SYGNIA

2025

ANNUAL THREAT REPORT

Actionable Insights from the
Frontlines of Incident Response

TABLE OF CONTENTS

INTRODUCTION

Are you prepared for adversaries who exploit vulnerabilities in places you haven't thought to look?

Are you ready to defend against attacks that bypass some of the most common and traditional security controls?

Based on our frontline incident response work throughout 2024, Sygnia's Threat Report brings you insights from real cybersecurity incidents, focusing on critical threat vectors shaping today's threat landscape.

In this report, we share three real-world use cases and discuss how ransomware groups are evolving their tactics, how threat actors are weaponizing trusted supply chain relationships for persistent access, and how identity-based attacks are exploiting permission gaps to move laterally and escalate privileges. Drawing from these incidents and the expertise of our incident responders and senior security architects, we provide field-tested strategies to enhance ransomware readiness, improve identity governance, and secure critical infrastructure against these evolving threats.

EXECUTIVE SUMMARY

Based on our incident response investigations throughout 2024, the 2025 Sygnia Threat Report underscores the urgent need for organizations to adapt their defenses across three types of cyber threats. The discussion of each threat type includes attacker TTPs and provides recommendations to improve your readiness and resilience against them.

1 

RANSOMWARE TACTICS evolved beyond traditional encryption-based attacks, with threat actors increasingly focused on data theft and leveraging public exposure for extortion. Our teams observed attackers targeting under-protected systems like virtualization infrastructure and Network Attached Storage (NAS) appliances as persistence points to remain stealthy. The attackers typically spend one to two weeks preparing for data exfiltration and mass encryption - providing a critical but often missed detection window.

2 

SUPPLY CHAIN VULNERABILITIES resurfaced as an attack vector, with threat actors compromising trusted third-party relationships to maintain persistent access. Our investigations uncovered sophisticated groups who maintained long-term presence by blending their malicious activities with legitimate vendor operations, exploiting the limited visibility organizations typically have over third-party connections and access patterns.

3 

IDENTITY-BASED ATTACKS intensified as organizations accelerated their cloud adoption, with threat actors demonstrating increased sophistication in exploiting authentication systems and permission models. We observed attackers systematically chaining together minor permission gaps to achieve meaningful privilege escalation, while leveraging compromised service accounts and SSO trust relationships to move laterally between environments - highlighting critical weaknesses in how organizations monitor and control identity access.

This report equips CISOs and security teams with practical insights and actionable defensive measures across these three domains, drawn directly from our incident response experience to help organizations better detect, prevent, and respond to today's sophisticated attacks.

RANSOMWARE TRENDS

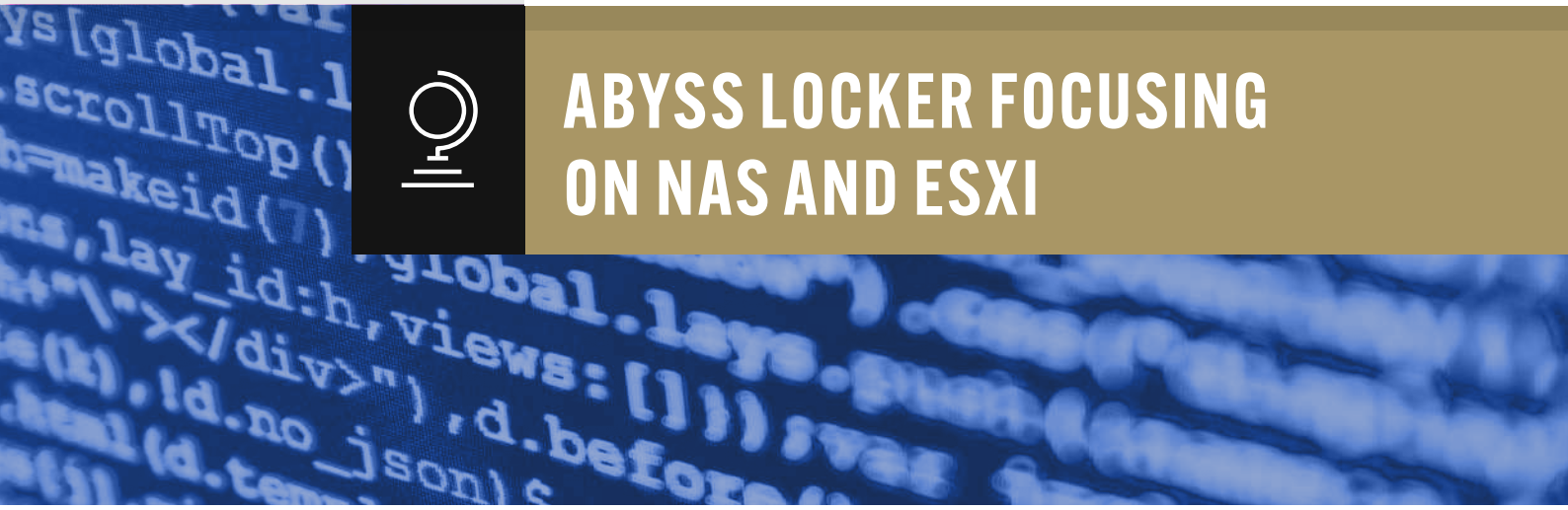
Often, threat actors are sidestepping encryption altogether, focusing on stealing sensitive data and extorting organizations with the threat of publicly releasing it

Ransomware attacks continue to evolve beyond encryption for ransom demands, with attackers increasingly turning to data theft and extortion tactics. Often, threat actors are sidestepping encryption altogether, focusing on stealing sensitive data and extorting organizations with the threat of publicly releasing it — which is often a stronger pressure point than denying access to the data via encryption. Our incident response experience reveals that while attackers can spend mere hours inside compromised networks before executing their attacks, the average "dwell time" (from initial infiltration to impact) for ransomware threat groups is between one to two weeks, providing a limited but critical detection window.

In parallel, virtual environments have become prime targets, allowing attackers to cripple entire infrastructures with minimal effort. By exploiting under-protected systems, including VMware ESXi hosts, and Network Attached Storage (NAS) appliances, attackers can rapidly encrypt virtual machines and exfiltrate massive amounts of stored data for maximum impact.

CASE STUDY

ABYSS LOCKER FOCUSING ON NAS AND ESXI



ATTACKER:

Abyss Locker ransomware group

ATTACK TYPE:

Ransomware

NOTABLE TACTICS:

Dwell time of 2 weeks from initial infiltration to start of data exfiltration

Used compromised VPN credentials for initial access

Exploit Network Attached Storage (NAS) appliances, domain controllers, file servers and ESXi hosts

Throughout 2024, our incident response teams encountered multiple post-encryption incidents attributed to the Abyss Locker ransomware group, a threat actor that emerged in mid-2023 and continues its operations today. Across all investigated incidents, the group maintained an average dwell time of approximately two weeks between initial network infiltration and the commencement of data exfiltration and encryption. While their initial access vectors varied, they frequently used compromised VPN credentials. Their post-exploitation activities followed consistent patterns that successfully compromised victim organizations.

After gaining initial access, this threat group targeted Network Attached Storage (NAS) appliances. In multiple observed cases, their methodology included logging into the appliance's web application interface using the 'admin' credentials, modifying system configurations to enable remote SSH connections, and subsequently connecting to those appliances from their initial foothold, such as the VPN IP pool. The group then deployed a malware beacon on the compromised NAS appliance to communicate with their external command and control (C2) infrastructure. Disguised as a legitimate system process on a device that is rarely monitored, this beacon enabled persistent access to internal network resources without relying on their initial infiltration method.

CASE STUDY | ABYSS LOCKER FOCUSING ON NAS AND ESXI

- Forensic evidence has revealed how the compromised NAS appliances served as primary pivot points for the threat actor's lateral movement operations. From these appliances, they expanded their access to other critical network resources, such as domain controllers and file share servers. As their attack progressed, the group extended their reach to multiple ESXi hosts via SSH connections, implementing similar persistence mechanisms that further facilitate their lateral movement throughout the network.

- After establishing sufficient access and privileges within the compromised environment, they began the final phase of the attack. At this stage, the threat actors initiated data exfiltration efforts using the 'rclone' tool to transfer sensitive data from compromised file shares to external locations. Following the successful exfiltration of data, they deployed their encryption payload across the network, specifically targeting VMDK files on the compromised ESXi hosts, effectively crippling the organization's virtualized infrastructure.

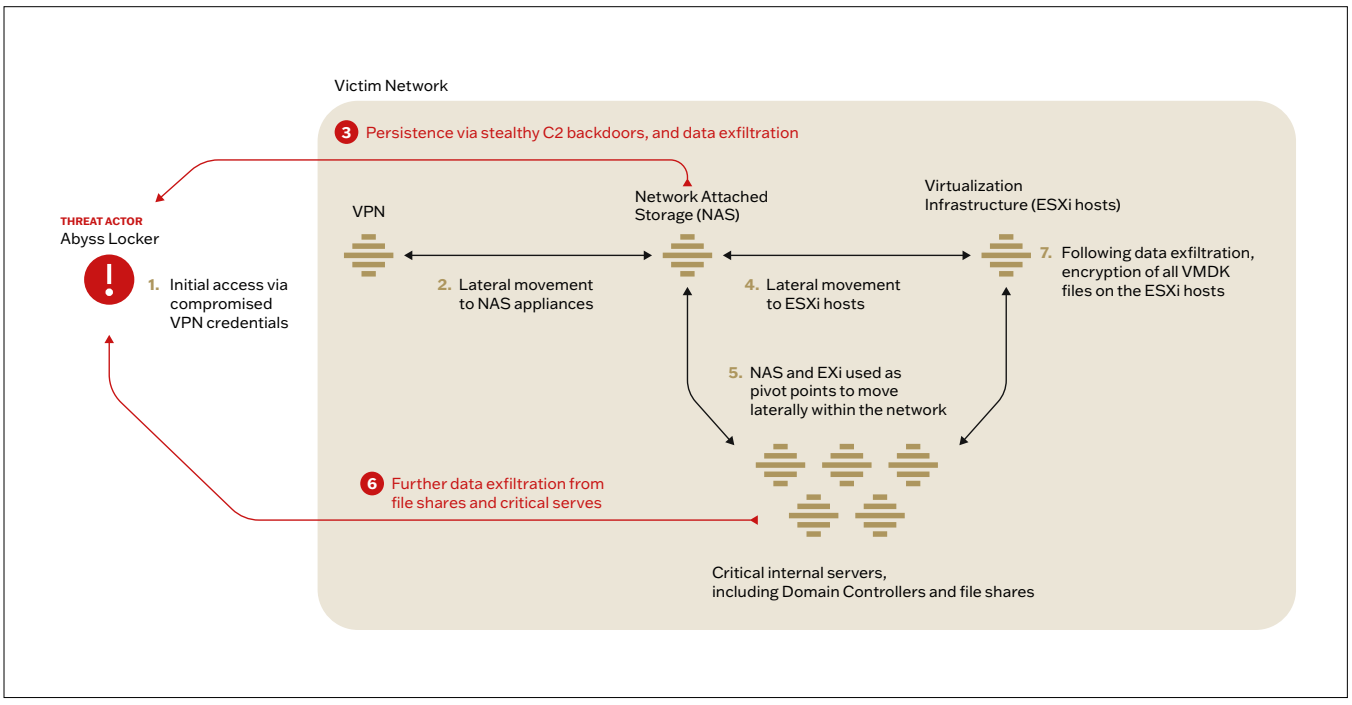


Figure 1: Abyss Locker ransomware attack flow

RANSOMWARE

KEY TRENDS

RANSOMWARE DWELL TIME AND DETECTION OPPORTUNITIES

Ransomware attacks exhibit varying timelines depending on their objectives. While attacks involving only data exfiltration may take mere hours or a few days from start to finish, incidents including mass encryption typically require more extensive preparation. Sygnia's incident response engagements reveal that with encryption-focused attacks, threat groups typically spend one to two weeks inside a compromised network, with data exfiltration usually occurring just before encryption to avoid premature detection. This "dwell time" provides a critical, yet often missed, detection window. Although threat actors leave digital traces that trigger security alerts, these red flags are often not addressed in a timely manner, with containment efforts starting only after encryption or data exfiltration has occurred. However, Sygnia's engagements have shown that acting decisively on early alerts can effectively contain the threat, preventing data breaches and operational disruptions. This reinforces the importance of vigilance and early detection.

SHIFT TO DATA-THEFT EXTORTION

Ransomware operators are increasingly prioritizing data exfiltration over encryption, recognizing the threat of reputational damage due to a data breach can often times be a more effective extortion tactic. It is evident in many high-profile incidents, where organizations are threatened with the exposure of sensitive data, rather than just the loss of access. The potential reputational damage from a public data leak often outweighs the impact of encryption. Known as the "name and shame" approach, this method has proven to be highly effective across industries, especially in sectors like finance, healthcare, and critical infrastructure, where the exposure of sensitive data carries substantial legal and financial repercussions. This shift reduces the need for sophisticated encryption tools, which have higher detection signatures, allowing even lower-tier groups without advanced toolsets to execute high-impact data-theft extortion attacks. Consequently, data visibility, classification, and robust protection are now essential components of ransomware defense strategies, especially as organizations face steep potential penalties from regulations such as GDPR and CCPA.

RANSOMWARE

KEY TRENDS

RANSOMWARE TARGETING VIRTUAL INFRASTRUCTURE:

Virtualized environments, particularly VMware ESXi systems, are increasingly favored targets for ransomware operators due to their central role in managing entire enterprise infrastructures. By compromising a single hypervisor, attackers can control numerous virtual machines, maximizing impact with minimal effort when they encrypt all the hosts managed on the critical ESXi hosts at the final stage of the attack. Recent campaigns illustrate how threat groups such as Abyss Locker, Akira and Black Basta, cripple entire networks by targeting ESXi hypervisors, capitalizing on the inherent centralization of virtual environments to disrupt critical operations in one coordinated strike. Sygnia has found that these environments are often under-monitored and lack comprehensive security controls, especially preventive ones, leaving organizations unprepared for such attacks. One of the contributing factors is that these appliances typically do not have the capability to support standard host-based security agents, including EDR solutions. As the cybersecurity landscape evolves, demand is growing for specialized solutions that provide robust monitoring and hardened access controls for virtualized infrastructures.

EXPANSION TO NON-STANDARD SYSTEMS FOR PERSISTENCE AND PIVOTING:

Ransomware operators are increasingly using under-protected systems like NAS appliances and ESXi hosts as persistence points, and pivoting tools for lateral movement within networks. By installing beacons and persistence mechanisms on these under-protected systems, attackers can maintain stealthy access to the victim network. As described in the case study above, Sygnia's incident response teams have observed attackers leveraging NAS and ESXi systems to launch remote connections and move laterally in the target network, facilitating evasion of standard detection methods. These systems are often overlooked in security programs as they fall outside traditional endpoint protection strategies, lack compatibility with standard security agents, and possess sensitivity as targets that is frequently underestimated. Looking ahead, Sygnia expects the exploitation of overlooked network devices and appliances as attack pivot points to become increasingly prevalent among threat actors.

RANSOMWARE

RECOMMENDATIONS

IMPLEMENT ISOLATED, IMMUTABLE BACKUPS:

As ransomware tactics increasingly sidestep encryption defenses, organizations must focus on ensuring their backup strategies are robust and resilient. Backups should be logically and physically isolated from the production environment to prevent attackers from accessing and destroying them during an attack.

Action Items:

1. Establish an isolated, immutable backup environment with limited access, ensuring that backups cannot be altered or deleted by unauthorized users once written.
2. Conduct periodic testing of the restoration process to confirm backup integrity and ensure isolation from the production environment.

STRENGTHEN VIRTUAL ENVIRONMENT SECURITY AND RESTRICT OUTBOUND TRAFFIC:

Ransomware actors targeting virtual environments frequently exploit weak or misconfigured access controls. Virtualization platforms should be treated as critical infrastructure components that require the same, if not higher, level of protection as domain controllers and other sensitive assets.

Action Items:

1. Enforce strict access controls for hypervisors and virtualization platforms and block direct outbound internet connectivity, except for whitelisted connections originating from hypervisor hosts. Implement network segmentation to isolate virtualization management interfaces and hypervisor hosts from the general network.
2. Ensure hypervisor patching is up to date.

EXTEND VISIBILITY BEYOND STANDARD SYSTEMS:

Establish visibility over critical systems such as hypervisors and Network Attached Storage (NAS) appliances. This enables the detection of suspicious commands, unauthorized access attempts, and configuration changes that could signal malicious activity.

Action Items:

1. Configure all non-standard systems, including hypervisors and NAS appliances, to send logs to the organization's centralized monitoring platform, enabling real-time alerting and analysis.
2. Conduct regular testing to confirm that alerts for unauthorized access or suspicious commands are promptly detected and escalated.

PRIORITIZE HIGH-QUALITY ALERT TRIAGE FOR EFFECTIVE THREAT DETECTION:

Threat actors almost always leave traces of their activity, triggering security alerts that are often overlooked or not properly investigated. Organizations must invest in efficient alert triage processes and ensure security teams aren't overwhelmed with low-fidelity and noisy alerts that distract from true positives. When prevention fails, swift detection and response to these early warning signs is the difference between stopping an attack and facing a full-scale ransomware incident.

Action Items:

1. Establish a high-quality alert triage process that filters out low fidelity alerts and prioritizes critical anomalies, enabling security teams to identify swiftly genuine threats. Conduct regular reviews of alerting accuracy to confirm that critical alerts are escalated promptly, reduce noise and improve response effectiveness.

RANSOMWARE

RECOMMENDATIONS

2. Evaluate the need for a third-party managed SOC with proven capabilities if the in-house SOC is unable to manage the organization's threat landscape effectively or if maintaining an in-house SOC is too resource intensive. Partner with a managed SOC provider that offers:
   a. Advanced threat detection and response capabilities.
   b. 24/7 monitoring and incident escalation.
   c. Expertise in handling advanced threats specific to your organization's industry and risk profile.
   d. Integrated threat intelligence and proactive threat hunting.

PREPARE FOR DATA EXTORTION SCENARIOS WITH STRUCTURED EXERCISES AND POLICIES:

Establish a comprehensive approach to data extortion preparedness, incorporating ransomware-specific tabletop exercises and clear, predefined policies on ransom payment and incident escalation.

Action Items:

1. Conduct ransomware-specific tabletop exercises to simulate extortion scenarios.
2. Clarify roles and responsibilities, and identify critical decision points for involving senior leadership, legal advisors, and technical experts.
3. Create a ransom payment policy that includes guidance on weighing legal, financial, and reputational risks and protocols for communication with both attackers and public stakeholders during an extortion event.

SUPPLY CHAIN ATTACKS

Supply chain attacks exploit trusted relationships with vendors, contractors, and service providers

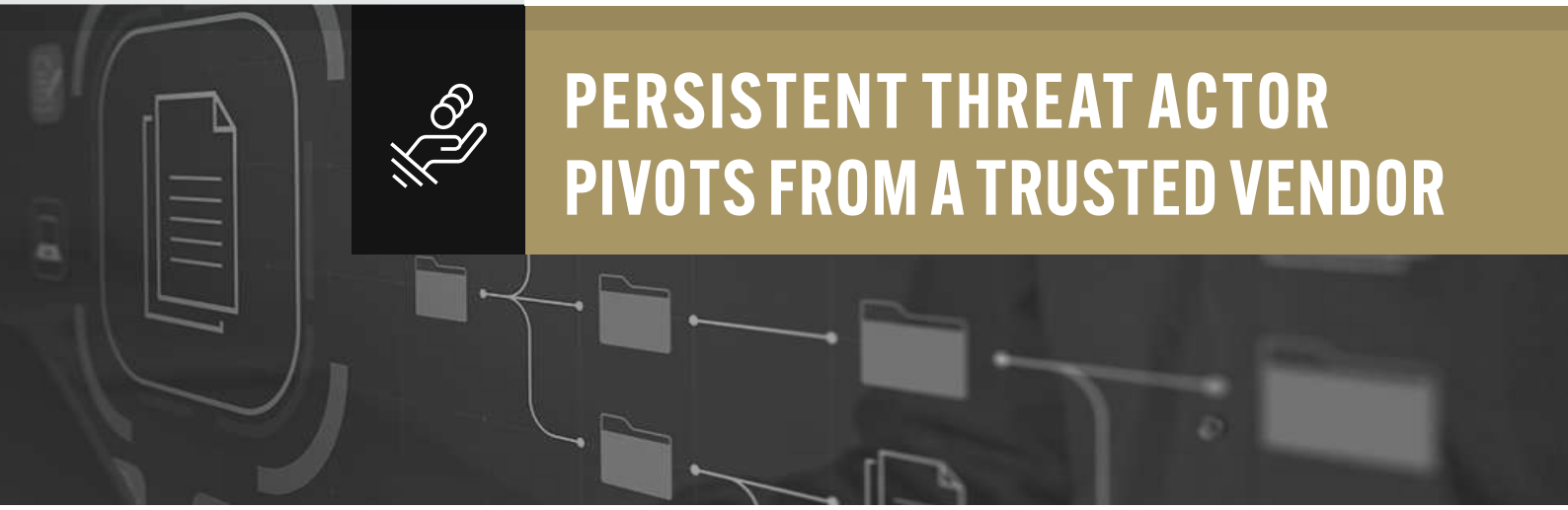
In today's interconnected business environment, supply chain and third-party vulnerabilities have emerged as significant entry points for cyber attackers. Supply chain attacks enable threat actors to bypass traditional security defenses by exploiting trusted relationships with vendors, contractors, and service providers. Ransomware groups such as BlackCat (ALPHV) often use compromised third-party credentials to infiltrate critical internal systems and perform undetected lateral movement. The evolving threat landscape demands a proactive approach to securing supply chains, as any gaps in third-party security can expose entire organizations to significant threats.

As organizations increase their reliance on external providers for critical operations, the need for stringent vendor oversight and continuous monitoring has become paramount. Third-party vendors like managed service providers (MSPs), IT vendors, and cloud hosting providers are frequently granted privileged access to internal networks, making them prime targets for attackers. Compounding the issue, organizations often lack visibility into vendor security practices and lack detection over the connectivity between their vendors' environment and their own. As a result, organizations often remain unaware of security breaches stemming from compromised third-party environments until they surface in their own core network.

This section outlines essential trends and recommendations for mitigating risks within the supply chain. Key trends include the heightened threat posed by third-party vulnerabilities, the challenges associated with dependency on external service providers, and the critical need for visibility of potential third-party threats. To address these challenges, actionable recommendations are provided, including strengthening supply chain security through multi-factor authentication (MFA) and regular audits, implementing continuous monitoring of third-party activity, and establishing a third-party incident response framework. By adopting these measures, organizations can bolster their resilience against supply chain attacks, ensuring a proactive and structured defense against the evolving threats targeting modern business ecosystems.

CASE STUDY

PERSISTENT THREAT ACTOR PIVOTS FROM A TRUSTED VENDOR



ATTACKER:

APT group

ATTACK TYPE:

Long-term persistence

NOTABLE TACTICS:

Maintain persistence within the target network for years

Use third-party legitimate connectivity for access

Used vendor's systems for backdoor access to victim environment

Advanced Persistent Threat (APT) groups often employ sophisticated strategies to maintain long-term, undetected presence within target networks, unlike ransomware operators who reveal their presence through encryption or extortion demands. During a recent incident response engagement, Sygnia encountered an APT group that had successfully maintained persistence within a client network for several years, demonstrating the sophisticated nature of the attacker's operational security.

Following initial threat remediation and removal of malicious tools, Sygnia implemented advanced monitoring capabilities to identify potential attempts for the threat actor to resurface. Within weeks, suspicious activities matching the threat actor's known patterns were observed originating from a third-party service provider's network. This vendor maintained legitimate interconnectivity with our client's environment to support continuous customer operations throughout the course of the investigation and remediation activities. Investigation revealed the threat actors were leveraging existing vendor permissions to move laterally through Remote Desktop Protocol (RDP) connections, accessing the client's internal servers and databases. This access method proved particularly challenging to mitigate, as the organization's daily operations relied heavily on the vendor's ability to access these systems for customer support and maintenance.

CASE STUDY | PERSISTENT THREAT ACTOR PIVOTS FROM A TRUSTED VENDOR

As Sygnia's incident response teams pivoted to the vendor's environment to continue our in-depth investigation, we uncovered this specific APT group's tools and attack patterns across more than a dozen compromised systems within the vendor's network. Historical log analysis indicated that this access through the vendor occurred a few times in the past year. This approach allowed the threat actor to retain backdoor access to the victim's environment, which was difficult to identify as their activities blended with legitimate vendor operations.

This case highlights how sophisticated threat actors exploit the trusted relationships between organizations and their third-party vendors, using legitimate access channels to maintain persistent network access while evading detection mechanisms traditionally focused on external threats.

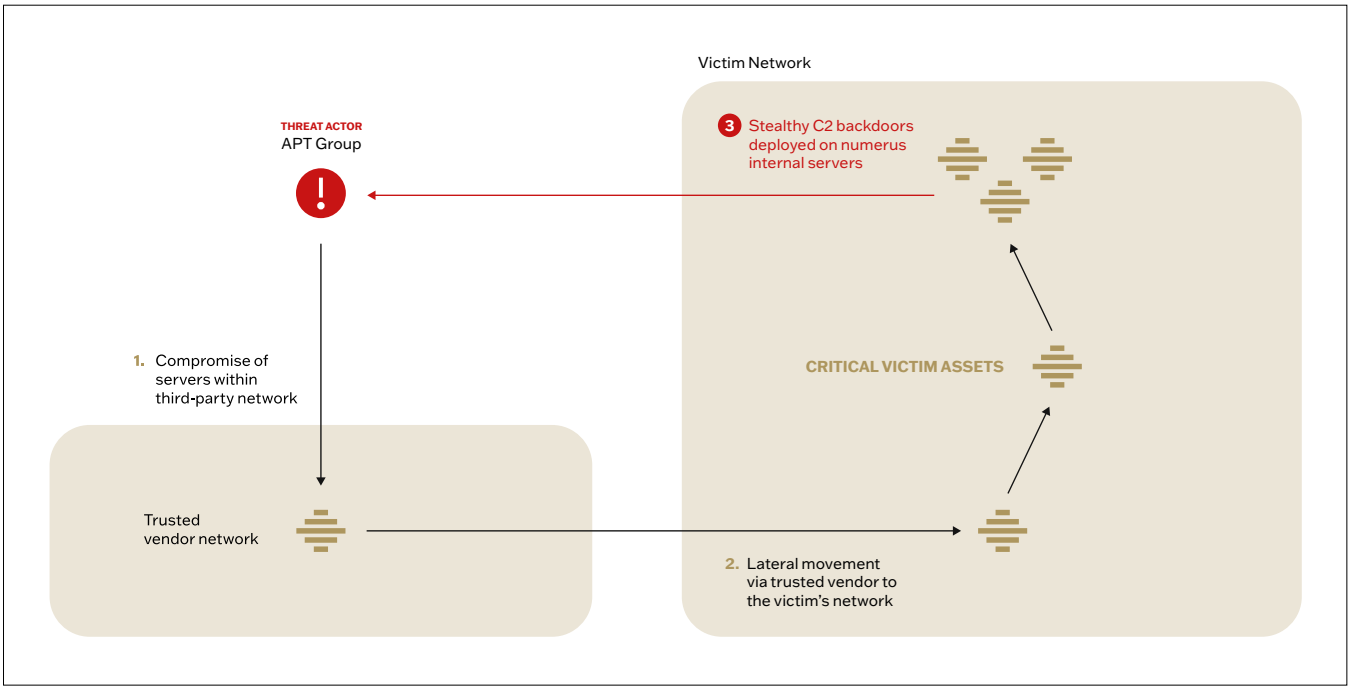


Figure 2: Attack flow exploiting trusted third-party vendor

SUPPLY CHAIN ATTACKS

KEY TRENDS

INITIAL ACCESS VIA COMPROMISED THIRD-PARTY VENDOR:

Supply chain attacks are becoming a primary strategy for threat groups seeking indirect access to larger targets. Threat actors often compromise smaller, less-secure vendors and use their trusted credentials to infiltrate critical internal networks. Numerous groups, including Chinese advanced persistent threat (APT) groups recently observed by Sygnia's IR team, exemplify this approach, leveraging trusted third-party credentials to move laterally without detection within a victim's network. Sygnia's research highlights the need for rigorous third-party risk management, including multi-factor authentication (MFA), least-privilege access, and continuous monitoring of third-party activity. The interconnected nature of modern ecosystems make these supply chain vulnerabilities a favored attack vector, with organizations that fail to address these risks remaining particularly susceptible.

LATERAL MOVEMENT USING PRIVILEGED VENDOR ACCOUNTS:

Increasing reliance on third-party providers for core functions has expanded the attack surface for organizations. Vendors and contractors often have privileged access to internal systems, making them attractive entry points for attackers. Commonly affected service providers include IT support, cloud hosting, and managed service providers (MSPs), who often handle sensitive data or control key systems. Throughout the past year, Sygnia observed numerous threat actors exploiting legitimate third-party vendor permissions to achieve extensive lateral movement within target organization networks. This reliance of many organizations on external providers increases the potential for severe disruption in case of a breach and highlights the need for organizations to monitor and secure their vendors' security practices as rigorously as their own.

VISIBILITY GAPS IN THIRD-PARTY VENDORS ENABLE THREAT ACTOR ACCESS TO INTERNAL NETWORKS:

Many organizations lack full visibility into the security practices and real-time activity of their third-party vendors, leaving gaps that attackers can exploit. Even when vendors undergo initial vetting, ongoing monitoring is often limited or inconsistent, meaning that any changes in a vendor's security posture might go undetected. Additionally, third-party security incidents can go unreported or undiscovered, leaving organizations unaware of potential vulnerabilities introduced by their supply chain. During multiple incident response engagements, Sygnia documented threat actors repeatedly accessing target networks through compromised vendor systems. The attackers exploited the limited visibility organizations have over third-party connections, using this blind spot as a persistent infiltration vector. Improving visibility into vendor environments is essential for detecting and mitigating risks posed by third-party connections and activities.

SUPPLY CHAIN ATTACKS

RECOMMENDATIONS

STRENGTHEN SUPPLY CHAIN SECURITY:

Third-party risk management is essential to protect against ransomware introduced through the supply chain. Enforcing strict access controls, multi-factor authentication (MFA), and conducting security audits for all vendors minimizes vulnerabilities that could be exploited for lateral movement into the organization.

Action Items:

1. Conduct annual security audits of all third-party access points, implementing MFA and access controls for vendor connections.
2. Document identified vulnerabilities in a risk management plan.

LIMIT ACCESS AND SEGMENT NETWORK CONNECTIONS FOR THIRD PARTIES:

Restrict vendor access to necessary resources and consider network segmentation to prevent lateral movement within the network. Network segmentation limits the extent of access vendors have and minimizes the potential impact of a third-party breach.

Action Items:

1. Configure segmented network zones for third-party access, applying least-privilege principles to restrict access to only required systems.
2. Revoke unused access and permissions.

IMPLEMENT CONTINUOUS MONITORING OF THIRD-PARTY ACTIVITY:

Continuously monitor after third-party activity within your network to identify suspicious actions or unauthorized access attempts. Continuous monitoring enables rapid detection of anomalous behavior involving trusted vendors, enhancing real-time threat response capabilities.

Action Items:

1. Deploy a continuous monitoring system that tracks vendor activities in real-time, with automated alerts for unusual access patterns or unexpected configuration changes.

ENHANCE VENDOR VETTING AND RISK ASSESSMENT PROCESSES:

Strengthen initial and ongoing vendor risk assessments to evaluate each vendor's security posture. This includes assessing the vendor's access scope, the sensitivity of the data they handle, and their cybersecurity practices, with frequent re-evaluations to adapt to evolving threats.

Action Items:

1. Document vendor risk assessment processes.
2. Conduct a periodic risk assessment for each third-party supply chain vendor and update access controls as needed.

ESTABLISH A THIRD-PARTY INCIDENT RESPONSE FRAMEWORK:

Develop a third-party incident response framework to coordinate response efforts in case of a breach involving a supply chain vendor. This framework should outline protocols for incident escalation, communication, and containment measures when a third-party security incident impacts the organization.

Action Items:

1. Create an incident response framework with designated roles and communication protocols established for immediate response and containment.

IDENTITY PROTECTION AND ZERO TRUST

There is a growing trend of attackers targeting non-human identities which often lack robust security monitoring and security controls

In 2024, our incident response teams observed a significant surge in the frequency and severity of cloud identity attacks. This aligns with the broader organizational shift toward cloud-only environments. In response, threat actors are adapting their tactics, increasingly focusing on identity-based attacks targeting cloud infrastructure.

Attackers continue to exploit vulnerabilities in identity protection, making multi-factor authentication (MFA) and identity governance critical areas of focus. However, not all MFA implementations provide equal security. Simpler methods, such as SMS-based or email-based codes, are increasingly bypassed by attackers using advanced techniques like session-cookie theft, adversary-in-the-middle (AiTM) phishing, and SIM swapping. These sophisticated methods enable threat actors to circumvent standard MFA defenses, gaining unauthorized access despite the presence of additional authentication layers.

As organizations continue to migrate to cloud infrastructure, misconfigured Identity and Access Management (IAM) policies create openings for lateral movement and privilege escalation within cloud ecosystems. The growing use of insufficiently monitored service accounts and the ability to pivot between environments through SSO connections create additional attack vectors for threat actors. Additionally, AI-driven attacks create a formidable challenge. Threat actors are leveraging AI to automate social engineering, impersonate users through deepfakes, and craft highly authentic phishing messages, elevating the stakes for identity defenses.

Strengthening identity protection requires strategic action. Organizations should start by improving identity governance through regular, automated audits that enforce least-privilege access and reduce the risk of credential misuse. Adopting Zero Trust principles, such as just-in-time (JIT) access and continuous verification, can further limit attacker movement by re-evaluating access for sensitive operations.

This section provides a focused analysis and actionable strategies to fortify identity protection, preparing organizations to tackle today's complex identity-based threats.

CASE STUDY

LINKEDIN TO EC2: STORY OF A STATE-SPONSORED CLOUD BREACH

ATTACKER:

Nation-state

ATTACK TYPE:

Identity Theft

NOTABLE TACTICS:

Used social engineering on LinkedIn and WhatsApp to connect with employees of the target organization

Bypassed MFA and other security controls

Modified a Lambda function to execute code on EC2

In mid-2024, our incident response teams responded to an attack by a state sponsored threat actor who targeted an organization's cloud environment to steal specific digital assets. The group demonstrated advanced capabilities, resources, and perhaps most crucially, the patience to execute a carefully orchestrated attack. The attack began with social engineering on LinkedIn and WhatsApp, where they posed as individuals seeking technical advice from a few of the organization's key development staff.

Through persuasive communication, they convinced these employees to download and run what seemed like harmless code on their corporate laptops, which the employees used regularly for software development. Behind the scenes, this code inconspicuously harvested access keys and credentials from the employees' devices. The attackers were able to gain access to the organization's Microsoft 365 tenant and authenticate against Entra ID using captured session tokens. This technique not only bypassed multi-factor authentication but also circumvented other security controls in place. The group also discovered AWS access keys on the compromised devices, giving them two ways into the AWS environment - through direct API access and the web console via their compromised Entra ID users.

CASE STUDY | LINKEDIN TO EC2: STORY OF A STATE-SPONSORED CLOUD BREACH

Once inside AWS, the threat actors methodically hunted for the target assets while looking for ways to expand their reach. Though their initial permissions didn't give them direct access to their objectives, they discovered an interesting weakness: they could modify a Lambda function that, when triggered, could execute code on several previously inaccessible EC2 instances. By gaining control over these instances, they were able to craft fraudulent API calls that finally gave them access to the critical assets they were after.

This incident highlights a critical pattern Sygnia commonly observed. While this case involved an advanced state-sponsored threat actor, similar attack methodologies are increasingly employed by less sophisticated threat groups. Once initial access is achieved through compromised credentials or access keys, attackers systematically explore and exploit existing permissions, seeking opportunities for privilege escalation and lateral movement until reaching their objectives. While organizations may invest heavily in IAM permissions and least-privilege models, it's often only through red team attack simulations that these small but critical gaps can be identified - the very same gaps that threat groups are increasingly skilled at finding and exploiting.

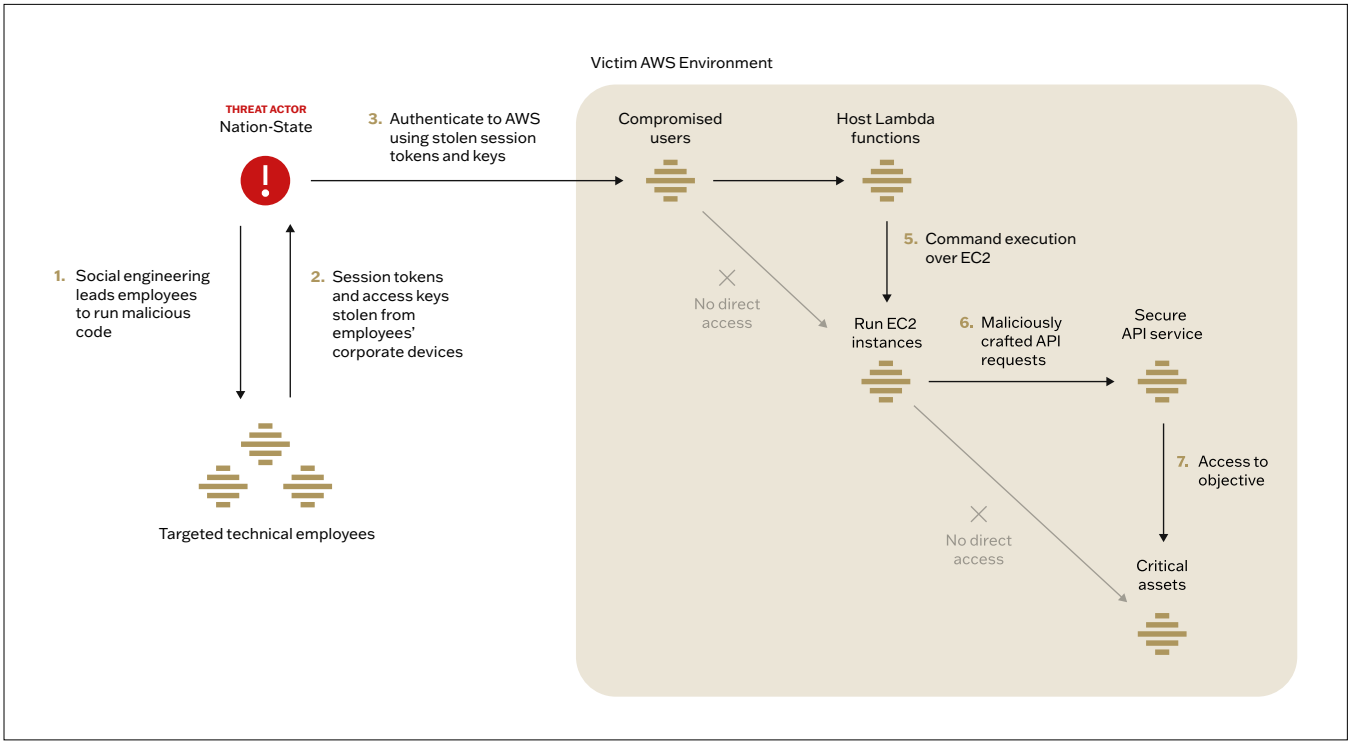


Figure 3: Process flow of social engineering attack exploiting compromised credentials

IDENTITY PROTECTION AND ZERO TRUST

KEY TRENDS

MFA BYPASS TECHNIQUES:

Attackers have refined methods for bypassing multi-factor authentication (MFA), using phishing kits, SIM swapping, social engineering, push MFA fatigue, and session-cookie theft. Phishing kits often employ "man-in-the-middle" (MiTM) attacks, positioning themselves between users and authentication providers to intercept one-time passwords (OTPs) and session cookies as users log in. Once the session cookie is captured, attackers can impersonate the user without needing further credentials, effectively bypassing MFA. These MiTM kits often use reverse proxies that replicate legitimate login screens and capture both credentials and session cookies for seamless, unauthorized access. SIM swapping, where attackers hijack a user's phone number to intercept SMS-based MFA codes, is another technique that remains effective due to weak telecom security. Combined with targeted social engineering, these methods allow attackers to bypass MFA with high success rates. Additionally, attackers exploit MFA push notification fatigue - repeatedly sending authentication requests until frustrated users approve one in order to make them stop. While sometimes effective, this method risks detection as unusual MFA prompts can also lead users to report suspicious activity.

AI-DRIVEN ATTACKS:

Attackers are leveraging AI to automate and enhance various stages of identity-based attacks, including the creation of deepfake audio and video for impersonation, as well as machine-learning algorithms to optimize phishing messages. AI-driven phishing uses natural language processing (NLP) to analyze the tone and structure of corporate communications, generating highly convincing emails that bypass standard filters. Deepfake technology is increasingly used to impersonate executives or other high-privilege users in voice verification systems, thereby bypassing identity verification controls.

PERMISSION MINING AND LATERAL MOVEMENT:

Threat actors are increasingly adopting sophisticated techniques to systematically explore and exploit identity permissions within cloud environments. After gaining initial access, attackers carefully map out existing permissions, looking for seemingly minor misconfigurations that can be chained together for privilege escalation. They leverage tools to automatically enumerate roles, policies, and trust relationships, identifying subtle paths to higher privileges. Advanced groups are particularly adept at finding hidden permission paths through nested roles and cross-account trusts, often exploiting legitimate features like AWS Lambda functions or Azure managed identities to move laterally. This methodical approach allows attackers to gradually expand their reach while maintaining stealth, as each individual step may not trigger alerts. For example, in the use case above, the threat actors edited a Lambda function to run commands on EC2 instances and make API requests. Each step was legitimate within the instance's permissions and expected in day-to-day operations. A clear indication of attack is only possible when looking at the complete chain of events.

IDENTITY PROTECTION AND ZERO TRUST

KEY TRENDS

SERVICE ACCOUNT EXPLOITATION:

There's a growing trend of attackers targeting non-human identities, particularly service accounts, which often lack robust monitoring and security controls. These accounts, critical for automation and system operations, frequently hold extensive privileges but receive less security scrutiny than human users. Attackers exploit this oversight by targeting service account credentials stored in configuration files, environment variables, or code repositories. Once compromised, these accounts are particularly valuable as they often have persistent access, and their automated nature means suspicious activities may go unnoticed for extended periods. The challenge of distinguishing between legitimate automated activities and malicious actions makes detecting these compromises especially difficult. Standard security controls like MFA are often not applicable to these identities. Additionally, threat actors often hide in plain sight by creating backdoor users with elevated permissions, using naming conventions to make them look like legitimate service accounts.

CROSS-ENVIRONMENT SSO PIVOTING:

Threat actors are increasingly exploiting Single Sign-On (SSO) infrastructure to pivot between different cloud environments and services. By compromising identities in one environment, attackers leverage SSO trust relationships to gain unauthorized access across multiple connected systems. This technique is particularly effective in modern enterprises where SSO is widely implemented for user convenience and operational efficiency. While SSO generally strengthens security by reducing the number of credentials that need to be protected, attackers who successfully compromise these centralized identities exploit the trust relationships between identity providers and service providers to move between Microsoft 365, AWS, GCP, and other cloud services, as well as utilizing it for remote access to on-premise networks.

IDENTITY PROTECTION AND ZERO TRUST

RECOMMENDATIONS

STRENGTHEN IDENTITY GOVERNANCE:

Tighten identity governance to reduce the risk of compromised credentials leading to broader breaches—a primary concern with cloud identity attacks and MFA bypass tactics. With stronger governance, permissions are limited and regularly reviewed, preventing adversaries from using stolen or privileged credentials to move laterally across environments.

Action Items:

1. Conduct regular, automated audits of permissions to verify least-privilege access, especially for service and high-privilege accounts.
2. Protect your sensitive credentials and API keys in a key vault.
3. Scan code regularly and automatically to detect hard-coded or mishandled secrets.
4. Auto-rotate credentials.
5. Use cloud workload identities (e.g., attach AWS IAM roles) where applicable.

ADOPT ZERO TRUST PRINCIPLES:

Apply zero-trust principles to counter threats associated with MFA bypass and AI-driven attacks by ensuring that every access request is validated continuously. By enforcing re-authentication and context-aware access, organizations limit the effectiveness of session-cookie theft and impersonation tactics seen in advanced phishing and deepfake attacks.

Action Items:

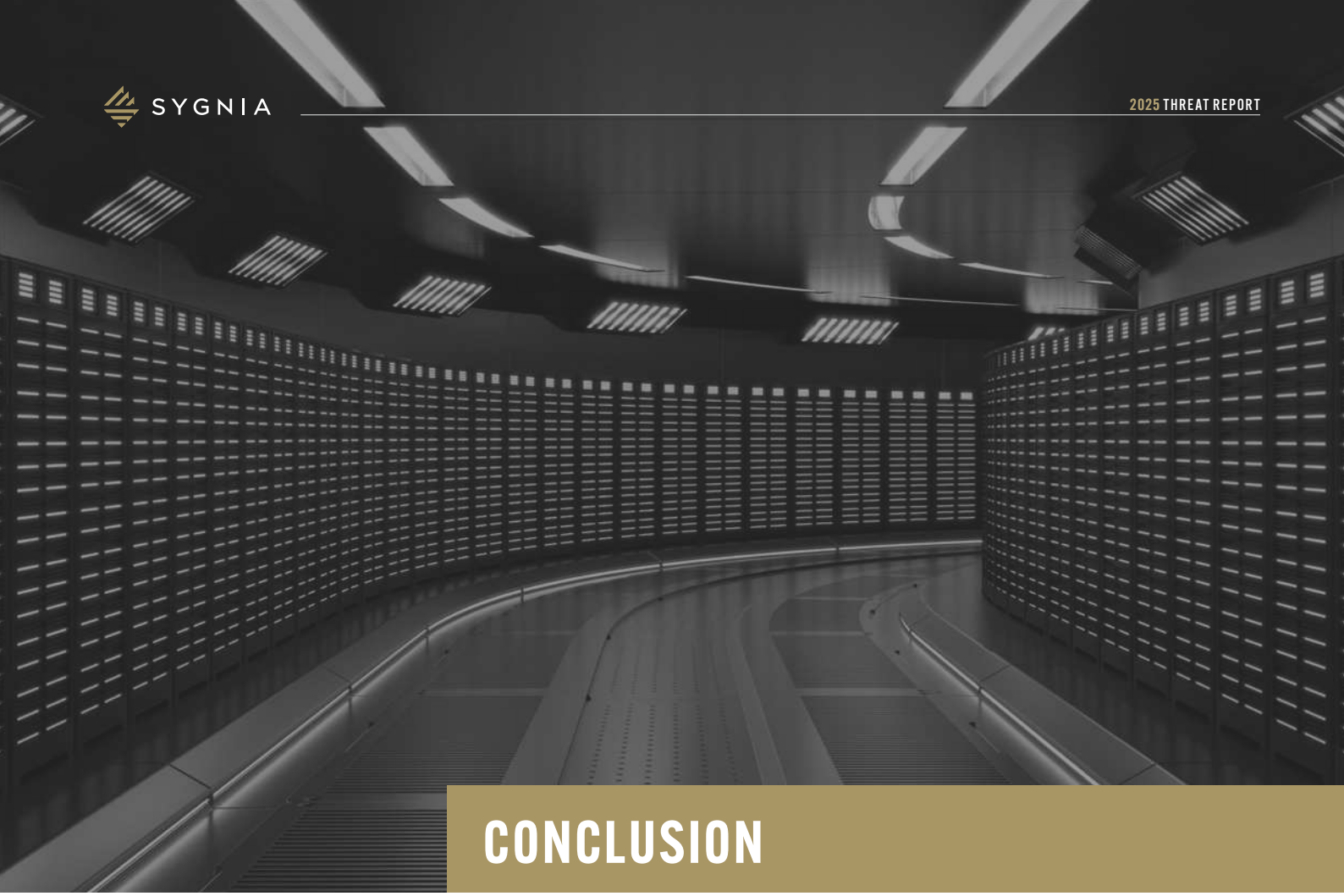
1. Implement just-in-time (JIT) access for high-sensitivity operations, requiring re-authentication for privileged actions.
2. Transition from legacy remote access VPNs to Zero Trust Network Access (ZTNA) for all remote connections to ensure granular, policy-based access control.
3. Enforce strong authentication methods internally, such as requiring MFA even for access within the corporate network and enforce secure, token-based service-to-service authentication for internal APIs.

CONDUCT IDENTITY-FOCUSED RED TEAM ASSESSMENTS:

Regular red team exercises specifically targeting identity systems and access patterns are crucial for uncovering subtle permission gaps and trust relationship vulnerabilities. These assessments validate the effectiveness of identity controls and reveal potential attack paths that threat actors could exploit through permission mining and lateral movement techniques.

Action Item:

1. Include identity-focused attack scenarios in red team exercises, specifically testing for permission chain exploitation, service account vulnerabilities, and SSO trust relationship weaknesses.



CONCLUSION

To build resilience, validate specific risks to your organization, map threats to operational realities and prioritize cybersecurity strategies to address the most critical risks

The threats identified in this report—ransomware evolution, supply chain exploits and identity-based intrusions—underscore the urgency for security leaders to adopt strategies that address both current and emerging risks.

To build resilience in 2025, begin by conducting a comprehensive revalidation of the specific risks to your organization. This involves closely examining the identified threats—ransomware evolution, supply chain exploits, and identity-based intrusions—and mapping them to their operational realities. This step ensures that cybersecurity strategies address the most critical risks to the organization while minimizing efforts on less relevant threats.

Once the threat landscape is clearly defined, select the action items from the appendix that are most relevant to your organization's context. Each organization has unique vulnerabilities, operational constraints, and resource capacities, so tailoring the focus of your cybersecurity efforts is essential.

Next, develop a cohesive strategy that integrates these action items into a structured implementation plan. This plan should detail timelines, resource allocation, and success metrics to ensure accountability and track progress. Consider layering your defenses and phasing initiatives based on immediate impact and organizational readiness. For example, prioritize foundational improvements, such as visibility and threat detection, before rolling out complex changes like Zero Trust architectures or advanced monitoring solutions.

By following this structured process, starting with re-validating your threat landscape, customizing your response with targeted action items, and crafting a practical strategy, your organization will be well-positioned to mitigate risks and bolster resilience against both current and emerging cybersecurity threats.

APPENDIX: ACTION ITEMS CHECKLIST

Status	Chapter	Action Item
☐	Ransomware Trends	Establish isolated, immutable backups and regularly test restoration processes.
☐	Ransomware Trends	Conduct periodic testing of the restoration process to confirm backup integrity and ensure isolation from the production environment.
☐	Ransomware Trends	Enhance visibility by centralizing and monitoring logs from critical systems, including hypervisors and NAS appliances.
☐	Ransomware Trends	Enforce strict access controls and restrict outbound traffic from virtual environments.
☐	Ransomware Trends	Conduct ransomware-specific tabletop exercises to simulate extortion scenarios, including best practice policies and playbooks, with guidance for necessary action during an extortion event.
☐	Identity Protection	Conduct regular, automated audits of permissions to enforce least-privilege access.
☐	Identity Protection	Implement just-in-time (JIT) access and zero-trust for high-sensitivity operations
☐	Identity Protection	Implement regular red team assessments focused on finding subtle permission gaps and identity-based attack paths.
☐	Supply Chain Security	Conduct security audits and implement MFA for all third-party vendor connections.
☐	Supply Chain Security	Establish a third-party incident response framework with clear escalation protocols.
☐	Supply Chain Security	Deploy a continuous monitoring system that tracks vendor activities in real-time, with automated alerts for unusual access patterns and unexpected configuration changes.
☐	General Recommendations	Transition from legacy VPNs to Zero Trust Network Access (ZTNA).
☐	General Recommendations	Establish a high-quality alert triage process that filters out low fidelity alerts and prioritizes critical anomalies, enabling security teams to swiftly identify genuine threats.
☐	General Recommendations	Evaluate the need for a third-party managed SOC with proven capabilities.

SYGNIA

CONTRIBUTORS

Nital Rozin, Omer Kidron, Eran Liloof, Oren Biderman, Haim Nachmias, Matan Naftali, Rena Stern

WANT TO KNOW MORE ABOUT ONE OF OUR SOLUTIONS?

As the trusted advisor and cybersecurity service provider of leading organizations worldwide, Sygnia protects the enterprise through a variety of solutions that are aligned with the current threat landscape. From OT and Cloud Security to Ransomware Readiness, our Enterprise Solutions are borne out of frontline experience and a deep understanding of the threat actor mindset.