WHITE PAPER

Cyber Defense Systems Explained

How the new model of cyber defense delivers resilience for the Agentic AI era.

SOPHOS

Executive summary

On paper, security coverage for most organizations looks solid. They've piled up dozens of security products over the years. However, according to Gartner, "On average, organizations have 45 security tools that often work in silos, creating complexity, blind spots and unidentified exposures that adversaries target."[1] So while there is no shortage of tools, there is a shortage of connectivity between them.

Attackers are already exploiting the gaps between the tools, moving across email, identity, endpoint, and network in a matter of minutes. AI is increasing the speed, scale, and scope of cyber threats at an unprecedented rate enabling sophisticated multi-layered attacks to be executed broadly.

Auditors, regulators, and cyber insurers now expect a constellation of evidence that fragmented cyber products struggle to produce. Most organizations still struggle to answer three basic questions: are we protected, where's our biggest risk, and are our investments working?

A new model for cyber defense is taking shape to secure the AI era. The security platform is evolving to the cyber defense system. These are its defining traits:

- **A single real-time view of the environment** fed by every control point from any vendor.
- **Responses coordinate automatically** across control points: email, identity, endpoint, network, and more.
- **Agentic AI responds to the speed and volume of modern attacks** while human experts set the boundaries and stay accountable for outcomes.
- **Continual learning** with every new insight, every threat stopped across the entire user base strengthening defenses everywhere, automatically.
- **The unit of defense shifts from individual products to an architecture that connects them**, including both technology architecture and a network of human expertise.

A cyber defense system is...

A unified security architecture where every control point shares a real-time view, responds as one, learns continuously, and operates at machine speed under human accountability.

Agentic AI era threats are already happening

In late 2025, researchers documented the first known cyber espionage campaign run mainly by AI rather than people. The AI carried out an estimated 80 to 90% of the operation on its own, at a speed and scale no human team could match.

Source: Anthropic, November 2025

1. *Gartner, "Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System," Neil MacDonald, December 12, 2025*

SOPHOS

Your security challenges in the AI era

Years of sensible, threat-by-threat buying decisions have resulted in an environment so complex that the complexity itself became the exposure. Now that stack of uncoordinated products is up against AI-speed attackers and is failing to keep pace. How did we get here?

Shortfalls of the platform approach

Nearly every large cybersecurity vendor claims their platform can do everything you need. They sell point solutions for the threat-by-threat buyer that are aimed at working together as a single platform unit.

The platform philosophy of building a unified system was on the right track, but what they're often selling is a patchwork of hastily built or acquired tools meant to cater to past hype cycles or pump up a stock price. The promises fall short:

- **They promise a "single pane of glass**," but when they're tested in the real world, responders still need to hop between multiple consoles.
- **They promise shared data**, but the platform products can't analyze that data together to detect an attack across identity, cloud, and endpoint.
- **They promise integration**, but each product keeps its own data model and response actions stay siloed across domains.

All of the platform work: configuration, customization, making a workflow that uses all of the parts together, is left to the customer.

As per Gartner®, "Simply adding more tools onto the stack won't provide the intelligent cyber defense fabric that organizations need to mitigate AI-orchestrated attacks like the one Anthropic recently identified."

Neil MacDonald
Gartner | VP, Distinguished Analyst and Gartner Fellow Emeritus

Gartner, Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System, Neil MacDonald, 12 December 2025 GARTNER is a trademark of Gartner, Inc. and/or its affiliates

Cross-domain attacks outsmart fragmented defenses

Fragmented data models and analysis in platform products are great for an attacker. The following attack scenario shows us why:

- **Step 1:** A convincing email slips into an inbox.
- **Step 2:** The recipient enters their password on a fake sign-in page.
- **Step 3:** The attacker logs in from an unfamiliar location.
- **Step 4:** The attacker quietly adds a mailbox rule to watch the traffic.
- **Step 5:** The attacker uses their access to reach a file share and exfiltrate data.

Five steps, each landing on a different domain.

- **Email security** sees the message.
- **The identity solution** sees the odd login.
- **The endpoint protection** notes a small anomaly.
- **The firewall** logs the outbound connection.

Every product registers its own piece, and every product is technically doing its job. Yet **none of them sees the whole picture**, because none of them pass what they know to the others while the attack is still in motion. It just looks like noise, not one attack narrative. The chain only becomes obvious later, when it's too late.

This type of lateral movement is common in modern attacks, and it's also commonly missed. The Sophos State of Ransomware 2026 report showed that 55% of cybercriminals succeeded in encrypting data even when the firewall detected the attack.

Machine-speed attacks, human-speed response

Now take that cross-domain attack and compress the attack timeline from days to minutes. That's what AI has done. A defense that waits for a person to notice an alert in one product and cross-reference that with another product is already too late. The problem isn't slow defenders, it's slow, one-tool-at-a-time responses. Highly manual workflows cannot keep up with an automated attack. By the time an operator has formulated a response, the attacker has already moved on to the next stage.

Expertise is scarce. Noise is not.

Throwing people at the problem is not really an option, because the people are not there. The cybersecurity skills shortage is real, and it is not easing. In ISC2's 2025 workforce study, 95% of security teams reported at least one skills gap, and 59% called it critical or significant, up from 44% the year before.

At the same time, the amount of work keeps growing. A small team can end up responsible for more products, alerts, and dashboards than it could ever reasonably monitor. Most of those alerts amount to noise, but someone must find the signal hiding in them.

AI was supposed to ease that pressure, but in some environments, it has done the opposite.

Adding AI as yet-another-bolted-on-product creates the same issues: more noise and alerts because it wasn't built to natively interact with the rest of the platform's products. Now the cyber team doesn't just have to sift through false positives, it also has to deal with AI hallucinations.

The cybersecurity poverty line is real

The cybersecurity poverty line is the line below which an organization cannot be effectively secured. It isn't defined by an organization's size, budget, or whether they have a CISO or not. In fact, there are many well-funded organizations sitting below the line.

The cybersecurity poverty line is a strategic capability threshold.

Does your organization merely own security technology, or are they able to run it as a system? Large teams can spend heavily on tools nobody has the expertise to operate, while a disciplined 200-person manufacturer can operate a defense system that outperforms much larger organizations. Many organizations unknowingly sit below the poverty line because they assume that the capability to run security as a system was already in place internally.

For these organizations, the biggest gap is not a missing tool. It is the lack of a clear strategy and the orchestration needed to make existing controls work together against AI-accelerated threats. They keep investing, but they still struggle to answer three basic questions:

- Are we protected?
- Where are our biggest risks?
- Are our investments actually working?

Regulators are requiring more proof of resilience

Regulators and cyber insurers don't care if you own the right products. Instead, they are more often forcing organizations to show:

- Coordinated control across domains.
- Retained, auditable evidence.
- Consistent, timely disclosures.
- Tested, real-world resilience.

These new regulations are heavy burdens for organizations that still have a security estate spread across dozens of products, each with its own data model and retention period. Producing the evidence an auditor or insurer asks for can become a full-time job: exporting logs from separate systems, stitching them together by hand, and hoping the result still tells a coherent story. A control that cannot be demonstrated is, for compliance purposes, a control that does not count.

The common thread

None of these problems are solved by adding another product or button to a console. They share a single root cause: Defenses that operate in isolation fail when the threats against them operate in concert. Closing that gap requires something different, not one more new product.

Cyber defense systems: A modern approach to security

If the problem is fragmentation, the answer is not consolidation for its own sake. Buying one product that tries to do everything and fails is no better than having multiple good products that don't coordinate well.

Instead, organizations should be searching for a cyber defense system: A set of security products and services that are designed to function as one unified system. Every control point should contribute to a shared understanding of the environment and respond as part of a coordinated whole. The system should be well-connected, synchronized, automated, intelligent, and adaptive. Five principles describe what that looks like in practice.

1 Synchronized, autonomous control points

A cyber defense system starts with control points. These are the technologies and services where security telemetry is observed, and security rules are enforced. Control points can both see and act on what is happening to them. Endpoint, firewall, email, identity, productivity tools, and more are all control points.

2 One shared view, in real time

A defense system differs from a platform by having one shared understanding of what is happening across the environment. Each control point feeds what it sees into a common data layer in real time with no delayed copying or reconciliation. That gives the entire system a single, shared view of events in real time. No blind spots, no gaps in the response.

3 Coordinated response across every layer

A coordinated response starts with a detection in one layer that can automatically trigger an action in the others without an analyst having to relay the signal from one console to the next.

A suspicious sign-in can prompt extra scrutiny at both the endpoint and email layers. A malicious file on a device can cause the firewall or network to block the connection it is trying to make. The system responds as one because it already sees an attack as one. And when an attack moves fast, that kind of coordination matters.

SOPHOS

4 Agentic AI with human accountability

Speed is the deciding factor. Attacks that unfold in minutes can't be stopped by defenses that wait for a human to notice. That's why AI needs to sit at the center of the system, not at the edges.

In a cyber defense system, AI is the architecture; it's built in not bolted on. AI correlates signals across every layer, spots the shape of an attack as it emerges, and drives detection, investigation, and response at machine speed. This AI-native system is distinct from AI that's bolted onto a single product and can only see that product's data.

AI built into a defense system can reason across everything the system sees. However, machine speed response without human accountability is a liability, not an advantage. Cyber defense systems don't remove people from security. Instead, they direct them to where human judgment matters most: setting the boundaries, handling novel or high-risk decisions, reviewing incidents, and staying accountable for outcomes.

AI handles the speed and the volume. The routine triage and the fast, high-confidence actions.

Human experts define the trust boundary: what the AI can decide on its own, and when it needs help. They step in when the context is unfamiliar or the stakes are high.

As the system earns trust, that boundary can expand. But accountability always stays with human experts.

AI handles the speed and the volume.

Human experts define the trust boundary.

5 Compounding intelligence

Defense systems learn. A threat encountered anywhere becomes knowledge everywhere. The endpoint sees what the firewall saw. The email gateway tells the identity layer what it caught. Every tool learns alongside the others and builds on what came before. This all happens without any manual configuration. The defense system's intelligence compounds with more users and more patterns observed, allowing the system to evolve as quickly as AI-driven attacks will.

SOPHOS

From platforms to cyber defense systems

Taken together, these five principles define a category of their own. Defense systems are the evolution of the platform, optimized for the AI era. A platform is usually just a set of products behind a shared console, tied together by a login and a licensing agreement rather than by design.

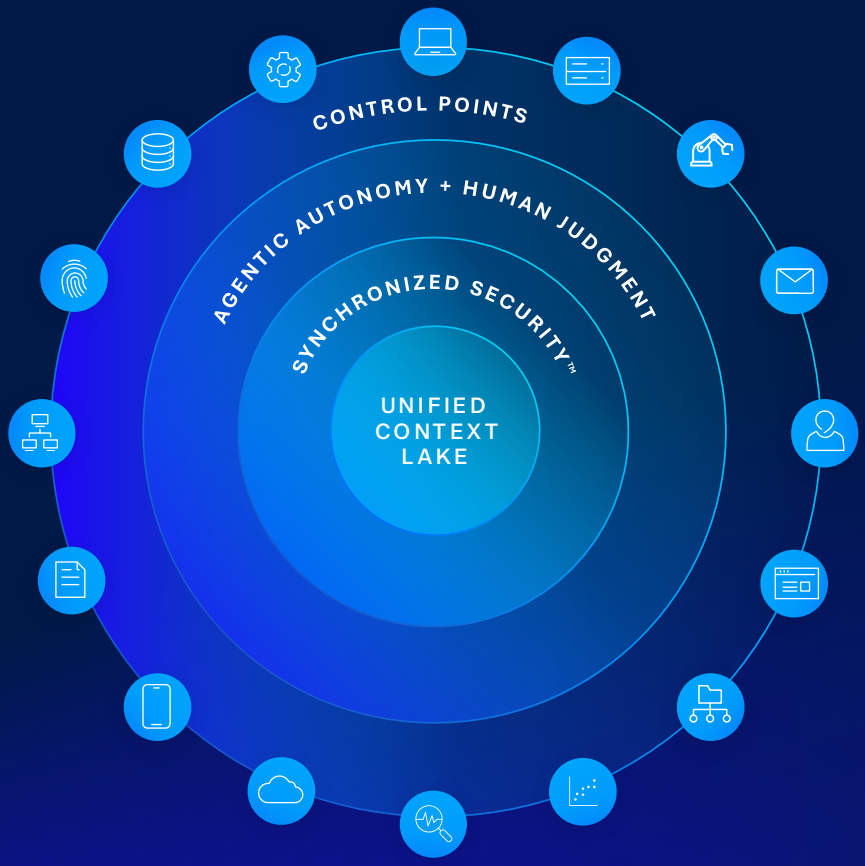
A cyber defense system is different. Its data is shared, AI is built in, response is coordinated, and human experts stay in charge. It's an architecture designed to run as one product rather than a collection of products arranged to look like one.

Sophos Fusion: The Sophos cyber defense system

Sophos Fusion is the industry's most complete cyber defense system, engineered for a world where threats move at AI speed. Enabled by the Sophos AI-Native Cybersecurity Defense System architecture and 500+ Sophos and third-party integrations, it sees everything, connects everything, and enables your defenses to respond as one.

Sophos Fusion turns the cyber defense system principles into practice: a single, open architecture where every control point operates as one, powered by agentic AI, with human judgment to protect organizations from AI-enabled threats that move faster than defenders can respond.

The more of the Sophos portfolio a customer activates, the more value Sophos Fusion delivers.



Synchronized, autonomous control points

Each control point you already own provides continual real-time threat intelligence and carries out response actions. The architecture is fully open: it integrates natively with Sophos products and with more than 500 third-party technologies, so the investments you have already made become part of one coordinated defense rather than sitting in isolation.

It also includes the deepest Microsoft security integration on the market, across all Microsoft plans rather than only the most expensive, so even organizations on entry-level Microsoft licensing can strengthen their defenses with that telemetry.

One shared view, in real time

All telemetry from every control point flows in real time into the unified context lake, a single shared data layer. There's no aggregation delay and no separate data store at each control point. Think of it as a shared nervous system: every control point senses what every other control point senses, the moment it happens. That shared understanding is what makes coordination possible.

Coordinated response across every layer: Synchronized Security™

Synchronized Security™ is the connective tissue that turns shared understanding into coordinated action across Sophos Fusion. It enables Sophos and non-Sophos control points to automatically respond to threats together.

A detection at the endpoint can trigger a response at the firewall. A compromised identity can lock down access across the environment. A suspicious email can raise scrutiny at every other layer. The more Sophos solutions you deploy, the more Synchronized Security™ benefits you unlock.

Think of a modern building's fire suppression system: a sensor in one room doesn't just sound an alarm; it closes fire doors, reroutes airflow, and starts sprinklers on nearby floors. Sophos Fusion works the same way, as one coordinated whole. It can do this because the data is already unified. No extra configuration or action is required.

Agentic AI with human accountability

Sophos Fusion detects, investigates, and responds at machine speed but never without human oversight. Every action stays within boundaries defined and continuously tuned by human experts. That's what makes it agentic AI: AI that can reason through new situations, not just follow fixed playbooks.

A useful analogy is autopilot in aviation. The system can fly the plane, but the pilot sets the parameters, monitors the instruments, and takes over when the situation is unfamiliar or high-risk.

In Sophos Fusion, this agentic capability is delivered by Fusion AI, Sophos' native agentic AI. Sophos has more than 50 AI models built into its defenses, all continuously refined with real-time threat intelligence. For example, Sophos Email uses 20+ models, including proprietary natural language processing (NLP) models that analyze the text, tone, context, and structure of emails, to identify phishing and business email compromise attacks.

Sophos MDR, a 24/7 service where Sophos experts monitor and respond on your behalf, operates the world's largest Agentic SOC (security operations center) using the Sophos Cyber Defense System. It is the industry's largest managed detection and response operation, protecting more than 40,000 organizations. It resolves 52% of incidents end-to-end with AI, with an average of 89 seconds from alert to automated response, while human experts remain accountable for the decisions that carry organizational risk.

Compounding intelligence

The Sophos Cyber Defense System learns from every attack, not just attacks on your organization. Every threat encountered across the 625,000+ organizations Sophos protects feeds back into Sophos Fusion, along with every edge case an analyst resolves and every new environment that comes online. Sophos X-Ops enhances that with its own deep expertise and real-time threat intelligence that is then pushed out to every Sophos product and every customer automatically, improving their defenses.

It works a lot like a biological immune system. Each threat the body encounters becomes part of permanent memory, cataloged, understood, and ready the next time it appears. Sophos Fusion works the same way. A new customer is protected on day one against threats it has never seen before, because the system already has.

That is why the 625,000+ figure matters. It reflects the breadth of experience that lets protection and intelligence compound. The more the system sees, the better it gets at defending everyone inside it.

Sophos Fusion: Where you experience a cyber defense system

The Sophos AI-Native Cybersecurity Defense System is the architecture. Sophos Fusion is where you experience it. One place to manage your Sophos control points, see the full picture from every connected control point, and take action.

That means there is nothing extra to buy or switch on, and no need to change how you work today. Every Sophos control point is already part of Sophos Fusion, so the moment you deploy one, you are inside the architecture. And as you add more Sophos or third-party control points, more of the system comes to life, feeding a richer shared view and creating more value across everything you already run.

The attack viewed from Sophos Fusion

Let's return to the multi-stage attack from earlier. A poisoned email, a stolen credential, an unusual sign-in, a mailbox forwarding rule, and lateral movement toward sensitive data. In Sophos Fusion, telemetry from Sophos Email and the customer's Microsoft environment flows together into the unified context lake. Sophos XDR then correlates those signals as they arrive, recognizing the sequence as one connected attack rather than five unrelated alerts.

From there, Synchronized Security™ coordinates the response across email, identity, endpoint, and network. Agentic AI acts at machine speed, while Sophos MDR analysts take direct action and make the high-risk calls. The attack that might slip past isolated products is caught by a system that sees the whole picture.

What Sophos Fusion means for your organization

Sophos Fusion delivers cyber resilience for the Agentic AI era, across four areas that matter to the business.

- **Protection from AI-accelerated threats that move faster than defenders can respond.** Multi-stage attacks are caught and contained early, even as AI accelerates their speed and scale, because every control point shares context and responds together rather than each acting alone.

- **Increased impact from your people and investments.** Agentic AI absorbs the noisy, routine work of triage and response, so your existing team and existing control points achieve more without added headcount or complexity. Every connected tool, Sophos or not, contributes to the outcome.

- **An elevated compliance and cyber insurance posture.** Round-the-clock coverage, retained cross-layer context, and coordinated response give you the evidence auditors, regulators, and insurers expect, from one searchable record instead of logs exported by hand. The same architecture that improves protection improves your ability to demonstrate it.

- **A cybersecurity strategy aligned to your business.** By connecting and coordinating your defenses, Sophos Fusion lets you move from managing tactical dashboards to operational confidence, with clear visibility into where your gaps and biggest risks sit and whether your investments are working. It is how organizations of any size, with or without a CISO, can finally put the strategy they have always wanted in place.

All Sophos customers are already part of Sophos Fusion, the Sophos defense system. It's an automatic, seamless upgrade, defending customers against AI-era threats.

Getting started with Sophos Fusion

Every Sophos solution is part of Sophos Fusion, making each one an entry point rather than a standalone tool. Getting started is as simple as deploying a Sophos product or service – Sophos MDR, Sophos XDR, Sophos Endpoint, Sophos Firewall, and Sophos Email are common starting points. The more solutions you add, the more of the architecture you unlock.

There is no need to change the other third-party control points that you rely on today. Integrate them into Sophos Fusion to provide continual real-time threat intelligence and execute response actions. Start where your risk is greatest, then expand at your own pace.

Ready to begin? Talk to a Sophos expert to map the right starting point for your environment, or learn more at sophos.com/fusion.

Conclusion

For years, the default response to each new threat was to add another product, and that habit created the fragmentation that attackers now exploit. AI has only made the problem worse by widening the gap between how fast an attack moves and how quickly a console-by-console response can keep up. More products won't close that gap. A cyber defense system will.

A cyber defense system shifts the unit of defense from individual products to the architecture that connects them:

- One shared view
- Coordinated response across every layer
- AI built in to act at machine speed
- Human experts keeping judgment and accountability where they belong

Securing the AI era means making everything you already own work together as one. Sophos Fusion, the Sophos AI-Native Cybersecurity Defense System, is how you put that model to work without replacing what you already own today.

SOPHOS

Ready to discuss your cyber defense needs for the AI era?

Speak to a Sophos expert today.

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