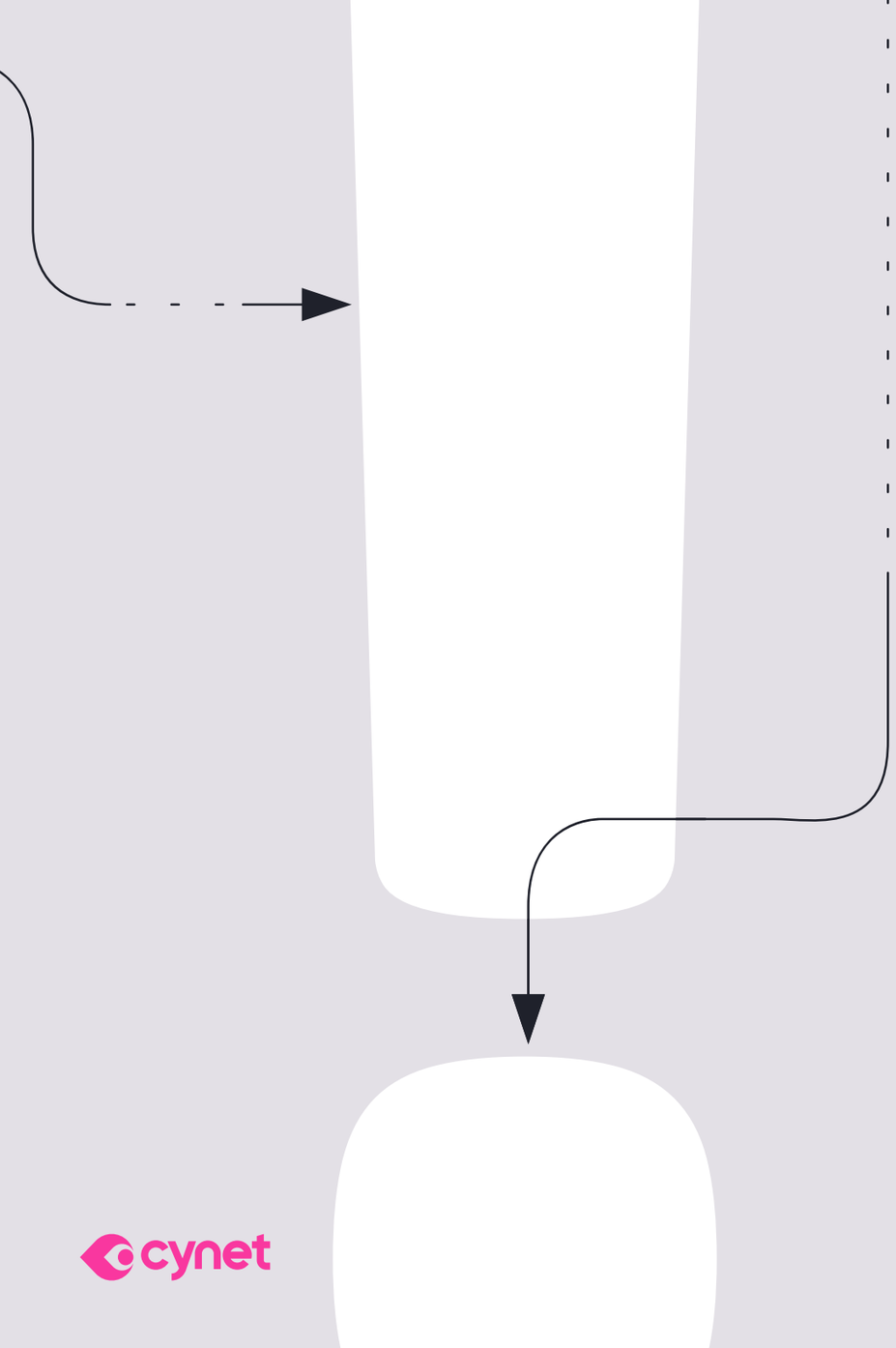
Action 10
Manage 3rd Party Risk

Your organization's cybersecurity is only as strong as the weakest link in your supply chain. Taking proactive steps to assess and manage the cybersecurity practices of your third-party vendors and partners is essential for overall resilience. Ponemon's 2022 Data Risk in the Third-Party Ecosystem Study found that 59% of organizations surveyed experienced a data breach caused by one of their third-party providers.



Percent of organizations that experienced a data breach or cyber attack caused by a third party

- Establish a comprehensive vendor risk management program to assess the security practices and controls of third-party providers and partners.
- Conduct regular audits and security assessments of vendors to ensure they adhere to industry standards and compliance requirements and to identify and address any security gaps or vulnerabilities.
- Implement contractual obligations and enforce security requirements through service-level agreements (SLAs) and data protection clauses to mitigate the risk of third-party vulnerabilities impacting your organization.
- Establish clear incident response and communication protocols with vendors, ensuring a coordinated approach in the event of a security incident or data breach involving third parties.



Conclusion

Implementing solid cybersecurity protections for your organization doesn't have to be complicated. By following these ten steps and selecting the right cybersecurity providers, you can establish a strong defense against cyber threats, even if you have budget and resource constraints.

Remember, cybersecurity is an ongoing effort that requires continuous monitoring, adaptation, and collaboration with trusted partners to stay ahead of evolving threats. Regularly assessing and updating your security measures, staying informed about emerging threats, and fostering a culture of security awareness within your organization are key elements of a strong cybersecurity strategy. By embracing the insights and recommendations presented in this eBook, you can effectively defend against cyber threats and build a resilient security foundation.

About Cynet

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating their entire security operations while providing enhanced visibility and protection, regardless of the security team's size, skill or resources and without the need for a multi-product security stack. It does so by natively consolidating the essential security technologies needed to provide organizations with comprehensive threat protection into a single, easy-to-use XDR platform; automating the manual process of investigation and remediation across the environment; and providing a 24-7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting - at no additional cost.

Learn More