SOPHOS

Security made simple.

Synchronized Security; A Revolution in Protection

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

Increased Attack Surface, Complexity and Sophistication of Attacks

Business today, whether small or large, must live and learn to thrive in a world of ever increasing Cyber Risk. Risk is rising for many reasons, including an increasing attack surface and the increasing complexity and sophistication of attacks.

First, with the large number of mobile devices and cloud services being used by employees, and virtual and cloud infrastructure being deployed by organizations of all sizes, the so-called "attack surface" has expanded dramatically. Consider these facts:

- The average user in the UK has 3.1 connected devices (source: statista.com)
- Companies with 250-999 employees use 16 approved cloud Apps, those with 1000-4000 use 14, while the largest enterprise only use 11 ". (Source: Okta Business@work, 2015)
- Industry estimates puts Infrastructure as a Service revenues at greater than $16B in 2015 (Source Gartner, http://www.gartner.com/newsroom/id/3055225)
- By the end of 2015, 4.9 billion "things" will be connected to the Internet. By 2020, that number will grow to 25 billion. (Source: http://www.gartner.com/newsroom/id/2905717, 2014)

With this increased attack surface, the world has seen an increasing number of attacks and successful breaches leading to increased data losses.

Second, the complexity and sophistication of attacks has continued to increase. Even less skilled attackers have access to sophisticated commercially supported toolkits on the grey and black markets. These "kits" are well tested and even commercially supported and not always easy to detect or defeat. For example, the UnRecom Remote Access Tool Kit, or RAT, first reported on Threatgeek.com in May 2014, has gone through several iterations including AlienSpy and most recently JSOCKET, and has been implicated in everything from data breaches to having a role in a political assassination (Source:Threatgeek.com).

Unfortunately, small and midmarket businesses seem to be disproportionately victims of the growing number of confirmed data loss reports. According to the Verizon 2015 Data Breach Investigation Report:

- In 2014, there were 79,790 security incidents of which 2,122 were confirmed data losses
- This represents a respective 26% increase in security incidents and an astronomical 55% increase in data breaches compared to 2013.

- Midmarket enterprises accounted for over 53% of confirmed and classified data losses, despite accounting for only 1.4% of incidents.
- The smaller business incidents and data losses take place across a wide variety of industries, with Financial Services, Accommodation, Retail, and Healthcare leading the way

The combination of increased attack surface with the complexity of attacks leading to increased losses should raise the alarm and force the question of what we should do differently.

Small Teams, Stretched Resources, Tight Labor Market

While attacks and breaches increase, the natural reaction would be to "throw more people" at the problem. However small and midsize business have small IT security teams, and expanding or re-deploying resources, even it were an effective strategy is not a realistic option for smaller organizations. As you can see from Figure dedicated IT Security teams at small and mid-size are very limited in size and bandwidth:

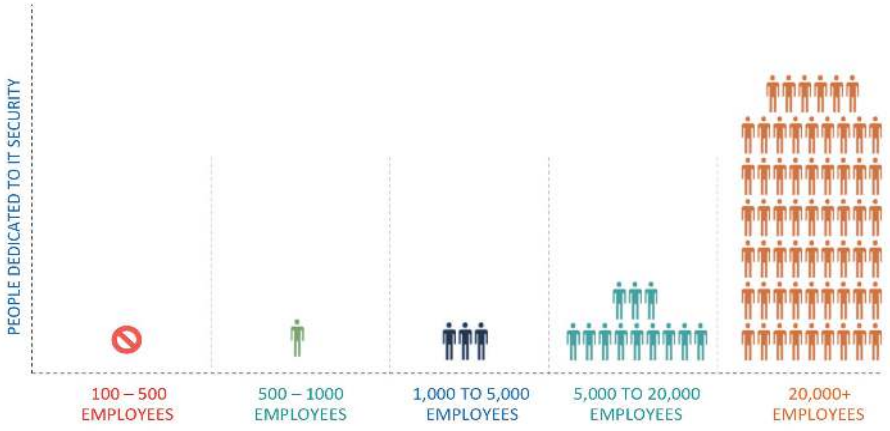

Figure 1: Midmarket IT Security Organizations are Small and Resource Constrained (Source: US Dept of Homeland Security, 2014)

And even if management desires to expand their security teams, they are faced with a tight and 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"

In summary, the combination of increased risk, increased volume, sophistication and success of attacks, and small and resource constrained teams have left organizations at an unacceptable level of risk.

Section 2: Wait a Minute, What about All That Investment 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. From yesterday's anti-virus, IPS, and Web, mail and network gateways, to today's suites, UTMs, sandboxes, and Endpoint detection and response solutions, we still live in a world of independent and complex products. Faced with attackers who are launching coordinated attacks at our entire IT ecosystem, it's no wonder we are not keeping pace. An attack may start at an endpoint, but then will propagate across our network, finally stealing our information over our outbound Internet connection.

In response to this reality, IT security professionals and vendors 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 in order to quickly detect and remediate risk and stop data loss is proving as hard as 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 lack of them, speak for themselves. As we have seen, data loss and risk continues to increase, with no sign of abating. Staff is stretched. According to a recent Ponemon Institute report, 74% of breaches go undiscovered for more than 6 months. And worst of all, mid-market companies seem to be having an even harder time at mitigate this risk than their better resourced larger peers. Clearly, the answer is not another un-integrated point product, more consoles, more people, or unwieldy SIEMs. In total these approaches are not succeeding. We must find a better and more effective approach.

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 and endpoint security as completely different entities. It is just like putting one security guard outside the building and another inside the building, but not allowing them to talk to each other. Synchronized security is revolutionary and yet so simple – we handed each security guard a 2-way radio, so that when one of them spots an issue the other knows about it instantly.

What if we started over with a fresh and radical approach that started with a different mindset in order to enable IT Security teams to successfully defend against today's Cyber risk reality? One that delivered better protection and by enabling automated and Real-time communication between network and endpoint security solutions. One that was synchronized across the entire threat surface? And one that was highly automated, so it couldw do all this without adding staff or workload. 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 and devices, to defend against attackers who attack the whole, not a piece part

Efficient – The solution must lower the team's workload while improving protection. It cannot add another layer of technology and workload

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

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, non-comprehensive, resource intensive and in total, 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	Desired Solution
Threat centric, operates independent of nearby objects and events	Ecosystem centric, operates with full awareness of nearby objects and events
Specialized silo'd point products	Coordinated products
Effectiveness requires increased headcount	Effectiveness through automation and innovation; no increased headcount
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 and network security solutions to continuously share meaningful information about suspicious and confirmed bad behaviour across an entire organization's extended IT ecosystem. Leveraging a direct and secure connection called the Sophos Security Heartbeat, endpoint 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.

As an 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 discovered to be compromised, synchronized security allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential information or sending data to a Command and Control server. This type of discovery and incident response, which could take weeks or months, has been reduced to seconds with synchronized security.

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.

Today's world of Cyber risk, with its increased risk surface and complexity and volume of attacks, combined with small teams and very tight labor markets creates a very challenging world for IT security teams in small and midsized organizations. Today's layered approaches are not succeeding, and the efforts to solve their shortcomings with analytics and more analysts are also falling short.

Synchronized Security; A Revolution in Protection

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 in the past. To do this, we must implement new solutions that are simple, yet effective, automated and coordinated, in short synchronized via technology innovation such as the Sophos Security Heartbeat. The good news is that this capability is available today from Sophos and can be evaluated easily. To learn more and see how synchronized security from Sophos can enable you to win in today's risky world, 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
© Copyright 2015. 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.

2.15.GH.wpna.simple