REPORT

Stopping real-world attacks: Lessons for business leaders from the 2026 cyber frontline

Practical steps to reduce business cyber risk based on analysis of 661 incidents remediated by Sophos X-Ops, as detailed in the 2026 Sophos Active Adversary Report

SOPHOS

Introduction

The 2026 Sophos Active Adversary Report offers an evidence-based look at how today's attackers operate in real environments, drawing on insights from incidents remediated by the Sophos Emergency Incident Response and Sophos Managed Detection and Response (MDR) teams.

These insights give organizations a practical view of the attack techniques most likely to drive high-impact incidents. By learning what adversaries are actually doing in real-world attacks, businesses can strengthen their defenses and meaningfully reduce their cyber risk.

Key Learnings

- **Identity is now the primary attack vector**, with 67% of intrusions beginning with compromised credentials or other identity-related tactics.

  ACTION: Reduce risk of credential compromise and put defenses in place to detect and respond to identity-based attacks.

- **Ransomware actors strike when defenders aren't watching**, overwhelmingly deploying ransomware and exfiltrating data during nights and weekends.

  ACTION: Ensure 24/7 security operations coverage to detect and neutralize attacks whenever they occur, working with external specialists if needed.

- **Firewall vulnerabilities remain a high-impact entry point**, with attackers frequently exploiting flaws like the critical-rated Improper Access Control vulnerability in SonicWall SonicOS and targeting misconfigured or unpatched devices.

  ACTION: Prioritize reducing exposure of edge devices, including timely patching and hardening of controls.

- **Threat actors are getting faster at attacking Active Directory (AD)**, with attackers now reaching AD in just three hours and 24 minutes on average.

  ACTION: Make sure you can detect and respond to attempted AD attacks before the are exploited.

- **Missing telemetry leaves organizations blind to early warning signs**, making it harder to trace attacks or identify early indicators of compromise.

  ACTION: Leverage security telemetry from a range of sources and retain logs long enough to improve detection, investigations, and incident response outcomes.

Identity is now the primary vector

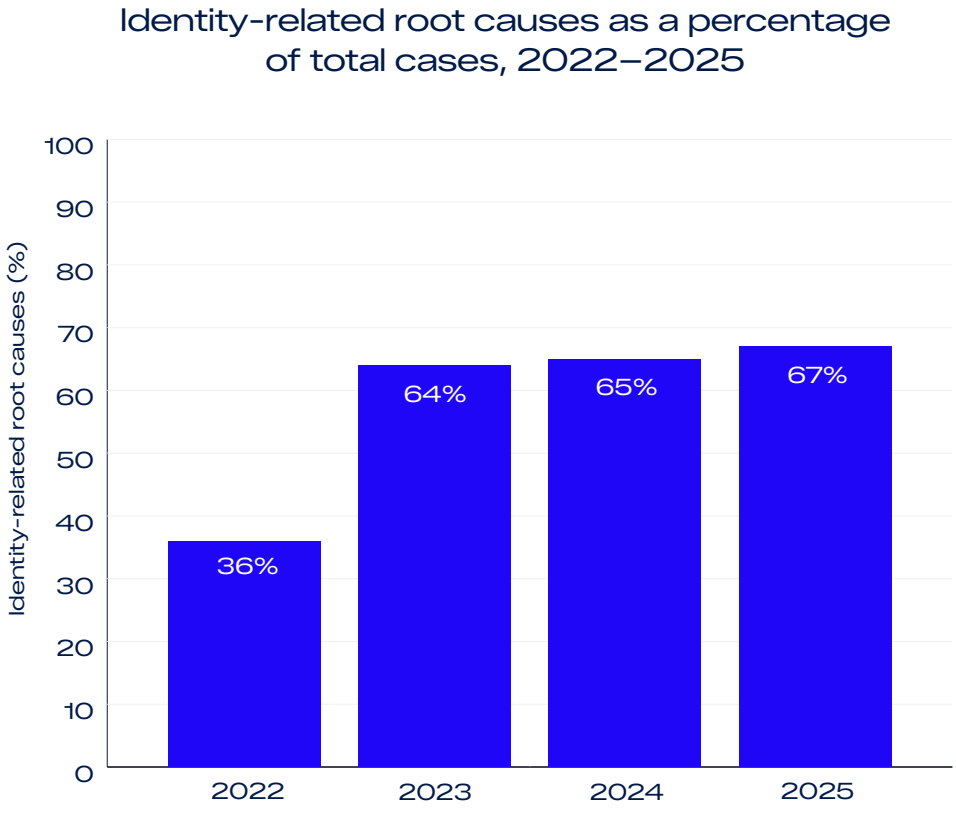
Identity-based attacks continue to dominate the threat landscape: 67% of the incidents studied began with brute-force attacks, phishing, authentication token theft, abused trusted relationships, or other credential-compromise attacks.

While the credentials used in these attacks are often gained through leaks on the dark web following an earlier breach, phishing emails, and by threat actors capturing legitimate users' keystrokes, in many cases victims never discover how their credentials were originally obtained.

Once attackers can impersonate a legitimate user, they can quietly move through the environment — enabling ransomware deployment, data theft, and even business email compromise (BEC).

67%

of attacks start with identity-related tactics.



Practical steps to stop identity-based attacks

To reduce identity-driven attacks, organizations should begin by enforcing multi-factor authentication (MFA) everywhere, particularly on accounts with administrative or remote access privileges.

From there, businesses should focus on good identity hygiene and having ongoing visibility into how their credentials are being used across the environment. This includes understanding where logins originate, whether privilege levels are changing unexpectedly, and if activity aligns with normal patterns for the user or system involved.

Defenders can protect against brute-force attacks by setting a threshold for failed login attempts before a user is locked out or requiring MFA.

Additionally, businesses should conduct regular access reviews to revoke unnecessary or excessive privileges, search for dormant identities, and regularly review their identity lifecycle management processes (provisioning, updates, and deprovisioning).

It's crucial to detect when credentials are being abused, not simply used, so organizations can contain malicious behavior as soon as it begins. Taken together, strong authentication controls, continuous monitoring, and rapid detection of credential misuse form the backbone of effective identity security.

Preventing identity-based attacks: How Sophos can help

Sophos Managed Detection and Response (MDR) uses rich identity telemetry to rapidly detect credential abuse and intervene 24/7 — often within minutes — before attackers turn access into impact.

Sophos Identity Threat Detection and Response (ITDR) further strengthens and extends Sophos MDR's identity protection by performing more than 80 continuous identity posture checks, uncovering weak configurations, and flagging high-risk identity exposures early. When paired with Microsoft Entra ID, organizations gain central identity management plus deeper telemetry that feeds directly into deeper telemetry that empowers security analysts.

Ransomware actors strike when defenders aren't watching

88%

of ransomware payloads are deployed during non-business hours.

Ransomware actors deliberately target victims on the days and times when IT and cybersecurity teams are most likely to be operating at a limited capacity to avoid being detected, often exfiltrating data and encrypting files during major holidays, nights, and weekends.

Evidencing this approach, 88% of ransomware payloads (i.e., when adversaries attempt to encrypt files) are deployed during non-business hours. These out-of-hours attacks are spread across all days of the week with a slight increase on Thursdays and Fridays, when workers are more likely to be on vacation or logging off early. Similarly, 79% of data exfiltration actions take place in off-hours.

Practical steps to stop ransomware

Speed is critical for detecting and responding to ransomware attacks before significant damage is done, making 24/7 monitoring a must-have for organizations of all sizes.

Companies should strengthen their ransomware resilience by ensuring that security operations specialists — internal staff, an external specialist provider, or a combination of both — are watching their environment at all hours and are able to swiftly neutralize adversary actions.

Beyond constant visibility, organizations should put emphasis on ensuring strong ransomware defenses within their endpoint protection and wider security controls. This includes deploying technology that can recognize suspicious behavior well before encryption begins, stop attempts to encrypt files locally and remotely, and automatically block and automatically roll back malicious activity.

Ransomware defense: How Sophos can help

Sophos MDR is the world's most trusted MDR service, delivering 24/7 detection and response proven to neutralize even the most sophisticated ransomware attacks. Leveraging AI, automation, and an unmatched team of global cybersecurity experts, Sophos MDR monitors your environment around the clock, detecting and stopping attacks before they can impact your business.

Sophos Endpoint uses behavioral analysis and proprietary CryptoGuard technology to automatically block and roll back unauthorized encryption, including remote ransomware (the technique that's used in 70% of successful human-operated ransomware attacks according to the Microsoft Digital Defense report).

Firewall vulnerabilities remain a high-impact entry point

The rise of identity-driven attacks doesn't mean that unpatched vulnerabilities have stopped mattering. In fact, when attackers do turn to exploits, they make the most of every opportunity.

In the 2026 Active Adversary dataset, more than two-thirds (67%) of the incidents that started with a CVE involved CVE-2024-40766, a SonicWall SonicOS firewall vulnerability that had to be repeatedly patched over the course of the year. This pattern highlights a critical weakness for many organizations: Once a perimeter device is exposed, attackers will keep coming back to it repeatedly until it is fully secured.

What's equally concerning is how long many firewalls and other edge systems remain vulnerable after a fix is available. Across all confirmed exploited vulnerabilities in the dataset, the median time between a vendor publishing an advisory or patch and an attacker exploiting that flaw was 322 days — almost a full year of opportunity for adversaries.

The median gap between the release of a public proof-of-concept and real-world exploitation was similarly long, at nearly 297 days. In fact, some of the CVEs used in attacks dated as far back as 2008, underscoring how long unpatched weaknesses can persist in production environments.

Practical steps to reduce risk from firewall vulnerabilities

To reduce the risk of firewall exploitation, organizations need to prioritize rapid patching of perimeter systems and maintain a disciplined process for deploying security updates quickly after they are released.

Firewalls and edge devices remain high-value targets because they sit at the network boundary, and any delay in patching gives attackers an opportunity to strike. Businesses should also look for solutions designed to minimize this exposure window by incorporating secure development practices, offering timely hotfixes for critical vulnerabilities, and continuously monitoring device health.

Choosing technology that reduces the likelihood of misconfiguration and improves the speed of remediation can significantly limit the chances of an attacker breaching the perimeter.

17 years

The age of the oldest CVE exploited in the 2025 dataset.

Reducing exposure via insecure firewalls: How Sophos can help

Sophos helps organizations reduce the risk of firewall exploitation by combining secure engineering practices with rapid, automated protection mechanisms that limit attackers' opportunities to strike.

Sophos Firewall is built on Secure by Design principles, including a hardened operating system, real-time hot fixing for critical vulnerabilities, and continuous integrity checks that ensure appliances remain healthy and uncompromised. These hotfixes don't require any downtime, removing the need for security administrators to schedule a specific patching window.

All these capabilities shorten the window between vulnerability disclosure and protection — an interval that attackers repeatedly target across the industry.

Sophos also provides proactive monitoring of deployed devices to spot emerging issues quickly and maintain a strong security posture over time. With Sophos Managed Risk (available as an add-on for Sophos MDR), organizations gain expert-led vulnerability insights and guidance on which exposures to prioritize, helping them stay ahead of the fast-moving threats that routinely target perimeter systems.

Threat actors are getting faster at attacking Active Directory (AD)

Attackers' appetite for compromising Active Directory (AD) has only intensified, with their time-to-target accelerating to a median of three hours and 24 minutes once inside an organization. That's significantly faster than last year's average of half a day (about 12 hours).

Active Directory security is critical because once attackers gain access, they can escalate privileges, move laterally, and ultimately take full control of an organization's identities, systems, and data — often enabling ransomware, data theft, and long-term persistence.

Hardening the Active Directory environment: What organizations should do first

Reducing the risk of an Active Directory compromise requires a defense-in-depth approach that combines zero-trust with additional controls around AD access, strong identity protection, and continuous monitoring.

Organizations should pair strong account controls with ongoing hardening of their AD environment, specifically enforcing:

- Least-privilege access.
- Continuous verification.
- Use of robust authentication with MFA.

Together, these capabilities help limit the damage attackers can do if they gain initial access to the organization.

At the same time, businesses need to ensure that domain controllers, supporting infrastructure, and privileged accounts are continuously updated and kept in a secure configuration.

Just as importantly, organizations should have tools in place to detect early signs of AD-focused activity — such as unusual privilege escalation or lateral movement — so they can intervene before attackers gain full control. Strengthening these foundational areas allows organizations to reduce the likelihood and impact of an AD breach.

Harden your Active Directory (AD) environment by enforcing:

- Least-privilege access.
- Continuous verification.
- Use of robust authentication with MFA.

Preventing Active Directory compromise: How Sophos can help

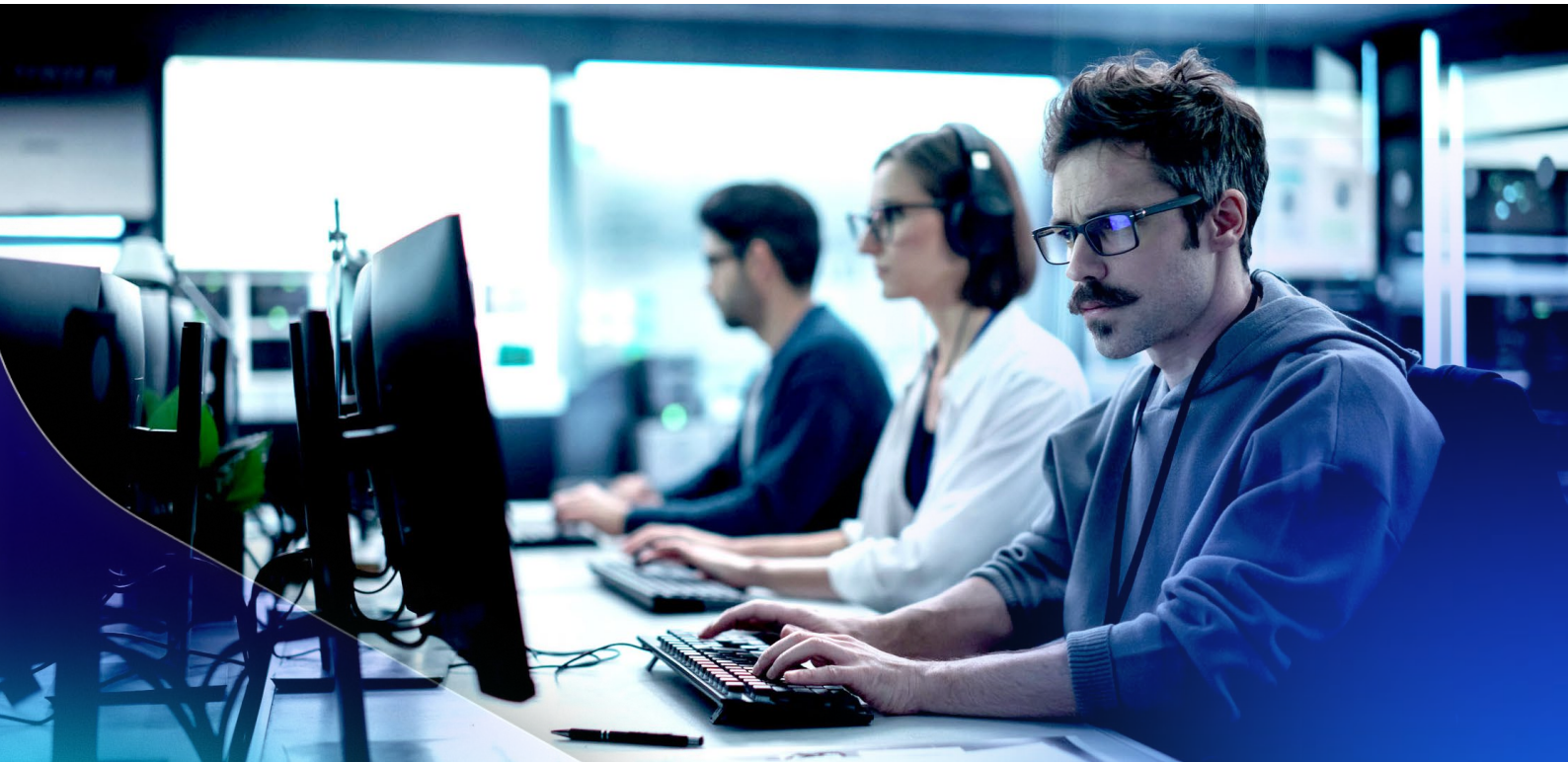
Sophos strengthens Active Directory protection by giving organizations deep visibility into identity activity and the ability to stop AD-focused attacks before they escalate.

Sophos MDR and Sophos XDR, combined with Sophos ITDR, defend against key MITRE ATT&CK Credential Access techniques — including high-impact threats like Golden Ticket attacks, which exploit compromised AD accounts to grant adversaries broad, long-term access.

By correlating endpoint, identity, and network telemetry, Sophos identifies suspicious privilege escalation, lateral movement, and credential misuse early, enabling analysts to intervene before attackers gain domain-level control.

Sophos Firewall also integrates directly with Active Directory to enforce user-based policies and strengthen authentication controls at the network boundary, helping organizations ensure that only authorized users and devices can access critical resources.

Sophos Workspace Protection includes Zero Trust Network Access technology that integrates with AD to enforce MFA and continuous verification to prevent access to AD, apps, and systems with compromised credentials. Together, these capabilities provide a layered, always-on defense that helps organizations detect AD-focused threats quickly and disrupt them before they become business-impacting incidents.



Missing telemetry leaves organizations blind to early warning signs

Missing or incomplete telemetry is increasingly creating headwinds for defenders, making it harder for them to understand how attacks unfolded or spot early signs of compromise.

Incidents with missing logs caused by short data-retention doubled compared to last year, with the problem especially pronounced on firewall appliances that retained logs for only seven days — and, in some cases, just 24 hours.

When critical telemetry disappears quickly, responders lose the historical context needed to distinguish suspicious behavior from routine activity. These blind spots have become even more dangerous given how quickly attackers now move.

Outdated infrastructure compounds the problem: 13% of Windows Server systems identified in the dataset were already end-of-life, with another 27% soon to be, reducing visibility and increasing risk.

Eliminating telemetry blind spots: What organizations should do

To reduce these blind spots, organizations should ensure they are retaining logs and security telemetry long enough to support both real-time detection and retrospective investigation.

This includes extending retention for firewall logs, endpoint data, identity activity, and AD-related events, so analysts have enough historical evidence to identify anomalies and trace attacker actions accurately.

Businesses should also review data-retention defaults on critical systems, many of which store logs for far too little time to be useful during an incident. Strengthening visibility across the environment, especially fast-moving identity and AD activity, is essential for spotting subtle warning signs before they escalate into full-scale compromises.

Additionally, organizations should identify and remove unsupported or end-of-life (EOL) systems from the environment. EOL devices lack security updates and logging improvements, creating blind spots attackers can exploit — and keeping them in production can jeopardize a company's ability to make a cyber insurance claim after a breach.

Addressing telemetry gaps: How Sophos can help

Sophos provides organizations with the advanced visibility and long-term telemetry needed to detect attacker behavior early and reconstruct incidents with confidence.

Sophos Firewall supports up to 30 days of log retention, with options to expand storage for environments that require deeper history. Sophos MDR services include a default 90-day telemetry retention window, which can be extended to a year.

Sophos MDR also integrates seamlessly with hundreds of existing security and IT tools at no extra cost, allowing organizations to centralize telemetry from their current investments and close visibility gaps without replacing solutions. Together, these capabilities help organizations maintain the data needed to identify early signs of compromise, track attacker movement, and respond quickly before issues escalate.

Learn more

For more insights into the current threat landscape, read the full 2026 Sophos Active Adversary report.

Want personalized guidance for your organization? Speak with a Sophos expert or your Sophos partner to understand how MDR, firewall, endpoint, and identity solutions can work together to reduce risk.

SOPHOS

For more insights into the current threat landscape, read the full 2026 Sophos Active Adversary report.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com