SOPHOS

Cybersecurity System Buyers Guide

With 83% of IT managers in agreement that cyberthreats have become harder to stop over the last year, more and more organizations are moving from isolated security point products to an interconnected cybersecurity system.

Choosing a cybersecurity system is a big decision. And with many vendors talking about cross-product integration, what should you look for and how can you be sure of making the right choice?

In this guide we explore the key factors to consider when choosing a cybersecurity system. We also take a look at how Sophos' Synchronized Security system stacks against other vendors, including Fortinet, SonicWall, Cisco, Palo Alto Networks, and Microsoft.

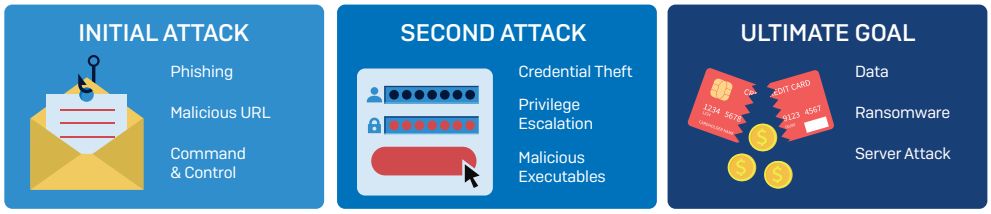
Point products are no longer enough

Despite constant technology enhancements and heavy financial investment, the reality is that cybersecurity is not getting any easier for today's organizations. Indeed, 87% of IT managers agree that malware threats have become more complex over the last year, and businesses lose on average seven working days a month identifying and fixing infected computers.[1]

Cyberthreats work as a system

To understand the root cause of these issues, we first need to look at the threats we're trying to stop. Cybercriminals don't use single techniques and technologies in their attacks. Instead, they use multiple techniques in connected, coordinated assaults.

For example, they might start with a phishing email that includes a malicious URL, clicking on which connects you to a command and control center. Using a combination of credential theft, privilege escalation, and malicious executables, they then carry out their ultimate goal, which could be stealing your data, or holding your data for ransom.



Unconnected point security solutions struggle to fight back against these complex, coordinated attacks. This is where cybersecurity systems come in: integrated products working together to outsmart today's hackers.

> **System**, noun.
> A regularly interacting or interdependent group of items forming a unified whole.
>
> Source: Merriam-Webster

Your IT infrastructure works as a system

Your IT system is fundamental to the effective, safe-running of your organization. This connected network of devices, networks, data and workloads enables people to work productively – sharing data, accessing resources, tracking activities.

As technology has evolved, so have our IT systems, with mobile devices and cloud-based workloads sitting happily alongside more traditional elements. While this IT expansion is a business enabler, it has also created visibility challenges for today's organizations: only 16% of CISOs are able to collect, analyze, and respond to 75% or more of their security event telemetry.[2]

You can't control what you can't see. By correlating and consolidating data from across the IT infrastructure, a cybersecurity system can deliver enhanced visibility into security risk and user behaviors across the organization. It enables IT to see hidden threats and take informed action.

What makes a system

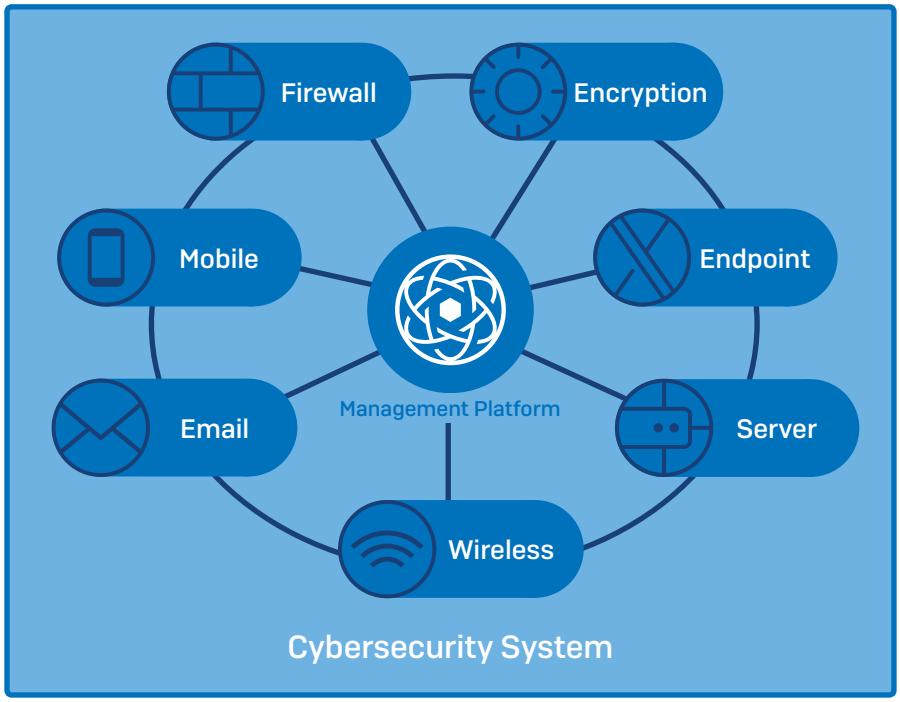
While security vendors are increasingly talking about cross-product integration and cybersecurity systems, what they mean can vary significantly. With this in mind, it's worth taking a moment to consider what exactly a cybersecurity system is.

At the heart of any effective system there are four core elements:

1. **Central management:** See and control everything in one place
2. **Integrated components:** Different elements working harmoniously together
3. **Automated actions:** Sequential behavior based on pre-agreed criteria
4. **Extendability:** The system can grow as requirements grow

These four elements are what transform point products into a system. The stronger each of these components, the stronger the system. A system with deep integration will outperform one with weak integration.

The same principles apply to cybersecurity. The cybersecurity technology platform sits at the heart of the system, enabling IT teams to manage all their security services (endpoint protection, firewall, mobile, email, wireless, encryption, user education) via a single interface. These services actively work together, sharing information and automatically responding to issues and events. The greater the integration, the more effective the system.



Central management, integrated components, automated actions and extendability are at the heart of a cybersecurity system

Delivering value to the business

A cybersecurity system should add value to the whole business as well as the IT team. An effective solution will enable you to:

- **Mitigate cyber risk.** Reduce your exposure to attack and significantly enhance response times in the event of an infection.
- **Increase visibility.** Get deeper and broader insights into your security across your whole estate, enabling you to make informed, accurate decisions.
- **Improve productivity.** Reduce the impact of cybersecurity on both the IT team as well as users across the whole organization.
- **Save money.** By moving from point products to a cybersecurity system, you can reduce onboarding, integration, and training costs, as well as the day-to-day system management overheads. Non-IT functions such as purchasing and legal also benefit from consolidating vendors.
- **Demonstrate the value of security.** By reducing time spent fixing day-to-day issues, a cybersecurity system can free up IT teams to work on business-focused projects. The enhanced protection and resulting drop in user downtime also enables the wider organization to appreciate the value of security.

What to look for in a cybersecurity system

To get maximum benefit from a cybersecurity system there are four key aspects to consider.

1. **Breadth of Protection**
   You may not need or want to adopt an all-in cybersecurity system at once, but you should ensure there are options to extend it in the future. Most people start with a small system, for example two security components working together, and then expand to include other solutions as and when they are ready. To future-proof your investment, ensure that your system can grow with your business.
   - **Range of security services.** How extensive is the cybersecurity system? What products are available to you should you need them? Does it meet your broader cybersecurity needs or just focus on one area?
   - **Communication between components.** How do the products share information? Products with a simple one-way communication are only able to deliver limited additional benefits as part of a system. Conversely, products that continuously share information across the system offer a much wider range of security and resourcing advantages.
   - **Ease of expansion.** How easy is it to add new products to the cybersecurity system? And how easy is it to get up and running with the new technologies?
   - **Additional costs.** Do you need to buy additional products or subscriptions to get the benefits of a cybersecurity system, above and beyond the individual solutions? When considering costs, think about both the cost of purchasing security products as well as the cost of training and on-boarding.

2. **Product Integration**
   The point of a security system is to be more than the sum of the individual parts. Individual products working together to deliver benefits that are not possible on their own. The core benefits of a security system fall into two camps: automation and visibility. Key areas to explore are:

   - **Zero-touch, automated response.** How do the products work together to automate previously manual tasks? What level of automated incident response does it offer? For example, if an infection is detected, does the system simply flag it for the admin to take action, or does it automatically secure the device, clean up the infection, and then bring the system back online once it's healthy?
   - **Cross-estate visibility.** How does the product integration elevate your visibility across the organization? Does it deliver real-time incident analysis and cross-estate reporting, giving you instant insights that you can act on? How useful is it at helping you identify unknown threats?

A cybersecurity system should deliver zero-touch response and cross-estate visibility.

When considering product integrations think about what will be most useful to your organization. You need to consider what your challenges are, and what system capabilities will be most advantageous to you.

3. **Operational Efficiency**
   The easier the system is to use, the better you can take advantage of the capabilities it offers. Highly complex, difficult-to-use solutions are of limited benefit and can be onerous for the IT teams that need to manage them. Particular areas to focus on are:

   - **Usability.** How quickly and easily can you deploy, monitor, and manage the system? How many management consoles do you need to use? The more you can do in one place the better.
   - **Overhead.** Is the system cloud-based or do you need to fund and maintain on-premises servers?
   - **Consistency.** Are the screens and visual representations consistent across the displays? Once you're familiar with one display, can you easily interpret others, or do they all look different?

4. **Product Leadership**
   Moving to a synchronized security system should not involve compromising on protection. You should get the best of both worlds. Start with products that are great on their own, and even better together.

   - **Industry validation.** Look for products that perform well in both efficacy tests (for example, SE Labs, AV-Test) and also market analyst ratings (such as Gartner Magic Quadrant reviews).
   - **Customer feedback.** What do customers using the cybersecurity system have to say? What benefits have they enjoyed? And has it lived up to its promises?
   - **Recognized leaders.** Consider products that are recognized as leading by industry analysts.

How vendors stack up

Breadth of protection

Security Products	Sophos Synchronized Security	Fortinet Fortinet Security Fabric	Microsoft Intelligent Security Graph	SonicWall Capture Cloud	Cisco Stealthwatch and Identity Services Engine (ISE)	Palo Alto Application Framework
Endpoint	✓	✓	✓	✓ (SentinelOne)	✓	✓ (Traps)
Endpoint Detection and Response (EDR)	✓	✓	✓	✓	✓	✓
Server	✓	✓	✓	✓	✓	✓
Firewall	✓	✓		✓	✓	✓
Email	✓	✓		✓	✓	
Mobile	✓		✓		✓	
Wireless	✓	✓		✓	✓	
Disk encryption	✓		✓			
Security awareness training	✓					
Cloud-based workloads	✓	✓	✓		✓	✓
Additional subscriptions required for products to work together		✓[1]			✓[2]	✓[3]

1. FortiGate Endpoint Telemetry and Compliance license required to integrate FortiClient in Security Fabric. IOC service on FortiAnalyzer required to get visibility of compromised hosts.
2. Cisco Network Orchestrator Trusted Access required.
3. Threat Prevention/ WildFire subscription required.

Product integration

	Zero-touch automated response	Cross-estate visibility
Sophos Synchronized Security	‣ Continuous monitoring of device health status via Security Heartbeat™, enabling automated incident response ‣ Automatic isolation of compromized endpoints wherever the infection is detected: endpoint or network ‣ Lateral movement prevention stops threats traversing the network ‣ Automatic restriction of Wi-Fi access for compromised endpoints ‣ Automatic restriction of Wi-Fi access for non-compliant mobile devices ‣ Automatic scanning of endpoint devices on detection of malicious email ‣ Encryption keys are automatically revoked on detection of malware or an intruder	‣ Synchronized App Control identifies all apps on the network, including previously unknown network and cloud apps ‣ Threat Cases provides full chain of events for an incident, including all files touched and URLs/IPs communicated with ‣ Correlation of network traffic to individual apps on individual computers
Fortinet Fortinet Security Fabric	‣ Automatic isolation of compromized endpoints if the firewall detects an infection	‣ Displays a graphical map of all connected Security Fabric devices ‣ Endpoint status monitoring identifies if FortiClient is installed ‣ Security Rating shows the security posture of the organization (licensed separately)
Microsoft Intelligent Security Graph	‣ Endpoint investigation can be triggered automatically in Defender ATP	‣ CASB uses the Windows Defender ATP client to identify unknown cloud apps ‣ Windows Defender ATP and Office 365 ATP share data to help track a threat from email delivery through endpoint execution
SonicWall Capture Cloud	‣ Automation of complex firewall deployment and management tasks ‣ Endpoint protection client simplifies deployment and management of TLS/SSL certificates	‣ Cloud App Security (CAS) provides visibility of cloud apps (in Analytics license)
Cisco Stealthwatch and Identity Services Engine (ISE)	‣ Network access control provided by ISE based on compliance and other factors ‣ Cisco Threat Response allows security operations teams to manually investigate and respond to threats	‣ Cisco AMP tracks threats across email, firewall and endpoint
Palo Alto Application Framework	‣ Response capabilities depend on the application used. Remediation is typically enforced at the network layer, such as blocking URLs or IP addresses	‣ Apps can access security intelligence from the network and endpoints

Operational efficiency

Management Efficiency	Sophos Synchronized Security	Fortinet Fortinet Security Fabric	Microsoft Intelligent Security Graph	SonicWall Capture Cloud	Cisco Stealthwatch and Identity Services Engine (ISE)	Palo Alto Application Framework
Cloud hosted management	✓		✓	✓	✓	
Single management console	✓	✓		✓		
Common interface across all products	✓	✓		✓		

Product leadership

Product Leadership	Sophos Synchronized Security	Fortinet Fortinet Security Fabric	Microsoft Intelligent Security Graph	SonicWall Capture Cloud	Cisco Stealthwatch and Identity Services Engine (ISE)	Palo Alto Application Framework
Gartner Magic Quadrant for Endpoint Protection Platforms (2018)	Leader	Niche Player	Visionary	Visionary	Visionary	Niche Player
Gartner Magic Quadrant for UTM/Enterprise Firewalls (2018)	Leader	Leader	NA	Challenger	Leader	Leader

Synchronized Security from Sophos

First launched in 2015, Synchronized Security brings together Sophos' market-leading endpoint and network protection in a powerful, deeply integrated cybersecurity system. At the heart of Synchronized Security is Sophos Central, an intuitive security platform that enables IT teams to see, manage, and control everything through a single web-based interface. Products share real-time information via a Security Heartbeat™, enabling them to respond automatically to threats and deliver unprecedented cross-estate cyber risk visibility.

Customers agree that Synchronized Security transforms cybersecurity.

90% of customers agree they have greater control over their network traffic with Synchronized Security

85% of customers agree Synchronized Security has improved their security posture

84% of customers agree Synchronized Security helps deal with the increasing pressure on IT[3]

For more information on Synchronized Security and how it can transform your cybersecurity, visit www.sophos.com/synchronized.

Learn more at www.sophos.com/synchronized

This information in this document is based on Sophos's interpretation of publicly available data as of the date of preparing this document. This document has been prepared by Sophos and not the other identified vendors. The features or characteristics of the products under comparison, which may have a direct impact on the accuracy or validity of the comparison, are subject to change. This document is intended to provide a broad understanding and knowledge of factual information about various products and may not be exhaustive. Anyone using this document should make their own purchasing decisions based on their requirements, research original sources of information, and not rely only upon this document when selecting or purchasing any product. Sophos makes no warranty as to the reliability, accuracy, usefulness, or completeness of information in this document. **The information in this document is provided "as is" and without warranties of any kind.** Sophos retains the right to modify or withdraw this document at any time.

Endnotes

1. The Dirty Secrets of Network Firewalls, Sophos, 2018
2. Forbes.com, Chief Information Security Officer Priorities For 2019, January 17, 2019
3. Respondents who expressed an opinion in survey of Sophos Synchronized Security customers Q2, 2018

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

North America 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

SOPHOS