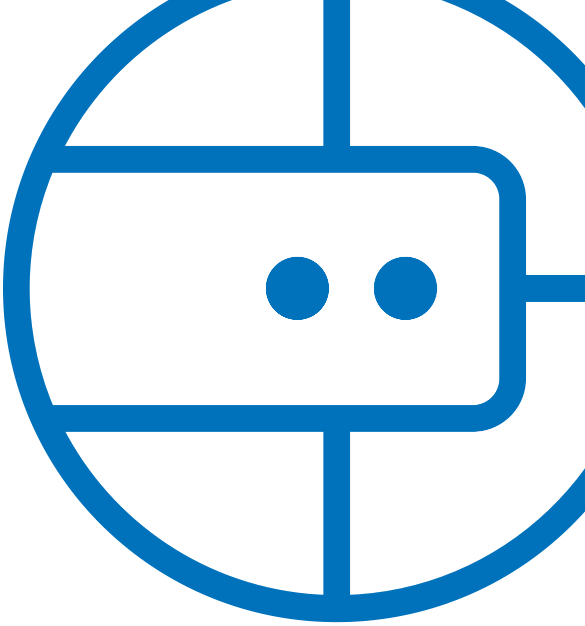
SOPHOS



Server Protection Buyers Guide

Cyber threats to servers continue to evolve in complexity and viciousness at an alarming rate. Devastating ransomware outbreaks such as WannaCry and NotPetya highlighted the need for strong anti-ransomware capabilities. Systemic vulnerabilities exploited by the likes of Spectre and Meltdown showed that anti-exploit, application control, and investigative tools such as EDR are key components of any server security plan.

As servers are often an organization's most valuable endpoints, the pressure is on for IT managers to select highly effective protection. It is not enough to run a security solution designed for desktops on your servers – you need solutions designed with server workload protection at their core.

This guide aims to give you practical advice on key features and capabilities to look for when selecting security for your servers, as well as questions to ask vendors to make sure that features work exactly as they should.

Server Environments

Depending on the needs of your organization, you may be running your own servers on-premises, hosting your data in the public cloud, including Amazon Web Services (AWS), Microsoft Azure, or the Google cloud, or any hybrid of these. So as a bare minimum you need a security solution that lets you easily manage these different setups in a consolidated fashion.

Ideally, that solution will offer additional benefits, such as consistent policy deployment across your servers that can be managed centrally. Automated deployment (such as via scripting) of server protection in the cloud is vital so they can be spun up (and down) when necessary to meet demand, without interaction from the server admin.

And straightforward licensing options are more important than ever before as organizations opt for mixed deployment environments. Look for a vendor that offers a single license type, whether cloud, on-premises, or a mixture of the two and save yourself from a complicated mix-and-match process.

Key Product Capabilities and Features

Modern server security has evolved to stay ahead of increasingly advanced threats. To keep your servers secure, whether on-premises or in the cloud, look for a range of features that defend against unknown threats, ransomware, exploits, and hackers:

- **Anti-ransomware** – Some solutions contain techniques specifically designed to prevent the malicious encryption of data by ransomware. Often techniques that are specifically anti-ransomware will also remediate any impacted files – by rolling the file back to an unaffected state, for example. Ransomware solutions should not only stop file-targeting ransomware, but also disk ransomware used in destructive wiper attacks that tamper with the master boot record. And specific to servers is the need to stop remote or rogue endpoints from encrypting files on network shares or other connected servers.
- **Server lockdown/whitelisting/default deny** – Prevent unauthorized applications from running on your servers by whitelisting permitted applications. Buyers should look for a solution that can automatically identify trusted applications, and also allows for user customization to minimize the time and effort required to create a secure ruleset. Additionally, locking down or unlocking a server should not require downtime.
- **Anti-exploit** – Anti-exploit technology is designed to deny attackers by preventing the tools and techniques they rely on in the attack chain. For example, exploits like EternalBlue and DoublePulsar were used to execute the NotPetya and WannaCry ransomware. Anti-exploit technology stops the relatively small collection of techniques used to spread malware and conduct attacks, warding off many zero-day attacks without having seen them previously, without requiring a signature. Comprehensive exploit prevention also provides protection for servers that can't be patched quickly, or even when there are no available patches.

[1] Gartner Top 10 Security Projects for 2018

- **Endpoint Detection and Response (EDR)** – EDR gives IT managers the power to proactively hunt down evasive threats and deep-dive into security incidents to understand their scope and impact. Ideally your chosen solution should include EDR that helps you hone in on areas of interest by reducing the amount of information you need to sift through and providing intelligence on suspect files to help you make an informed decision.
- **Anti-hacker** – Servers are a prime target for hackers as they typically contain an organization's most sensitive data. Look for solutions that include specific capabilities to stop persistent attacks by hackers occurring in real time. Some examples of required anti-hacker mitigations for servers include credential harvesting prevention, lateral movement prevention, code cave mitigation, privilege escalation protection, and process migration protection.
- **Machine learning** – There are multiple types of machine learning methods, including deep learning neural networks, random forest, Bayesian, and clustering. Regardless of the methodology, machine learning malware detection engines should be built to detect both known and unknown malware without relying on signatures. The advantage of machine learning is that it can detect malware that has never been seen before, ideally increasing the overall malware detection rate. Organizations should evaluate the detection rate, the false positive rate, and the performance impact of machine learning-based solutions.
- **Incident response/Synchronized Security** – Server tools should at a minimum provide insight into what has occurred to help avoid future incidents. Ideally, they would automatically respond to incidents, without a need for analyst intervention, to stop threats from spreading or causing more damage. It is important that server security tools communicate with other network security tools such as the firewall to detect compromised servers and provide visibility of all applications running on the server.
- **File integrity monitoring** – You want to protect critical system files and data from any unintentional changes, and optionally monitor key application locations. Sophos Central Server Protection continuously monitors and tracks unplanned and unexpected changes to help identify potential PCI DSS security breaches.
- **Application control** – Provides control over which applications are permitted to run on the server to reduce the attack surface. Ideally the vendor will filter applications by category to simplify and speed up configuration.
- **Centralized management** – The console should enable easy management and visibility of mixed server environments – for example, alerts, events, and reports all filtering through into one easy-to-access and easily understood view.
- **Workload discovery and protection** – Protection in the cloud depends on protecting each instance or VM [virtual machine] and each storage bucket. Discovery of workloads and storage buckets running in public cloud environments such as Amazon Web Services (AWS) and Microsoft Azure is essential because attackers have been known to take advantage of unused cloud regions and repurpose them – for cryptomining, for example. Products with native API integration with public cloud platforms display new workload instances and storage, including in regions that may not be actively in use.

Management and Reporting

Most of the time you aren't logging into your servers unless there is an issue. Which means for management purposes there are two main requirements:

1. Straightforward deployment and monitoring of all your servers

2. Easy-to-use interface that lets you quickly respond if an issue arises

In many cases, deploying point solutions from multiple vendors for different servers in different environments can cause management challenges due to multiple consoles. This can quickly become a liability when dealing with larger server estates. Responding to a serious attack requires fast, decisive action that isn't hampered by wasted time spent trying to locate the critical information needed to make a decision. Look for solutions that consolidate information onto a 'single pane of glass,' making it as simple as possible to locate what's important.

Some solutions also offer the ability to integrate your server with your network security (firewall) and share threat intelligence. For example, if a server is identified as compromised, it can be isolated from the network to prevent further damage to your organization. Traffic and applications from the server can also be accurately seen, allowing for prioritization of important applications or denying of unwanted apps.

For ease of deployment, allowing scripted setup – particularly for cloud deployments – means a server admin's time can be spent elsewhere. Default-deny application whitelisting, or category-based application control, allows for faster configuration of what should and should not be permitted to run on a server, versus a purely manual setup.

Product Comparison Checklist

After reading the previous sections to determine your base requirements, use this table to evaluate solutions from different vendors and assess their suitability for your organization.

Feature Comparison			Intercept X Advanced for Server with EDR	Trend Micro Deep Security	Symantec Cloud Workload Protection	Microsoft Enterprise Mobility + Security	CrowdStrike Falcon Prevent / Falcon Spotlight
MANAGE		Single Console to protect Server, Endpoint, Mobile, Email and Wi-Fi	✓	✗	✗	✗	✗
		AWS/Azure Workload Discovery	✓	✓	✓	✓	✓
		Automatic Scanning Exclusions (e.g., Exchange, SQL Server)	✓	✗	✓	✓	✗
		Virtualization: Thin Agent with Centralized Scanner	✓	✓	✗	✗	✗
PREVENT	REDUCE ATTACK SURFACE	Web Filtering (Block malicious websites)	✓	✓	✓	✓	✗
		Web Control (Control access to potentially inappropriate sites)	✓	✗	✗	✗	✗
		Application Whitelisting (Server Lockdown)	✓	✓	✗	✓	✗
		Category Based Application Control	✓	✗	✗	✗	✗
		Peripheral/Device Control	✓	✗	✗	✗	✗
		Patch Assessment	✗	✓	✓	✓	✓
	BEFORE IT RUNS	Machine Learning Malware Protection	✓	✓	✓	✓	✓
		Exploit Prevention	✓	✓	✓	✓	✓
		Data Loss Prevention	✓	✗	✗	✓	✗
DETECT		Anti-Hacker (e.g. credential theft and code cave protection)	✓	✗	✗	✓	✗
		Ransomware protection (behavior detection and rollback)	✓	✓	✗	Detection but no rollback	Detection but no rollback
		Disk and Boot Record Protection	✓	✗	✗	✗	✗
		File Integrity Monitoring (FIM) / Change Monitoring	✓	✓	✓	✓	✗
RESPOND		Synchronized Security (out-of-the-box integration with firewall)	✓	✗	✗	✗	✗
		Threat Chain Visualization	✓	✗	✗	Requires Defender ATP	✓
		Threat Hunting	✓	✗	✗	Requires Defender ATP	✓

Centralized Security

Protection for your servers forms a vital part of an organization's security strategy. But, factoring in other endpoint devices, mobile phones, network security, encryption, and more, managing all this can become difficult. Indeed, for many vendors, each additional area of security mandates an additional console and policy framework, many of which look and feel different and provide no integration of security across the various devices and infrastructure components.

Sophos Central lets you manage all your Sophos security solutions from one console. It is designed to be a single pane of glass, with an intuitive, consistent interface as you move between your different products. And best of all, Sophos products are engineered to work together, providing you with better security. For example, your servers work with your firewalls to automatically identify, isolate, and remediate compromised servers in seconds.

Evaluating Server Security:
Top 10 Questions to Ask

To evaluate a server protection solution, start by asking the vendor the following questions:

1. Does the product support different server deployments, such as on-premises, cloud, and hybrid?
2. Is automated application whitelisting/default deny included in the product at no additional charge?
3. Does the product have technology specifically designed to stop and then roll back ransomware?
4. What technology exists to prevent exploit-based and file-less attacks? What anti-exploit techniques are leveraged, and what types of attacks can they detect?
5. How does the product defend against persistent attacks by active adversaries?
6. What techniques does the product use to detect unknown malware threats? Does it use machine learning to always seek malicious attributes and behaviors?
7. For products claiming to leverage machine learning, do they have third-party confirmation of detection accuracy? What about false positive rates?
8. What visibility into an attack does the vendor provide, such as root cause analysis?
9. Does the product automatically respond to threats? Can it automatically clean up a threat in response to an incident?
10. Can the product natively integrate with public cloud (e.g. AWS/Azure/Google), including the ability to automatically discover cloud workloads?

Conclusion

As cyber threats continue to evolve in complexity and viciousness, it is vitally important to have effective protection in place on your servers. Understanding the threats and the key security technologies needed to stop them will enable you to choose the best possible server protection for your organization. And that protection needs to be designed with server workloads in mind – it isn't good enough to just run endpoint protection that hasn't been adapted for server environments.

Statements contained in this document are based on publicly available information as of June, 2018. This document has been prepared by Sophos and not the other listed vendors. The features or characteristics of the products under comparison, which may directly impact the accuracy or validity of this comparison, are subject to change. The information contained in this comparison is intended to provide broad understanding and knowledge of factual information of various products and may not be exhaustive. Anyone using the document should make their own purchasing decision based on their requirements, and should also research original sources of information and not rely only on this comparison while selecting a product. Sophos makes no warranty as to the reliability, accuracy, usefulness, or completeness of this document. The information in this document is provided "as is" and without warranties of any kind, either expressed or implied. Sophos retains the right to modify or withdraw this document at any time.

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

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

19-05-09 NA (PS)