



Sophos Server Application Whitelisting

Moderner Schutz für Server – einfach und zuverlässig

Von **Tsailing Merrem**, Senior Product Marketing Manager

Um raffinierte Angriffe auf Unternehmensserver abzuwenden, bedarf es leistungsstarker Sicherheit. Aber eine Lösung zu finden, die den geeigneten Grad an Schutz bietet und trotzdem effektiv und kosteneffizient bereitgestellt und verwaltet werden kann, ist alles andere als einfach. Um zu verhindern, dass raffinierte und unbekannte Bedrohungen auf Server gelangen, gilt das Whitelisting von Anwendungen als vielversprechende Lösung, war jedoch bislang kompliziert und kostspielig in der Umsetzung. Sophos bringt leistungsstarkes Server Application Whitelisting jetzt über die Cloud in Unternehmensumgebungen und bietet damit die ideale Lösung zum Schutz von Servern und den darauf gespeicherten vertraulichen Daten.

Unternehmensserver effektiv schützen – eine besondere Herausforderung

Weil auf Unternehmensservern heutzutage große Mengen geschäftskritischer Daten gespeichert werden, haben sie sich zum beliebten Ziel für Malware und Zero-Day-Angriffe entwickelt. Die Integrität und Verfügbarkeit von Servern sicherzustellen und die Vertraulichkeit der auf Servern gespeicherten Daten zu wahren, sollte daher für alle heutigen Unternehmen höchste Priorität haben. Bislang blieb Unternehmen nichts anderes übrig, als ihre Server mit Endpoint Security zu schützen. Bei Endpoint Security wird jedoch keine ausreichende Unterscheidung zwischen Servern und Endpoints getroffen, sodass extensive Konfigurationen und Optimierungen erforderlich sind, was den Vorgang sehr kompliziert macht.

In jüngster Vergangenheit hat sich das Whitelisting von Anwendungen in Unternehmensumgebungen als wirksamere Methode zum Schutz von Servern vor raffinierten und unbekanntem Bedrohungen etabliert. Mit Whitelisting können Unternehmen das Serverbetriebssystem und die auf ihm installierten Anwendungen mit einer Standard-Ablehnungsregel schützen, anstatt sich auf bekannte schädliche Anwendungen zu konzentrieren (Zugriff standardmäßig erlauben). Diese Methode bietet proaktiven, signaturfreien Schutz vor bekannten und unbekanntem Bedrohungen und stellt sicher, dass nur von der IT autorisierte Anwendungen auf dem System ausgeführt werden.

Herkömmliches Whitelisting von Anwendungen ist jedoch mit einem erheblichen Verwaltungsaufwand verbunden, nicht nur bei der Anfangsbereitstellung, sondern auch bei der Wartung und beim Change Management. Unternehmen mittlerer Größe mit begrenzten IT-Kenntnissen und -Ressourcen lassen sich daher oft von der Implementierung dieser Methode abschrecken oder sehen sich gezwungen, in kostspielige Beratungsleistungen zu investieren.

Sophos Server Application Whitelisting – einfacher und effektiver Schutz für Server

Sophos Cloud Server Protection bietet mittelständischen und pragmatischen Unternehmen eine besonders einfache Whitelisting-Lösung für Serveranwendungen. Sophos Cloud Server Protection besticht durch effektive Sicherheit, optimierte Server-Performance, eine schnelle Bereitstellung und einfache Verwaltung. Außerdem ist Sophos Cloud Server Protection die einzige Lösung, bei der das Whitelisting von Anwendungen mit speziell auf Server abgestimmtem Malware-Schutz und HIPS (Host-based Intrusion Prevention System) kombiniert wird. So bleiben Server effektiv vor neuen und Zero-Day-Angriffen (z. B. speicher-/skriptbasiert oder DLL-Injection) geschützt.

Mit dem branchenweit ersten „One-Click Server Lockdown“-Feature scannt die Lösung den Server automatisch auf Malware, nimmt „Fingerabdrücke“ der Anwendungen, ermittelt den „Grundstock“ der Whitelist-Anwendungen und nimmt dann den Lockdown des Servers vor. Im Lockdown-Modus können die Anwendungen in diesem Grundstock weder ersetzt noch manipuliert werden. Sophos ServerAuthority erkennt jedoch Serveranwendungen und passt seine Konfiguration an, um vertrauenswürdige

ÜBERSICHT

Sophos Server Application Whitelisting bietet in Kombination mit modernem Malware-Schutz und HIPS leistungsstarke Server-Sicherheit, die sich einfach bereitstellen und warten lässt.

HIGHLIGHTS

- ▶ One-Click Server Lockdown
 - ▶ Automatische Vertrauensregeln zur Anpassung an Server-Umgebungen
 - ▶ Kombination mit Anti-Malware und HIPS zum Schutz vor inhaltsbasierten und Zero-Day-Angriffen
 - ▶ Automatische Antivirus-Scan-Ausnahmen zur Optimierung der Performance
 - ▶ Cloudbasierte Sicherheit und Verwaltung
-

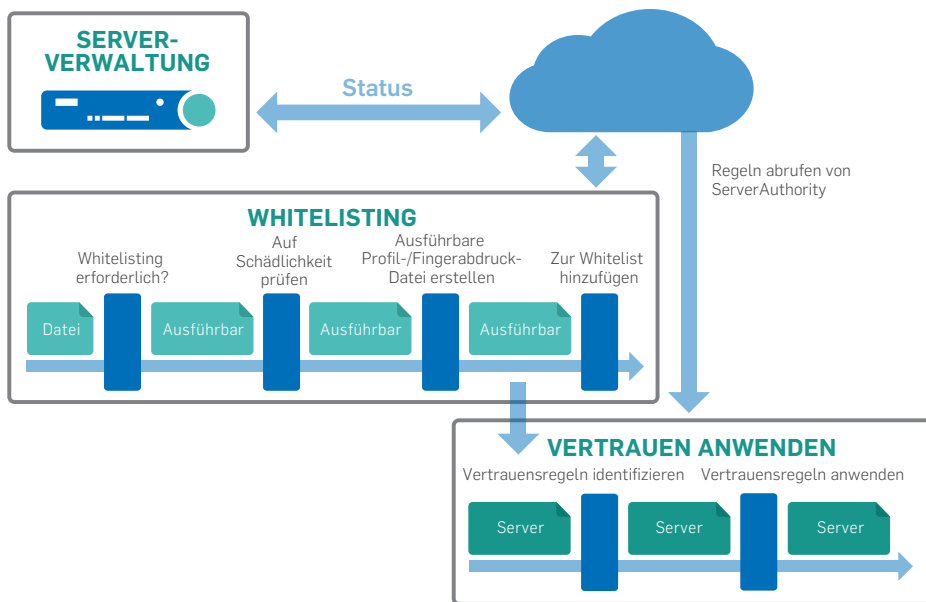
Sophos Server Application Whitelisting

Änderungen automatisch zu ermöglichen. Außerdem werden automatisch Antivirus-Scan-Ausnahmen eingerichtet, die für eine hohe Performance sorgen. Mit diesen Funktionen werden langwierige und zeitaufwendige manuelle Konfigurationen und Regelaufstellungen überflüssig. Die kontext-sensitive Sicherheitsengine von Sophos kontrolliert das System kontinuierlich und beugt damit inhaltsbasierten Angriffen vor.

Sophos Server Application Whitelisting beschränkt sich nicht nur auf Anwendungen, sondern setzt auch DLLs und Skripte auf die Whitelist. Sophos ServerAuthority sperrt automatisch die Verbindung zwischen Anwendungen und den ihnen zugeordneten Dateien (z. B. DLLs und Skriptdateien) und schützt das System so vor speicherbasierten Angriffen. Weil hierzu keine individuelle Regeln erforderlich sind, werden Konfigurationsfehler vermieden.

Die Lösung ist darauf ausgelegt, die Performance von Serveranwendungen zu steigern. Auf die individuell gestaltbaren Benachrichtigungen und Reports kann über die integrierte Sophos Cloud Konsole von überall aus zugegriffen werden. In der Verwaltungsoberfläche erhält der Serveradministrator eine zentrale Übersicht über alle Server, Anwendungen und den Schutzstatus.

So funktioniert Sophos Server Application Whitelisting



One-Click Server Lockdown

Mit Sophos Server Application Whitelisting lassen sich Server mit nur einem Klick in einen sicheren Zustand versetzen („Server Lockdown“). Sie müssen keine physischen Server mehr einrichten, keine Richtlinien konfigurieren, keine Anwendungsbestände anlegen und auch keine Regeln für das Change Management mehr verfassen. Was früher mit tage- oder sogar monatelanger Arbeit verbunden war, ist nun mit nur einem Klick erledigt. Dieser eine Klick löst einen kompletten Systemscan auf Malware aus, katalogisiert Anwendungen und baut Vertrauensbeziehungen zwischen Anwendungen, Updatern und Systemdateien auf.

Automatische Vertrauensregeln mit ServerAuthority

Sophos Server Protection passt sich dank Sophos ServerAuthority dynamisch an die Serverumgebung an. Anwendungen auf der Whitelist werden erkannt und es werden erforderliche Vertrauensregeln angewendet, um sicherzustellen, dass nur vertrauenswürdige Quellen Anwendungen auf der Whitelist aktualisieren können. So wird nicht nur die Integrität von Anwendungen gewahrt, sondern auch sichergestellt, dass Anwendungen unterbrechungsfrei aktualisiert und gepatcht werden.

Sophos ServerAuthority pflegt eine Liste beliebter Serveranwendungen wie Domain Controller, Exchange Server und SharePoint und wendet automatisch empfohlene Antivirus-Ausnahmen an, mit denen Dateien und Verzeichnisse vom Scan ausgeschlossen werden, die die Performance oder Stabilität beeinträchtigen könnten.

Gebündelte Sicherheit

Durch Kombination von Sophos Server Application Whitelisting mit Sophos Server Antivirus bündeln wir beide Technologien, um der heutigen Bedrohungsvielfalt Einhalt zu gebieten, und stellen damit sicher, dass Ihre Server optimal geschützt bleiben. Die Lösung nutzt zudem das „Live Protection“-Feature, eine cloudbasierte Verbindung in die SophosLabs, über die verdächtige Dateien in Echtzeit geprüft werden können.

Moderner, speziell für Server entwickelter Schutz

Sophos Server Protection unterscheidet klar zwischen Benutzer- und Serverrichtlinien. Die Standard-Server-Richtlinie ist darauf optimiert, auf Serverbetriebssystemen ein Gleichgewicht zwischen Performance und Schutz zu schaffen. Richtlinien können einem einzelnen Server, einer von Active Directory definierten Gruppe, manuell innerhalb der Konsole oder der gesamten Umgebung zugewiesen werden.

Fazit

Unternehmensserver vor bekannten und Zero-Day-Angriffen zu schützen, wird immer wichtiger, aber auch immer schwieriger. Sophos Server Application Whitelisting bietet einfachen und leistungsstarken Serverschutz, der branchenweit einmalig ist. Die Lösung beinhaltet One-Click Server Lockdown, Sophos ServerAuthority für automatische vertrauenswürdige Quellen von Änderungen und integrierte Anti-Malware- und HIPS-Funktionen. So wird mittelständischen und pragmatischen Unternehmen eine einfache Bedienung und Verwaltung, optimierte Performance und wirksamer Schutz für Server geboten.

Sophos Cloud Server Protection

Weitere Informationen finden Sie unter www.sophos.de/server.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

Oxford, GB | Boston, USA
© Copyright 2015. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

06.15NOLA.wpde