

What to Look for in a Cybersecurity System

With 83% of IT managers in agreement that cyberthreats have got harder to stop over the last year, more and more organizations are considering moving to a cybersecurity system rather than relying on unconnected security point products. In fact, ESG Labs research has revealed that 62% of enterprise organizations are now willing to buy a majority of their security technologies from a single vendor¹.

Choosing a cybersecurity system is a big decision - you want a solution that will meet both your current and future needs. But what should you look for to be sure of making the right choice? In this guide we explore the key factors to consider when choosing a cybersecurity system, including the eight attributes ESG Labs believe every cybersecurity technology platform must offer¹. We also take a look at how Sophos Synchronized Security stacks against these criteria.

Benefits of a cybersecurity system

Cybersecurity systems offer a number of advantages over a traditional, siloed point product approach to IT security:

- **Faster, better protection:** Automated incident response from products engineered to work together significantly reduces response time from hours to seconds. Real-time cross-product communication enables the discovery of previously hidden threats and unseen risks.
- **More impactful security insights:** Real-time incident analysis and cross-estate reporting give IT teams the deeper, more useful insights they need to manage their security effectively.
- **Simpler IT security management:** With all security product managed through a single technology platform, IT teams no longer need to spend time jumping from console to console. Time spent becoming familiar with new products is greatly reduced thanks a single cross-platform approach.

Top five factors to consider when choosing a cybersecurity system

Cybersecurity systems vary greatly in scope, coverage, and benefits. When choosing a cybersecurity system there are a number of key factors you should consider:

1. Level of product integration.

The greater the level of product integration, the more powerful the cybersecurity system. 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 and have adaptive, automated policies offer a much wider range of security and resourcing advantages.

2. Breadth of protection.

The needs of organizations change. A cybersecurity system should provide many different layers of security and be able to grow based on your organization's needs. Focus on systems that offer products and technology to cover all your IT security needs. 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.

3. Ease of use.

Cybersecurity systems are not new. Historically, advanced cybersecurity systems used to be exclusive to the largest organizations. They would manually stitch together multiple point products and burn significant IT hours with whole IT teams triaging the results. Today, technology enhancements mean that cybersecurity systems are now realistic options for organizations of all sizes. It's important to choose a solution that you can both activate and also manage easily.

What to Look for in a Cybersecurity System

4. Quality of protection.

Moving to a cybersecurity system should not involve compromising on protection. Fortunately, you can have the best of both worlds: products that are great on their own, and even better together. Look for products that perform well on their own as confirmed in independent, real-world testing, as well as working together in a system.

5. Future roadmap.

Cybersecurity is a fast-moving industry, with both threats and protection technologies advancing at an incredible rate. In this environment, it's important to ensure that your security platform will continue to evolve ahead of the threats. To future-proof your investment, ensure you choose a system with a strong roadmap that will further enhance your protection while relieving the pressure on IT.

What to look for in a security technology platform

The foundation of a cybersecurity system is the technology platform on which it's based. ESG Labs identified eight attributes they believe every cybersecurity technology platform must offer and then asked 232 cybersecurity professionals to identify the three they considered the most important [1]. Their survey revealed that, in descending order, IT professionals most value:

1. Coverage that includes **major threat vectors** like email and web security. [38%]
2. **Central management** across all products and services. [33%]
3. Capabilities across **threat prevention, detection, and response**. [31%]
4. Coverage that **spans endpoints, networks, servers, and cloud-based workloads**. [27%]
5. **Cloud-based back-end services** (i.e., analytics, threat intelligence, signature/rules distribution, etc.). [26%]
6. **Openness** (i.e., open APIs, developer support, ecosystem partners, etc.). [22%]
7. A combination of tightly-coupled **products and services** (i.e., products and managed service options offering central command-and-control). [20%]
8. **Multiple deployment options** (i.e., on-premises, cloud delivered, hybrid, etc.). [18%]

While all these criteria are valuable, the larger and more demanding your organization is, the greater the number of criteria you should look to achieve in your cybersecurity system.

How Sophos Synchronized Security Stacks Up

Synchronized Security isn't just a product you buy – it's a concept that enables Sophos endpoint and network security solutions to work in tandem, sharing threat intelligence to offer a unified front against threats. Managed through the Sophos Central platform, Synchronized Security connects Sophos' award-winning product portfolio into one easy-to-use platform. Customers can start with just a few products and add others as their needs grow. See how it stacks up.

| Area | Factor | Sophos Synchronized Security |
|----------------------|------------------------------|---|
| Cybersecurity System | Breadth of protection | Sophos Synchronized Security encompasses Endpoint, Server, Firewall, Email, Mobile, Wireless, Encryption, and Phishing Training. Products work together and respond automatically to threats across the system. 85% of customers agree Sophos Synchronized Security has improved their security posture. ² |
| | Level of product integration | Each product shares threat, health, and security information in real time via a patented Security Heartbeat™. Adaptive policies enable them to respond automatically to threats. |
| | Ease of use | Deploy, monitor and control all your IT security through a single intuitive web-based console: Sophos Central. 81% of customers agree it's easy to get started with Sophos Synchronized Security, and 84% agree it's helped relieve the pressure on IT. ² |
| | Quality of protection | Sophos is committed to open, real-world testing for all products and is a founding member of AMTSO (www.amtso.org). Sophos products have received many awards, including: #1 for Enterprise and Small Business Endpoint protection in SE Labs testing April-June 2018. ³ Best UTM Solution at 2018 SC Awards. ⁴ 100% protection score for Android malware in every AV Test since September 2014. ⁵ 'Leader' in the Gartner Magic Quadrants for Endpoint and UTM. ⁶ Visit www.sophos.com for more details of product reviews and awards. |
| | Future roadmap | Synchronized Security has been at the heart of the Sophos strategy for many years. It is backed by a strong roadmap for both individual products and the complete cybersecurity platform. |

What to Look for in a Cybersecurity System

| Area | Factor | Sophos Synchronized Security |
|--|--|--|
| ESG Labs Technology Platform Attributes ¹ | Coverage that includes major threat vectors like email and web security. | Yes. Sophos provides extensive, powerful protection from email and web-borne threats, as well as other vectors such as infected USB devices. |
| | Central management across all products and services. | Yes. Manage, monitor and control security products through the Sophos Central platform. |
| | Capabilities across threat prevention, detection, and response. | Yes. Sophos Synchronized Security enables your defenses to be more coordinated than the attackers. It elevates your protection by blocking complex attacks, identifying hidden threats and unknown risks, and automatically responding to incidents. |
| | Coverage that spans endpoints, networks, servers, and cloud-based workloads. | Yes. Sophos is a leader in both endpoint and network security, protecting both on-premises and cloud-based workloads through integration with Microsoft Azure and AWS. |
| | Cloud-based back-end services (i.e., analytics, threat intelligence, signature/ rules distribution, etc.). | Yes. Sophos Central is a cloud-based platform that delivers instant security updates and real-time analytics. Sophos protection is powered by SophosLabs, a global network of threat experts that runs 24 hours a day, 365 days a year. |
| | Openness (i.e., open APIs, developer support, ecosystem partners, etc.). | Partial. Sophos integrates with Remote Monitoring and Management (RMM) and Professional Services Automation (PSA) systems, enabling easy management by managed security partners. The API gateway within Sophos Central enables integration with nearly any off-the-shelf Security Information and Event Management (SIEM) solution. A broader API program is on the roadmap. |
| | A combination of tightly-coupled products and services (i.e., products and managed service options offering central command-and-control). | Yes. Sophos works with a global network of security partners who offer a wider range of managed service options, enabling customers to choose the level of support that best suits their organization. |
| | Multiple deployment options (i.e., on-premises, cloud-delivered, hybrid, etc.). | Yes. Sophos offers a range of deployment options, including on-premises, cloud-delivered (AWS, Azure), and hybrid. However you deploy you can manage your protection through a single web-based console. |

Conclusion

Sophos Synchronized Security ticks all the boxes for a modern cybersecurity system by delivering better protection, impactful insights, and a simpler approach to IT management. Whether your needs are small or great, Sophos Synchronized Security ensures that your organization has the best protection on the market, and saves your IT team valuable time by automatically remediating issues.

For more information on Sophos Synchronized Security and to see it in action visit www.sophos.com/synchronized.

Citation:

¹ [ESG Labs Blog](#), August 29, 2018.

The views, opinions, and information in this evaluation of Sophos Synchronized Security against ESG Labs' Technology Platform Attributes are those of Sophos alone, and do not represent any view, opinion, or endorsement from ESG Labs.

² Respondent who expressed an opinion in survey of Sophos Synchronized Security customers Q2, 2018.

³ SE Labs endpoint protection test report (April - June 2018).

⁴ 2018 SC Awards.

⁵ AV-TEST Best Android Security Awards.

⁶ Gartner Magic Quadrant for Unified Threat Management, Jeremy D'Hoinne, Adam Hills, Rajpreet Kaur, 20 June 2017. Gartner Magic Quadrant for Endpoint Protection Platforms, Ian McShane, Eric Ouellet, Avivah Litan, Prateek Bhajanka, 24 January 2018.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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