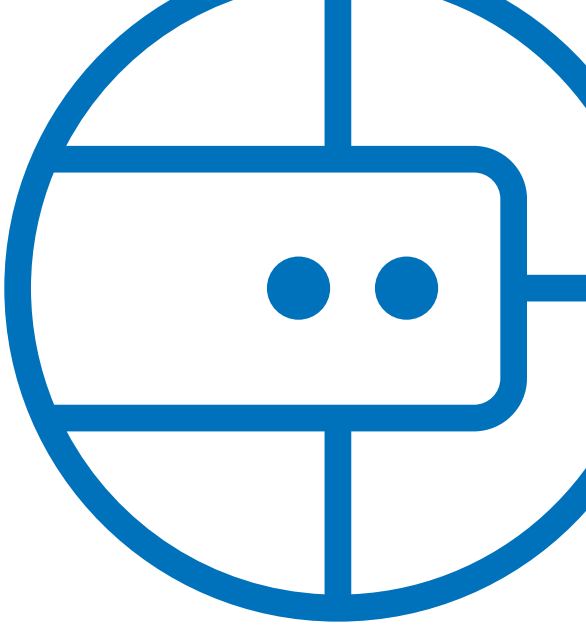
SOPHOS
Security made simple.



Server Protection Buyers Guide

Servers are different from other computing endpoints. They contain the majority of business-critical data and intellectual property, and run business-critical applications. Servers are the lifeblood of any organization, which is what makes them so appealing for attackers with financial or disruption-driven goals – an attack on your servers has the potential to create serious reputational harm and damage to you and your customers. Depending on their methods, attackers may also want to compromise those servers, including Linux servers, so they deliver malware to others.

Many servers aren't being protected

According to Verizon's 2016 Data Breach Investigations Report (DBIR)[1], servers are currently the most frequently attacked asset. Since users need continuous access to servers for file storage and business applications, keeping them secure, available, and performing at optimum levels is non-negotiable.

Businesses worldwide detected 42.8 million security incidents between 2010 and 2014[2], up by 48%. And it has only gotten worse since. The number of data breaches increased by an annual growth rate of 33% (CAGR)[3]while the number of malware sample families jumped from around 80 million to almost 350 million within the same period[4].

Industry data shows that servers are still under-protected, despite evidence that servers are a prime target for attacks. A March 2016 SpiceWorks survey by Sophos revealed that 49% of server admins do not run anti-malware on their servers. Worse still, Linux servers are protected even less. SophosLabs, examining just a single week's worth of malware-infected servers, found close to 180,000 new infections, and around 80% were hosted on Linux[5].

SophosLabs security expert Chester Wisniewski took a week's worth of known bad website data from SophosLabs and worked backwards to investigate some important questions: Which platform hosts the most malware? How does it get there? And what can we do about it?

Watch the podcast:

"Malware on Linux: When Penguins Attack"

[1] Verizon Data Breach Investigations Report 2016, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
[2] PWC, The Global State of Information Security Survey 2015
[3] Risk Based Security Security, Inc.
[4] SophosLabs
[5] SophosLabs, When Penguins Attack

To address today's threats, let's examine the top four considerations or suggested rules for selecting protection for your servers in light of the following concerns:

- Is anti-malware effective on Linux?
- What is the performance impact of running anti-malware on a server?
- Does it just produce too many false positives that result in loss of time and productivity?
- Will it interfere with business applications?
- Will it take too much time to deploy and manage?

Considerations for securing your servers

1. Effective server protection requires different approaches to address different types of attacks.

Not all server protection techniques are created equal. Many have become ineffective, or still focus on yesterday's threats. Malware perpetrators have become more organized and sophisticated, and have become emboldened by the financial rewards of their previous actions. These malware attacks pose a serious threat to the security of an organization's crucial applications. Worse still, many sources, including the Verizon DBIR[1] and a SpiceWorks survey by Sophos, reveal that servers, especially Linux servers, remained infected for a very long time and those infections often remained undetected, enabling ongoing exploitation and exfiltration of data.

The ever-growing and complex structure of many advanced threats makes it necessary to utilize more than just signature-based antivirus. Instead, we need to turn to a broad variety of next-gen anti-malware approaches, each capable of blunting different vectors of attack. Whether it's preventing an attack before it reaches the server, neutralizing it before it runs on a server, or detecting and stopping a running threat, all have become essential components of a next-gen strategy to provide effective server protection. Additionally, the growth of ransomware has made stopping these attacks as soon as possible crucial.

How Sophos Server Protection can help:

Sophos Server Protection protects both virtual and physical servers, running Windows, Linux, or UNIX operating systems. We are the only solution offering cloud-managed protection for servers that also includes HIPS (Host-based Intrusion Prevention System) behavior analysis, Server Lockdown with application whitelisting, and Malicious Traffic Detection, along with the ability to control what applications and peripherals can run on a server. This breadth of techniques, including the new advanced anti-ransomware capabilities that Sophos introduced with its new Sophos Intercept X endpoint product, enables you to blunt attacks with the most appropriate approach, whether from a known exploit, a previously unknown or zero-day attack, or a ransomware attack. Ransomware is the number one malware attack affecting organizations today, encrypting your files and holding them hostage until the ransom is paid, causing massive disruption to business productivity. Sophos uses innovative techniques offering you the right protection at the right time for your servers.

[1] Verizon Data Breach Investigations Report 2016, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Attack Vectors	Sophos Responds: The Right Protection at the Right Time
Ransomware tries to encrypt organization data	‣ CryptoGuard on the server prevents the malicious spontaneous encryption of data by all forms of ransomware—even trusted files or processes that have been hijacked. ‣ Server Lockdown prevents any untrusted applications from running. ‣ Application Control can block Wscript, which is often used by ransomware to run scripts. ‣ Anti-malware and HIPS behavior analysis to block known and unknown ransomware. ‣ Malicious Traffic Detection detects traffic to command and control servers to get encryption keys.
Exploit kit tries to run on server	‣ Server Lockdown prevents any untrusted applications from running. ‣ Web Control intercepts categories of inappropriate websites from malicious redirects.
Malware tries to communicate with command and control centers attempting to initiate exfiltration or to encrypt for ransomware	‣ Malicious Traffic Detection monitors, alerts and acts when applications try to send traffic to known Command and Control URLs.
Malicious code or document tries to exploit OS or application vulnerabilities	‣ Server Lockdown prevents any untrusted applications from running. ‣ Peripheral Control can monitor and block devices, so, for example, USB devices are prevented from propagating malware or exfiltrating data.
Malware is downloaded/installed	‣ Server Lockdown prevents any untrusted applications from running. ‣ Pre-execution emulation looks for known malicious behaviors that might be delayed intentionally. ‣ Heuristic analysis to detect variants of known malware and currently unknown malware based on its operation. ‣ SophosLabs Live Protection for real-time threat intelligence identifies suspicious behavior patterns. ‣ HIPS runtime behavior analysis.
Storage device with malware or with intent to acquire data is attached to server	‣ Peripheral Control monitors and can block devices. For example, USB devices are prevented from propagating malware or exfiltrating data. ‣ Sophos will detect malware on removable media as it is read by the endpoint.
User uses a server to access the internet and attempts to go to compromised site or malicious ad, or; User attempts to download illegal torrents, which may contain malware	‣ Web Control blocks inappropriate URLs based on SophosLabs research and categories selected by the Admin. ‣ Download Reputation tracks trustworthiness of file downloads.
A user tries to run Potentially Unwanted Applications (PUA) or non-compliant applications such as iTunes or Dropbox	‣ PUAs are detected and alerted. ‣ Application Control blocks use of specified categories and/or individual applications you don't want run. ‣ Server Lockdown prevents additional software from running unless authorized by the admin (default deny).
Any of the above	‣ With communication between the firewall, the server, and associated endpoints, Sophos Synchronized Security ensures immediate coordination to thwart the most sophisticated and coordinated attacks. Plus automated identification and isolation of endpoints or servers based on Sophos Security Heartbeat™, means less time spent responding to incidents.

2. Server performance should not be impacted by security measures.

One of the primary reasons frequently stated for not protecting servers better from hacking is the concern that those measures would negatively impact server performance. Given that servers are the hub of an organization's activities and must be continuously available, optimized server performance is crucial. Any anti-malware solution that you choose should have a minimal impact on your server workload and users' productivity.

How Sophos Server Protection can help:

Sophos Server Protection minimizes the performance impact of securing your servers, utilizing a variety of server-specific approaches:

a. **Default policies** – Sophos offers default policies that are designed to give you the best balance of performance and protection. You do not need to spend time thinking about which features to activate or use sparingly. Simply apply the Sophos Recommended Settings at the click of a button in the management console.

b. **Automatic scanning exclusions** – Sophos applies a range of common vendor-recommended exclusions, negating the need for you to manually determine which files, folder, and processes to exclude. All you need to do is turn on auto exclusions in the management console.

c. **No repeated scans of same files** – Sophos uses in-engine caching that prevents needless rescanning of files between updates.

d. **Lightweight updates** – Sophos keeps its anti-malware updates small to make them faster and require fewer server resources to download, process, and install each update.

e. **Local cache** – Sophos Server Protection retrieves updates for all your servers and stores them locally in a cache for all servers to access when performing updates, reducing bandwidth requirements.

f. **Randomized update timing** – Sophos mitigates update storms by starting updates at different times and in random sequences. Each server, by default, will update at a random point within its set time slot to avoid a situation where they all update together.

[6] Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald and Peter Firstbrook

3. Since servers are different from other endpoints, servers should be protected with server-specific technologies.

The ability to categorize and control which applications can run on your servers is a powerful technique to prevent infections.

As Gartner states[6], "It is much more effective to apply a default deny application control model to server workloads than it is on end-user-facing endpoints... The use of whitelisting to control what executables are run on a server provides a powerful security protection strategy."

How Sophos Server Protection can help:

Sophos Server Lockdown takes application whitelisting one step further. With Sophos, you can whitelist your applications and lockdown your servers so that all other applications are denied by default. Sophos one-click Server Lockdown automatically scans the server and identifies and profiles your allowed applications along with all their associated scripts and files. Sophos then automatically creates trust rules – you do not need to manually create and keep updated lists of applications and their associated files. Sophos Server Protection is the only solution to offer whitelisting tightly integrated with server anti-malware and HIPS, so that you get effective protection against known and zero-day attacks, for example in-memory, DLL injection and script-based attacks.

Sophos also provides automatic scanning exclusions for key business applications, like Exchange or SQL. Since these are known commercially available applications, there is no need to scan these applications. The result is less risk to production applications, fewer false positives, and fewer resources spent needlessly rescanning files.

4. It should be easy to deploy and manage

Server security does not need to be complicated. Since there are typically multiple servers running on multiple platforms, a multi-platform server protection solution should support all server platforms to make it easier to set consistent policies for compliance and threat protection.

How Sophos Server Protection can help:

Sophos Server Protection supports a broad range of platforms, so you can protect every server in your organization. We offer protection on Windows, Linux, and UNIX platforms, both physical or virtual. Choose the best method to deploy our server protection. You can choose Sophos Central, our cloud-managed management services hosted by Sophos, unifying security management of your servers, endpoints, wireless devices, and mobile devices as well as email protection and web gateway, and then synchronizing those with the security of your network. Or, deploy your own on-premise management server using Sophos Enterprise Console. For your virtual servers, our full-featured server agent runs with a low-memory footprint on popular hypervisors, such as vSphere, Hyper-V, and XenServer.

And as we've discussed, Sophos has made it easy to whitelist applications with Server Lockdown. Sophos is the only vendor to offer server-specific application whitelisting with integrated HIPS behavior analysis, as well as eliminating tedious cataloguing of applications and their associated files and script. Sophos has simplified deployment to an automated process that takes minutes or hours instead of days or weeks of manual effort. Unlike our competitors, Server Lockdown can be deployed while the server is online and running, with no reboot required, as seen below.

Server-specific products from:	Sophos	Kaspersky	McAfee	Symantec	Carbon Black	Trend Micro
AV + Anti-malware (Windows, Linux and Unix)	✓	✓	✓	✓	No Unix	✓
Cloud-based management	✓				✓	✓
Device Control (USBs)	✓			✓	✓	
Malicious Traffic Detection	✓					✓
Anti-Ransomware	✓	✓				
File Integrity Monitoring				✓	✓	✓
Automatic Exclusions for common applications (Exchange, SQL)	✓					
Point & Click Application Control (category blacklisting)	✓	✓		✓	✓	
Application Whitelisting	✓		✓	✓	✓	✓
One-Click Server Lockdown	✓					

Sophos offers optimum policy configuration for your servers. You can control whether peripheral devices can be used or which particular devices are used. Application Control lets you set policy for dozens of categories of applications. Web Control and Download Reputation can also easily focus server use on appropriate tasks.

But don't take our word for it. Sophos has been praised for its simple, easy-to-use management:

- In this report by PC Mag when compared with other competitors
- Our superior ease of management in the cloud was validated by an independent test by Tolly[7]:

Security Solution	Sophos	Kaspersky	McAfee	Symantec	Trend Micro
Number of Deployment Steps (Deployment and Basic Configuration)	24	38	81	51	51
Number of Management Steps (Policy, Responses to Blocked Device & Allow Potentially Unwanted App)	22	32	40	51	51

[7] Tolly Test Report, Sophos Endpoint Protection Usability https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/Tolly-Report-on-Usability-of-Sophos.aspx

Here are some of our customers' experiences with Sophos Central Server Protection Advanced:

"Administration is really easy. It gives me a single pane of glass. It's always running and doesn't slow my stuff down, so it works extremely well with my SCADA server."[8]

Jason Hamlin, Lynchburg Water Resources, Lynchburg, VA

"With Sophos Central in place, managing the on-premises servers is off my plate. For us, it's a huge advantage to have a respected company like Sophos managing the backend. Ultimately, it's not so much a time saver as it is avoidance of a problem."[9]

Shawn Umansky, Saint Michael's College, Burlington, VT

Conclusion

There's a lot to consider as you protect your servers. Sophos Server Protection offers comprehensive threat protection for your physical and virtual servers and it doesn't slow you or your servers down. Designed to secure business-critical servers, Sophos Server Protection integrates server application whitelisting with advanced anti-malware, HIPS, and anti-ransomware providing you effective protection against zero-day attacks. Protection for your Windows, Linux, and UNIX systems, optimized for virtual environments – it is server security made simple, only from Sophos.

[8] Customer Case Study, Lynchburg Water Resources
[9] Customer Case Study, Saint Michael's College

Sophos Server Protection

Register for a free 30-day evaluation at sophos.com/free-trials

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

16-10-24 WPNA (DD-2469)

SOPHOS