WHITE PAPER

Carbon Black® App Control

Observations and Strategies for Success

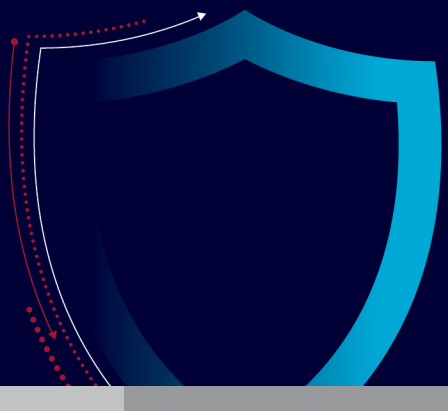


TABLE OF CONTENTS

Executive Summary

It's widely recognized that antivirus software is insufficient to protect organizations, large or small, from advanced threats and targeted attacks. In response, organizations increasingly look to adopt proactive approaches to organizational security, such as application control, to ensure the fidelity and security of intellectual property.

While highly effective, application control is not always a frictionless technology and requires security personnel, company end users, and management, who may be accustomed to signature-based solutions, to think differently about security.

There's no silver bullet solution when it comes to cyber security. But when done right, application control can help organizations protect their most important assets and become more efficient, accountable and productive in the process.

This white paper, based on experiences gathered from more than 1000 application control deployments, provides a blueprint organizations can adopt to help ensure their successful application control deployment. It also outlines how our unique trust-based approach and dedicated support of customers can greatly simplify the process of achieving high enforcement in your environment.

Overview

You may have heard that application control is too hard, but the fact is that's not true, and this paper will explain why. With the rise of advanced threats and targeted attacks, it's clear that endpoint security is no longer a set-it-and-forget-it solution. This paper will explain why deploying proactive solutions such as application control—that provide real, proven, high levels of security—no longer has to be too hard.

No matter how open or dynamic your environment, there's a straightforward path to success with application control. The path maybe different for each organization and, at times, may take you down a path less traveled. However just because a landscape is unfamiliar doesn't mean it's too hard, and that is what this white paper will explain.

THERE'S NO SILVER BULLET SOLUTION WHEN IT COMES TO CYBER SECURITY. BUT WHEN DONE RIGHT, APPLICATION CONTROL CAN HELP.

Like anything worth doing, there are better ways and inappropriate ways to accomplish something, and the same holds true for application control. Broadcom products have helped thousands of organizations successfully deploy application control in their environments. Along the way, we've developed a set of proven strategies and leading technology solutions to ensure your success. This paper will outline how you can employ these best practices to successfully deploy an application control solution in your environment.

In security, we talk about the observe, orient, decide, act (OODA) loop. The next section of this paper will help you observe the new landscape, orient yourself within the end-user landscape, and safely navigate the deployment process, so you can quickly get on to what you do best: keeping your organization secure.

The New Threat Landscape

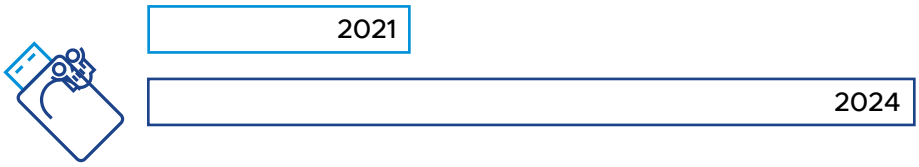
What's different about cyber security today than 10 years ago? The answer is simple: more hackers and more endpoints. Back then, there were fewer hackers and relatively few devices connected to the Internet. The threat actors numbered no more than a few thousand.

Fast-forward to today, and now your refrigerator, wristwatch and car are online. Half of the world's 7 billion people are connected. Nations have standing cyber armies tens of thousands strong. And for every cyber soldier, there are a dozen or more hackers making careers in private markets.

Yes, careers.

Ten years ago, hacking was mostly about egos. Who could get in, who could wreak havoc; it was all graffiti, all bragging rights. Motivations were personal . Today, hacking is a more than $5 billion business, with shops, guilds, and even regular work hours. Hackers have their own formal markets and even private currencies in which to buy, trade and profit off your secrets.

Figure 1: Ransomware is part of more than one-third of all security breaches, tripling in frequency since 2021, according to Verizon's 2024 Data Breach Investigations Report.[1]



Hacking is no longer a game but a strategic threat. Hackers now have the same motivation, resources, organization and staffing as you and your business. You aren't dealing with someone trying to break in through a back window; you're dealing with a true peer, a professional. In a lot of ways, you're dealing with an entity not unlike your direct market competition.

If yours is like most organizations, you don't treat hackers with the same focus and attention you place on your competition. But if you did, how would that change your perspective? How would you envision, plan, budget, motivate and execute security if the security threat were as big and knowledgeable as your competition? If that's not how your team is addressing security today, it should be.

HACKING IS A MULTIBILLION-DOLLAR BUSINESS

Moving from Passive Protection to Proactive Defense

Firewalls are real security. Antivirus is real security. The U.S. Coast Guard cutter along our shores and the Transportation Security Administration (TSA) guard at the airport checkpoint are real security. But their threat landscape is like ours was 10 years ago. For the most part, the volume is low and motivations are personal. That allows them to focus on more passive, perimeter-based security.

When the threat landscape changes from small bands of random threat actors to large armies with focus and motivation, that kind of security is no longer sufficient. You don't just need a fence and a lookout; you need a fort and an army.

If you have no idea how to build a fort, and the idea of having to keep guard scares you, then you're worried that application control is too hard. And that's because, up until recently, the tools were limited, and real security was assumed to be the province of well-funded security experts. The technologies and automated solutions that Carbon Black® App Control offers have changed that.

There will be additional effort and planning, but the layouts are similar, and your intuition will often guide you in the right direction.

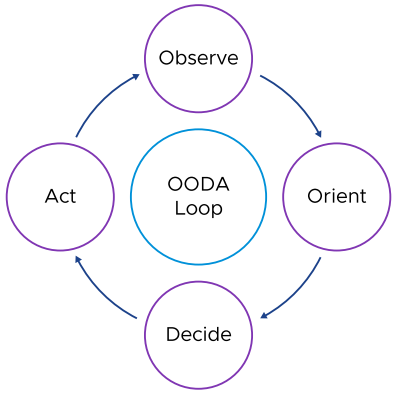
Here's how your role will change as an application control guard:

- Incidents happen more often, and you have to sound the alarm and take action.
- Expect to allocate more staff time to the solution.
- Delegate tasks across existing functions to spread out responsibility.

The difficulty of application control isn't the raw work, it's the time it takes to change perspectives. End users don't like change, as anyone who has worked in IT operations can attest. But they will change when properly educated and informed.

Traditional antivirus solutions and other machine learning controls allow all applications to run unless they are known to be malicious or they exhibit known- bad behaviors. In a world where 70% of malware is used only once, this approach doesn't work because you simply can't know what is bad ahead of time. Using antivirus for protection is like scanning a crowd for a threat actor, only you have no idea what they look like.

Figure 2: The OODA Loop



Why Application Control is Essential

Application control reverses this paradigm and focuses on identifying and only allowing the execution of known and trusted code. This approach is far more effective at blocking new and unknown malware, along with generalized malware techniques, because it doesn't need to know what is bad ahead of time.

For your company, application control seeks to create an internal software environment not dissimilar from the Apple App Store, where only approved apps are allowed to run, except you get to decide what's allowed.

Application control solutions have come a long way in limiting the setup and administration burden associated with identifying trusted software. Leading application control solutions, such as App Control, also include real-time access to software reputation scores on known-good applications and malicious programs from Carbon Black Cloud, as well as access to detonation engines and even metadata on all binaries, such as prevalence, age, code-signing information, and known vulnerabilities associated with that software.

Application control provides numerous operations and security benefits when compared with traditional antivirus, such as the following:

- Reduces malware infections and speeds up incident response due to real-time visibility
- Improves detection of insider threats and risky end-user behavior
- Blocks unwanted potential backdoor applications (torrents, remote access, spyware tools, security probes) that antivirus does not detect
- Reduces vulnerabilities by limiting software sprawl
- Allows early warning of potentially malicious new files by identifying gray files, even in monitor-only mode; advanced solutions can send unknown files to a malware sandbox for automatic analysis
- Blocks common malware techniques and indicators of compromise (IOCs) via policies (for example, no execute from trash bin, no double filename extensions, and no header extension mismatches)
- Provides granular incident response investigation capabilities, including a rapid search of all PCs for a given file or process, centralized removal of unwanted or malicious software already deployed, and blocking any newly discovered malware before antivirus signatures are available

When implemented correctly, application control will provide the highest level of protection against malware infections and targeted attacks. When leveraged as part of IT operations, it can have the additional benefit of reducing the operational burden of uncontrolled application sprawl and volume license control.

Organization Change and the Importance of Education

It's important to understand that the journey to high enforcement is as much about behavioral change as it is technology. For those accustomed to unfettered access to the Internet and applications of their choosing, it may seem like an insurmountable affront to their workplace freedom.

You need to know this and be prepared to handle these objections. The training is straightforward and the disruption is minimal, but adopting new habits takes time. Here are five examples of the most common behaviors and mindsets that create barriers to successful application control and what you can do to tear them down.

Don't Limit Me

No one welcomes security controls. Even security professionals tire of the restrictions they place on themselves, but they accept them because they know the restrictions are needed. Don't expect everyone in your organization to welcome application control. However, there will be those who understand the importance of protecting their personal information and your organization's intellectual property. Utilize these individuals to spread the cause throughout the end users. Change will be slow, but keep everyone focused on the value, and it will happen.

You'll Hurt my Productivity

A firewall is relatively easy to implement because it obstructs only auxiliary value, often in a way that only causes latency and no permanent effects. However, disrupting users' workstations and applications stands directly in the way of their productivity. Be prepared to minimize the disruption and continue to explain the value of change in protecting their intellectual property.

But you're already familiar with this kind of implementation. If you remember the early days of deploying antivirus, or the last time you had a major antivirus vendor change, you're on the right track. If you've deployed endpoint data loss prevention (DLP) or rolled out full disk encryption, consider yourself more than prepared for the relative ease of deploying App Control.

If you think this is like rolling out an application, it isn't that easy. If you think it will be like taking away user administration rights, it isn't that hard. Think "affordable and effective endpoint security agent," and you're on the right path.

There's Too Much Gray Area

Security professionals live by a set of core principles. They train in and are certified by these principles. One of the rules security professionals follow is if it will cost more to protect an asset than the value of that asset, then do not protect the asset. Think about that for a minute. If you consider the operational cost of that, well it's free, and you do nothing. If you analyze it from a profit perspective, it makes sense; you're simply cutting your losses. Still, from an emotional standpoint, it's difficult to accept. No one wants to take a loss.

As you are now going to be doing security like the pros, you will need to become familiar with this type of decision-making to be able to navigate in this gray area. At first, your security team won't want to build just a fort, they will want the perfect castle. And your operations team won't tolerate any infrastructure or end-user impact ever (even though this is IT and it happens every day). Helping your organization come to terms with the nuance may actually be one of the hardest parts of deploying application control.

CARBON BLACK APP CONTROL CONFORMS TO THE UNIQUE WAY YOUR ORGANIZATION WORKS

As a business leader, you're already familiar with limited resources and too many asks. You make tough decisions every day; most of them are successful, and you recover from the ones that aren't. In IT, stuff happens. In security, compromise is inevitable. The goal is just to stop as many threats as you can and react quickly when something gets through.

If you think App Control is a perfect castle and you can let users run wild inside it, you're still thinking too easy. If you think that your security team is going to be tied up endlessly approving application updates, you're still thinking too hard. Think "mostly automated mechanisms built around appropriate risk tolerances," and you're on the right path.

I Never Had To Do That Before

In the new threat landscape, the most common way to break in is to phish. Basically, this means you convince, cajole or otherwise fool a user into installing a hijacked application. The second most common way is to make use of an exploit and then make like IT. You use one of the vulnerabilities you've read about in the papers to catch hold of some IT administrator or operation, and then make your way to your ultimate target.

Attacks show as anomalies, no matter how subtle they are. But anomalies only exist when there are norms to compare them against. When users are allowed to do anything possible, it becomes impossible to see the anomalies. Getting user to do it the same way can get you a huge security win.

It's a common application control technique to allow users to self-serve, so long as they follow a process. While it's not perfectly secure, it does increase security by orders of magnitude. Asking IT to run tools from a sandbox folder or asking users to drag installers to a safe-prompt folder, can change security triage from impossible to affordable.

Are you ready to ask employees, just in some circumstances, to change their work habits just a little bit? If you're not ready to make requests of your employees, you may not be ready to respond to the new threat landscape. At Broadcom, our experience is that users care about their jobs and the success of their company, and that when you communicate effectively with them, you can successfully ask them to change behavior. They, too, are concerned about the future.

Isn't the Free Antivirus Good Enough?

The old way of doing cyber security has become commoditized to the point where Microsoft and a host of smaller vendors offer their antivirus products for free. Why are they able to offer these for free? Because the old ways aren't working, and the value gained from implementing them is declining.

Real security can't be free; its value should be reflected in its price. It can't be because of the explosion of hackers and endpoints. You have to match the enemy, and that includes in terms of finances.

But it's not an easy adjustment to go from free to budgeting a percentage of your IT spend. It's not just the emotional aspect; it requires real decisions about resources, and real effort to change operations. However, it's also true that just throwing money at something will not fix the problem. IT security is about reducing risk to a manageable level, and every decision should be based on the ROI you expect to gain in terms of risk reduction.

If you're still hoping there might be a shortcut, you may not be ready for application control. But if you've made the adjustment, you're ready to take the next step.

Implementation Methodology

Let's say you've decided to go down the path of implementing application control for your employees, but you have no idea where to begin. You understand antivirus and you've deployed firewalls, but application control is a whole new situation. Wouldn't it be great if you could access people who have successfully deployed application control in a variety of industries, across a wide range of user types, with tools that were flexible and comprehensive?

This is where our teams can help. Our teams have spent the past 10 years managing successful implementations in companies large and small, controlled and open, onshore and offshore, in every industry—and with integrating into the larger security stack. They operate according to a documented methodology that's proactively shared with every customer. When you implement App Control, the Professional Services team will guide you through that methodology, help adapt its flexible parameters to the needs of your organization, and provide you with reports and deliverables that document your progress.

Step 1: Utilize Big Hardware to Accommodate Big Data

If you're familiar with App Control, you already know that continuous real-time recording of file operations and process executions is critical to it and to any modern security technology. You may have guessed already that this means big data, and that, in turn, means big hardware.

We will begin by making sure you have the right infrastructure to handle your needs. There will be a very strong focus on database storage performance and throughput. We will provide sample specifications, throughput requirements, and test tools, so you can shape the infrastructure to your existing vendors and operations.

Step 2: Configure to Your Organization

If you've tried deploying other application control solutions before, you've probably discovered that most of them require your organization to conform to the way their technology works. App Control conforms to the unique way your organization works by including rich approval mechanisms, such as trusted publishers, trusted directories, software reputation, detonation engines, and more, along with dynamic policy groups. During the design workshop conducted at the beginning of every project, we will assess your organization's security posture and culture, IT operations, and aesthetics to determine which features are right for your use cases .

This assessment takes about an hour during our face-to-face time in the design workshop. We ask if your general security posture will be open or closed, if your IT operations model is staff- or automation-centric, and if the answers are different for different areas. We then recommend what features to use as part of your primary trust strategy, and help you understand the security footprint and operational characteristics.

Step 3: Build Approval Policies

You may be thinking of application control as an actual allowlist. That comparison isn't always helpful, but there are times when it's perfectly true. If files aren't approved, then they aren't allowed to execute. We need to look at the list of files arriving on computers and see if they are getting approved. You may be thinking there are a lot of files to look at. Ours is a policy-based approach, not a list-based approach.

CONTINUOUS LEARNING IS PART OF THE MODERN INDUSTRIAL LANDSCAPE, AND IT APPLIES TO SECURITY

Our experience shows that policies chosen as part of the primary trust strategy will often approve 90% or more of the relevant files right away. For the remaining 10%, we then leverage a data-centric, iterative approach that allows us to identify the additional use cases that generate the most files and affect the most machines. Field-tested design patterns for many use cases, and a straightforward syntax for creating rules, enable additional policies to be developed quickly.

Step 4: Solve For the Last Mile

By implementing just a few policies, or primary trust strategies, you can cover 90% or more of all file approvals. But if you're familiar with the 80/20 rule, you know that 80% of success takes 20% of your effort, and then getting to 100% success takes the other 80% of your effort. In some cases, often for highly controlled, fixed-function environments, you won't have to worry about the 80/20 rule with application control because the primary trust strategies solve 100% of the problem. Even in more dynamic environments, they often solve 95% to 98% of the problem. It is that final 2% that can require careful handling and may take significant effort.

What is it about this final 2% that can make it so hard? It is infinite variety and lack of consistency.

For example, in a large company with 10,000 application servers, the issue with the final 2% is logistical, not technical, due to varied ownership across the organization. Often, individual applications are hosted by no more than 20 servers. So that means there are potentially 500 different application behaviors and updater workflows that need to be accommodated for application control. And it's likely that each of these applications is overseen by a different group. While in practice, relatively few of these applications actually need accommodation and the rules for them are quick to author, but simply reaching out to 500 different operators can take time and effort. In this case, the challenge is human rather than technical, but it is one you should respect and include in your implementation timelines.

Another example is entrepreneurial end users. In this case, consider the creative and entrepreneurial end users who sit in cross-functional roles and often are provided very wide latitude for getting their job done. These people tend to use a huge variety of tools, may be creating their own lightweight automation, and may even be using consumer or personal applications to meet job requirements. In such a mass of what seems like random behavior, it can be hard for even the most seasoned administrator to discern what to allow and the best accommodations for various workflows. In this case, the issue is technical as several custom rules or policy groups may need to be set up to meet the unique needs of a small group of users. Communicating goals, process, requirements and expected outcomes to these user groups prior to deployment will help them understand their role in educating you on their work needs.

MAKE SECURITY LESS ABOUT ENFORCING CORPORATE POLICY AND MORE ABOUT CATCHING THREAT ACTORS.

Step 5: Use Metrics to Manage

Many questions arise during the implementation process:

- How do I know if we're in the easy or hard part of the 80/20 rule?
- How do I know which users are or will be the harder ones to lock down?
- How can I know which users are more stable and if I should try to lock them down first?
- How can I account for unknowns if I'm trying to build a project plan?
- How can I know how many phone calls will show up at the help desk?
- How many incidents are going to get escalated to the security operations center (SOC) team?
- How long is this going to take, and when will I be done?

To answer these questions, you must first have a firm understanding of your environment and the technology resources that will be required. To help customers navigate this planning process, App Control provides you and our services team with data-driven intelligence about your environment, and our services team leverages a metrics-driven methodology. So no matter the situation, there is an agile and efficient way to deal with the areas that, by their nature, must be more flexible.

Step 6: Delegate Tasks

Modern security can't be just set it and forget it. Hackers bring the human element in huge volume, and we must do the same to combat them. Luckily automation can still do most of the work, so we can focus on the high-value exceptions and action items.

Part of completing your App Control implementation is making sure the right teams and personnel are prepared to handle those infrequent but important exceptions. The best teams are those with diverse sets of skills and experiences, so you might find yourself with a team made up of IT, security and help desk professionals as well as end users.

Building a team often starts with delegating. Being able to delegate appropriate tiers, run booking and scripting activities is part of what makes staffing an App Control deployment affordable and effective. The trick is now to try and make security experts out of everyone, but rather to delegate tasks that naturally fit with existing skills and processes. Adding minor items to a local allowlist is something that can be easily delegated to the help desk, to managers and leads, or even to users themselves via a self-service mechanism—no console access required. This part is easy to accomplish but also critical to ongoing operation. Luckily, automation can still do most of the work.

Step 7: Automate Continuous Learning

As you handle exceptions in human fashion, triaging and remediating the anomalies you see on a weekly basis, you will begin to see patterns. Some of the patterns may cause you to wonder if there might be better ways to configure your policies, or possibly even to automate some of the work you're doing manually.

Continuous learning is part of the modern industrial landscape, and it applies equally well to security. As you become increasingly familiar with our technology and how it operates in your environment, you most certainly should make improvements where you see fit.

If you think full automation is part of that improvement loop, App Control includes a rich REST API out of the box and offers access to a comprehensive set of partner integrations. You can quickly integrate App Control into your security stack, and customize your engineering and orchestration, without needing to be a senior programmer. Integrating App Control into your security information and event management (SIEM), sandbox, firewall, threat intelligence, and analytics platforms will allow you to automate actions and enrich the quality of alerts before they show up on your screen.

Success Stories

You may be familiar with the old phrase, knowing is half the battle. We hope this paper has increased your understanding of what it takes to implement application control efficiently, and how our technology and services help make it easy. Of course, the other half of the battle is knowing you're surrounded by people who are going through it with you, and understanding what you can learn from their experiences.

With that in mind, here are some brief stories based on our customers' real experiences with application control.

Internet Giants with Young End Users

Many of us are familiar with the stereotypes common for millennials and Generation Y. Certainly one is that they require flexibility and creativity in their work culture, which doesn't necessarily lend itself to security discipline, at least not in the more traditional sense.

Some well-known Internet giants harnessed that culture to their advantage. Their entire business model is designed around fostering flexibility and creativity, and driving value with the best outcomes. They are continuous innovation machines, where everything is constantly changing.

Some of those companies have App Control installed in a fully locked-down, high-enforcement mode. They aren't even using a block-and-ask user bypass mode. They accomplished that by focusing purely on outside persistent threats. When you make security less about enforcing corporate policy and more about catching threat actors, that allows you to get creative. In addition, they found that trusting users, peers and leads to make good security decisions will work if you give them the right scope and context. Still, a third factor is related to an understanding that a breach is inevitable, and a strong program of detection and response, such as that offered by Broadcom, is a cornerstone of any robust security program.

These companies host some of the most open and dynamic work environments and yet they've got application control locked down. Being comfortable with the nuances of security is the key to their success.

Companies with Lots of Business Units

Even controlled environments can show chaos, depending on how you think about it. There may be strict corporate policies about software procurement, but with a huge number of teams and departments, the massive variety of approved software becomes unfathomable. Companies with many lines of business, or that have grown by acquisition, may have many hundreds of different business-critical applications deployed.

What once seemed like a straightforward approach can now seem like a bit of chaos. This can be especially true if some of the problems are very sticky to diagnose, or if the end users are propagating irresponsible and negative rumors

about the project. Overlay competing schedules and priorities, and suddenly making application control successful has become a long process.

It's like riding a bicycle 100 miles. Part of it is knowing how to ride for endurance. Part of it is having prior experience getting there successfully or having faith that you'll be able to do so. There is a skills piece, but also a psychology piece.

Some of our customers have, in fact, gone through this long process. The most important keys to their success were mandate and consensus. Hearing from executives how important it was, and communicating with users about meeting their needs, not just once but repeatedly, is what made the process both bearable and fruitful. Ongoing incremental successes build powerful momentum because each incremental success delivered immediate security improvements for all involved.

Companies Facing a Breach

Just as having the right perspective can make a project successful, a misguided perspective can cause delays and failure.

It's not uncommon for customers to be in a breach situation when they first choose to purchase. They are experiencing the new security landscape firsthand, and they need to stop the breach as quickly as possible. A customer may think, "It's just a list. I can build a list. How hard is that?" We don't mean to say that customers oversimplify what it takes. Rather, in coming at it from this list perspective, they design the wrong methods for getting configuration built correctly and swiftly.

The difficulty is that, in a breach situation, forces have already been assembled, expectations have already been set, and no one wants to hear that they must go back to the drawing board. This is especially true if days or weeks of planning have already occurred, or when authorities have set deadlines for getting controls in place. Taking a step back is hard enough when you're in a panic, and much harder still when you're already headed down a certain road.

Broadcom understands and provides an emergency workshop that allows customers to take a step back. Typically, within just one day of face-to-face interactions, they are able to realign their expectations about how application control works. This crucial moment of planning results in swifter and more efficient implementation, and better management of stakeholder expectations. Taking a methodical approach turns difficult situations into long-term wins.

Companies with an Organized Environment

We know what happens when an environment is open and dynamic, when it is large and varied in character, and when a perspective is still shifting paradigms. But what happens when none of that is true? What happens when the environment really is highly controlled and well understood, when there is a limited amount of possible configurations, and when there's time to understand the necessary changes and the right approach?

In that case, application control can be quick and easy. The strongest and oldest customer base of App Control is point-of-sale systems. Generally, the configuration of these machines is highly controlled and infrequently changed, and they come through a very short list of well-understood channels. There are only a few types of machines and functions, and usually one or only a few markets and regions. Despite the high-profile breaches you've read about in the news, most point-of-sale customers aren't in a difficult situation but are instead working proactively for both security and compliance reasons.

CUSTOMERS WHO HAVE TRIED AND FAILED TO IMPLEMENT OTHER APPLICATION CONTROL SOLUTIONS CAN FIND SUCCESS WITH CARBON BLACK APP CONTROL

Not every point-of-sale installation meets all these criteria, but when they do, implementations are simple, straightforward, efficient and quick. Application control can be cheap and easy in the right circumstances.

Companies with a wide selection of rarely used legacy applications Any application control solution will have certain common limitations. As previously mentioned, any endpoint security agent can impact performance and interoperability, which can be exacerbated under certain conditions. Application control configuration needs to be fully cached so agents can operate robustly offline. But what happens if unusual conditions cause that configuration to be too large or to have very specific and unusual needs?

First, imagine a giant repository of legacy software—10 years' worth of high-end applications. While any given application is hardly used at all, there's often an urgent need to check out a particular version from a particular year. At any moment, you may need to test or review one, so all of them must be available and approved by application control. Furthermore, they aren't delivered by any software management agent, such as Microsoft Endpoint Configuration Manager or BigFix, so there's no way to just enable their installer. They all sit on a plain old file server, so each file must be explicitly approved. In this scenario, the offline cache becomes bloated, and checking it against each file execution becomes a drag on performance.

Imagine that the way the code in these legacy applications works is diametrically opposed to how active endpoint security agents do their jobs. The code relies on massive parallelization, stopping and starting scores of small programs hundreds or even thousands of times per second. When it's deployed against a high performance computing infrastructure, it works great. But when simulated on a regular workstation, it's already slow. If an endpoint security agent has to track and enforce against every execution, the overhead becomes too much. If the user base is used to high-end computing response times, the combination becomes impossible. Application control will not work for this organization

Though it happens rarely, some customers do come to the conclusion that application control isn't the right choice for them. Having that amount of control would have been great, but it ends up being too unwieldy and restricting.

Conclusion

In the end, application control isn't too hard. The amount of money and effort required to invest in deployment significantly pays off with real, proven high levels of security. The trick to deciding if application control is right for your organization is understanding what models to use for deployment, and what sort of traps to expect. Different customers require different approaches, and some take more time and effort than others. But the right fit can be found for every situation, and the Professional Services team can help you get there. Our technology makes the new threat landscape a challenge your organization can successfully combat.

CB-AppControl-Success-WP100 December 18, 2024