

Synchronized Security: A Revolution in Protection

Questions? Contact us.
Rodney Spriggs: 703-939-1335, rspriggs@instrulogic.com
InstruLogic Main Office: 540-338-2222, 21 Main St, Round Hill VA 20142

Section 1: Living in Danger Zone, Today's World of Cyber Risk

"Highway to the Danger Zone. I'll take you, right into the Danger Zone"

– Kenny Loggins, *Danger Zone*

Attacks Increase in Number, Complexity, Sophistication

All businesses today, large or 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 average user in the UK has 3.1 connected devices.¹
- **Apps:** Companies with 250 to 999 employees use 16 approved cloud apps, while those with 1,000 to 4,000 employees use 14; the largest enterprises use an average of 11.²
- **Cloud:** Industry estimates puts Infrastructure as a Service revenues at greater than USD\$16B in 2015.³
- **Internet of Things:** By the end of 2015, an estimated 4.9 billion "things" were connected to the Internet. By 2020, that number will grow to 25 billion.⁴

As these attack vectors broaden, we've seen more attacks, more successful breaches, and increased data loss.

As the attacks increase in sophistication, the commercially supported toolkits available on the grey and black markets have made it possible to conduct such attacks with less skill than ever before.

These "kits" are well-tested and not always easy to detect or defeat. For example, the UnRecom Remote Access Tool (RAT) Kit, first reported on Threatgeek.com in May 2014, has gone through several iterations, including AlienSpy and most recently JSOCKET. This kit has been implicated in everything from data breaches to having a role in a political assassination.⁵

Unfortunately, research indicates small and midmarket businesses disproportionately fall victim to the growing number of confirmed incidents of data loss. According to the Verizon 2016 Data Breach Investigation Report:

Threat Landscape

Malvertising
IoT darkweb
Angler Trojan
RAT Cryptowall
Phishing DDoS
TOR injection
Fiesta JSOCKET
Wassenaar PlugX
AlienSpy SSL

Synchronized Security: A Revolution in Protection

- In 2015, there were 100,000 security incidents, of which 3,141 were confirmed data losses.
- These numbers represent a 23% increase in security incidents, and an astronomical 48% increase in data breaches compared to 2014.
- Organizations with less than 1,000 employees accounted for 20% of confirmed and classified data losses, despite accounting for less than 1% of incidents.
- Smaller business incidents and data losses take place across a wide variety of industries, with the largest numbers of attacks taking place in the financial services, accommodation, retail, and healthcare sectors.

Further, the Privacy Rights Clearinghouse estimates that 51% of data breaches in 2014 were caused by hacking or malware, while the Verizon report finds that money is the main motivator behind the perpetrators of these attacks. For the small and medium businesses most at risk, the cost can be catastrophic.

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, increase security. But many business have small IT security teams. Expanding or redeploying resources just isn't an option for many small or mid-sized organizations.

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

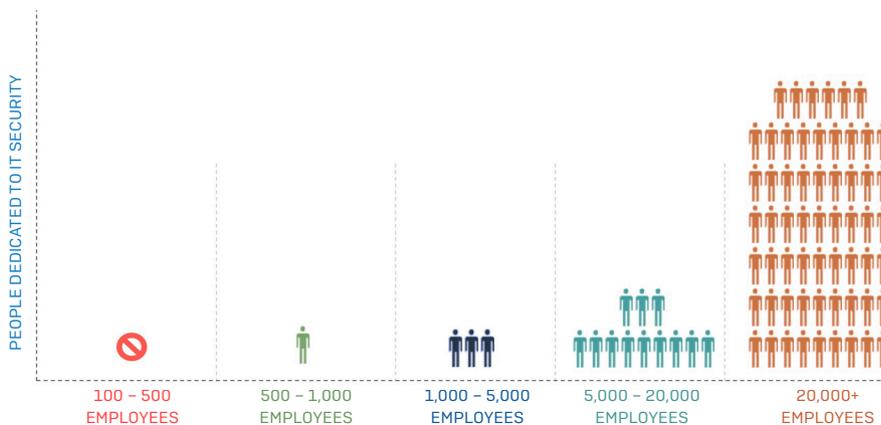


Figure 1: Midmarket IT Security Organizations are Small and Resource Constrained
(Source: US Dept of Homeland Security, 2014)

Even if management wants to expand their security teams, they face another obstacle: an extremely competitive job market. According to the BurningGlass 2015 Cybersecurity Job report, cybersecurity job openings have grown by 91% from 2010 to 2014, 325% faster than IT jobs overall, and “in the U.S., employers have posted 49,493 jobs requiring a CISSP, recruiting from a pool of only 65,362 CISSP holders nationwide.”

We’re facing a far greater number of attacks more sophisticated (and successful) than ever before – and there simply isn’t enough trained staff. Organizations face an unacceptable level of risk.

Section 2: Wait a Minute, What about All the Investments We’ve Made?

“All the king’s horses and all the king’s men, Couldn’t put Humpty together again.” – Mother Goose

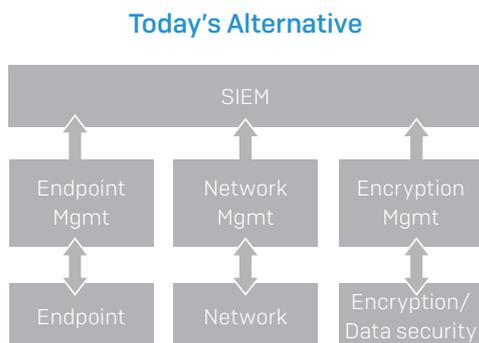
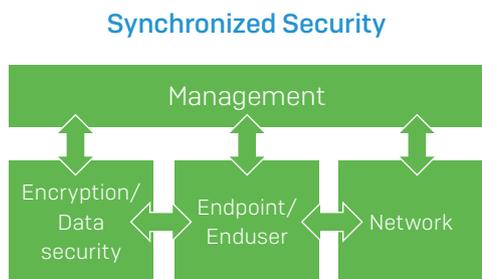
Layered and poorly integrated. Complex and myopic. Independent of nearby context. Decisions in isolation. All of these descriptions can be applied to our current security investments.

We still live in a world of independent and complex products, from antivirus, data encryption, web, mail, and network gateways to more modern products like suites, UTMs, sandboxes, endpoint protection, and response solutions. Attackers launch coordinated attacks on our entire IT ecosystem. It’s no wonder we’re struggling to keep pace. An attack might start at an endpoint, but look at how quickly it can propagate across an entire network, stealing unencrypted information over our outbound internet connection.

IT security professionals 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. As we have seen, data loss and risk continues to increase, with no sign of letting up. Staff is stretched thin. 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.



Synchronized security offers a simpler, more responsive and more effective security model. Due to high levels of automation, synchronized security also requires far less security professionals to manage and maintain.

Section 3: Synchronized Security, a New Approach

A New, Revolutionary Idea

"You say you want a revolution, well, you know we all want to change the world." – The Beatles, Revolution

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. Synchronized security hands each of those guards a smartphone so they can coordinate and communicate with each other quickly and efficiently. It's a simple, but at the same time revolutionary concept.

What if wanted to start over with a fresh approach to IT security? A more successful approach, delivering better protection, that enabled automated and real-time communication between the network, endpoint security, and encryption solutions? That synchronized across the entire threat surface? One that was highly automated, to avoid needing more staff or increasing workloads?

To accomplish this, we need a system that is:

Ecosystem-centric. We must prevent, find, and stop breaches across the entire IT ecosystem by operating with full awareness of nearby objects and events.

Comprehensive. The solution would need to be comprehensive and cover our whole IT "system," multiple platforms, devices, users and data, in order to defend against coordinated attacks

Efficient. The solution must lower the team's workload as well as improve protection. It cannot add another layer of work for overburdened staff.

Effective. The solution must effectively prevent, detect, investigate, and remediate today's threats across the entire threat surface.

Synchronized Security: A Revolution in Protection

Data-centric. The solution is not focused only on devices and networks, but also protects valuable information wherever it lives, whenever it is accessed.

Simple. Simple to buy, simple to understand, simple to deploy, and simple to use.

This list seems like a tall order indeed. Today's IT security products are the opposite: threat-centric, complex point products, resource intensive and not as coordinated as the attacks they defend against. Clearly, innovation is needed to succeed. This challenge is summarized in Figure 2.

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

Delivering this simplicity with effectiveness in today's environment, requires a significant technology innovation, one we call the Sophos Security Heartbeat.

The Sophos Security Heartbeat

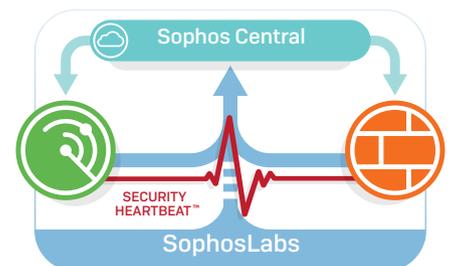
"Like the Beat Beat Beat of a Drum Drum Drum"

– Cole Porter, *Night and Day*

Synchronized security allows next-generation endpoint, encryption and network security solutions to continuously share meaningful information about suspicious and confirmed bad behavior across an entire organization's extended IT ecosystem. Leveraging a direct and secure connection called the Sophos Security Heartbeat, endpoint, encryption, and network protection act as one integrated system, enabling organizations to prevent, detect, investigate, and remediate threats in near real-time, without adding any staff.

For example, when the Sophos next-gen firewall detects an advanced threat or an attempt to leak confidential data, it can automatically utilize the Sophos Security Heartbeat to take a series of actions across both the network and endpoint to mitigate risk and stop data loss instantly. Similarly, if a protected endpoint is found to be compromised, synchronized security allows automated and near-instantaneous isolation of this endpoint, including temporary revocation of encryption keys, preventing it from leaking confidential information or sending sensitive data to a Command and Control server. This type of discovery, protection, and incident response, which ordinarily could take weeks or months, has been reduced to seconds with synchronized security.

Sophos Synchronized Security leverages the Security Heartbeat, Sophos Labs and Sophos Central to deliver simple, highly effective security across endpoints and networks.



Synchronized Security: A Revolution in Protection

For the first time, we also see encryption playing a meaningful role in threat protection. Encryption, encryption keys, and the ability to share and decrypt files are now tied directly to your security health, trust and integrity of the user, the systems and the applications. Because of this, risk can be assessed and action taken that enforces encryption policies, preventing rogue actors from obtaining protected information. And even if these encrypted files are stolen, they'll be unreadable to the attacker. In addition, mobile devices that are out of compliance with your policy can be blocked from accessing protected applications and data. This combination of protecting users, networks, devices, and data in an integrated and synchronized fashion is unique, powerful, and easy.

Summary

"A connecting principle, linked to the invisible, almost imperceptible, something inexpressible. If you act, as you think, the missing link, Synchronicity." - The Police, Synchronicity.

We're surrounded by cyber risks. More attacks, growing complexity of those attacks, and not enough people to fight them create a perfect storm of IT security challenges, particularly for small to mid-sized organizations.

Existing layered approaches to IT security are not succeeding, and the efforts to solve their shortcomings with analytics are also falling short.

The current methods of complex, threat-centric, headcount-dependent, myopic solutions will not meet the needs of resource-constrained IT security teams. To reverse the trend of increasing incidents and breaches, we must take a much different approach than we have in the past.

We must implement new solutions that are simple yet effective, both automated and coordinated. In short, synchronizing security via technology innovations like the Sophos Security Heartbeat. By synchronizing protection of data, endpoints, and networks, security teams and infrastructures are now now equipped to quickly and effectively react and respond to today's threats. To learn more about Sophos Security Heartbeat, and to see how synchronized security from Sophos can help protect your organization better in today's high-risk environment, visit Sophos.com/heartbeat.

¹ Statistica.com

² Okta Business@work, 2015

³ Gartner, <http://www.gartner.com/newsroom/id/3055225>

⁴ Gartner, <http://www.gartner.com/newsroom/id/2905717>, 2014

⁵ Threatgeek.com

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

Oxford, UK

© Copyright 2016. Sophos Ltd. All rights reserved.

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK

Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2016-09-05 WP-NA [NP]

SOPHOS