



WHITE PAPER

Synchronized Security™ Explainer



Synchronized Security

Synchronized Security™ is at the heart of Sophos Fusion, Sophos' industry-leading AI-native cybersecurity defense system. It's the connective tissue that turns threat insights across every connected control point – Sophos and third-party – into a coordinated response to threats.

In their Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System¹, Gartner identified that “Organizations need an intelligent overlay that connects the different elements of their cybersecurity toolset to proactively and reactively respond to risks and threats at machine speeds.” Synchronized Security is a key element of how this is delivered in Sophos Fusion.

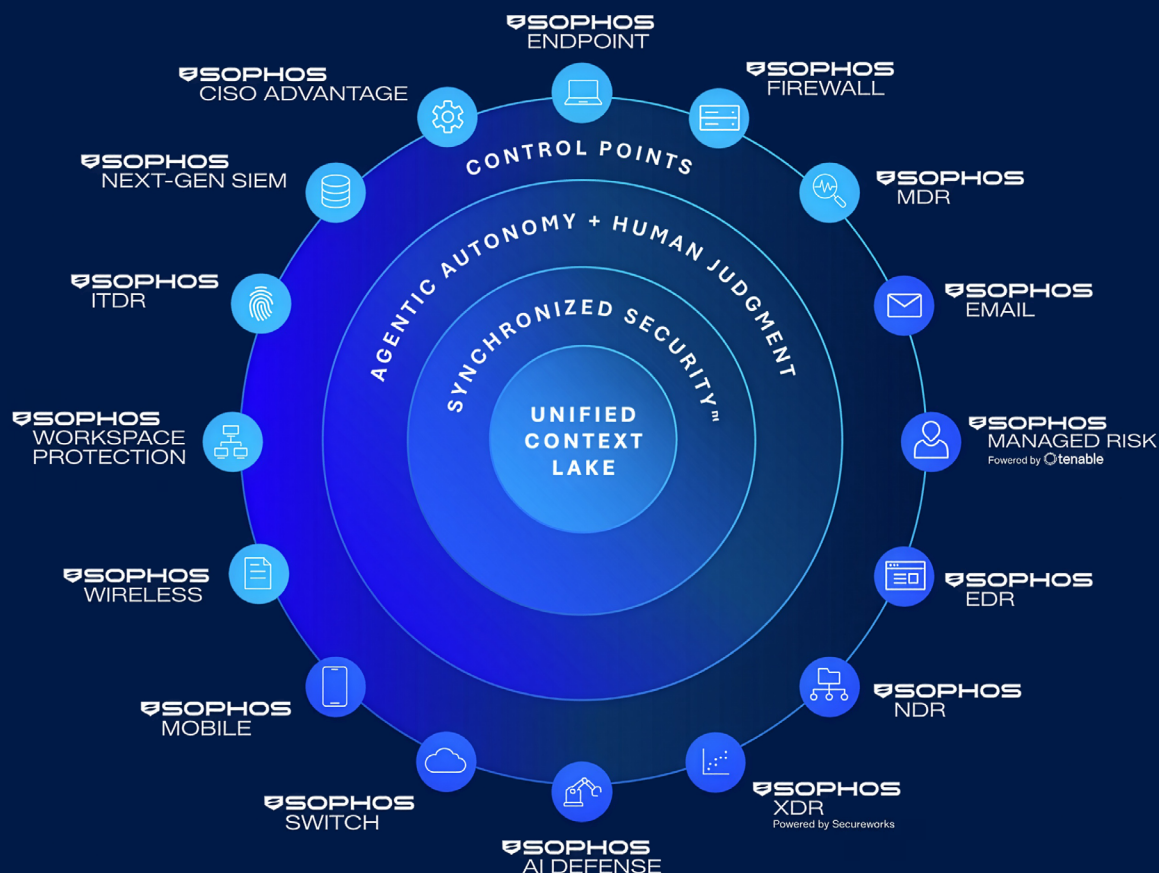
This guide explains how Synchronized Security works, the benefits it delivers, and how organizations can take advantage of it.

¹ 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.



Quick summary

- ▶ Synchronized Security is a core element of the Sophos Fusion defense system and is included automatically – no need to buy an additional module or license extra components.
- ▶ It enables a coordinated response to threats across connected control points. Getting started requires two or more control points working together inside Sophos Fusion.
- ▶ Synchronized Security works with both Sophos and non-Sophos control points. Response actions in individual customer environments depend on which controls are connected to Sophos Fusion, and the level of autonomous action the customer grants over each control point.
- ▶ Sophos XDR is at the heart of Synchronized Security, correlating signals from across the customer environment into a single attack chain and allowing for automated or human-led response actions across the defense system.
- ▶ Sophos solutions can also work together without Sophos XDR, adding additional Synchronized Security depth.
- ▶ Synchronized Security builds on the battle-proven foundational capabilities Sophos launched in 2015.



Why coordinated response matters

Security tools have historically been built to do one job well. An endpoint agent secures the device it runs on (e.g., desktop, laptop or server). A firewall monitors what crosses the network. An email service controls what lands in the inbox. Each is good at its job, and blind to everything outside it.

Attackers understood this a long time ago. A modern intrusion is not a single event in a single place. It crosses identity, email, endpoint, and network by design, because the space between them is exactly where the gaps are, and attackers exploit them.

The consequence is familiar to anyone who has run a security team. Individual solutions see only their own domain, identifying seemingly disparate anomalies. Each one looks survivable on its own. Nobody has the time or the context to recognize the anomalies as the same attack until the damage is done.

AI has widened the gaps. Attacks now run at machine speed and at volumes the industry has not seen before. However, most defenses still run at human speed, with an analyst moving between consoles and correlating by hand.

Adding another product to the estate does not close that gap. Instead, organizations should look at connecting the products they have already invested in. This is precisely what Synchronized Security does inside Sophos Fusion.



What Synchronized Security delivers

Coordination transforms the speed, scale and scope of threat response, changing the outcome of an attack. When endpoints, network, and other controls act together, containment happens in seconds — not after someone notices and reacts. A compromised endpoint is isolated immediately before an adversary can move laterally, reach sensitive data, or establish persistence. Plus, since the response is automated, it works overnight and at weekends when there is often reduced human coverage.

Coordination also closes the gaps attackers rely on. Third-party control points that previously only raised alerts start actively contributing to the defense instead. Existing security investments stop sitting in isolation and become a part of the coordinated response.

The operational impact on a security team is immediate. Routine containment happens without analyst intervention. When human investigation is required, the analyst starts with cross-layer context already assembled, instead of piecing it together by hand across several consoles.

The same coordination makes protection easier to prove. Cross-layer context is retained, and a coordinated response leaves a consistent record of what was found and what was done about it. That is the control narrative auditors, regulators, and insurers expect. The architecture that improves protection also improves a customer's ability to demonstrate it.

The defense also strengthens as it grows. Every new control point connected to Sophos Fusion sends additional signal into the unified context lake and opens another place to respond from – without a matching increase in operational effort. More coverage does not mean more work.

For managed service providers, the same coordination runs consistently across every customer environment, including those that mix Sophos and third-party control points. Automated containment reduces manual triage and remediation overhead.

How it works

Synchronized Security starts with telemetry. Every connected control point reports what it sees into the unified context lake as it happens. Endpoint, firewall, email, cloud, network, identity, and productivity tools all feed the same lake. Third-party control points feed it alongside the Sophos ones. Nothing waits in a queue to be aggregated, and there is no secondary data store to reconcile later.

Sophos XDR interprets the shared picture and does the work an analyst would otherwise do by hand. It ties related events together and resolves them into a single attack chain rather than a run of separate alerts. Correlation is the part that matters, because one control point only ever sees a fragment.

Response actions then travel back out to the control points. Sophos XDR supplies the machinery: SOAR automation, playbooks, case management, and a broad set of response actions. Most run automatically without human intervention. Where judgment is needed, an in-house analyst can trigger the same action manually using Sophos XDR, as can a Sophos MDR analyst.

Two-way integration with third-party control points means Sophos Fusion can pull and push data through the integration. For example:

- ▶ It can pull in telemetry from a non-Sophos firewall and push back an IP address for the firewall to block.
- ▶ The ServiceNow integration opens, updates, and closes cases.
- ▶ Active Threat Response in Sophos Firewall uses API-triggered responses to third-party threat feeds to shut a compromised or unauthorized device out of the network.

Uniquely, Sophos control points also act on one another directly without any involvement from Sophos XDR. The built-in Security Heartbeat carries a device's health status from Sophos Endpoint to the other Sophos control points – a Green status is healthy, Yellow status is potentially compromised, and Red status is compromised.

The other Sophos control points are built to act on the device health status. Once the control points are connected to the same Sophos Fusion account, the core responses do not need additional setup. Capabilities that leverage the health state, such as a firewall rule that gates internet access or a Sophos Workspace Protection policy, are configured by the customer before they take effect.

Collect



Correlate



Respond

Sophos Fusion gathers telemetry, Sophos XDR builds context, and automated response actions push enforcement back to the control points.

One capability, multiple dimensions of coordination

Synchronized Security was initially released in 2015, a world-first at the time, and has expanded in scope in the more than a decade since. The depth of coordination between control points differs from one customer environment to the next depending on the exact mix of control points they have in place.

Coordination runs deepest between Sophos control points as they are engineered to work together from the ground-up. Third-party control points join through the integrations in Sophos Fusion, and the response actions vary based on what the other vendor exposes.

Coordination depth also depends on the level of control a customer hands Sophos Fusion over each control point. That choice belongs to the customer, and the fact that it exists is the point rather than a shortcoming. Ask most organizations whether an infected endpoint should be pulled off the network without anyone approving it, and the answer is yes. Ask whether a system should rewrite a firewall policy to reduce exposure on its own, and the answer varies.

Firewalls are the example that makes the tension obvious. In the end, blocking a compromised endpoint is a firewall rule change. Plenty of organizations are wary of automated changes to firewall configuration, and their change control processes exist for good reason.

Customers can write their own automations and playbooks and run them beside the ones Sophos provides. A customer running Sophos Endpoint decides for themselves what a compromised device means for their Fortinet firewall, covering how that firewall behaves, and how it is configured. Once written, those automations run inside Sophos Fusion like any other coordinated response.



Synchronized Security in action

Coordination is easier to recognize with examples. The use cases below show the same capability operating at different depths rather than a list of separate features.

Coordination between Sophos products

When Sophos Endpoint finds a threat on an endpoint or server, it sets that device's Security Heartbeat health status to Red. The new status is automatically shared with the other connected Sophos control points via the Security Heartbeat. Several responses follow automatically:

- ▶ Sophos Endpoint attempts to remediate the threat, which can include blocking and rolling back encryption by ransomware, or deploying a higher level of control to hold back an active adversary.
- ▶ Sophos Firewall limits the device's internet access, cutting any connection to a command-and-control server, and stops it from reaching healthy devices.
- ▶ Sophos Wireless, Sophos Switches, and Sophos Workspace Protection restrict the device's access to network resources, limiting the impact of the compromise further.
- ▶ Healthy endpoints are advised of the Red health status and will reject network connection requests from the affected device.

The same mechanism catches problems that never announce themselves as an infection. An endpoint or server sending large volumes of spam or phishing emails is set to a Red health status. Sophos Endpoint then looks for previously unidentified malicious users or applications, and Sophos Email blocks the messages before they reach an inbox.

An endpoint or server can stay in the Red health status for seconds or even days, depending on the remediation required. Once clean, the device's health status returns to Green and access is restored automatically across the system.

The value shows most clearly when nobody is watching. A server compromised late on a Friday night is cut off in seconds, instead of giving an adversary the whole weekend to move through the network.

SCENARIO

Sophos Endpoint finds a threat and sets the Security Heartbeat health status to Red. The new status is shared automatically with every connected Sophos control point. When the endpoint threat is removed, the same cycle is followed to restore access.

SIGNAL

COORDINATED RESPONSE



Sophos Endpoint and a third-party firewall

Coordination is not limited to Sophos control points. A customer running Sophos Endpoint alongside a Fortinet firewall can have a compromised device trigger a response at the Fortinet firewall. The customer defines what that response is and how far it goes, which keeps the automation inside their own change control boundaries. The automation and playbook (SOAR) capabilities from Sophos XDR make this possible, working with the Fortinet integration in Sophos Fusion.

Microsoft technology and telemetry

Almost every organization runs Microsoft technology, and identity is the leading vector for ransomware attacks. A stolen session token or a compromised account gives an adversary a legitimate way in, and no amount of endpoint containment helps if the account itself remains compromised. Response must reach into the Microsoft environment to complete the remediation.

Locking the account is the clearest example: Sophos Fusion can lock a compromised Microsoft account to shut the adversary out and then unlock it once the account is safe to use again. The account is treated as a control point like any other – something the system can see and act on, not something an administrator handles separately after the fact.

The integration is two-way. Telemetry from a range of Microsoft sources feeds the same unified context lake as Sophos control points, Microsoft Entra ID and Microsoft Graph Security among them. So, a Microsoft signal can drive a response at a Sophos control point just as readily as the reverse. A suspicious sign-in surfaced by Microsoft can isolate a Sophos-protected endpoint, without either side being configured to watch the other.



The networking edge, wired and wireless

Switches and access points are rarely thought of as part of a defense. They are infrastructure, bought to move traffic and keep people connected, and most organizations treat them accordingly. Yet they sit at the point where every device meets the network, which makes them one of the earliest places a compromised or unauthorized device can be stopped.

In Sophos Fusion, Sophos Switches and Sophos Wireless access points work as control points: they contribute what they see about connected devices, and they can act on what the wider system finds. Administrators can identify new or unauthorized devices, clients on an unexpected SSID, or a device connected to the wrong switch port.

Active Threat Response, a Synchronized Security capability in Sophos Firewall, turns that context into action. Using the telemetry in the unified context lake, a device can be blocked at the wired or wireless access layer before it moves further into the network. Customers choose whether to enable Active Threat Response, keeping the decision to allow automated blocking at the access layer in their hands.

Third-party networking devices follow the same pattern as the third-party firewall example above.



Sophos AI Defense uncovers shadow AI usage

Coordination is not only about malware and intrusions. Sophos AI Defense is a control point in Sophos Fusion that governs how AI is used across an organization. It interprets AI activity telemetry from a variety of Sophos products in the unified context lake, alongside every other signal, visible to Sophos EDR, Sophos XDR, and Sophos MDR. Sophos AI Defense is designed to surface the granular details of AI usage, and once that information is in the unified context lake, it runs through the same Synchronized Security functionality as everything else.

Shadow AI shows why this is needed. An employee starts using an AI tool nobody knows about, pasting source code and customer records into it. The browser sees the pasted data, the endpoint sees the application, and the firewall sees traffic to an AI service from a device that may not be managed at all. No control point sees the whole picture, so the tool goes undiscovered.

Sophos AI Defense assembles those signals and assesses them in context, giving a security analyst the evidence they need to understand what happened. It combines telemetry such as identity, permissions, behavior, data exposure, and the location of both the user and AI model, which separates acceptable use from activity that is unmanaged, overprivileged, or against policy.

Enforcement then runs at the control points:

- ▶ Sophos Workspace Protection controls the browser, including copy and paste, uploads, downloads, and screenshots.
- ▶ Sophos Endpoint restricts access to AI applications and websites across user groups and device types.
- ▶ Sophos Firewall controls AI service traffic at the network layer, including unmanaged devices and non-browser activity.
- ▶ Sophos products can inspect prompts, uploads, and AI interactions in real time, keeping source code, customer records, and financial data inside the business.
- ▶ An administrator can block a specific AI tool across the estate from Sophos Fusion.

Policy is not the end of it. A violation or unauthorized agent behavior surfaces in the same Sophos EDR, Sophos XDR, and Sophos MDR workflows as any other detection, handled with the automation and playbooks already used for identity, endpoint, and network threats. How far the coordination reaches depends on which control points are connected to Sophos Fusion.

82%

of organizations have discovered unknown AI tools or workflows in their environment.²

² Cloud Security Alliance, The Shadow AI Agent Problem in Enterprise Environments, 2025

Coordination beyond threat response

Between Sophos control points, coordination goes further than sharing a threat verdict. One control point can ask another a direct question and act on the answer. An endpoint or server protected by Sophos Endpoint already knows most of what a Sophos Firewall cannot tell you about network traffic. Three exchanges show what that makes possible: identifying the application behind traffic on a port, identifying the user behind a session, and deciding whether a device is fit to be given access at all.

Synchronized Application Control

Take an unclassified connection on an unusual port. A firewall inspecting it in isolation sees a stream of packets and little else. Sophos Firewall can ask Sophos Endpoint which application is sending and receiving on that port and get an answer about which application is responsible. Customers can then permit or block the application on that basis. Over time, this also builds an accurate picture of what is running on the network, which is usually more varied than anyone expects.

Identities, not IP addresses

User identity works the same way. Sophos Endpoint passes authenticated user information to Sophos Firewall, so policy can be written around people and their identity rather than around user or IP addresses that change. It removes a mapping exercise that administrators would otherwise maintain by hand, and that tends to drift out of date.

Only healthy devices connect

Access decisions benefit too; a traditional VPN has no way of knowing whether a device is health or not, and admits the endpoint based on its credentials alone. However, Sophos Workspace Protection checks the device's health state with Sophos Endpoint before granting anything, so a compromised endpoint never reaches network applications or data.

Exchanges like these are not a fixed set. Each one exists because Sophos built it, and Sophos has kept expanding the capabilities over time. What is shared between Sophos control points today is considerably richer than what was shared between them a decade ago.

None of this begins as threat response, but it rarely stays separate from it. An application nobody can account for, or a user signed in where they have no business being, is ordinary operational detail right up until the moment it is not. Visibility that makes a network easier to run makes an emerging threat easier to spot.

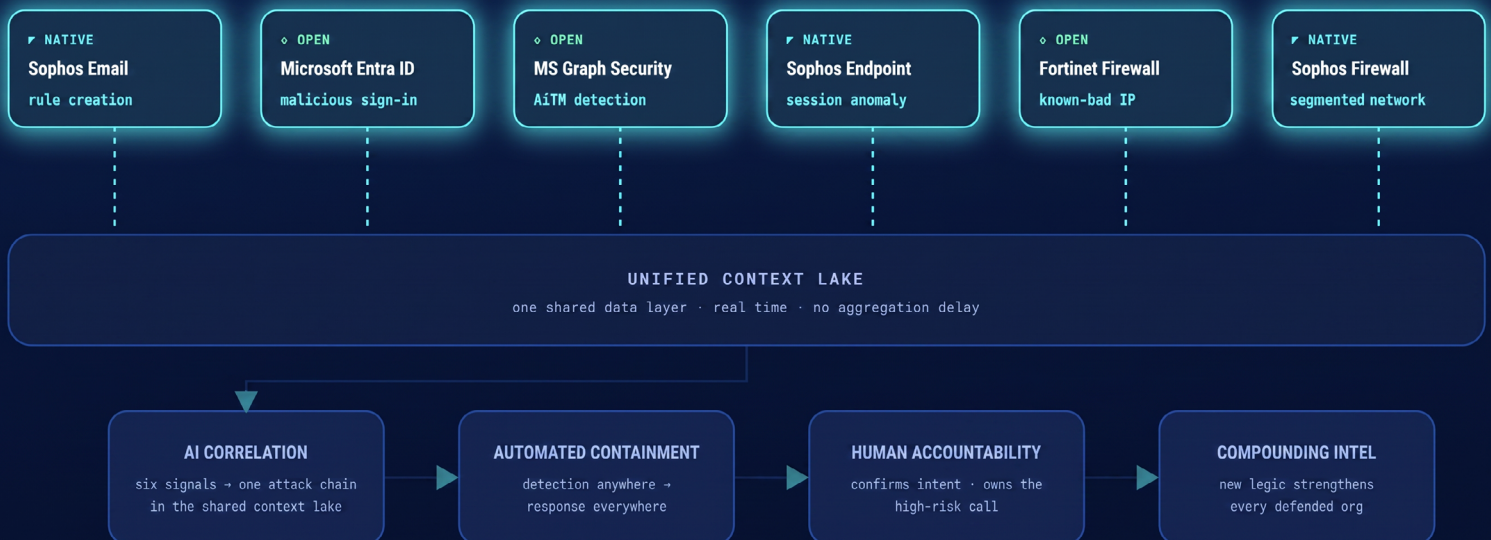
A coordinated response across a hybrid environment

This real-world example from Sophos MDR shows Synchronized Security in action. The impacted organization was a Sophos MDR customer running Sophos Endpoint and Sophos Email, alongside Microsoft Entra ID, Microsoft Graph Security, and a Fortinet firewall. They also ran a Sophos Firewall on a separate network. Every one of those control points fed the same unified context lake.

- ▶ The attacker opened with an AI-assisted lure, using a phishing page hosted on a legitimate site. The user clicked and entered their password.
- ▶ The kit stole the live session token rather than the credential. In doing so, the attacker managed to bypass multi-factor authentication, rendering a password reset ineffective.
- ▶ The adversary signed in from known attacker infrastructure and created a quiet inbox rule hiding any emails from one specific supplier, which is the setup for wire fraud.
- ▶ Four control points registered something suspicious – Sophos Endpoint, two Microsoft solutions, and the Fortinet firewall. No single signal was loud enough to trigger a response.
- ▶ A purpose-built Sophos detection fired and the individual signals resolved into one attack chain.
- ▶ The sign-in was blocked, sessions were revoked, and the endpoint was successfully isolated. Malicious IP addresses were blocked at the Sophos Firewall, using telemetry surfaced by the Fortinet firewall.

A human then closed the case. An analyst confirmed that the inbox rule named a specific supplier, which is what identified it as preparation for wire fraud.

CONTROL POINTS · NATIVE + OPEN



SOPHOS AGENTIC SOC

How customers enable Synchronized Security

Synchronized Security is not a product, a SKU, or an add-on, and there is nothing extra to license. Customers gain it automatically when two or more control points work together inside Sophos Fusion, regardless of whether the control points are Sophos or non-Sophos.

Sophos Endpoint and Sophos Firewall managed through the same Sophos Fusion account is a common starting point. Coordination between them is active as soon as both are connected to that account, with nothing additional to configure. Use cases that build on the health state, such as using the health state as part of firewall rules or Sophos Workspace Protection policies, are set up by the customer.

Coordination with third-party control points starts by integrating the control point in Sophos Fusion, which supports native Sophos and 500+ third-party integrations. However, the level of automated responses available varies from one control point to the next. Active Threat Response in Sophos control points is one example, enabled by the customer, not by default.

Sophos provides automations and playbooks that execute automatically via Synchronized Security, covering a wide range of use cases. Customers can add their own where a default automation does not suit their environment, as described above.

Sophos Endpoint coordinating with Sophos Firewall

To confirm Sophos Endpoint is coordinating with a firewall, open the Computer summary in Sophos Fusion. It shows the serial number of the Sophos Firewall receiving that endpoint's Security Heartbeat.

Agent Summary	
Last agent update	Aug 15, 2026 12:29 PM
Agent Version	2026.1.1.4 Release Notes 
Assigned Products	Software Agent mode ✓ XDR Device Encryption + Versions Core Agent 2026.1.1.4
Security Heartbeat Firewall	X131083HQ82MWB4

Sophos Firewall policies with Synchronized Security

A firewall rule can optionally require a Green health state before a device is allowed to reach the internet. Unprotected devices (i.e., those not running Sophos Endpoint) would then be unable to connect, as would any device with a questionable health state.

▼ Configure Synchronized Security Heartbeat

Minimum source HB permitted

☐ GREEN ☐ YELLOW ☒ No restriction

☐ Block clients with no heartbeat

Minimum destination HB permitted

☐ GREEN ☐ YELLOW ☒ No restriction

☐ Block request to destination with no heartbeat

Bringing it together

The problem was never a shortage of security tools. It was that the tools an organization already owns tend to work in isolation, and attackers have built their methods to exploit the gaps between them. Synchronized Security enables your security tools to work as a unified, coordinated defense.

If you run two or more control points inside Sophos Fusion, Synchronized Security is already working on your behalf. Connect more control points, and it reaches further. The non-Sophos tools you have already invested in are brought into the response rather than left reporting from the sidelines.

How much runs automatically remains your decision. Coordination that ignored your change control processes would not be worth having, so the depth of automation is set by you, control point by control point.

That is the practical value of the Sophos cyber defense system. Not a longer list of products, but the ones you already run responding together at machine speed, faster than an AI-accelerated attack can move between them.

To learn more, visit
[www.sophos.com/
synchronizedsecurity](https://www.sophos.com/synchronizedsecurity)

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