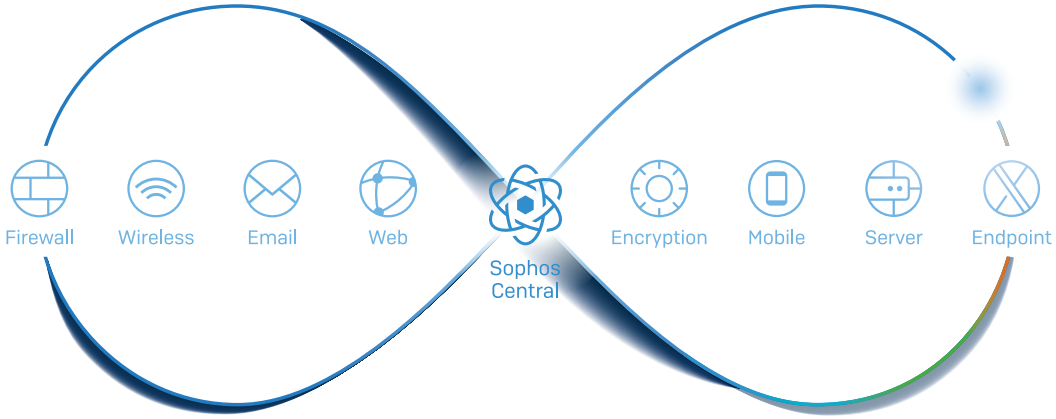
SOPHOS
Cybersecurity made simple.



Synchronized Security in a Connected World

A Sophos Whitepaper August 2018

Connectivity is one of the defining characteristics of the 21st century, permeating every aspect of our lives. The words we speak ("Can I connect with you to discuss?"); how we listen to music, with web-based music platforms and wireless speakers controlled via a mobile phone; and even to the way we maintain relationships, connecting to friends and family across the world through social media platforms. Everything is connected.

Connectivity is also fundamental to our IT infrastructure. We absolutely depend on it for both our business or personal lives. We build our networks to enable all the different elements of our lives to link up, to be part of a system rather than work in isolation. As technology continues to advance, so too does our dependence and use of connectivity. Extending our connectivity from office-based wired connections to a truly global network, 90% of the time the phrase "limited email access" when we're out of the office is simply a time-worn excuse rather than a genuine state of disconnect.

Unsurprisingly, today's enterprising cybercriminals have enthusiastically embraced connectivity. They use a range of connected techniques in their malware attacks: a phishing email leads to an initial foot in the door, followed by a malware infection through exploitation of a known or unknown defect, then an escalation of privileges or a lateral movement across the network to spread the infection across different devices. A single compromised device can mean your network and connectivity are held hostage or used for malicious intent. Essentially, they exploit our IT connectivity to achieve their malicious ends.

Seeing the wood for the trees

Unfortunately, cybersecurity has struggled to see the wood from the trees when it comes to connectivity. Technology companies have focused on creating products that focus on one specific part of the problem, yet don't connect with each other. For example, endpoint protection products connect a range of data points to identity if a file is malicious or benign. Firewalls connect multiple technologies – deep learning, IPS, sandboxing, etc. – to stop malicious traffic. Yet these two pillars of our cybersecurity defenses work in isolation, unconnected from each other.

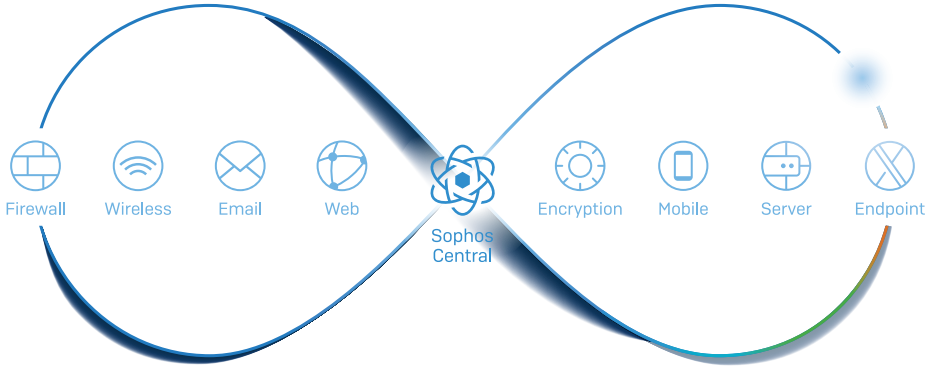
While this approach has resulted in strong individual solutions, it misses the bigger picture: as both technology and cyberthreats become ever more connected, point security products, no matter how good they are, can only ever have limited impact.

The result of our current, unconnected approach is that despite significant financial investment in security solutions, cybersecurity is not getting any easier – we continue to face the same core challenges we did 10 or even 20 years ago. Indeed, rather than making progress in the fight against cyberattacks, 83% IT managers agree that threats have actually got harder to stop over the last year[1].

In addition to exacerbating security risks, our disconnected approach to cybersecurity also puts a heavy burden on IT teams. Manually correlating data between systems and identifying appropriate actions burns valuable hours. A busy administrator may not mentally assemble the disparate events across the various products in order to realize that there is an attack or compromise underway. Indeed, research[1] shows that mid-sized organizations spend on average seven days per month identifying and remediating infected computers. It is unsurprising that 48% IT managers[2] are putting in extra hours on a regular basis.

Synchronized Security: Cybersecurity as a System

Pouring more and more money into individual point security solutions is no longer a realistic long-term solution. While standalone cybersecurity solutions can address specific vectors of attack, cybercriminals will continue to be able to exploit the gaps between point solutions and take advantage of the lack of connectivity. Organizations need a layered approach to security, one where products connect and share information. It's time to embrace this new approach. It's time for Synchronized Security.



Synchronized Security is cybersecurity as a system. Security solutions connect with each other in real time via a Security Heartbeat™, working together to combat advanced threats. This automation enhances your defenses, responding automatically to events, so you can mitigate risk and slash the time and effort spent managing IT security. Only through connecting the big cybersecurity dots in this way can you create a system that transcends point challenges and enables you to create long-term security strategies that work for your business.

Synchronized Security is built on three pillars: Discover, Analyze, and Respond. These pillars enable security components to become more than the sum of their parts by working together to stay ahead of the attackers.

Synchronized Security: Cybersecurity as a System

Discover Identify unknown threats	**Analyze** Get instant insights	**Respond** Respond automatically to incidents
Products automatically share information to reveal hidden risks and unknown threats.	Real-time incident analysis and cross-estate reporting deliver instant insights.	Adaptive policies automatically respond to infections and incidents – in seconds.
‣ See ALL network traffic, enabling identification of risky apps and malicious traffic ‣ Identify risky users by correlating behaviors across multiple activities	‣ See the full chain of events for an incident, including all files touched, and URLs / IPs communicated with ‣ Correlate network traffic to individual apps on individual computers	‣ Instantly isolate compromised devices, stopping attacks in real time ‣ Restrict access on trusted networks for non-compliant devices ‣ Initiate an endpoint scan on detection of outbound spam.

Synchronized Security in Action

The more security services that share real-time information in a Synchronized Security system, the more you can benefit from their inter-connectivity. Here are three of the ways Synchronized Security elevates your protection while simplifying IT security management.

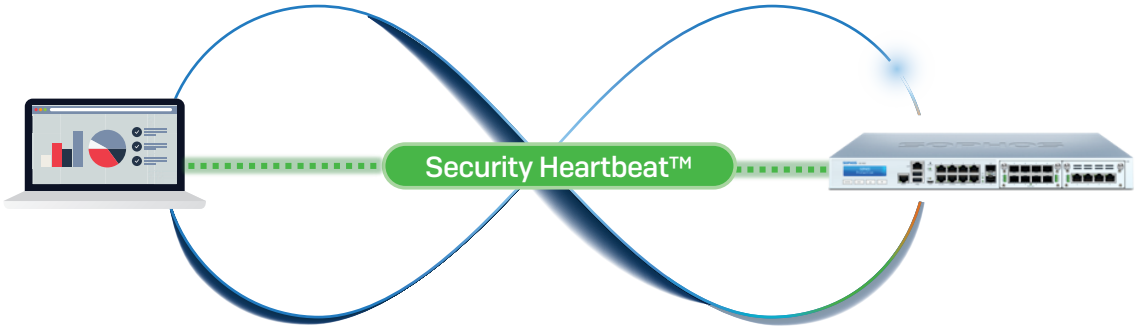
Slash incident response time: 3.3 hours to 8 seconds

Identifying and remediating infected computers is a laborious task, taking on average 3.3 hours per machine[3]. Synchronized Security's automated threat response slashes that down to just 8 seconds[4]. It automatically responds to threats and provides detailed analysis of exactly what happened across your entire infrastructure so you can prevent future recurrences.

1 Malware Detection
Sophos Endpoint detects a malware attack

2 Cross-Estate Communication
Sophos Endpoint shares infection status with the security system, triggering automatic responses

3 Device Isolation
XG Firewall instantly isolates the computer, preventing the attack from spreading, and communication with C2 servers



5 Access Restored
XG Firewall restores network access. Root Cause Analysis provides detailed view of what happened

4 Clean-up
Sophos Endpoint automatically cleans up the infection. Once the malware is removed, Sophos Endpoint shares this update with the cybersecurity system

Take back control of your network

A recent survey[3] revealed that IT managers can't identify almost half (45%) of the traffic running through their network. As a result, they cannot block risky or malicious traffic – instead, it flows through the organization unchecked and unhindered. There would be a public outcry if an airport announced they could only security scan half their passengers, and so they allowed the other half through unchecked. Yet we allow this risky behavior on our networks every single day.

Synchronized Security is the simple, elegant solution to this problem. The endpoint always knows the true identity of an application – even if it tries to disguise itself from the firewall to avoid being blocked. By enabling the endpoint and firewall to share application identity information in real time, the firewall can identify all the network traffic and the IT team can take back control of their network. With the information to hand, they can enhance security by blocking malicious apps while speeding up business applications by de-prioritizing non-work traffic.

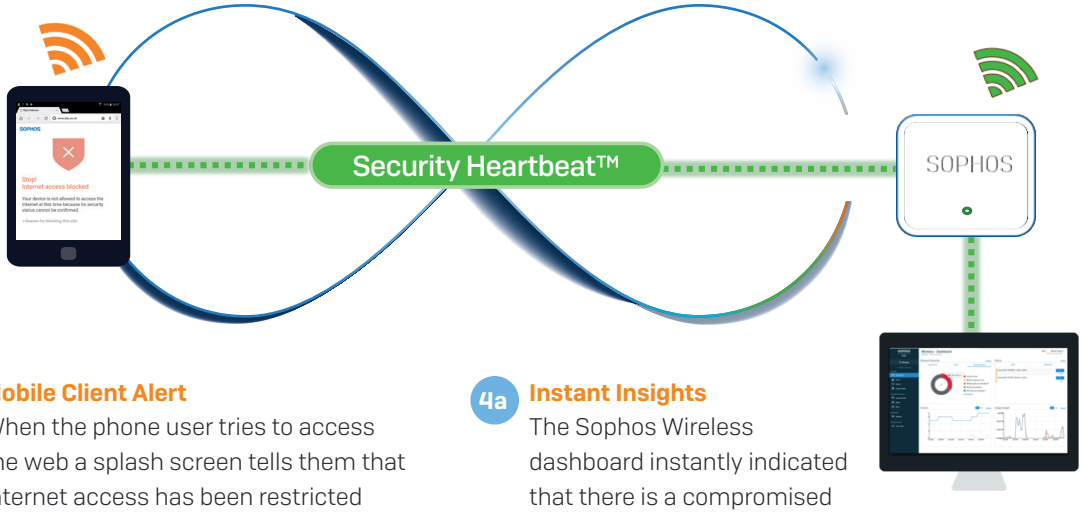
Reduce risk from mobile devices

Mobile devices are just as much a door to your organization's data and systems as your desktops and laptops. Mobile devices travel with us everywhere, connecting to a wide variety of protected and unprotected networks, making their security state questionable. Allowing compromised devices to access the network increases your risk of attack. Yet on its own the wireless network cannot make any judgement as to the health of the devices connecting to it. Again, Synchronized Security, this time between the mobile and wireless solutions, provides the answer to the problem.

1 Compliance violation
A user creates a compliance violation on a phone secured through Sophos Mobile

2 Cross-estate Communication
Sophos Mobile sees the violation and shares it with the rest of the system, triggering predefined actions

3 Deny Network
If 'the deny network' rule is selected in Sophos Mobile, Sophos Wireless will restrict internet access



4b Mobile Client Alert
When the phone user tries to access the web a splash screen tells them that internet access has been restricted

4a Instant Insights
The Sophos Wireless dashboard instantly indicated that there is a compromised device (a red heartbeat)

Cybersecurity: From Business Cost to Business Enabler

Cybersecurity is traditionally associated with cost and inconvenience. For finance teams it's an often significant line in the IT budget. And for the wider organization it's a dull necessity that takes IT teams away from delivering business-enabling projects.

Synchronized Security turns all this on its head. The enhanced protection it delivers reduces downtime while freeing up valuable IT staff to work on growing the business. Examples of how Synchronized Security enables IT to enable the business include:

Operational cost savings

- Save day-to-day IT security resources by controlling all your IT security through a single console.
- Reduce resources spent making disparate products play well together by using solutions engineered to work together.

- Be up and running with new products quickly – no new interface to learn.

Vendor consolidation

- Streamline purchasing by working with a single supplier for all IT security solutions.
- Simplify ongoing vendor management with a single point of contact for all support needs (technical, sales, finance).

Cyber risk mitigation

- Stop hackers moving across your network to find a more valuable person (e.g. escalated privileges) or asset (e.g. server).
- See how the threat entered and spread with full root cause analysis, enabling you to act to prevent future security risks.
- Identify risky apps and users through visibility of all network traffic.

Improve productivity

- Reduce user downtime from infections and incidents with adaptive policies that automatically respond to threats. Slash average response time from 3.3 hours to 8 seconds[5].
- Improve response speed by managing all your IT security through a web-based platform that can be accessed from any location.
- Avoid downtime from product compatibility by choosing solutions engineered to work together.

Complete estate visibility

- See and control all your IT security services in one place – anytime, anywhere – through the web-based platform.
- See all network traffic, enabling identification of risky apps and malicious traffic.
- Identify risky users by correlating behavior across multiple activities.

Enhance the profile of IT

- Reduce downtime from infections and incidents from hours to seconds.
- Free up IT to better support the business by working with a single vendor, and single support team.
- Avoid downtime from product compatibility with solutions engineered to work together.

A System That Works

There is a huge difference between a clever concept and a cybersecurity system that enhances your defenses day in, day out. History is full of ideas that sound great in theory but don't work in practice. Feedback from IT professionals using Sophos Synchronized Security confirms that it delivers profound benefits across their organization:

90%
agree they now have greater control over their network traffic

85%
agree Synchronized Security has improved their security posture

84%
of customers say Synchronized Security helps deal with increasing pressure on IT

Enterprise-grade – for everyone

Until now, cybersecurity systems used to be the exclusive preserve of the largest organizations, who had the extensive resources needed to stitch together data from multiple products and burn IT hours triaging the results. Sophos Synchronized Security is different. It's enterprise-grade protection, automated, for everyone. It provides the detailed information needed by security specialists while being simple enough for smaller organizations to use with limited staff. In fact, 8 out of 10 users confirm that it's easy to activate[6].

As strong as the weakest link

Like all other systems, a cybersecurity system is only as strong as its weakest link. While connecting individual security components delivers significant advantages, it can't make up for fundamental weaknesses in those components in the first place. Sophos Synchronized Security enables multiple award-winning security services to work together, further amplifying the benefits to organizations, providing quality components that are excellent on their own and even better together.

Conclusion

We live in an interconnected world and, with almost half the planet now using the internet, we're only going to get even more connected in the years to come. Burying our heads in the sand and continuing to focus on individual point security products is not the answer – not only does it leave us vulnerable to threats, it also increases the cost of IT security to the business.

Rather than resisting connectivity, it's time to actively take advantage of an integrated approach by moving to cybersecurity as a system. By working together, security solutions can detect, analyze, and respond automatically to incidents and infections. This slashes response time and enables IT security to switch from being a business cost to a business enabler.

1 State of Endpoint Security Today, Sophos, January 2018
2 Sophos Small Business Survey, 2018
3 Dirty Secrets of Network Firewalls, Sophos, 2018
4 ESG Labs, 2016
5 ESG Labs
6 Sophos Customer Survey, 2018

Synchronized Security

Learn more at sophos.com/synchronized

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

2018-09-04 WPNA (NP)

SOPHOS