SOPHOS

Security made simple.

The Sophos Security Heartbeat:

Enabling Synchronized Security

Today organizations deploy multiple layers of security to provide what they perceive as 'best protection'; a defense-in-depth approach that includes multiple products and technologies on their networks and endpoints in an effort to defend against known and emerging threats. These deployments of host and network-based firewalls, content inspectors, malware analyzers, and event managers do a respectable job of defense, however there is a fundamental deficiency in their deployment in that they fail to make one another better. Our industry describes the underlying condition as "technology silos" where our control and enforcement points operate in isolation, rarely sharing information in any rapid, meaningful or practicable fashion. Such a lack of communication, or synchronization, means that we have been missing the chance to make our firewalls smarter by giving them contextual insights that only our endpoints have, or giving our endpoint protection the ability to objectively assess their state of integrity or compromise based on network activity and context. The opportunity for improvement seems both obvious and vast.

The response to these recognized weaknesses has been to put more 3rd party technology and people in place to attempt to overcome this lack of contextual connection between endpoint and network defenses.

One such example is that there are plenty of Security Information and Event Managers (SIEMs) type-tools being proposed to IT Security teams that try pulling information, alerts and events from the two worlds of network and endpoint protection into one place. This approach has three fundamental challenges; firstly, it tends to put all the effort into normalizing and structuring the event data from disparate sources, and very little into extracting actionable information from the resulting sea of data. Secondly, this approach is inherently "after the fact" investigation, and thirdly, these tools drive up staffing and headcount requirements to build and monitor the fragile and complex correlation rules they depend on. On the chance that an analyst, if you even have one available, has managed to trawl through the events, the bad guys are already long gone with your data.

Until now, integrating the information from multiple products in order to act effectively across the organization has been slow and tedious, and often impractical. Seeing this challenge in our customer base, Sophos has released a revolutionary new technology which we call the Sophos Security Heartbeat.

A new approach was needed, built to work in a synchronized way, establishing real-time communications between network and endpoint products enabling automated and coordinated action, but without creating yet another layer of complexity and cost. The Sophos Security Heartbeat has been developed to solve this problem and to deliver a new level of protection to organizations and their resource-constrained IT Security teams. This paper outlines the basic design and functionality of the Sophos Security Heartbeat and shows how it delivers better and faster protection through synchronized security.

Synchronized Security, a Simple Solution to a Vexing Problem

Imagine posting security guards inside and outside of your building, but not giving them 2-way radios to communicate with each other. Instead, they separately send information to a centralized system with a human scanning for any information that might be meaningful to either of the individual guards. Now imagine many buildings with fences and exterior guards around them as well as interior guards in every room, all sending summaries of what they see to a central authority who must make sense of those signals. The exterior guards work for a different manager than the inside ones, and the information being sent by the guards is hard to identify because their IDs are constantly changing, so we may not know who is sending any given message. And lastly, intruders are constantly challenging your defenses with new innovative and stealthy techniques. Amazingly, this is precisely the situation that IT security teams face today.

Dealing with these threats and complexity has created nearly insurmountable challenges for even the world's most sophisticated organizations. They have deployed scores of analysts and new technologies such as big data warehouses and SIEM's to coordinate and make sense of this distributed, silo'd set of endpoint and network solutions. The typical deployment, greatly simplified, looks like Figure 1.

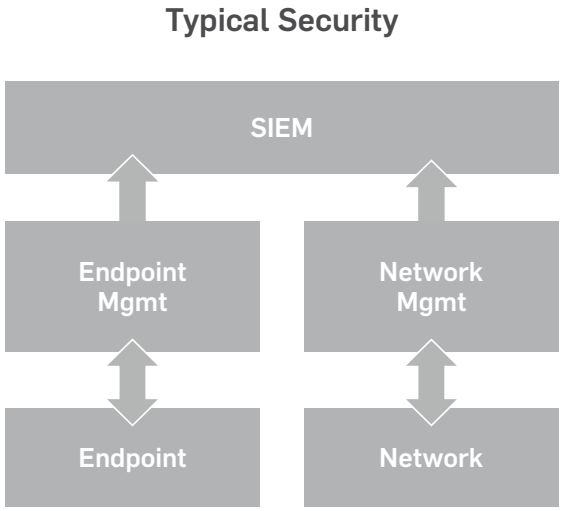

Figure 1: Typical solutions try to correlate and make sense of data and require headcount and scarce expertise

And while there is some merit to this approach; it is resource intensive, requiring specialized and highly skilled staff in order to make sense of incoming signals to find real problems. But even in that case, it does nothing to speed the process of responding to new threats. Because the management and implementation of endpoint and network products remains isolated, it is a complex, challenging and fragile process to attempt to coordinate activity across these products.

Most IT Security organizations can't possibly hire or react fast enough to protect themselves by implementing, maintaining and using these complex and silo'd products. This results in inefficacy and ineffectiveness. And when that happens, the attackers win all too often.

Now for the first time, endpoint and network protection can operate as one integrated system, enabling organizations to more quickly and efficiently prevent, detect, investigate, and remediate threats. As shown in Figure 2, an alternative, synchronized security framework unifies management and connects endpoint and network security solutions directly to each other, allowing them to communicate with each other in real-time.

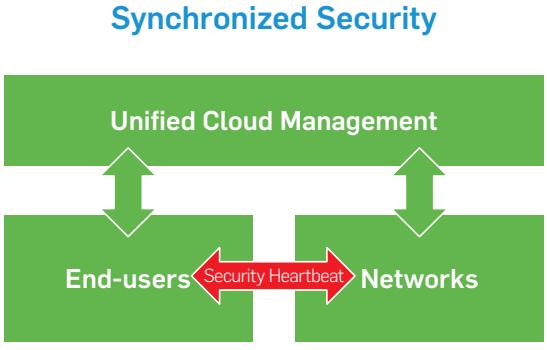

Figure 2: Synchronized Security simplifies and unifies communication and management

By sharing contextual intelligence via a security heartbeat this framework can discover advanced threats faster, actively detect compromises across endpoints and networks, and automate incident response by isolating systems and blocking exfiltration. Simplified management makes the framework easy to set up and manage without requiring additional security event managers or staff analysts. In short, synchronized security provides better protection in a more cost and time efficient manner than other approaches. Table 1 summarizes the difference between these approaches.

	Synchronized Security	Typical Security
Intelligence	Shared	Isolated
Correlation	Automated	Manual and partially automated
Unknown Threat Discovery	Contextually assisted	Unassisted
Incident Response	Highly targeted	Imprecise
Additional Product and Headcount Investment	None	Significant
Management	Simple and unified	Complex and silo'd

Table 1: Characteristics of Synchronized vs. Typical Security

The Sophos Security Heartbeat – Enabling Synchronized Security

The Sophos Security Heartbeat connects the Next-Generation Sophos Endpoint Clients to the Sophos Network Security Gateways, creating a secure channel for real-time information sharing between products. Enabled and managed from Sophos Cloud, the Security Heartbeat is easy to set up and manage. It utilizes secure communications to pass intelligence, events, information and commands between deployed endpoints and network firewalls. firewalls.

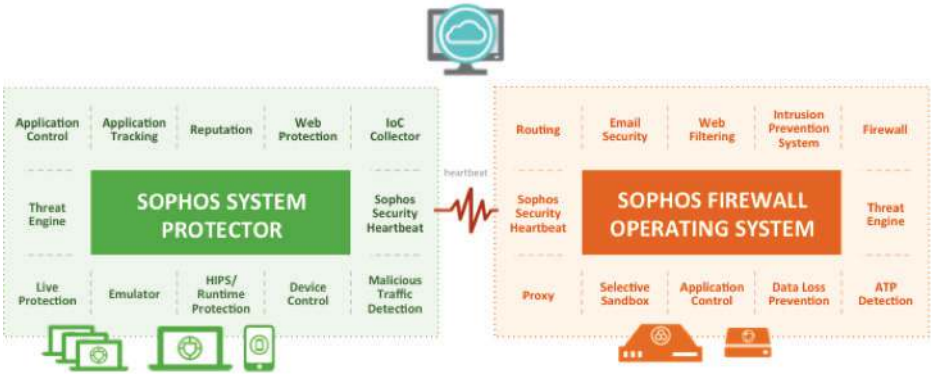

Figure 3: The Sophos Security Heartbeat connects Sophos Next Generation Endpoint and Network Protection

As shown in Figure 3, the Sophos Security Heartbeat is an integrated capability in the Sophos Next-Generation Enduser Security and Network Firewall products. The Security Heartbeat allows the Sophos endpoint and network security solutions to continuously share meaningful information about suspicious and confirmed bad behaviour across the entire organization's extended IT ecosystem.

By deploying Sophos Security Heartbeat, organizations can find advanced threats sooner, automatically identify compromised systems, automate incident response and have instant visibility into endpoint security status.

Setting Up The Sophos Security Heartbeat – Simply Register and Go!

Setting up the Sophos Heartbeat is fast, straightforward and simple.

You simply enter your Sophos Cloud credentials into the Sophos Firewall User Interface and the Firewall will automatically identify itself and register with our SaaS version of the Sophos Management Console. From that point on, you can see all registered Firewalls in the Sophos Cloud UI. This is shown in Figure 4 and 5.

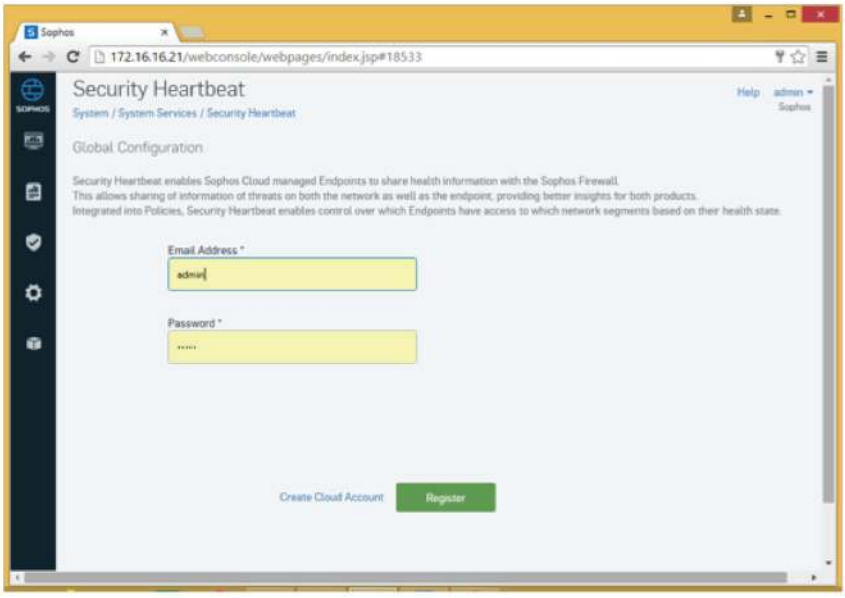

Figure 4: Simply enter your Sophos Cloud credentials to register a Firewall for the Security Heartbeat

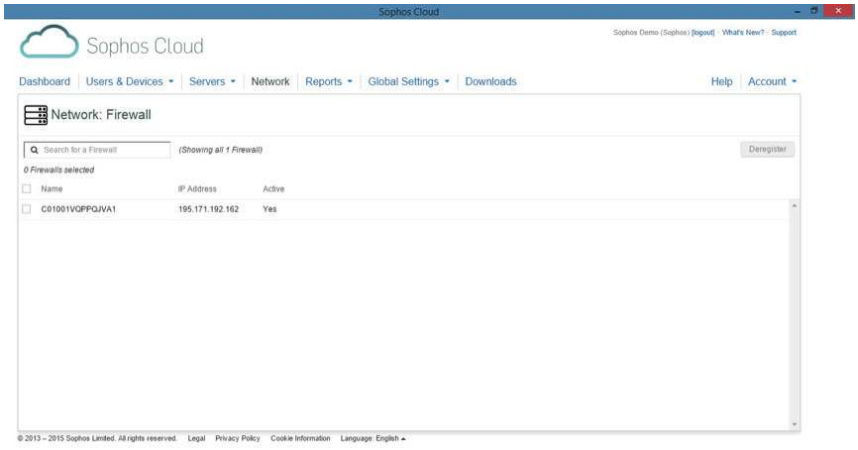

Figure 5: The Sophos Firewall is now registered with the Sophos Cloud

As soon as the first Firewall is registered with the Cloud, the following all happens automatically, using our SaaS service as a "trusted independent witness":

- The computers receive security information that enables a Heartbeat connection to the Firewall.
- The Firewall receives security information that enables a Heartbeat to the computers.
- Each computer starts to send connection requests to a Firewall that could protect it. Computers connect to the nearest available registered Firewall (their default gateway).
- If the Firewall sees a connection request, it checks the security information to confirm that it is one of your endpoints and completes the connection if valid
- The computer also validates that the Firewall is yours by checking its security information received from Sophos Cloud.

That's it. No complex rules, configurations or updates. You are now ready to see the Sophos Security Heartbeat in action.

Sophos Security Heartbeat in Action

With the Firewall and endpoint clients now connected via the Security Heartbeat, system health information now starts to flow from the connected endpoints to the Firewall as well as the Sophos Cloud management system.

As endpoints connect via the Security Heartbeat to the Firewall, the Sophos Firewall Manager dashboard is populated with the all the registered endpoints and their corresponding health status as shown in Figure 6. Client health status can be **red, yellow or green**.

Figure 6: Firewall dashboard displays the health of connected endpoints as Green, Yellow or Red. in this case, ninety-seven endpoints are Green, one is Red and two are Yellow.

What Health Status Tells You?

Table 2 summarizes the meaning of the Green, Red and Yellow Indicators. Red indicators should be dealt with immediately while Yellow indicates risk, but not necessarily urgency.

Possible Alert Triggers	Red	Yellow	Green
Malware Detected	X – Active	X- Inactive	
Potentially Unwanted Application		X - Detected	
Malicious Network Traffic	X – Communication from endpoint to known or suspected bad host		
Sophos Security Software Not working correctly	X – System may lack protection		
No detections, Security software working correctly			X

Table 2: Endpoints report health status to Sophos Firewall and Cloud based on simple but powerful triggers, allowing staff to speed discovery and prioritize follow-up

In addition, the Sophos Endpoint software use the Security Heartbeat to send detailed information to Network Firewall Dashboard, allowing staff to drill down into details as shown in Figure 7.

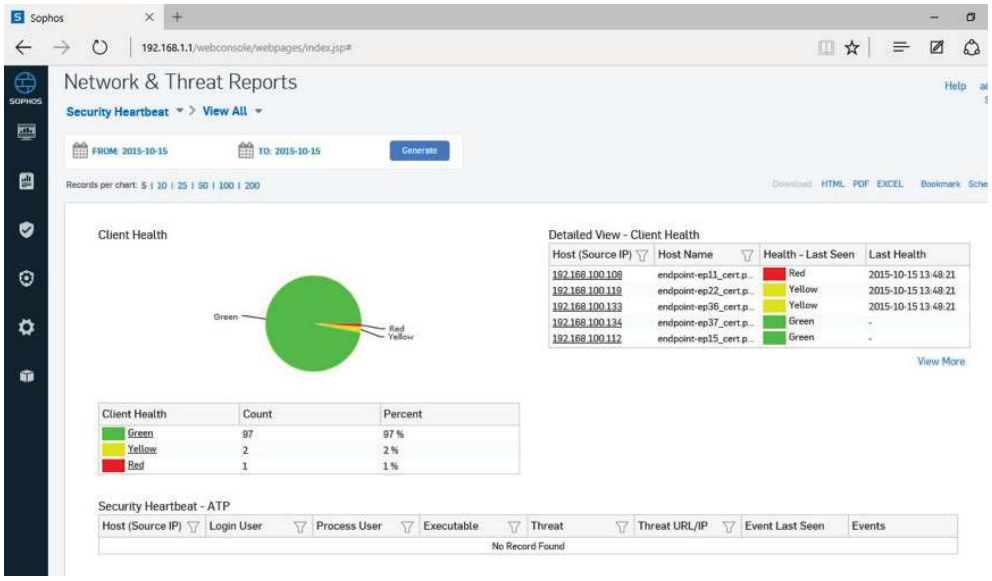

Figure 7: Drilling into client health dashboard shows details of health status and triggers by client

Automated Incident Response

Knowing the status of client health is one thing, but acting effectively and quickly is another matter altogether. Sophos Security Heartbeat enables Firewall administrators to set up simple and highly effective policies that leverage endpoint health status to provide automated incident response. This automated response isolates compromised systems, blocks potential exfiltration, and increases protection of the organization.

As shown in Figure 8, Firewall rules can be easily created, taking advantage of the real-time visibility of endpoint health. Here we have created two rules, Amber and Red as an example, but an organization can create and customize as many of these policies as needed to match the requirements of their business. Our Amber rule will allow Internet access to systems in yellow or red health state, but block access to Salesforce.com as a precaution. Our Red rule blocks all Internet access from those clients with red status. When a system changes status, these rules provide network level protection prior to system remediation, dramatically lowering the risk of loss.

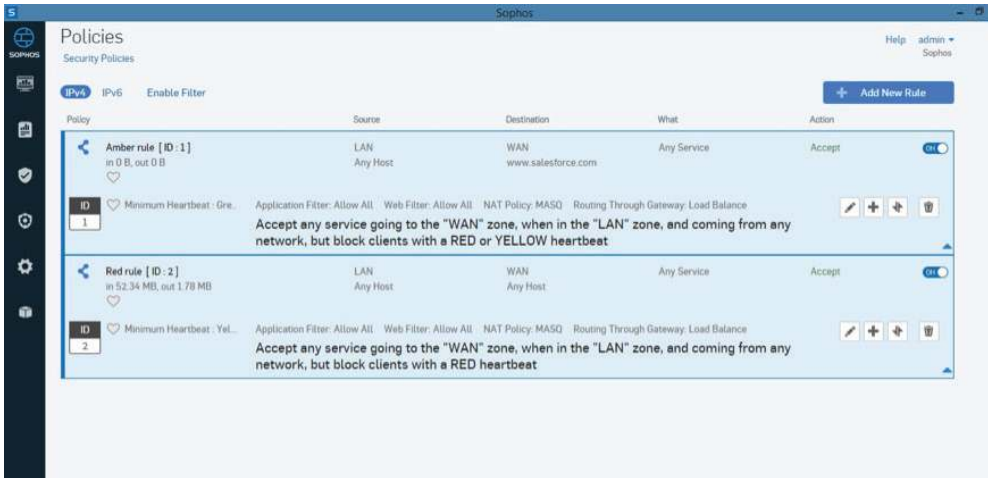

Figure 8: Simple Firewall policy can be set to enhance protection leveraging the information provided by the Sophos Security Heartbeat

Figure 9 shows the notification screen that an end-user will receive after this Amber rule is enforced by the Sophos Firewall.

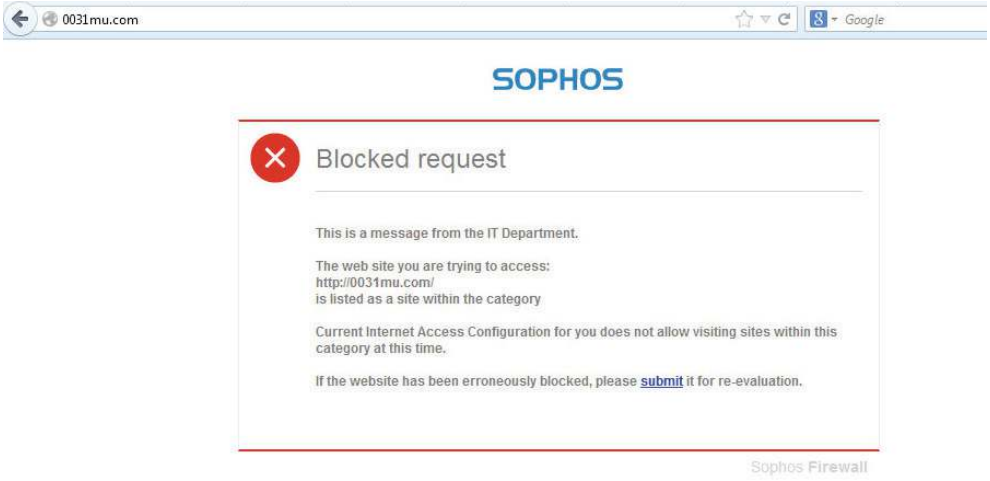

Figure 9: End-user message after enforcement of the Amber rule

Advanced Threat Protection (ATP) with Sophos Security Heartbeat

The Sophos Security Heartbeat automates ATP alerting and response between the Sophos Firewall and Sophos Endpoints, dramatically reducing investigation time, threat detection and remediation.

For instance, if the ATP feature on the Firewall detects suspicious traffic, it will utilize the Security Heartbeat to see if the traffic is coming from an endpoint with an active heartbeat. If this is the case, the Firewall will use the Security Heartbeat to get the machine name, the logged in user, and the process name that triggered the Firewall ATP alert. This step alone can often take hours and days of manual labor in traditional environments without a Heartbeat service.

This information is then displayed in the ATP Alert screen of the firewall as shown in Figure 10.

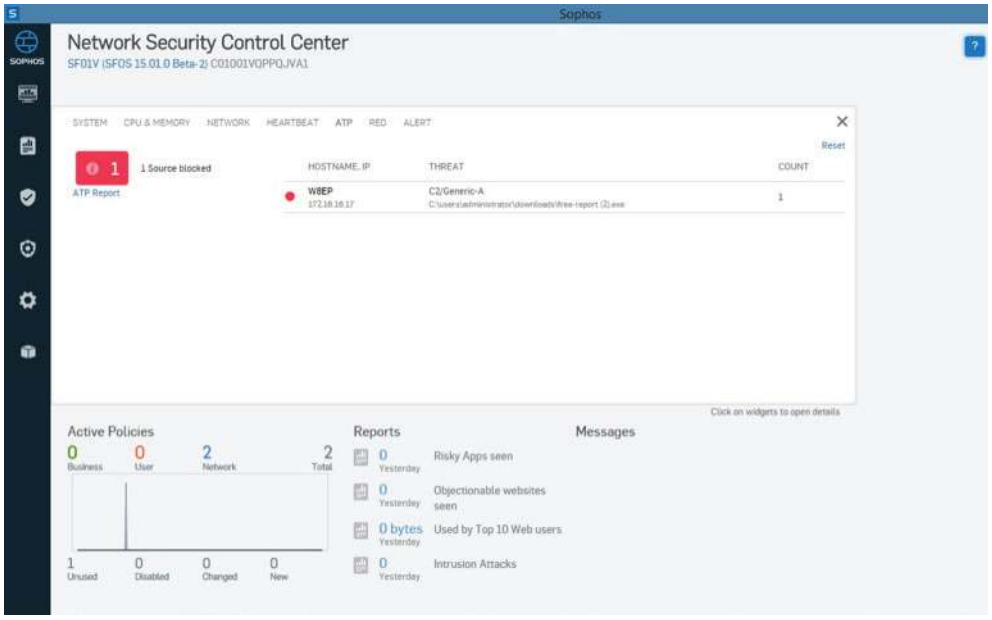

Figure 10: ATP alerting in Firewall user interface

After actively identifying the endpoint affected by the advanced threat, the endpoint simultaneously alerts the Sophos Saas Management Console as shown in Figure 11. With the same threat, machine, user, and process information sitting in both the endpoint (Sophos Cloud) and network (Sophos Firewall), the Security Heartbeat has enabled synchronized security.

Figure 11: ATP Alerting automatically reported in Sophos Cloud

Sophos endpoint protection now instructs the Host Intrusion Prevention (HIPS) feature of the Sophos Client to see if malware can be positively identified and remediated on the machine. As there is a suspicion of active malware on the computer, its health status turns Red. The Sophos Firewall now provides additional protection by enforcing policies such as the Red rule from above, eliminating any damage while remediation is in process.

Summary

The advanced threat protection example is an outstanding demonstration of the power and simplicity of synchronized security powered by the Sophos Security Heartbeat. All of this happens with NO manual intervention, no forensic investigation and no costly and time consuming identification processes, while delivering full visibility and audit trail of activities.

No staff, no mess, no time lags. Just synchronized security, delivering more and faster protection with no additional staff.

The threats faced by organizations today can seem daunting, and typical answers require a level of resources, specialized expertise and staffing that is just not available to most institutions. Synchronized security completely changes this dynamic, providing better protection through simple yet powerful communications and management between previously silo'd solutions, without adding staff or complexity. Organizations deploying the Sophos Security Heartbeat get instant visibility into endpoint health status, accelerated discovery of advanced threats, active identification of compromised systems and automated incident response.

To learn more and see how synchronized security and the Sophos Security Heartbeat can enable you to win in today's risky world, visit Sophos.com/heartbeat.

Sophos Security Heartbeat

To learn more, visit **sophos.com/heartbeat**

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

North American 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

Oxford, UK | Boston, USA

2015.11.02 WP-NA (GH)

SOPHOS