SOPHOS
Security made simple.

Sophos Application Whitelisting

Advanced Server Protection made simple

By Gail Ferreira, Sr. Product Marketing Manager, ESG

Sophisticated attacks on today's servers must be deflected with powerful, comprehensive protection. The challenge is finding a solution that provides the right level of protection, but can still be efficiently and cost-effectively deployed and managed. Application whitelisting keeps advanced and unknown threats from executing, but has typically been complex and costly to implement. Sophos brings power and simplicity to application whitelisting, making it the solution of choice for protecting physical and virtual servers and the business-critical applications that they run. But is application whitelisting a good fit for your server environment? Several key factors come into play when making that determination.

The Challenge of Protecting Servers

Servers, with their business critical applications, are prime targets for attack. Protecting the integrity of these applications and maintaining the uptime of the servers that run them remains a top concern of any organization today. Traditionally, organizations have deployed endpoint security to protect their servers. But endpoint security falls short in that protection, requiring extensive configuration and optimization for server performance, which makes for a complex process.

Application Whitelisting

Application whitelisting is increasingly finding its way into server environments as a recommended method to keep advanced and unknown threats from executing on servers. Whitelisting uses a default-deny approach to help organizations keep their operating system secure, as well as specific business applications being used on each server. Rather than focusing only on trying to detect malware and prevent it from running, application whitelisting instead prevents all untrusted and unknown applications from running. This offers proactive, comprehensive protection against known and unknown threats because it ensures that only authorized applications are able to run on the system.

As Gartner recently stated, "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." [1]

Overview:

Sophos Server Lockdown integrates application whitelisting with advanced anti-malware and runtime behavior analysis to deliver powerful server-specific protection while still keeping it simple to deploy and maintain.

Highlights:

- Single-click Server Lockdown creates a whitelist of authorized applications automatically
- Automatic trust rules, managed on your behalf by Sophos, allow trusted applications and updaters to execute without interference
- Add your own trust rules with ease, without unlocking the server
- Lock down servers without taking them offline or rebooting
- Centralized management for fast deployment

[1] *Gartner, Market Guide for Cloud Workload Protection Platforms, March 2016, Neil MacDonald and Peter Firstbrook.*

Better Server Protection

Sophos Server Protection offers application whitelisting with Server Lockdown that is tightly integrated with server anti-malware and HIPS (Host-based Intrusion Prevention System) behavior analysis in the Sophos Server Protection Advanced license. It provides proactive, comprehensive protection against known and unknown threats such as ransomware, in-memory, DLL injection, and script-based attacks as it ensures that only authorized applications are able to run on the system.

Sophos Server Protection offers application whitelisting with Server Lockdown

Simple Server Protection with Server Lockdown

Conventional application whitelisting comes with high management overhead, from initial deployment to ongoing maintenance and change management of all components and files associated with the whitelisted applications. Mid-sized companies — or any organization with limited IT resources — might be discouraged from implementing whitelisting or else be compelled to invest in expensive consulting services to make it work. Sophos offers the easiest server application whitelisting solution available, that includes the industry's first "one-click" Server Lockdown. provides a powerful security protection strategy." [1]

How Sophos Application Whitelisting Process Works

Sophos application whitelisting eliminates the need to manually create an application inventory (whitelist), set up complex policies and configurations, and write rules for change management – replacing days or even months of effort with just a single click. That single click initiates a top to bottom system scan of the server and a complete process to establish the application whitelist baseline, identifying all the associated files prior to locking the server down in a known good state.

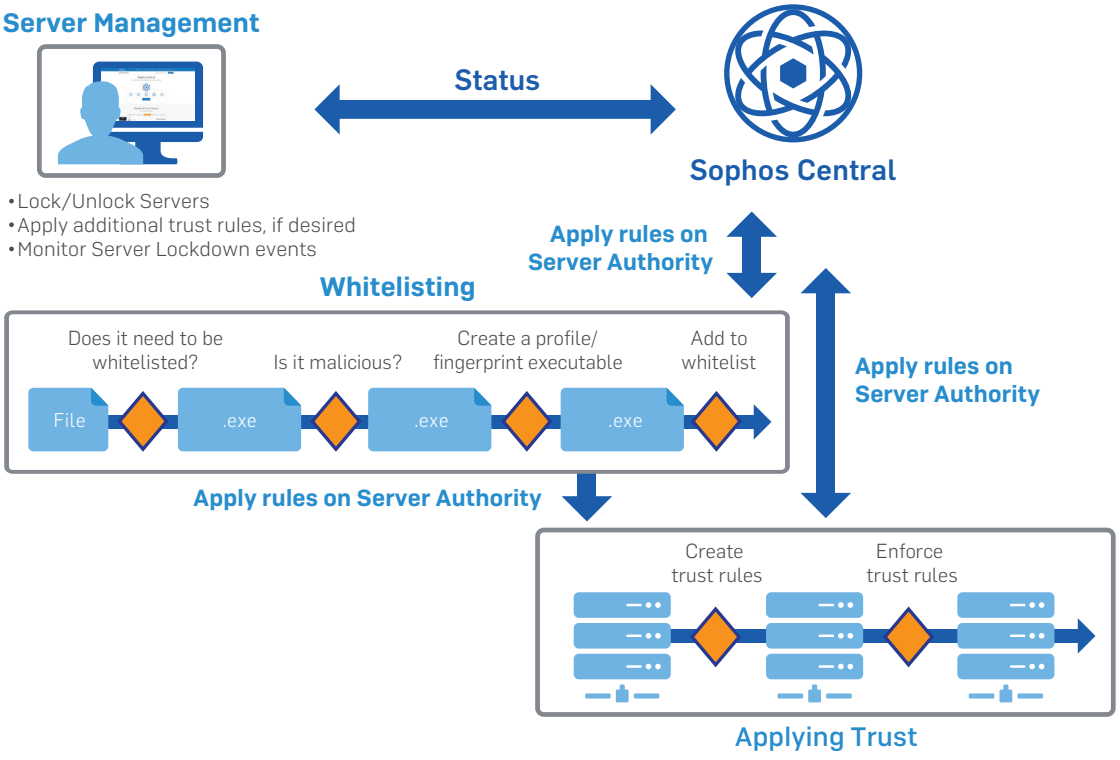
The Server Lockdown process uses Sophos ServerAuthority™ to identify or whitelist applications by:

1. Cataloguing or fingerprinting desired applications after scanning for any malware, verifying the current state as good and any existing applications as trusted.
2. Establishing a profile in ServerAuthority for each application to protect the integrity of those applications. This examines the relationships between those applications, along with associated necessary files such as DLLs and script files, as well as system files they use.

3. Automatically developing trust rules to ensure that only trusted sources can update those whitelisted applications. This trust between applications controls which executables can update existing applications. Sophos creates a data feed on trusted applications which automatically configures how the installed applications can be updated. Thus Windows updates or application upgrades are allowed to run without interference, but not ransomware.
4. Completing the lock down process, ensuring that only those approved applications are able to execute – eliminating tedious and time-consuming ongoing manual configuration and rule-setting.
5. Completing Server Lockdown without requiring a reboot of the server.

Note: In addition to the trust rules applied and maintained by Sophos, customers can add their own allow (trust) rules in the Sophos management console if needed to authorize additional software to run — without needing to unlock the server. Similarly, you can also block software that has previously been whitelisted/authorized, simply by adding it to the policy.

Once the server has been locked down, Sophos' context-aware security engine continuously monitors the system to prevent content-based attacks, utilizing anti-malware and HIPS behavior analysis to protect against memory and run-time attacks. In lockdown mode, only the baseline applications and all associated files and scripts can execute; they cannot be replaced or tampered with, except by trusted updaters. New applications will not be able to run unless allowed by the Sophos Central admin.



Advanced Protection Designed for Servers

Sophos application whitelisting is part of the Sophos Server Protection Advanced product, and draws a clear distinction between user endpoints and servers. The default server threat protection policy is optimized to balance performance and protection on server operating systems. Policies can be applied to a single server, to a group defined by you, or to the entire environment.

Other innovative features from Sophos work together to give you the broadest protection for your servers, for the data they contain, and for the business-critical applications that they run. These features include:

1. Pre-execution emulation, identifying suspicious behavioral patterns for early intervention.
2. Malicious Traffic Detection, monitoring traffic communicating from Windows or Linux servers to known Command and Control centers used by criminals and other threats to control and distribute their malware. If malicious traffic is detected, suspect executables are scanned, alerted, and potentially blocked.
3. Automatic scan exclusions of known business applications, eliminating unnecessary antivirus scans and ensuring those applications are not affected. These exclusions also improve performance and stability while still ensuring effective security and fewer false positives.
4. Application Control — policy-driven use of dozens of pre-defined application groups — allowing you to block use of specified categories of applications or individual applications you don't want to run.
5. Peripheral Control, preventing USB devices from propagating malware or exfiltrating data.

Conclusion

Today's environment urges you to protect your organization's servers from zero-day and advanced threats while ensuring the performance of critical applications is unaffected. Sophos application whitelisting (Server Lockdown) provides simple yet powerful server protection. Let Sophos do the work with a single click rather than manually cataloguing and configuring all the application components to set up default deny policies. Know that you have a known good state that is maintained by ServerAuthority.

Sophos Server Protection takes advantage of a broad variety of techniques to protect your servers. We have discussed application whitelisting, but Sophos also integrates server anti-malware, HIPS behavior analysis, and Malicious Traffic Detection to protect servers, countering threats with the most effective approach for each potential vector of attack. Sophos Server Protection is optimized for servers, not end user systems, and leverages SophosLabs for real-time threat intelligence. Take advantage of its optimized performance and effective protection for your servers, and enjoy unprecedented ease of use and management.

To find out more about
Sophos Server Protection visit ,
www.sophos.com/servers

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

2016-03-08 WP-UK (MP)

SOPHOS