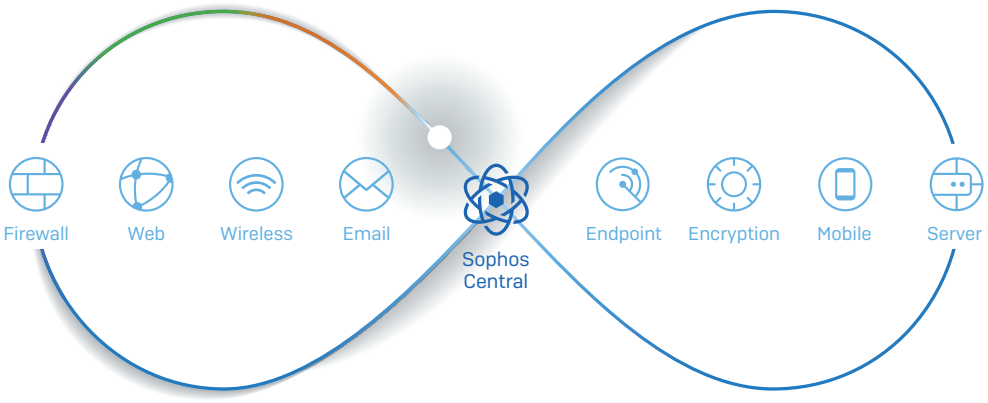
SOPHOS
Security made simple.



Synchronized Security: A Revolution in Threat Protection

A Sophos Whitepaper February 2017

Section 1: Today's World of Cyber Risk

Attacks Increase in Number, Complexity, Sophistication

All businesses large, small or in-between, must live and learn to thrive in a world with an ever-increasing threat of cyber risks. Those risks are rising for many reasons, from the growing attack surface to the increasing complexity and sophistication of such attacks.

Mobile devices and cloud services are being used by employees more and more, and organizations of all sizes are deploying virtual and cloud infrastructure. This has increased the so-called "attack surface" dramatically.

Consider these facts:

- **Devices:** The typical digital consumer now owns three connected devices.[1]
- **Apps:** Employees use, on average, 16 cloud apps at work – with Box, SalesForce and Microsoft Office 365 proving the most popular.[2]
- **Internet of Things:** Gartner forecasts that nearly 21 billion 'things' will be connected to the Internet by the year 2020.[3]

As these attack vectors broaden, attacks are on the rise with more successful breaches, and increased data loss.

Commercially supported malware toolkits, available on the grey and black markets, make it possible to conduct more and increasingly sophisticated attacks with less skill than ever before.

And, cybercriminals are copying the cloud-based business models used by legitimate organizations, offering malware-as-a-service (e.g., Ransomware as a Service) complete with money-back guarantees. This further reduces the technical skills required to carry out a cyber-attack, while ensuring the tools used are constantly updated.

The unfortunate result of all these developments is that the cybercriminals are now moving too fast for most organizations to keep up. According to the Verizon 2016 Data Breach Investigation Report:

- Hacking and malware are the top two causes of data breaches.
- Attackers are getting even quicker at compromising their victims – the time to compromise is almost always days or less, if not minutes or less.
- The detection deficit (i.e., the time between compromise and detection) is getting worse and it's taking longer to identify the attacks.

Further, the Verizon report finds that financial gain is the main motivator in over 80% of these attacks. For small and medium businesses, the cost can be catastrophic.

We are experiencing increased attacks, rising complexity of attacks, and increased losses from them. We have to ask: What do we need to do differently?

Small Teams, Stretched Resources, Tight Labor Market

One would think the natural reaction to increasing attacks would be to throw more people at the problem — hire staff to enhance security. However, since businesses have small IT security teams, expanding or redeploying resources just isn't an option for many small or mid-sized organizations.

As shown in Figure 1, before you reach large enterprise environments, dedicated IT security teams are very limited in size and resources.

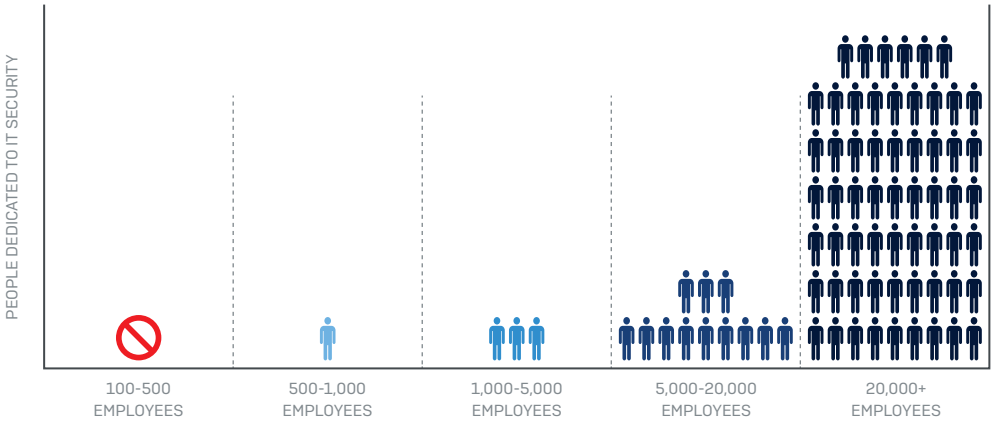


Figure 1: Midmarket IT Security Organizations are Small and Resource Constrained (Source: US Dept of Homeland Security, 2014)

Even if management wants to expand their security teams, they face another obstacle: a serious shortage of IT security resources. Research by Enterprise Strategy Group reveals that a massive 46% of organizations believe they have a problematic shortage of cybersecurity skills.[4] This in turn puts further pressure on existing IT teams – to do more with less.

Despite a far greater number of attacks more sophisticated (and successful) than ever before, there simply isn't enough trained staff. Relying on available resources means that organizations face an unacceptable level of risk.

Section 2: Existing Security Approaches

Layered and poorly integrated. Complex and myopic. Independent of nearby context. Decisions in isolation. All of these descriptions can be applied to current security approaches.

When we look at the way the IT security industry has developed, it's easy to understand why. Security companies have focused on developing individual products that address specific points in the attack chain, rather than a holistic solution to the cyber threats we all face. As a result, the challenge of integrating disparate point products has fallen on over-burdened IT teams. It's like auto manufacturers producing the individual car parts and then asking customers to put them to together and make the finished vehicle.

IT security professional have attempted to "connect the dots" between data sources by employing correlation engines, big data warehouses, Security Information and Event Managers (SIEMs), emerging information sharing schemes like STIX and OpenIOC, and scores of human analysts. However, even with the most advanced tools, understanding data from a variety of point products so you can quickly detect and remediate risk to stop data loss can be like putting Humpty Dumpty together again.

Event and log correlation still depends on building and maintaining complex correlation rules, endless field mapping and filter definition, as well as hours of highly-skilled, hard-to-find analyst time and effort. SIEMs require considerable capital investments and ongoing operating expenses. And information sharing, while certainly key to the future of security, has not yet matured enough for widespread, simple adoption.

The results, or rather lack of results, speak for themselves. Data loss and risk continue to increase, with no sign of letting up, and staff is overstretched. According to a recent Ponemon Institute report, 74% of breaches go undiscovered for more than six months. And worst of all, mid-market companies seem to be having an even harder time mitigating risk than their better-resourced, larger peers. Clearly, the answer is not another non-integrated point product, more consoles, more people, or unwieldy SIEMs. These approaches are not succeeding. We must find a better and more effective approach.

> *Attackers launch coordinated attacks on an entire IT ecosystem, not against individual point products.*

Section 3: A New Approach to IT Security

For decades, the security industry has been treating network security, endpoint security, and data security as completely different entities. It's the equivalent of putting three security guards in your building – one outside the front door, one inside, and one in front of your safe – but not allowing them to talk to each other.

But as threats get more complex, and IT resources continue to be stretched, it's no longer possible to maintain this approach without compromising their protection.

Synchronized security is a best-of-breed security system where integrated products dynamically share threat, health and security information. The result: faster, better protection against advanced threats. It's like giving each of those guards a smartphone so they can communicate with each other and coordinate their activities to prevent any threat.

It's a simple, but at the same time revolutionary concept. To accomplish synchronized security, three things are needed:

1. **A central security system**
   At the heart of the synchronized approach is a central security platform that has threat and security context across all devices and data. It needs to be simple to use and enable you to manage all of your protection in one place. No more jumping from console to console, saving you time and effort on a daily basis.
2. **Next-gen technology**
   Synchronization should not be at the expense of depth of protection. Each security component needs to have the latest threat prevention technology built-in, so you always enjoy the most advanced protection.
3. **Intelligent protection**
   The security system needs to enable the security technologies to share information and automate response, including real-time isolation of any infected device which prevents both data loss as well as further infection within your business. The result is unparalleled protection against advanced, complex threats.

Today's Layered Security Solutions	Synchronized Security
Threat-centric, operates independent of nearby objects and events	Ecosystem-centric, operates with full awareness of nearby objects and events
Specialized siloed point products	Coordinated products
Effectiveness requires increased headcount	Effectiveness through automation and innovation; no increased headcount
Independent encryption management	Integrated encryption protection that automatically responds to threats
Complex	Simple

Figure 2: Today's Solutions Need to Change Dramatically

Section 4: The Sophos Approach

Sophos has pioneered the synchronized security approach. According to IDG, "no other company is close to delivering this type of communication between endpoint and network security products." So how do we do it?

Through Sophos Central, our award-winning security platform, you can manage all your Sophos protection in one place: endpoint, mobile, server, web, email, wireless, encryption and firewall. The difference between synchronized security and a central management console is dramatic. As Gartner describes it, synchronized security is "integration at the policy level" whereas a central console is merely "integration on the glass".

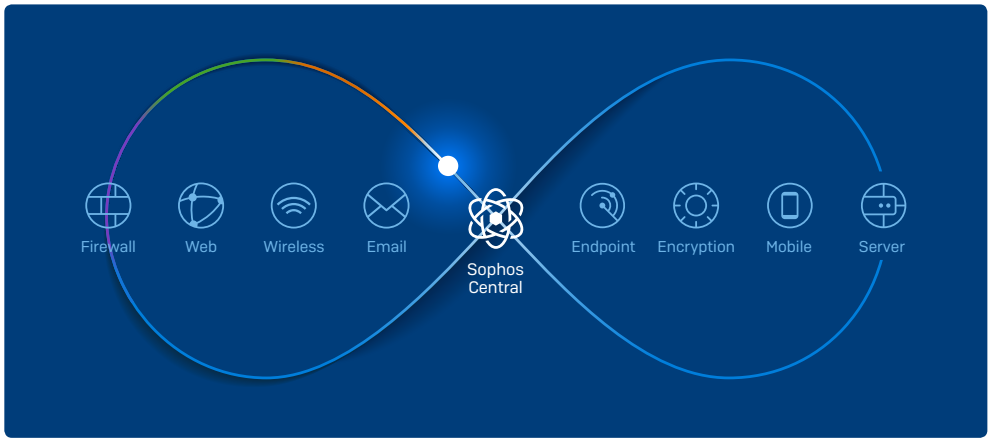


Figure 3: Synchronized Security with Sophos

Next-gen technology is built into our products, so you always have the latest in anti-ransomware, anti-exploit, anti-malware and ATP protection across all your devices and data. Recent industry awards and analyst recognition include:

- Only vendor named a Leader in the **Gartner** Magic Quadrants for Endpoint Protection Platforms and UTM.
- **Computing's** Best Firewall 2016
- Breakout Star in **Forrester** Encryption Wave 2016
- **SC Magazine** Excellence Award for Encryption and Network Firewall
- **AV Test** Best Android Security 2016

Synchronized security is made possible through our patented Security Heartbeat™, a secure communication link between Sophos products that enables them to share threat, health and security information and automate threat response. Dozens of technologies are working together in a coordinated fashion to provide the world's best protection against coordinated attacks. Sophos Security Heartbeat reduces threat discovery, protection, and incident response, which ordinarily could take hours, days, or weeks, to literally seconds.

Section 5: Synchronized Security: Stopping Today's Threats

In order to better illustrate the effectiveness of synchronized security, let's take a look at how it works in the real world with examples of a couple of today's most prevalent threats: botnets and ransomware.

Botnets

Botnets, where hackers control a network of innocent devices to carry out coordinated cyber-attacks, are now one of the top five global security threats we face. They're used for many different attacks, including:

- Cryptocoin generation, which mines for new online currency
- Data hacks via point of sale systems, as happened with Target
- DDoS or amplified DNS attacks, like the Mirai botnet that took down global websites
- Brute force password hacks and spamming

That health state and the botnet threat information are sent, via the Security Heartbeat, to the Sophos XG Firewall, which automatically isolates the compromised device by removing network access. This stops botnet malware from communicating with its command and control server for further instructions. This also prevents further infections from being spawned using this initial device.

The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed, to prevent any data theft.

This entire process, from detection to isolation and key removal, happens instantly and reduces incident response time from hours to seconds.

Once all affected machines are isolated and unusable by the botnet, our endpoint protection automatically removes the botnet malware.

After the systems have been automatically returned to their initial, clean state, the IT administrator can restore the endpoint health status to GREEN. This information is instantly shared with the rest of the security system via the Security Heartbeat. The XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.

Ransomware

Ransomware is a big business. It represents up to 35% of all IT threats worldwide and a successful attacker can earn up to $400,000 per month.

Ransomware usually arrives via email. As soon as the unsuspecting user opens the email and activates the ransomware, Sophos Intercept X's anti-ransomware technology stops the attack on desktops, laptops and servers, while Sophos Mobile Security protects mobile devices.

Synchronized security turns the at-risk devices to a RED health status in Sophos Central. This change of status, and associated threat information, is sent via the Security Heartbeat to the Sophos XG Firewall, which automatically isolates the infected device by removing network access. This prevents ransomware from communicating back to a command and control server and eliminating further infections.

The Security Heartbeat simultaneously contacts Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed. Similar to the botnet process, total time from detection to isolation and key removal is instant, reducing incident response time from hours to seconds.

Once everything is cleaned up, the IT administrator can return the endpoint health status to GREEN, which is instantly shared with the rest of the security system via the Security Heartbeat. The XG Firewall restores network access to the device, the encryption keys are returned, and the user is back up and running.

All this happens automatically – instantly. No need for you to do a thing.

Summary

The growth in complex and coordinated attacks is outpacing most organizations' ability to protect themselves. Overstretched IT departments struggle to respond fast enough to threats entering their ever-expanding IT infrastructure.

Continuing to manage disparate security products increases risk to businesses. Unless there is a distinct change in approach to IT security this will only get worse.

Synchronized security provides a best-of-breed security system where integrated products dynamically share threat, health, and security information to deliver faster, better protection against advanced threats. It gives you unparalleled protection and ease-of-use, making life easier for today's IT security professionals.

For more information and to try synchronized security for yourself visit sophos.com/heartbeat.

[1] Global Web Index, February 18 2016

[2] UK Business Insider, August 2015

[3] CNBC, February 2016

[4] ESG Brief, Cybersecurity Skills Shortage: A State of Emergency, February 2016

Synchronized Security

Learn more at 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

17-02-15 WPNA (DD-2560)

SOPHOS