# THE HIDDEN RISK IN MODERN FIREWALLS

Learn how you can prevent your firewall from being exploited in an attack

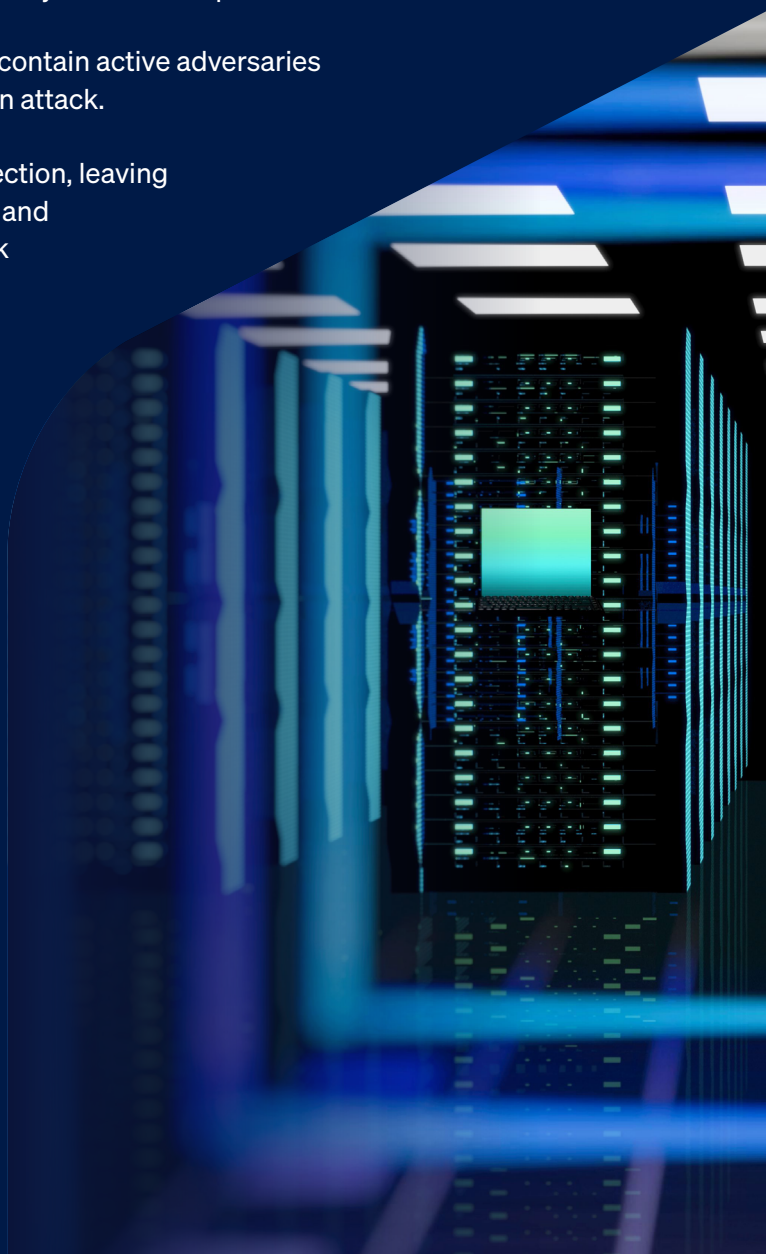
# Executive summary

Network firewalls face an unprecedented level of targeted attacks. There's a news headline nearly every day related to a new firewall vulnerability exploit, revealing a concerning truth: firewalls — the very systems designed to protect networks — present a significant risk and have become prime targets for sophisticated adversaries[1]. These attacks exploit not only vulnerabilities in the firewall software itself but fundamental weaknesses in how organizations approach network security.

This white paper introduces a comprehensive three-pillar framework for modern network security that addresses threats before, during, and after they are deployed:

- **Hardening:** Proactively reduce your attack surface through Secure by Design principles, automated patching, configuration auditing, and zero-trust access controls.
- **Protection:** Block threats before they reach the network with advanced inspection, AI-powered threat detection, and high-performance security without compromise.
- **Detection and Response:** Identify and automatically contain active adversaries operating on the network before they can complete an attack.

Most network security solutions primarily focus on protection, leaving network infrastructure vulnerable and unable to identify and respond to an active attack. This paper provides network security professionals and IT teams with a practical roadmap to implement all three pillars effectively.



# The current threat landscape

## Firewalls are under siege

Network firewalls sit at the boundary between trusted internal networks and the hostile outside world. This privileged position makes them exceptional high-value targets. Headlines have documented a steady drumbeat of attacks on major firewall vendors — some exploiting previously disclosed vulnerabilities that remain unpatched in production environments, others targeting sub-optimal default configurations or design flaws that create exploitable weak spots[2].

Frontier AI has added further fuel to the fire with regard to Agentic AI-driven cyberattacks. The Claude Mythos model from Anthropic discovered over 2,000 new zero-day vulnerabilities in just a few weeks, heralding a step change for adversaries and defenders alike.

While Frontier AI headlines focus on AI discovering vulnerabilities at scale, the more important story is how AI compresses response time — shrinking the window between vulnerability exposure and business impact.  It enables attackers to move faster, at greater scale, and with less friction than before.

The consequences extend far beyond individual organizations. When attackers compromise a firewall, they not only gain direct access to the network but potentially credentials and access to the organization's suppliers and customers, effectively obtaining the keys to the kingdom.

**2,000+**

zero-day vulnerabilities discovered by Mythos in just seven weeks

## The three pillars of network security

Effective network security requires a comprehensive approach that addresses threats across their entire lifecycle: before, during and after they are deployed. This creates three distinct but interconnected defense pillars:

### HARDENING

**REDUCE THE SURFACE AREA OF ATTACK**

Design, engineer, and maintain solutions to minimize risk, reduce exposure, and harden infrastructure against attacks

### PROTECTION

**BLOCK ATTACKS BEFORE THEY GET ON THE NETWORK**

Deploy the best protection possible to identify and block attackers and exploits from getting on the network

### DETECTION AND RESPONSE

**STOP ACTIVE ATTACKS DEAD IN THEIR TRACKS**

Utilize detection and response to automatically identify and isolate an active adversary

## The critical gap

Most network firewalls focus almost exclusively on real-time protection like traffic filtering, threat prevention, and intrusion prevention systems. While these capabilities are essential, concentrating solely on real-time traffic inspection leaves organizations vulnerable.

The daily headlines demonstrates that most firewalls and IT teams are failing to effectively harden their environment, i.e., reducing the surface area of attack. firewalls remain vulnerable, patching fatigue is widespread, end-of-life products persist in privileged positions, and remote access VPN continues to dominate despite its security shortcomings. Meanwhile, detection and response capabilities to stop active attacks before they can have impact are often entirely absent from most firewall deployments.

Addressing this imbalance requires deliberate focus on the neglected pillars, particularly hardening, which forms the foundation of a resilient security posture.

# Hardening network infrastructure — Reducing risk

Hardening involves proactively reducing the attack surface, removing weaknesses before attackers can discover and exploit them.

## Essential hardening strategies

1. **Minimize exposure:** Regularly review systems and infrastructure exposed to the internet, and in turn, reduce the number of potential entry points.

2. **Ensure systems are Secure by Design:** Select products built with security as a primary design principle.

3. **Audit configuration and keep software/firmware up to date:** Maintain security hygiene through continuous monitoring.

4. **Eliminate compromised identity as a vector:** Lock down access and authentication. Deploy multi-factor authentication (MFA) universally and transition from VPN to zero-trust network access (ZTNA).

## Minimize exposure

Regularly review your network infrastructure and assess where each component sits in its life cycle. If any part is approaching end of life, plan to replace it proactively. The cost of refreshing aging technology is far lower than the potential impact of a ransomware attack that exploits unsupported systems.

This is also an opportunity to simplify and consolidate your network infrastructure. If you rely on separate devices for firewall, VPN, ZTNA, SD-WAN, DNS, and web filtering, consider bringing these capabilities together on a single platform. Reducing the number of devices and solutions in your environment can lower complexity, improve efficiency, and strengthen overall resilience.

It is equally important to keep your infrastructure up to date. Firmware and software updates often include critical security patches for vulnerabilities that attackers could exploit. While applying them may take time, it is far less disruptive than dealing with the impact of a ransomware attack.

## Ensure systems are Secure by Design

The cybersecurity industry must embrace a fundamental truth: Businesses need secure products as much as they need security products. When adversaries target the tools built to defend organizations, they need security products that are themselves secure. Organizations should recognize vendors who demonstrate genuine commitment to security and transparency — including transparent disclosure of breaches, which represents the right approach even when it's uncomfortable.

**Businesses need secure products as much as they need security products.**

Key Secure by Design principles include:

- MFA integrated into all systems by default.
- Elimination of default passwords and credentials.
- Implementation of automated security patches that minimize disruption.
- Rapid and transparent vulnerability disclosure processes.
- Regular security audits and penetration testing.
- Secure development lifecycle practices embedded in product engineering.

## Audit configuration and keep systems up to date

Network firewalls are complex, which makes them prone to misconfigurations and risky settings that can create unintended openings for attackers. The challenge is knowing what is misconfigured and where those exposures exist. Sometimes the problem is obvious, but more often the gaps remain hidden until they are exploited. Most firewalls won't provide any insights whatsoever into risky configuration settings. Get one that will.

Patch fatigue is real but it doesn't need to be. Traditional patching processes create significant operational burden. Security vulnerabilities can be discovered at any time, and now with AI, at an alarming rate. The frequency of required updates can overwhelm administrative teams. Most firewalls advertise "automated updates," but these typically still require administrators to schedule downtime, apply firmware, and reboot devices.

Organizations should ask a simple question: Why can't patches be truly automatic? The answer is that most vendors haven't built their software to support real-time, over-the-air security updates. However, modern architectural approaches can enable automated hotfix capabilities that:

- Apply security patches automatically without administrator intervention.
- Require no system downtime or reboots.
- Bridge the gap between major firmware releases.
- Reduce the vulnerability window from months to hours or days.

Misconfiguration represents another common entry point for attackers. Complex firewall rule sets, poorly documented policy changes, and configuration drift over time can inadvertently leave access points open that should be secured.

The challenge is identification: How do administrators know what's misconfigured? Traditional firewalls provide no insights into configuration security. Modern approaches include automated health check capabilities that:

- Continuously audit firewall configuration against established best practices and CIS benchmarks.
- Provide dashboard visibility into passed and failed checks.
- Assign severity levels to each evaluated item.
- Enable drill-down to quickly adjust settings or document intentional exceptions.

These capabilities provide visibility that traditional firewalls lack, ensuring the security posture remains optimal even as configurations evolve over time.

## Eliminating compromised identity as an attack vector

67% of incidents investigated by Sophos in 2025 started with compromised credentials[3], making the elimination of identity-based attacks a central hardening priority. This requires embracing zero trust principles: Trust nothing, verify everything.

Organizations still relying on remote access VPN should treat migration away from it as a high priority. ZTNA provides a modern alternative to VPN that aligns with zero trust principles. Rather than granting broad network access, ZTNA provides granular access to specific applications and resources. If a device becomes compromised, ZTNA can automatically limit or block access until the device is remediated.

Even if an attacker compromises a device connected via ZTNA, they gain access only to the specific applications that user is authorized to access — not the entire network. The security perimeter moves to where it's actually needed: Around critical applications and data.

**67%**

of incidents investigated by Sophos in 2025 started with compromised identity

**ZTNA offers six key advantages over VPN:**

1. **MFA enforced:** MFA is required for all access without exception, eliminating compromised credentials and brute-force attacks as viable attack vectors.

2. **Device health part of Access Policy:** Device compliance and health status are continuously evaluated as part of access decisions.

3. **Works anywhere:** ZTNA functions equally well whether users are on the corporate network or working remotely, providing consistent security regardless of location.

4. **Transparent connectivity:** Modern ZTNA implementations provide transparent, reliable connections without the connection problems that frequently plague VPNs.

5. **Better visibility:** Organizations gain clear visibility into which resources users are accessing, supporting better capacity planning and license management.

6. **Easier administration:** Adding and removing users, deploying new applications, and managing access policies are all simpler with ZTNA than with a traditional VPN.

Hardening strategies must include eliminating remote access VPN and deploying zero trust architecture with universal MFA enforcement.

# Protection – Blocking threats at the gateway

Deploy comprehensive protection to identify and block threats before they reach the network. This includes advanced TLS inspection, AI-powered zero-day threat detection, and intelligent traffic analysis that maintains high performance without compromising security.

## Modern protection requirements

- **High-performance TLS 1.3 inspection:** The majority of web traffic is now encrypted, and attackers increasingly hide malware and command-and-control traffic within encrypted channels. Firewalls must decrypt and inspect TLS traffic intelligently, applying policy-based rules that balance security requirements with privacy considerations and performance impact.

- **Hardware acceleration:** Cryptographic operations and traffic inspection are computationally intensive. Modern firewall architectures should offload trusted applications and crypto operations to hardware acceleration paths, freeing resources for deep inspection of untrusted traffic.

- **AI-powered zero-day threat protection:** Signature-based detection remains valuable but is insufficient against new threats. AI-powered static file analysis combined with runtime dynamic sandboxing can identify and block zero-day threats before they reach the network — threats that traditional signature-based systems would miss entirely.

Protection capabilities AND performance should improve over time rather than degrading. Firewalls built on programmable architectures can receive both protection and performance enhancements through software updates, extending the effective lifecycle of hardware investments. Unlike traditional firewalls that become slower as new security features are added, modern architectures maintain or improve performance through continuous optimization.

# Detection and response – Stopping active attacks

When adversaries successfully penetrate defenses, they rapidly detect their presence and automatically contain the threat. Network detection and response (NDR), combined with cross-product coordination, can identify and isolate compromised systems before attackers achieve their objectives.

## Network detection and response (NDR)

Network detection and response uses AI and behavioral analysis to identify active adversaries already present on the network. Unlike perimeter defenses that analyze inbound traffic, NDR examines internal network traffic patterns for indicators of compromise:

- Unusual lateral movement between systems.
- Command-and-control communications to suspicious external hosts.
- Anomalous data access patterns.
- Privilege escalation attempts.
- Reconnaissance activities scanning internal resources.

NDR has traditionally been an enterprise-grade capability requiring separate products and significant investment. Forward-thinking organizations are now integrating NDR capabilities directly into firewall platforms, making this critical capability accessible to mid-market organizations.

## Automated response

Detection without response merely informs administrators that they've been compromised — often too late to prevent damage. Automated response capabilities enable immediate containment.

When a threat is detected anywhere in the security infrastructure — whether by the firewall, endpoint protection, email security, or an MDR analyst — you need a security solution that coordinates an automated response across all integrated security products. This can stop a compromised device from communicating with other systems, block it from accessing applications and data, and prevent it from moving laterally.

This automated response is especially valuable during off-hours, when 88% of ransomware attacks are deployed[4]. Consider the "Friday night scenario:" An attacker compromises a device late Friday evening when security staff are unavailable. Without automated response, the attacker has the entire weekend to move laterally, escalate privileges, and deploy ransomware. The organization discovers the breach Monday morning when encrypted files and ransom demands appear.

With an automated cross-product response, the initial compromise triggers immediate isolation. The attacker finds themselves trapped in a quarantined segment, unable to advance or move. Security teams return Monday morning to an active alert about a contained threat rather than a full-scale ransomware incident.

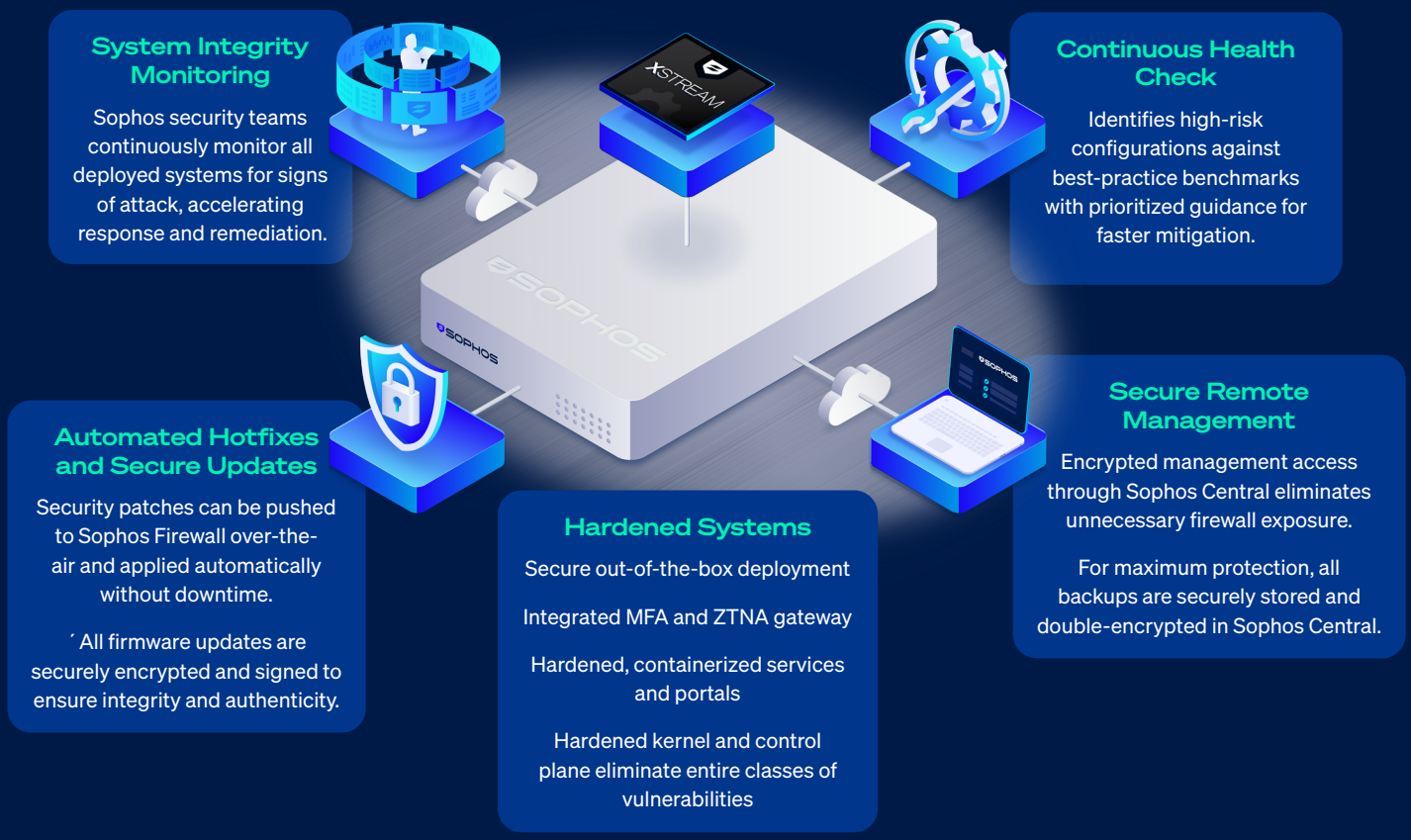
**88%**

of ransomware attacks are deployed during non-business hours

# Sophos Firewall: A complete solution

While the three-pillar framework outlined represents security best practices, implementing it effectively requires choosing infrastructure that supports all three pillars.

Sophos Firewall stands apart as one of the few solutions that has made significant investment across all three areas, delivering many capabilities that buyers won't find elsewhere.




## Secure by Design

Sophos Firewall addresses the hardening pillar through a comprehensive Secure by Design approach that eliminates the burden typically associated with maintaining secure infrastructure.

## Automated hotfix capability: Eliminating patch fatigue

Sophos Firewall's unique automated hotfix capability fundamentally changes the window of exposed vulnerabilities:

- Security patches are pushed over-the-air automatically as soon as Sophos develops and validates them.
- Patches apply without any administrator intervention.
- No downtime or reboots are required.
- Hotfixes bridge the gap between major firmware releases, ensuring continuous protection.

This architectural advantage reduces the vulnerability window from months to hours or days. When Sophos discovers and patches a vulnerability, all Sophos Firewall customers are protected immediately — without waiting for administrators to find time in their schedules or plan maintenance windows.

No other major firewall vendor offers truly automatic, zero-downtime security patching. This capability alone represents a transformational improvement in the hardening pillar.

## Health check: Continuous configuration auditing

**Sophos Firewall's Health Check feature provides unprecedented configuration visibility:**

- Continuously audits dozens of firewall configuration settings against CIS benchmarks and industry best practices.
- Presents passed and failed checks directly on the Control Centre dashboard.
- Assigns severity levels to each evaluated item (critical, high, medium, low).
- Enables drill-down to quickly adjust settings or document intentional exceptions.
- Updates automatically as best practices evolve.

This proactive configuration monitoring ensures security posture remains optimal even as configurations change over time. Administrators receive immediate alerts about potentially risky settings before attackers can discover and exploit them.

## Remote integrity monitoring

Sophos is unique in monitoring our entire install-base of Sophos Firewalls. Thanks to an integrated Sophos Extended Detection and Response (XDR) Linux Sensor we can monitor system integrity including :

- Unauthorized configuration changes.
- Rule exports.
- File tampering.
- Malicious program execution attempts.

This integrated sensor allows Sophos security teams to proactively monitor the entire customer install base for signs of attack — an additional security layer no other firewall vendor currently provides. When threats are detected, Sophos can respond immediately to help customers remediate whilst simultaneously pushing automated hotfixes to protect all other customers.

## Integrated multi-factor authentication and zero trust network access

Sophos Firewall integrates MFA across all administrative access points and includes an integrated ZTNA gateway, making it easy to adopt and deploy ZTNA and upgrade from vulnerable remote-access VPN.

# Powerful protection AND performance

While many vendors offer strong protection capabilities, Sophos Firewall delivers protection differently — ensuring comprehensive security without performance penalties that often force organizations to disable important security features.

## Xstream FastPath Architecture

Sophos Firewall's programmable Xstream Architecture intelligently manages traffic to deliver both maximum security and maximum performance**.** This approach ensures that enabling comprehensive security features — including TLS inspection, sandboxing, and IPS — doesn't degrade performance. Sophos Firewall also integrates AI-powered zero-day threat protection to identify the latest threats.

## Continuous performance and protection improvements

Unlike traditional firewalls that become slower as new security features are added, Sophos Firewall's programmable architecture enables both protection **and** performance enhancements through software updates. Customers receive ongoing improvements to their hardware investments without requiring equipment upgrades — protection and performance that improve over time rather than degrading.

## Unmatched detection and response

Most network firewalls offer virtually no detection and response capabilities. Once an attacker penetrates perimeter defenses, traditional firewalls have no mechanism to identify the intrusion or respond to it. This represents a critical gap that leaves organizations vulnerable to the most sophisticated attacks.

Sophos Firewall is unique in offering automated detection and response capabilities.

## Integrated Network Detection and Response (NDR)

Network detection and response has traditionally been an enterprise-only capability requiring separate products and significant investment. Sophos Firewall includes NDR as a standard feature within the mainstream protection subscription:

This brings enterprise-grade threat detection to organizations of all sizes, ensuring that adversaries who successfully penetrate perimeter defenses can be identified before they achieve their objectives.

## Synchronized Security: Cross-product automated response

Detection without response merely informs administrators that they have been compromised — often too late to prevent damage. Sophos Firewall's Synchronized Security provides automated, coordinated response across the entire security infrastructure.

When any Sophos product detects a threat, whether the firewall, endpoint protection, email security, workspace protection, or an MDR analyst, Synchronized Security automatically:

- Isolates the compromised device from communicating with other systems.
- Blocks access to applications and data.
- Prevents lateral movement across the network.
- Contains the threat until security teams can investigate and remediate.

### The "Friday Night Scenario" illustrates the critical value of automated response:

**Without automated response:** An attacker compromises a device late Friday evening when security staff are unavailable. The attacker has the entire weekend to move laterally, escalate privileges, and deploy ransomware. The organization discovers the breach Monday morning when encrypted files and ransom demands appear.

**With Synchronized Security:** The initial compromise triggers immediate automated isolation. The attacker finds themselves trapped in a quarantined segment, unable to advance. Security teams return Monday morning to an active alert about a contained threat rather than a full-scale ransomware incident.

This automated response capability is particularly valuable for organizations without 24/7 security operations coverage — precisely the mid-market organizations that traditional NDR vendors have historically ignored.

# Conclusion

Is my firewall reducing risk, or introducing it?

Network firewalls face unprecedented attack pressure. Headlines exposing vulnerabilities across multiple major vendors reveal an uncomfortable truth: The systems designed to protect networks have become prime targets for sophisticated adversaries.

The three-pillar framework presented in this white paper — hardening, protection, and detection and response — provides a comprehensive approach to network security that addresses threats before, during, and after they occur. Unfortunately, most firewall vendors concentrate almost exclusively on the Protection pillar, leaving critical gaps in hardening and detection and response capabilities.

Implementing this framework effectively requires selecting infrastructure that invests equally across all three pillars. Organizations should evaluate firewall vendors based on:

- **Secure by Design commitment** with evidence of implementation, not just pledges.
- **Automated patching capabilities** that eliminate downtime and patch fatigue.
- **Configuration auditing** that provides visibility into security posture.
- **Integrated Zero Trust** capabilities including MFA and ZTNA.
- **Network Detection and Response** for identifying active threats.
- **Automated response** capabilities that contain threats without human intervention.

The cost of replacing aging or inadequate infrastructure is dramatically less than recovering from a ransomware attack exploiting known vulnerabilities. The time to act is now before your organization becomes the next headline.

Security is a shared responsibility. Vendors must build secure products. Organizations must deploy them properly, maintain them diligently, and retire them when they reach end-of-life. Both parties fulfilling their responsibilities create a dramatically more secure ecosystem.

The key question you need to ask yourself: **Is my firewall reducing risk, or introducing it?**

The answer depends on whether your infrastructure addresses all three pillars of modern network security — or whether it leaves critical gaps that attackers are all too happy to exploit.

1, 2, 3 ,4 The 2026 Active Adversary Report - Sophos.

# To learn more about Sophos Firewall, visit sophos.com/firewall


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

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

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

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