LEARNING MADE EASY

VMware Carbon Black Edition

Application Control

for dummies®
A Wiley Brand

Protect air-gapped systems

Secure unsupported operating systems

Lock down critical infrastructure

Compliments of

vmware® Carbon Black

Steve Suehring

Application Control

VMware Carbon Black Edition

by Steve Suehring

for dummies®
A Wiley Brand

Application Control For Dummies®, VMware Carbon Black Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-394-22518-7 (pbk); ISBN: 978-1-394-22519-4 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Traci Martin

Client Account Manager: Cynthia Tweed

Table of Contents

Introduction

Application control, sometimes called *application allow listing*, is a means for controlling the software applications that can be run on a given computer or device. Application control flips the security paradigm of deny listing on its head. Rather than trying to prevent bad software from running, application control allows only good software to run.

Application control offers a simple solution to a complex problem: how to handle the ever-increasing number of threats to computers and devices on a corporate network. As security threats and malware have evolved, so too have the needs for technologies like application control. Gone are the days when malware may redirect the user's search engine. We're now well into times where ransomware prevails, where targeted attacks are common, and rapidly evolving threats cost organizations productivity, reputation, and critical data.

Traditional application control platforms center on the concept of *allow listing*, or allowing only known-good software to run. Coupled with this approach is a list of applications whose disposition hasn't yet been determined. Application control solutions range from simple ones that are host-based or run from the operating system itself to those that are robust, enterprise-grade platforms on which an organization can depend.

If allow list management and enterprise-level application control sound like a lot of work, they shouldn't. Modern application control platforms do away with the allow list concept entirely by providing rich approval mechanisms that alleviate the need for allow list management. Further, the maturity of many application control solutions means that the deployment can be done in phases and integrated with your existing environment to ensure good software simply runs. The key to good application control is to find a solution that allows software rolled out by IT to be automatically approved and reputable software downloaded by end-users to be automatically approved. The prevalence of robust solutions with automated capabilities, supported by professional services teams, means that application control has truly come of age at just the right moment.

About This Book

Application Control For Dummies, VMware Carbon Black Edition, is primarily a discussion of application control technologies. This book first looks at the history of application control along with a more thorough look at the threat landscape. Then, it emphasizes best practices for choosing an application control platform and deployment of the solution. Considerations for obtaining approval are included within this book as are suggestions for how to design and implement the solution.

I assume that you're looking for ways to improve the security posture within your organization. You may have extensive security knowledge already, or you may be approaching this book as someone tasked with investigating application control solutions. Either way, this book is appropriate for decision makers who want a quick, easy-to-understand guide on application control.

Icons Used in This Book

Throughout the book you see helpful icons that indicate special information is coming. Here is what those icons mean:

TIP

When you see the Tip icon, there's a suggestion that may be helpful to save some time when considering application control or the subject in that particular section.

REMEMBER

This icon is helpful for things that may have been discussed earlier in a chapter or the book and would be useful to recall for the current discussion.

TECHNICAL STUFF

Additional helpful information that may not necessarily be important to know at that moment is found when you see this icon.

IN THIS CHAPTER

- Introducing the threat landscape
- Knowing the importance of the endpoint
- Looking at how traditional antivirus works
- Approaching endpoint security

Chapter 1
Looking at the History of Application Control

Application control offers a simple solution in handling the ever-increasing number of threats to computers and devices that are located on-premises or in private or public clouds. This chapter introduces application control by first discussing the overall threat landscape along with traditional approaches to endpoint security.

An Introduction to the Threat Landscape

When assessing technology, make sure to separate fact from fiction. Doing so with an understanding of the origins of the technology helps to make an informed decision. This section provides a brief look at the threat landscape, both then and now. I promise to keep the history lesson brief.

Threats: Then and now

Fifteen years ago, a large number of devices were already connected to the internet. With the advent of smartphones, tablets, and the Internet of Things (IoT), that number has grown significantly. The number of attack vectors has grown right along

with those connected devices. *Attack vectors* are the paths or avenues that malicious activity may follow in order to successfully exploit a system.

At that time, the business of malware creation and hacking was in its infancy. Today, literal armies of hackers operate at the national level, and cyberattacks have become a big business. According to Cybersecurity Ventures, global cybercrime is expected to reach $10.5 trillion by 2025.

Tools for detecting, preventing, and remediating threats are more important than ever. But too often, security professionals find themselves fighting today's attacks with yesterday's tools. The threat landscape is an ever-evolving space in which attackers seem to have the advantage. Luckily, the methods for defending against cyberattacks have also evolved.


TECHNICAL STUFF

Not only has the number of attacks and attack vectors increased but also the scope and costs associated with remediation of a successful attack. According to Ponemon Institute's Cost of a Data Breach Report 2023, it's estimated that identification of a breach, even knowing that you've been successfully attacked, takes on average 204 days. Remediation takes another 73 days, and the final cost of a breach is $4.45 million. With these types of numbers, finding a new way to protect an enterprise becomes even more important.

ASSESSING THREATS

A primary means by which threats are assessed is to consider the confidentiality, integrity, and availability paradigm. Within this paradigm, confidentiality refers to keeping secret things secret. A threat that enables an attacker to gain access to information that they should not have would violate its confidentiality.

Integrity refers to the ability for an attacker to affect the information. For example, an attacker that can alter bank balances or medical records, even if they can't see the effects of that alteration, would violate the integrity of the data in question.

Finally, availability refers to an attack that prevents an organization from using its data or systems when it wants to, as it wants to. Denial of service is an obvious example of an attack that affects availability.

Assessing risk from the outside

Risks from the outside are sometimes the easiest to consider. Attackers come in many forms, whether through incidental or large-scale spam-based malware distribution, to people attempting random host scans for vulnerabilities, to targeted attacks.

A common attack vector is through malware distribution. The malware arrives through an approved pathway, such as email or a link to a seemingly innocuous website. Many times, the person clicking the link doesn't know that his device has been taken over by malware.

Behind the scenes, the malware begins looking for other hosts and devices to infect. At the same time, the malware may steal data or record keystrokes or perform other malicious activity on the infected host or device.

Another more serious threat is a *targeted threat*, where the attacker is actively trying to break into an organization's systems with specific intent. This type of attack is difficult to detect with passive technologies because those technologies rely on knowledge of previous attacks. However, an application control platform with rich approval mechanisms can be more effective at preventing targeted attacks because the attacker may be prevented from executing malicious code.

REMEMBER

Today's threat landscape isn't the same as it was 10 to 15 years ago. Criminals and nation states are behind most malware attacks. The random attacks still occur, but the targeted threat keeps security personnel awake at night.

Assessing risk from the inside

After a link with a malicious payload has been clicked or an email with malicious code has been opened, the threat becomes an internal threat. Within this internal threat category application control is very effective.

With application control, only those applications and related components that have been approved can be executed. This means that even zero-day malware threats won't be successful when application control is in effect.

Internal threats also include those that originate from the inside, from employees and contractors who are otherwise authorized to

be using computers and devices within your organization. These threats can be both intentional and unintentional.

For example, an employee may install software on her desktop PC to stream music or to connect her phone at work. While the intention isn't malicious, the effect can be quite serious. If the application contains malware or if the software isn't licensed properly, your organization can be liable for damages.

However, there are certain times when an employee or contractor has malicious intent. She may install a keylogger or other software to monitor transactions or perform other malicious activity.

In both cases, intentional and unintentional, passive monitoring such as antivirus (AV) or malware scanning may not deem the software a threat. Another method for defending against these types of attacks is necessary.

REMEMBER

Always consider internal threats to be at least as serious as those from the outside.

The Importance of the Endpoint

Enterprise computer security is no longer fought solely on the perimeter; both the perimeter and the endpoints need to be secured. This section discusses security at the endpoint.

What is an endpoint?

Endpoints are those systems that store intellectual property within an organization. Endpoints can be anything from a server to an end-user system such as a desktop, laptop, tablet, or mobile phone. Endpoints can reside on-premises or on private or public clouds. If the device can store intellectual property or if the device can be used as a platform for escalating privileges or carrying out other attacks, the device needs to be protected.

Why protect the endpoint?

The most valuable targets are those that contain data, whether customer data, or confidential documents, source code, and other essential elements of your organization. However, an attacker may not be able to easily identify systems that contain such data.

In these cases, an attack may be exploratory at first; the attacker collects information about the network topology and tries to remain undetected within the network.

Exploratory attacks need devices and systems on the inside of the network. Therefore, protecting these systems is just as important as protecting those with the actual data. In essence, the endpoint is the new perimeter.

How Traditional AV Works

Attacks on endpoints follow a similar pattern. The attacker may drop malicious code on the system, whether a rogue program that looks innocuous or other executable code that enables the attacker to then access the system. Today, most endpoints have traditional AV or similar tools to mitigate attacks. In some cases, those products use enterprise integration to make management easier.

Traditional AV software protects against known and well-defined threats. But that necessarily implies that the AV software knows about the threat in order to identify and protect against it. This is an important implication and not one that can be taken for granted.

After a piece of malware is known, a signature can be created for it. Assuming that the malware doesn't morph or change itself, the AV will catch the malware from that point forward. But that leaves a large gap between when a piece of malware is first seen, a signature created, and the AV updated. The AV-TEST Institute registers over 450,000 instances of new malware daily, so it's seemingly impossible for this traditional approach to keep up.

Security professionals have known for quite some time that traditional AV doesn't protect against unknown malware and certainly not against targeted attacks. AV is just not made for those types of threats and may give a false sense of security.

A *virus signature* is a collection of characteristics about that particular piece of malware. For example, it could be files that are changed on the system, registry entries, and so on.

Another problem with traditional AV is that it keeps a list of known bad software. It's as if you throw a party and rather than

inviting specific people, you try to keep a list of everyone who shouldn't be allowed in. That list would be impossible to manage. AV follows the same pattern: Keep a list of everything that's bad and let everything else run.

Today's enterprise needs to look beyond AV and toward endpoint protection that meets the needs of the dynamic workplace.

A New Approach to Endpoint Security

AV solutions, including next-generation AV (NGAV) solutions, will continue to be a part of endpoint protection, if for no other reason than meeting the requirements of audits.

REMEMBER

Even NGAV solutions are susceptible to the same limitations as AV. However, it's necessary and vital to consider how to truly protect your enterprise against the modern attacker.

Security takes two approaches — positive and negative:

- **Negative security,** including AV, is the ability to detect and thwart known bad events. It has provided a layer of security assurance for years. The ability to block known viruses, worms, and other bad event signatures has kept many systems from being compromised. However, new attacks have evolved that are outside the scope of the negative security model. The negative security model isn't bad; in fact, it's essential. It just isn't enough.
- **Positive security** identifies scenarios with a known degree of trust, only allowing access to trusted resources. The positive model assumes that a new scenario is untrusted and requires that trust be assigned before access and usage are granted. In the classic positive security model, only known good requests and known good results are delivered.

For a positive security model, organizations are looking toward application control. Application control provides a way for organizations to protect against entire classes of attacks. An application control solution is more advanced than traditional NGAV and offers better protection against the threats facing the modern enterprise. Application control can stop the more advanced attacks, including zero-day threats and targeted attacks.

Application control accomplishes this feat by using a default-deny policy.

A *default-deny policy* means that the only software that runs is the approved software, just like a party with invited guests. If software hasn't been approved to run, it doesn't run. Even with this advanced protection, application control solutions are resource-friendly, in part because the list of approved software is smaller than the list of known bad software, which results in reduced computing power and security engineering time.

With a default-deny policy, protection is available for malware that hasn't yet been seen. The default-deny policy found with application control means that enterprises find themselves protected, even when AV fails. This approach is necessary to protect the endpoints properly.

IN THIS CHAPTER

- Moving from reactive to proactive defense
- Understanding the value of default-deny policies
- Having an effective application control discussion
- Attaining industry validation of application control

Chapter 2
Understanding the Benefits of Application Control

This chapter discusses some of the direct benefits of application control. While many may be self-evident to security professionals, it's a good idea to look at those advantages to help see things that may be hidden from an initial view.

Within this chapter, you look at moving from a reactive to a proactive defense, the value of default-deny policies, how to frame the discussion of application control, and how industry analysts view application control.

Moving from Reactive to Proactive Defense

Antivirus (AV) software works well against known threats. Firewalls perform a vital service by blocking access to internal systems. Intrusion detection systems (IDS) help to determine that an attack has occurred.

What do all three of these security technologies have in common? All three — AV, firewalls, and IDS — are all reactive. The technologies work against known and defined threats and attacks. Today's security landscape has moved beyond these reactive technologies and requires proactive defense.

From deny listing to allow listing

Before I go too much further, let me get some terminology out of the way. You may be familiar with the terms *whitelist* and *blacklist*, but the industry is moving away from using these terms and replacing them with *allow list* and *deny list.* An *allow list* represents known-good activity — again, whether file-based, network-based, or otherwise — and is used in a positive security model. A *deny list* represents known-malicious activity, whether file-based, network-based, or otherwise. It is used in a negative security model.

In the context of security technologies, things on the deny list are typically blocked or prevented from running, and things on the allow list are typically allowed to run. Many security techniques and technologies are deny list-centric. That is, they assume all activity, whether network or system, is acceptable unless it meets certain known-malicious criteria.

AV software, which compares files and other activity against a database of known malicious code and signatures, employs a negative security model. The AV approach works well for known and well-documented threats but fails completely when faced with new, zero-day threats and activity. Even so, AV should continue to be considered an essential part of an organization's security solutions architecture.

A zero-day threat is one that hasn't yet been seen by AV and security vendors. A zero-day represents an imminent threat to an organization if the organization is running software or hardware vulnerable to the exploit.

Technologies like IDS provide a level of protection at a different layer, the network. These technologies examine network traffic for signs of malicious activity. Similar to AV, an IDS relies on the negative security model in the form of a database of known-malicious activity against which comparisons are made. If the activity is deemed suspicious, an alert is generated to an administrator who can then take the appropriate action.

As IDS platforms evolved, they became known as intrusion protection systems (IPS). The difference between an IDS and IPS is the ability not only to alert, as the IDS does, but also to actively block traffic deemed malicious. While the ability to block activity can be useful, it still relies on definitions that must be preconfigured and constantly maintained, just like IDS and AV.

The move from IDS to IPS represents a shift from reactive to active in security technologies. However, each of these technologies has something in common: They all require deny list maintenance in order to be successful. The technologies are only as good as their database, and if that database isn't updated regularly, no protection will exist against new threats.

It's safe to say that all enterprise-level AV products have a way to keep their definitions updated. IPS and IDS typically do as well. As definitions are updated, especially at the IPS level, an administrator is typically involved to make sure that the existing network activity isn't adversely affected by the definition update. It's also not unheard of that an AV update flags a "safe" file as malicious and begins blocking it. A security administrator's job is never done.

A false sense of security is also common when AV has been deployed. Sometimes AV or IDS/IPS definitions aren't updated. There may be "that one computer" that runs old software that simply doesn't play nice with the AV, or even worse, devices that silently fail to update for one reason or another. The reactive nature of the protection means that a malicious attack can begin from one of these devices and then move onto other devices before being detected.

The positive security model uses allow listing. Allow listing removes the need for a definition database of known-bad activity and instead assumes that activity isn't to be trusted until proven otherwise and allowed to continue. Allow listing, sometimes called *application protection and control,* offers a higher level of protection than AV and IDS/IPS.

Although allow listing requires a thorough examination of known-good traffic, all the technology platforms for application control can work in a listening mode. In listening mode, known-good traffic and usage patterns are found, thereby creating a baseline. The known-good activity is then added to an allow list and will be allowed when the platform is launched.

REMEMBER

Reactive security technologies, relying on a negative security model, offer value against known-bad threats, but they require maintenance and are only as good as their latest definition database.

The importance of allow listing

A firewall represents the most basic, yet essential, technology that employs both deny lists, known-bad, and allow lists, known-good. The firewall policy within most organizations uses a deny-by-default policy, whereby all traffic is blocked unless it has been specifically allowed. In this sense, the deny-by-default policy creates an allow list, where only known-good traffic is allowed to pass through the firewall.

Consider the opposite scenario with a firewall, where all traffic was allowed and only those threats that were known, only those ports known to be bad, are blocked. That wouldn't be an efficient or effective means to secure your organization. Yet this is what many organizations do when they employ only AV and IDS/IPS.

As threats evolve and become more sophisticated, reactive technologies provide less protection. Being able to know that the only applications executing are those that are approved is essential. This technique is known as an *application allow list.*

An application allow list is simply a list of approved applications and application components. Rather than trying to list everything that may be bad (as a deny list would do), an application allow list contains only those items that are approved. Application allow list

programs, also called *application control programs*, use that allow list to prevent malware and other malicious activity.

An application control platform will, by nature, work with allow listing of known-good applications and application components. It's important to develop an understanding of the types of application control that are available.

TECHNICAL STUFF

Application components include things like libraries and configuration files that are associated with a given application.

There are various means by which an application control platform can examine applications to determine their disposition. These include the following:

- **Filename:** Although too simple to be effective, a filename provides a rudimentary means to determine if an application is allowed to run.
- **Path information:** Like the filename, examining the path for the executable or related files is typically too simple to be an effective means for determining whether an application should be allowed to run.
- **File size:** The size of the run or application component can be used to determine if the file has changed. However, an attacker can also replicate the file size thereby rendering this an ineffective means for application control. However, when used in combination with other attributes, the file size can deter basic malware.
- **Publisher:** An application or application component that has been digitally signed by the publisher of that software can be an effective means to verify its authenticity. However, establishing that trust relationship based solely on the publisher can be a weak means to ensure full application control. For example, trusting that all applications from a certain publisher are authentic and safe to execute means that even applications that have active vulnerabilities will be executed from that publisher.
- **Digital signature:** Instead of assuming that all files signed by a given publisher are safe, another means for deny-by-default is to verify the digital signature of every file and application component. However, many publishers don't sign all their files, and digital signatures aren't possible for items, such as configuration files that have local changes.

- **File hash:** An effective means for verifying file authenticity is through a file hash, provided through cryptographic means. A file hash creates a unique value that's only associated with a given file at a given point in time. If the contents of that file change, such as when a new version is deployed, its file hash will also change. When combined with file path, filename, and other attributes, the file hash provides a powerful way to ensure an application and its components are unaltered. This assumes that the cryptography itself is strong and that hash collisions are few and relatively difficult to create.


TECHNICAL STUFF

A *hash collision* is when two different files share the same cryptographic hash value. When hash collisions are common or easy to create, an attacker can create a malicious version of a file that has the same cryptographic hash.

Some common traits of allow list technologies include the following:

- Control the applications that can run on a given device
- Can apply different enforcement levels to different devices or groups
- Can be deployed with a baseline set of known-good activity gathered from real information
- Can be applied using trust-based and policy-driven control
- Provide active protection against new threats, including zero-day and other advanced attacks

Knowing the Value of Default-Deny

The obvious benefit with application control is being able to determine which applications are allowed to execute and excluding those that can't. But application control technologies, through allow listing, enable your organization to achieve greater control over its operational environment. These benefits are often overlooked when considering whether the investment into application control is worthwhile.


REMEMBER

Default-deny means that privileges aren't granted automatically but are instead denied. In the context of application control, it means proactively preventing attacks based on trust and policies.

To someone on the operations staff, who's tasked with the thankless job of taking the first support call, any change that affects how your organization's users accomplish their jobs isn't viewed in a positive light. However, application control technologies have benefits for operations staff and can help to make their jobs much easier.

This section focuses on the benefits of application control within the operations side of your organization, including security operations.

Application support

From an operations standpoint, knowing which files and applications can run means less support because applications execute in a known environment. There are fewer cross-version and cross-application incompatibilities in an application control environment.

Operations support staff can require that all clients use standardized versions of applications within a tested and controlled environment. For example, if Application A requires a certain version of Application B, application control can ensure that only the correct version of Application B is installed. Imagine knowing what version of an application is installed without having to ask the user.

The ability to version-check software isn't unique to application control platforms. Technologies like Microsoft System Center have this capability. But an application control platform carries the built-in ability to do so and to check file versions across an application, not just the executable. Application control platforms can also version-check files that don't fit well within the normal professional packaged software paradigm, such as custom-built applications.

Software inventory

The inventory collected as part of application control serves as an inventory of software across an entire organization. In practical terms, application control provides a means by which your organization can ensure software compliance.

Application control also prevents unauthorized software from being installed on client devices. Software that's installed,

whether intentionally or unintentionally, can cause numerous issues within a network, even beyond the original device on which the software is installed. For example, software that scans the network for other similar devices may cause problems with other hosts or devices.

Unlicensed software is also an ongoing issue within many organizations. Application control technologies help prevent unlicensed software from being installed or used. Things like Group Policy enforcement already prevent many groups of users from installing software that uses a traditional Microsoft Installer (MSI) or executable installer.

However, what about software that doesn't require an MSI file or can run from other media? Application control technologies help prevent unauthorized and unlicensed software from running, so if the software is executing, you can be sure that it's received a blessing from operations to do so.

Security response

Operations staff are tasked with responding to the first call for help. It's through this first call that many security issues are first found. Application control technologies help when investigating an attack.

There may be a certain signature associated with an attack. For example, the attack may alter certain files on a given endpoint. Security and operations personnel can use that signature to help determine not only how the attack started but also if any other hosts are affected.

Knowing which hosts have been affected leads to knowing which hosts haven't been affected by a given piece of malware. Further, through the software inventory aspects of application control, the security response team will know in which hosts the infected software resides. For example, if a given software package can't be installed on a certain group of hosts, those hosts won't be affected by a malware event.

REMEMBER

With an application control solution, re-imaging of machines becomes less of an issue.

Security response and control leads directly into the discussion of overall host health, which is another benefit of application control.

Host health

Application control technologies can monitor the health of the host itself. Specifically, the files related to the host applications can be monitored by many application control platforms. In addition, some application control platforms can even prevent changes to these ancillary files, thereby protecting the host even further.

Some application control platforms can also prevent external media from being read from or written to. This can stop many avenues for attacks, whether it's a user attempting to run applications from a USB stick or someone trying to download data onto the USB stick. Some application control technologies can examine the serial number of a given external device to determine whether it is allowed to be used. This enables the organization to take advantage of external media for certain use cases while preventing its use for others.

Finally, some application control platforms offer memory protection for applications and data currently resident in the devices random access memory (RAM). This level of protection goes well beyond the simple monitoring of files and can further ensure the health of the host.

Discussing Application Control Effectively

Application control solutions also need to be discussed with management within the organization. Luckily, the discussion with management can be similar to that with operations. While management isn't tasked with taking the first support call, management does need to provide stable IT systems, a task further complicated by the need to plan at the organization level.

Considering your audience

The discussion for management and operations is somewhat similar insofar as both discussions have an educational aspect. There are other similar technologies available for application control. At the management level, there may not be an understanding of

the difference between a robust, full-fledged application control platform and a technology that appears similar.

Host-based application control can give a false sense of security when compared to the enterprise-wide technologies available for application control. Organizations typically don't rely solely on host-based firewalls. In the same manner, host-based application control shouldn't be viewed as an enterprise-wide solution.

When discussing application control with a non-technical (or semi-technical) audience, it's important to look beyond the technology itself and consider the non-technical benefits. Providing answers to questions like "How will application control help us be more productive?" and "What will happen if we don't implement application control?" is a start toward this thought process.

Another important step in obtaining approval for an application control project is to discuss how the project will be implemented, with specific milestones and deadlines. A phased implementation approach can be used as a basis for planning the implementation discussion with management. This discussion should begin with the benefits of application control as part of the security solution for your organization.


TIP

Success with application control sometimes means winning early champions by soft-launching in monitor mode and then slowly moving toward higher enforcement levels over time.

Tangible benefits of application control

Many of the benefits of application control that are seemingly technical also have a wider organizational impact. Some of those benefits are tangible and provide easily quantifiable improvements within the organization.

For example, consider software inventory. Every organization needs to maintain a controlled inventory of approved software and needs to know the devices on which the software is currently installed. Without application control, the organization must use and maintain another means for this software inventory.

However, application control not only maintains the software inventory but also ensures that only approved software can be executed. This benefit means that unauthorized software or rogue

installations of software are a thing of the past. With application control in place, your organization can use a single platform to monitor and maintain the health of the hosts. This leads to a reduction in costs for management and operations of the clients on and off the network.

Like software inventory, your organization should control the use of external media on its devices. Doing so prevents multiple avenues for attacks and security issues. For example, use of a rogue USB stick can lead to malware being installed on the computer if it's already present on the USB stick. Application control technologies prevent this.

Control over external media also prevents users from taking data. The intent of the user may be simply to take a spreadsheet home to work on it over the weekend or it could be to steal a customer list. Either way, the organization needs to maintain control over its privileged and confidential information. Application control platforms provide that control.

Some application control platforms can also help with compliance requirements. For example, PCI, HIPAA, SOX, NERC, and FISMA audits and compliance requirements may be met or even exceeded with deployment of an application control platform.

Intangible benefits of application control

When discussing application control at the management level, many of the benefits are intangible. The benefit of operations staff focusing more time being proactive rather than reactive isn't directly quantifiable. Yet the benefit does exist and is felt throughout the organization. This section looks at some of the intangible benefits that can be realized when deploying an application control platform.

Application control technologies can reduce the number and severity of support incidents, both security and non-security related. By ensuring a consistent and known set of applications on each host, compatibility issues become much less frequent. It's difficult to apply a direct cost to a simple reduction in support calls, though over time the effects of the reduction become tangible.

Application control technologies also help facilitate security response. The rich information available with an enterprise-level application control platform enables non-experts to assess the impact and determine the root cause. For example, if a host becomes infected with malware by clicking on a link in email, the application control technology can limit the impact of the infection across the organization and help recover the infected host by determining which file or files were altered.

In this way, application control technologies also help with overall host health. Monitoring file changes means that it's possible to know when a file changed and to see related changes, whether based on a known installation of software or a rogue software install.

Application control also helps to find undocumented job roles and business processes. For example, if users in the mailroom are being asked to track incoming inventory, an application control platform can help find that use case. Application control technologies, through allow listing, keep track of the applications that are authorized for a given group or set of hosts within an organization. Therefore, if the mailroom staff are attempting to execute an application for inventory, the use case can be properly documented. Without application control, that job function may never be found.

Getting Industry Validation of Application Control

Application control is considered by most experts to be the most effective form of attack prevention because it doesn't rely on knowing what's bad; instead, it knows what's trusted and allows it. This section includes an overview of how independent industry analysts view the benefits of application control and application control's place in securing today's modern enterprise.


TIP

Being based on an allow list means that application control provides a reasonable and accessible means to reduce risk from a variety of threats. Application control provides several key benefits when compared to security based on the negative security model, like AV, including the following:

- Reduction of malware infections and faster incident response due to real-time visibility
- Improvement of insider threat detection
- Blocking of unwanted and undesirable applications
- Limiting of the footprint due to unauthorized or unnecessary applications
- Identification of potential malicious activity by detecting new files and quarantining them in place, not allowing it to run
- Prevention of common attack vectors like Ransomware, Powershell attacks and other Living off the Land attacks
- Provision of centralized management capabilities for incident response, including the ability to search devices for specific files and processes

The National Institute of Standards and Technology (NIST) also provides guidance on application allow listing and recommends a phased approach to implementation. This phased approach is discussed in Chapter 4.

REMEMBER

Application control platforms have matured significantly and don't carry the burden of administration and maintenance that has been associated with allow listing technologies of the past.

IN THIS CHAPTER

- Implementing allow listing without a list
- Seeing the key elements of application control solutions

Chapter 3
Choosing an Application Control Solution

This chapter provides guidance and suggestions to help in assessment of application control solutions. Many solution vendors attempt to sell solutions that aren't really enterprise-ready and sometimes aren't even truly application control solutions.

One of the most important elements of an application control solution is the allow list. This chapter begins with a discussion of allow listing and how it works within the modern computing environment. You also examine some of the key traits exhibited by effective application control solutions.

Allow Listing without a List

One of the most common issues with traditional allow list technology is simply maintaining the list. Every time a new application needs to run, someone needs to approve it. Meanwhile, the person trying to run the application is left unproductive. The good news is that modern application control solutions no longer

rely solely on an allow list. This section discusses how robust application control solutions use policies and trust rather than just lists.

When evaluating application control solutions, two fundamental questions should be asked:

- How long will it take to implement the solution?
- What impact will the solution have on users?

Obviously, the length of time to deploy an application control solution depends on many factors. Some of those factors include the number of endpoints being protected and the maturity of the overall security infrastructure and processes. Application control implementations are typically accomplished in phases. This phased approach is recommended by The National Institute of Standards and Technology (NIST) and helps to ensure minimal impact. Chapter 4 discusses the phased approach in much more detail.

While the phased approach helps to minimize impact at deployment, it's also important to minimize any ongoing issues found with a robust security solution. Application control solutions should be able to allow known good software to execute without impact to the user.

But what about new and updated software? Application control would normally block new and updated software — software that hasn't yet been approved. Today's application control solutions should include rich approval mechanisms that enable your organization to automate many of the tasks associated with maintaining the solution.

The use of a policy-driven approach (see the later section "Policy-driven approvals" in this chapter) means that modern application control solutions no longer have the maintenance burdens once associated with this type of technology. ***Note:*** Not all application control solutions are policy-driven, so when evaluating solutions, this determination is important to make. Trust-based solutions are also important. The different ways an application control solution can use trust are discussed in the next section "Key Elements of an Application Control Solution."

Key Elements of an Application Control Solution

Several elements of modern application control solutions set them apart from traditional allow list solutions of the past. These elements help to make the application control solution more robust, more manageable, and more enterprise-ready. Conversely, application control solutions that are missing these elements may be more difficult and costly to manage. This section discusses some of the elements.

Policy-driven approvals

Policy-driven approvals are a central and key component to successful application control solutions. Policy-driven approvals mean that you're allow listing without a list. Approval of new and updated software is done based on trust. Policy-based trust can be driven by IT and through the cloud. The combination of both an IT-driven policy and a dynamic cloud-based trust policy minimizes the administrative effort required by IT while also minimizing user interruption.

IT-driven trust

IT-driven trust is defined by the software that IT deploys within your organization. By definition, this software is trusted and would therefore be allowed to run. The application control solution should automatically approve any files pushed or deployed by IT.

But beyond the normal software deployment process, an IT-driven trust scenario should include the ability to automate trust for things such as patch management, software repositories, self-updating applications, trusted users or publishers, software distribution systems, and the IT Help Desk.

Cloud-driven trust

A common issue that arises in dynamic organizations is the need for users to download and run software without having to go through a formal process and wait for IT to approve and install the software. For example, a development team may need to try a new framework or install software to migrate data. Having to go through a formal process would unnecessarily delay the development effort.

Application control solutions have typically not been palatable in these types of organizations. However, modern application control solutions can also utilize the cloud as another reference point when considering trust. This means that the application control solution can be configured to allow software downloaded by the user to run.

Obviously, allowing users to download and install their own software breaks the application control paradigm. But that's where the policy-driven, trust-based approach is key. In this scenario, software is evaluated based on an algorithm in the application control solution. That algorithm takes into account the threat intelligence gathered from the cloud and assigns a trust rating to the software.

From an IT perspective, a threshold for the trust rating can be set for the cloud-based trust scenario. Software below that threshold is still not allowed to run while software above that threshold is allowed to run. Essentially, this means that management of the application control solution requires no administrative effort.

Dealing with the unknown

What happens when both the IT-based and cloud-based trust policies are unable to assess the threat posed by a new file or application? These files aren't yet known to the application control platform and haven't been fully assessed as to whether they're malicious or innocuous.

In most cases, the application control solution should stop this application from executing. However, a more advanced application control solution enables your organization to define the trust threshold for unknown files and then define actions based on the trust value for that file. In other words, files below the trust threshold could be blocked while files that don't yet have a known trust value could be detonated (see the next section). The key is to find an application control platform that enables your organization to set these thresholds and to determine the actions taken.

Detonate and deny

The preceding section describes the ability to detonate an unknown file. In this context, detonation is a term used to describe deployment, installation, unpacking, or the like, in a secure area in order

to determine the contents and disposition of that file. For example, detonation may involve deployment into a virtual machine so the behavior of the file can be assessed.

REMEMBER

Through detonation a trust value can be assigned for a given file.

The normal behavior for application control is to deny by default. However, an application control solution should also be able to integrate with detonation services. The integration should be automatic, such that files are submitted to the service. If the files are found to be suspicious, the trust value can be assigned such that the file can't execute. Alternatively, the assessment results can be submitted to IT for further review.

Threat intelligence

Threat intelligence refers to the ability to determine the trust value for a given file. Cloud integration is the key component of modern threat intelligence. The real-time nature of the cloud, coupled with advanced and automated detonation, means that the application control solution can determine the disposition and trust value for a file as needed.

REMEMBER

To be most effective, threat intelligence needs to include the detonation along with any threat reputation scores available. By analyzing these sources of information, new intelligence can be applied immediately.

Open integrations

Many application control solutions are closed systems. The solutions don't play nice with others and certainly don't integrate with other systems well. When evaluating application control solutions, consider how well that solution integrates with your existing environment.

At a minimum, think about whether the solution under consideration can integrate with your security infrastructure, whether existing or planned. For example, integration with Security Information and Event Management Systems (SIEMS), log management systems, software delivery, and patch management are obvious. But even integration with your ticketing system is important. None of these should be taken for granted and ideally should be pre-built or included with the product to minimize the need for customization.

Speaking of customization, you may find the need to integrate with the application control solution in a different way, maybe from a custom ticketing system or other system. Some application control solutions offer open application programming interfaces (APIs) that help facilitate this scenario.

Automation

One of the largest challenges with application control has traditionally been the amount of manual administration and management required. With a modern application control solution, the amount of manual intervention is minimized.

Many of the common tasks associated with application control solutions can be automated but only if the solution supports the automation paradigm. For example, approvals of new software, file analysis, lockdown, file upload, and so on are all common workflows for application control administrators. If these can be automated, the amount of management and manual intervention can be reduced immensely.

The ability to automate these tasks and workflows means that your users enjoy rapid response while your organization reduces administrative costs and maximizes its return on the application control solution investment.

Flexibility

Application control isn't the same as deployment of a firewall, where one size fits all. Application control requires flexibility at the time of deployment and then continued flexibility to grow with your organization.

Application control solutions aren't meant to stop your organization from being productive as its needs change. The use of multiple methods for approval, such as IT-based and cloud-based trust, different levels of protection, and automated workflows are important things to consider as the needs of your organization change. For example, you may not need the custom API for the initial rollout, but then when a new type of system comes online, that API can mean the difference between integrating with the application control solution and having an outlier system. Flexibility enables the application control solution to become fully integrated and utilized over the long term.

IN THIS CHAPTER

- Implementing a phased rollout
- Using different levels of protection
- Automating security solutions

Chapter 4
Succeeding with Application Control

This chapter looks at application control with a specific focus on how it can be successfully deployed in a typical organization. The National Institute of Standards and Technology (NIST) recommends a phased approach for application control solutions. The goal is to find any issues early in the deployment, address those issues, and continue deploying the solution organization-wide.

Following the Steps of a Phased Rollout Approach

Providing an implementation plan is a key element toward obtaining approval and implementing the product itself. This section provides suggestions for the successful implementation of an enterprise-level application control platform in a typical organization. This approach can be used by organizations with a traditional life cycle approach to systems implementation and by organizations that use agile or agile-like methodologies.

A phased approach can be quite successful for enterprise-wide operational technology such as application control. The steps in this section can be used as a guide for such an approach.

REMEMBER

Although these steps aren't unique to the rollout of application control technologies, the steps do represent a means to be successful at implementation. The key takeaway is to find a solution that can offer the support needed to work through the phases successfully.

Step 1: Initial needs analysis

The initial needs analysis looks to identify the current operating environment within which application control will be deployed, along with the plan for use of the application control platform itself.

To accomplish the analysis, several sources of information are useful. For instance, a network topology is a typical source document that can be used to determine logical locations for enforcement points. Also relevant is the overall operating environment of client devices. For example, do all end-user computers authenticate with Lightweight Directory Access Protocol (LDAP) or a similar directory service? Further, does the network use role-based access control such as group-based membership? If the answer is "yes" to both then the directory service and group-membership can be leveraged for the application control platform rollout. For example, the application control technology may be rolled out in "monitor" mode for certain groups and "enforcement" mode for others.

If, however, the organization doesn't use a directory service or isn't using group-based authorization, the application control platform needs to be implemented through another means, such as device-by-device or in certain network segments.

But before I get ahead of myself, the primary deliverable for this needs analysis phase is to have a solid understanding of the existing environment along with the needs and expectations for the application control platform itself. Existing constraints are important to the conversation around the needs and expectations for the application control platform. If the application control platform must not interrupt certain mission critical hosts, these hosts aren't the ones that should be chosen to test the implementation. Also, if processing is heavier at certain times of the

week or month, these should be documented so performance isn't negatively impacted.

Systems with which the application control platform must interact should be documented and included in this analysis phase. For example, if there is a centralized logging system or standard built on which the system will be deployed, both should be included.

The key functional requirements of the system should be gathered during this needs analysis phase. For example, the hosts to be protected along with the level of protection should be included in the implementation plan. Application control platforms will have the ability to operate in a monitor mode or an enforcement mode. Many implementations begin in monitor mode and then switch to enforcement mode later.

A determination should be made as to what will be monitored by the application control platform. Most application control technologies can monitor application executables, ancillary libraries, configuration files, registry entries, and so on. In general, the more you monitor, the more you're protected. You should be able to monitor different things on different hosts. For example, you may choose a more stringent set of application control policies on certain high-value or highly vulnerable hosts and be less stringent on others.

REMEMBER

It may not be possible or even preferable to try to determine the correct balance of what to monitor during the analysis phase. Rather, it may only be after some hands-on time with the technology that you'll find the appropriate level of monitor and protection.

Another aspect of this initial phase is to develop policies for obtaining approval for an application to be trusted. For example, you may find applications that don't exist on the approved software list during the monitor mode deployment. The policy that users need to follow should be developed and documented now. With a cloud-based trust scenario, determining the trust threshold on which an application will be allowed to execute is also important.

Non-functional requirements such as acceptable levels of performance or performance impact should also be developed during this initial phase. Application control won't impact the performance of the end-user systems on which the software is deployed.

A common approach is to establish a baseline performance for tasks such as opening an application. This baseline can then be measured before and after installation of the application control software to ensure that the performance requirements are met.

Also consider things like the redundancy of the system itself as well as disaster recovery needs. It's likely that if an attack were underway the last thing you'd want is for the application control platform to go down. Analyze the needs around redundancy and consider the options available with the application control platform.

Step 2: Solution design

With the needs for the application control platform documented, designing the solution should be rather easy. The location of the application control enforcement points is determined by the previously gathered network topology and implementation plan.

The use of a directory technology like LDAP and group-based authorization also lead the solution design in a certain direction. For example, you may deploy a federated identity solution near the application control platform to avoid a performance impact on the primary directory service.

Finally, the decision to deploy with a pilot project also determines, at least in part, how the solution is implemented. You can undertake a pilot project in multiple ways. One option is to deploy in complete isolation to remove any adverse impacts on the production network. However, there may not be much value in such a proof of concept because the software won't be running in its true environment.

Another option is to deploy a true pilot project, where the solution is implemented but only to a small subset of individuals. Deploying in such a manner limits the overall impact of any possible, however unlikely, adverse consequences while at the same time maximizing the chance of success when the software is deployed to a wider audience.


TIP

The phased implementation, with a pilot followed by wider and wider grouped deployment, is typically the best path toward success for an application control platform. The ability to deploy in a controlled fashion minimizes possible support needs. The ability to show early success is also helpful within the organization and can gain champions for application control.

Step 3: Pilot implementation

The pilot implementation gives you a chance to experience application control in your own environment. Doing so provides the benefit of relative isolation while facilitating learning about the application control platform. You may try to implement first in a monitor mode and then go into an enforcement mode on the pilot implementation.

Just as it's important to deploy the pilot in isolation, it's also important to ensure that the hosts chosen for the pilot are under control of technical staff — possibly those who are in control of the pilot project itself. Deploying it to a non-technical audience may result in negative visibility for the technology at a critical time.

Before starting the pilot, any target hosts should be scanned for malware and existing security issues that could compromise the pilot implementation's validity. One of the first things that you'll do is to begin generating a policy for software that will be trusted.

REMEMBER

Modern application control solutions move away from allow lists and toward policy-driven trust. Ideally, the policy should approve 90 percent or more of the relevant files for your organization. The remaining 10 percent should use a data-centric, iterative approach to identification and assessment. This approach helps find additional use cases that generate the most files and affect the most devices.

Additionally, a solution that offers field-tested design patterns can help with assessment of additional use cases. The goal is to be able to develop policies for these use cases quickly, thereby making the final deployment easier.

Several aspects of the pilot should be examined to decide if the platform is appropriate and to look for ways to improve the implementation as the solution is deployed to a wider audience. These considerations include the following:

- **Overall suitability for needs:** Examine the functionality of the platform to figure out if it's the best fit for your organization. At its simplest, does the platform detect modifications to applications? You may install a patch or make other modifications to the application components to see if the application control platform detects the changes and how it reacts.

- **Ease of management:** Determine how well the platform fits within your existing workflows and the needs for the care and feeding of the platform itself. If the platform requires a lot of maintenance, that should be noted and considered as part of the larger overall rollout. However, note that it's typical for these types of platforms to require some amount of initial configuration, so be careful when extrapolating the amount of management needed for the larger deployment.
- **Performance:** Assess the platform's performance impact, including normal use cases and use cases where the host is expected to perform process-heavy transactions.
- **Platform security:** A security solution shouldn't create a security problem. Assess whether the platform itself has or creates security issues. Things like open ports, vulnerable third-party software, and so on can be examined to see if the platform itself is vulnerable.
- **Integration points:** Assess how well the platform integrates with other technologies in your network. For example, the platform should integrate easily with your directory service but may also integrate with centralized logging and alerting solutions. The pilot is the perfect time to learn about these integration points.

REMEMBER

The goal of the pilot is to prove out the platform with real-world scenarios while also helping you learn about the platform itself.

Step 4: General deployment

With the pilot successfully completed, you can begin to deploy the platform to a wider audience. Before starting a general deployment, some training needs to be provided to IT staff tasked with taking the initial support call. When an application control platform is deployed, a process is necessary to help users get up and running.

TIP

Deploy initially to a small number of hosts in order to assess the impact on the management servers as well as reduce the impact of unforeseen issues.

One method for deployment is to use a phased approach. With a phased approach, the solution is deployed to a small subset of hosts within a group. It's likely that any configuration concerns

will be found early; therefore, if you limit the number of deployed hosts initially, any such concerns can be addressed without overwhelming staff or end-users.

Within the context of a phased approach, new groups of hosts can be deployed in monitor mode at first. Doing so enables the security team to determine potential impacts to that group of hosts without impacting their productivity or use. In fact, there may be a subset of hosts on the network that never go beyond monitor mode. For example, dynamic machines belonging to sales personnel or solution architects that can't afford the potential of application denial that may occur in enforcement mode are candidates for a monitor-only scenario. Even in monitor mode, the application control platform provides the forensic benefits and the ability to track overall host health.

Step 5: Solution management and refinement

As the solution is deployed to wider and wider groups within an organization, the long-term maintenance of the solution will decrease. Monitoring of applications that haven't yet had a determination made on them is a task that's performed as part of routine security operations activities.

Several things occur during management — many of which are common to any enterprise software. Some of these common tasks include the following:

- **Applying patches to management stations:** The management servers for the solution need to be patched. One best practice is to test in an isolated manner.
- **Applying patches to client hosts:** The software deployed on each host also needs to be updated from time to time. It's important to test these updates by deploying to a limited set of hosts, just as you would as part of best practices for patch management.
- **Updating policies and support:** As with any security solution, you may discover changes to approval policies or other policies around the use of the solution. These aren't unique to application control technologies but will be something that occurs with this solution.

What has become far less common with modern application control platforms is maintenance, including

- **Updating approvals:** A frequent task, especially when other software was installed or updated, was to update the software approved to run. The complexity of the task was directly related to the application components being monitored. If extended components such as registry entries and configuration files were being monitored, the update would've needed to include those components. However, when using policy-driven trust and if automation is available, this task becomes much easier.
- **Testing the solution:** Regular tests of the application control platform were common to ensure that the solution was running properly on client devices.

Enabling Different Levels of Protection

A crucial element for any application control solution is the ability to deploy various levels of protection to different hosts. This is a key advantage of an enterprise-level application control solution over host-based or native application control software included in some operating systems.

This section looks at various levels of protection that may be applied within a typical organization.

Risk assessment: Revisited

Prior to determining which hosts or groups should receive which levels of protection, you need to understand the risks to various systems in your organization's network. For example, the risks for all client systems that use email are different than they are for those systems that have no internet access.

In addition, the risk level associated with an individual who has elevated privileges or access to confidential information is higher than it is for a standard employee who has basic access to the systems. For example, an attacker may target executives or human resources personnel within the organization and attempt to install malware or key loggers on those client devices.

TIP

When assessing risk, look not only at the software installed on the host but also the typical use cases for that device.

Enabling different enforcement levels

Risk is one factor in the decision of enforcement levels or modes for the application control solution. Another factor is tolerance for loss of productivity. Critical hosts on the network may not be the best hosts on which to learn about the nuances of the application control solution. In those instances, monitor-only mode may be preferred until after a pilot implementation. Devices used by executives may also be a good place to begin with monitor-only mode so as not to potentially disrupt their productivity during initial phases.

In this context, deploying in a monitor-only mode for highly visible or mission-critical hosts is one approach that can lead to success. When internal management of the solution has been refined and those critical hosts have been monitored for an appropriate period of time, the organization can look to move toward a higher level of enforcement.

A robust application control solution will be able to deploy to diverse groups and monitor different things on those hosts. For example, a high-risk group of hosts may use a monitoring or enforcement profile that includes all relevant application components, such as registry entries and configuration files, while another group of hosts may monitor only application executables.

When it comes to application control solutions, flexibility is key to success. The flexibility to monitor or enforce and the flexibility to deploy in a phased manner are both crucial for any application control deployment.

Don’t Set and Forget

While there may be a desire to set and forget with a security solution, that’s just not possible in today’s dynamic environment. Attacks are constantly evolving, and the perpetrators of those attacks are becoming more and more sophisticated. The types of

devices being deployed in today's enterprise, even compared to a few years ago, dictate that security solutions must evolve along with them.

Security solutions that feature automation can help alleviate the issues surrounding the need for constant and evolutionary management against modern threats. Ensuring that the right teams are available to address those threats, and the anomalies that occur because of new threats, is important.

IN THIS CHAPTER

- Looking at the best practices for analysis and design of the solution
- Deploying with limited scope and impact
- Expanding and improving the solution

Chapter 5
Ten Key Points when Considering Application Control

This chapter provides ten (okay, there's only nine) key points around selection and implementation of an application control solution. Remember that selection of your solution should be based on your needs and the abilities of the solution under consideration.

Look for Flexibility

A primary step in any system rollout is to analyze the environment in which the solution will operate along with the expectations for the new system. This analysis must include both the current and future needs within your organization.

TIP

A flexible solution enables you to match the application control implementation to your existing prevention strategy. Key questions to ask about an application control solution include the following:

- Will the system integrate with a directory service such as Lightweight Directory Access Protocol (LDAP)?
- Where will the endpoints and management servers be located?
- What level of availability is necessary for the enforcement points?
- Are there disaster recovery needs around the solution?
- Are there specific legal or regulatory requirements that the solution must meet around compliance?
- Who will manage the solution and what are the expectations for support?

Providing answers for these questions and any related questions that arise as part of the analysis helps determine the best architecture and appropriate implementation strategy for the solution.

Look for Policy-Driven Trust

When the application control solution is deployed, a new application will likely need to be approved. A modern application control solution should use policy-driven trust. With policy-driven trust, an application can be executed based on policies driven from IT and from the cloud.

IT-based trust includes things such as software deployed by IT through normal distribution channels. Cloud-based trust includes gathering threat intelligence from the cloud, including a trust rating for a given application. That trust rating can be combined with IT-configured thresholds to determine if the application can run.

The use of policy-driven trust helps automate the process of application control management and is a key element to being successful with application control.

Automate

While policy-driven trust helps to reduce both the cost and effort of application control, ideally more automation would be available. Maintenance of application control follows similar workflows and patterns. Any automation of detonation, approvals, and other processes reduces the workload of security administrators to perform other, innovative security related tasks.

Integrate

The ability to integrate with other products reduces the need for separate management of many aspects of the application control solution. Integration can take place between application control solutions, log management software, and other security assets within the network. Further, choosing an application control solution with an open Application Programming Interface (API) ensures that integrations and automation can be done for today's software and for those pieces of software not yet invented.

Pilot with Limited Scope

TIP

One of the most fundamental things you can do with an application control pilot is to implement the solution in limited scope. This means deploying the solution to a small set of hosts, ideally hosts used by the project team, and then improving the solution from there. By deploying in a limited manner, you can show early success and also learn about the technology.

Deploy in Monitor Mode

Most application control solutions have a way to monitor applications while learning about the environment. When used in monitor mode, the application is allowed to execute and the attributes of the application such as additional required components are recorded or audited by the application control solution. When deployed in monitor mode, data can be gathered from typical

hosts on which the solution will be deployed. Deploying in monitor mode gives the project team a chance to learn more about the application control platform without affecting end-users.

Expand the Deployment

You'll learn a great deal about the organization and its security needs by assessing risk and designing the application control solution. As you become comfortable with the application control solution, consider expanding to other groups or other hosts within the organization. Even if you do so in monitor mode, the information gathered is valuable for the final deployment.

Expand the Application Components

When first deployed, you may choose to monitor or enforce simply on the application executable alone. However, some high-value hosts require an additional level of protection. In these cases, or as your understanding of the application control solution expands, you can expand the components being monitored or enforced by the application control platform.

For example, you may monitor configuration files, application libraries, or other files related to an application to ensure that those components don't change. Doing so provides a greater level of protection than simply monitoring the application executable.

Test Before Deployment

As with any technology solution, you should always test before deployment. If hosts are in enforcement mode, then you should be rigorous in verifying all application and operating system updates before those updates are deployed to the hosts. If you're using policy-driven trust then patches pushed from IT will be automatically trusted, thereby alleviating the need to maintain the allow list.

Allow only trusted software to run

Application control secures critical systems, prevents unwanted changes, and ensures continuous regulatory compliance. By employing a positive security model, which enables a default/deny security posture, application control continuously protects against cyberthreats that evade traditional security defenses. Instead of a library or list of files to maintain, use automated approvals, such as IT and cloud-driven trust, trusted publishers, custom rules, and validated external sources, to protect your environment.

Inside...

- The value of a positive security model
- When is antivirus not enough?
- The benefits of application control
- Being proactive, not reactive
- Application control best practices
- Key elements of application control

vmware Carbon Black

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-22518-7
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.