WHITE PAPER

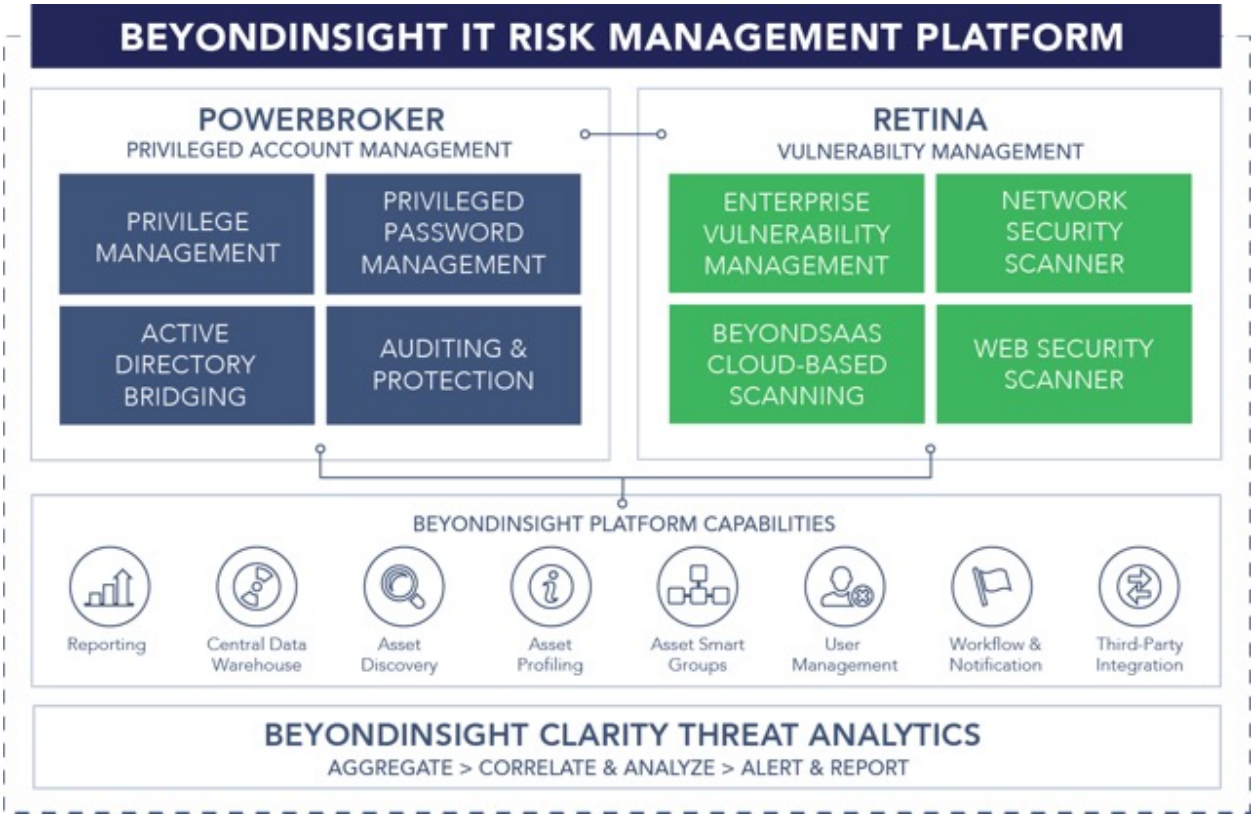
BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Application Control: The PowerBroker for Windows Difference

October 2014

Table of Contents



For the latest updates to this document, please visit:
http://www.beyondtrust.com

Warranty

This document is supplied on an "as is" basis with no warranty and no support.

Limitations of Liability

In no event shall BeyondTrust be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this white paper.

Disclaimer

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. BeyondTrust is not associated with any other vendors or products mentioned in this document.

Introduction

Application control solutions are designed to block the execution of unauthorized applications via whitelisting, blacklisting, and more recently "greylisting." They can be used to protect your organization's servers, workstations, laptops, tablets, and fixed-function devices. They can also thwart advanced persistent threats via policy enforcement and dynamic trust modeling. What's more, they typically do not require signature updates or labor-intensive list management for greylisting applications.

Application control solutions can offer several security and cost benefits, including:

- **Protection from unwanted applications:** Prevent undesirable code from running via executable files, Java apps, ActiveX controls, scripts, and specialty applications.
- **Reduced help desk costs:** Reduce the costs associated with identifying and removing inappropriate software by maintaining control over application installations and system configurations.
- **Patching flexibility:** Delay patch deployment until your regular patch cycle by ensuring that only trusted applications execute.
- **Centralized management:** All systems under management can report application usage, software metering, and rogue and malicious software to the solution.

However, there are costs to implementing application control in your organization.

The Default-Deny Approach to Application Control

Leading application control vendors leverage a "Default-Deny" model; under which trusted applications must be whitelisted to execute. To simplify management, these solutions provide catalogs of millions of trusted application hashes, while offering dynamic guidance to refine entries for new solutions. Examples of dynamic guidance include:

- The application is registered as a trusted publisher.
- The application must be installed from your trusted software delivery system. *
- The application must launch or be installed from one of your trusted directories. *
- New versions and installations must be installed from a trusted updater. *

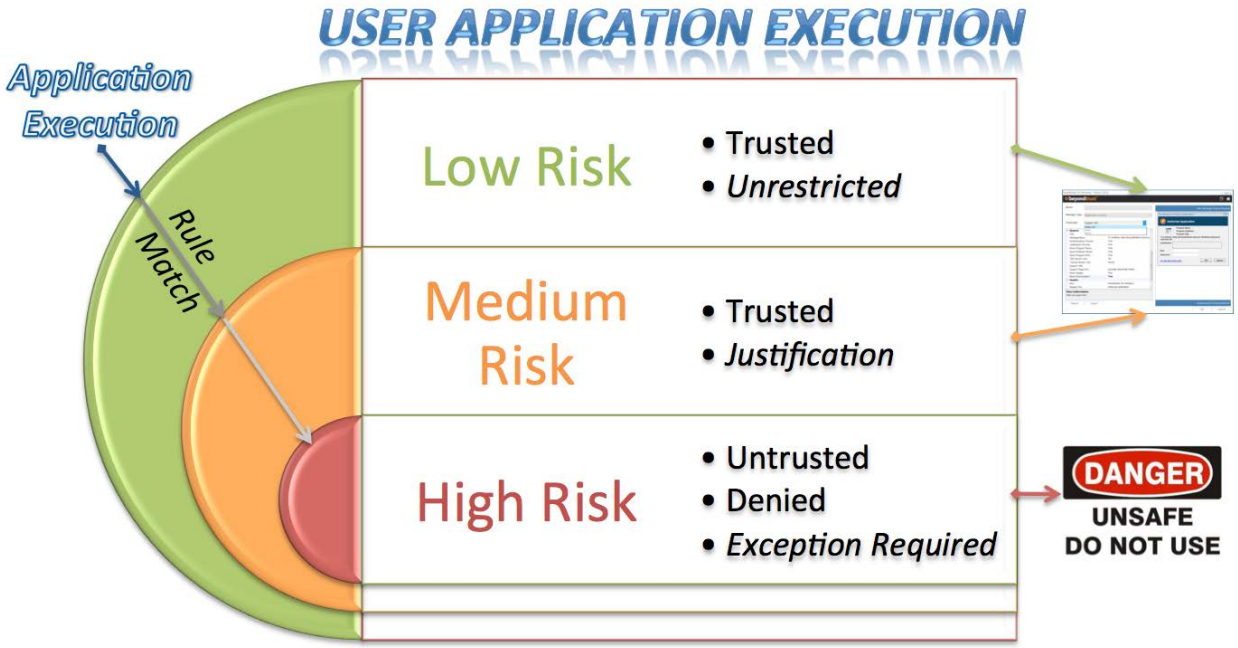
** These functions normally must be executed by users with administrative privileges and are restricted by standard users.*

Given the above criteria, application control vendors typically create mathematical models that define thresholds for trusting the application. The result determines the "file reputation" and identifies greylisting parameters.

To minimize end-user impact, application control vendors have taken a cue from other security solutions by creating different levels of "Trust." These vary in implementation from vendor to vendor, but here is one common model:

- **Low risk:** The end user is allowed to execute the software unrestricted, and the event is reported to a central console for further investigation or rule creation.
- **Medium risk:** The end user is prompted to confirm execution of the software, since its reputation or greylisting has reached a threshold that may be considered a threat.
- **High risk:** The application has been identified a real threat and is blocked from executing. In a "Default-Deny" model, this applies to all applications that do not match trust criteria. Custom applications, vendor-specific patches, and unsigned applications are generally blocked due to invalid parameters.

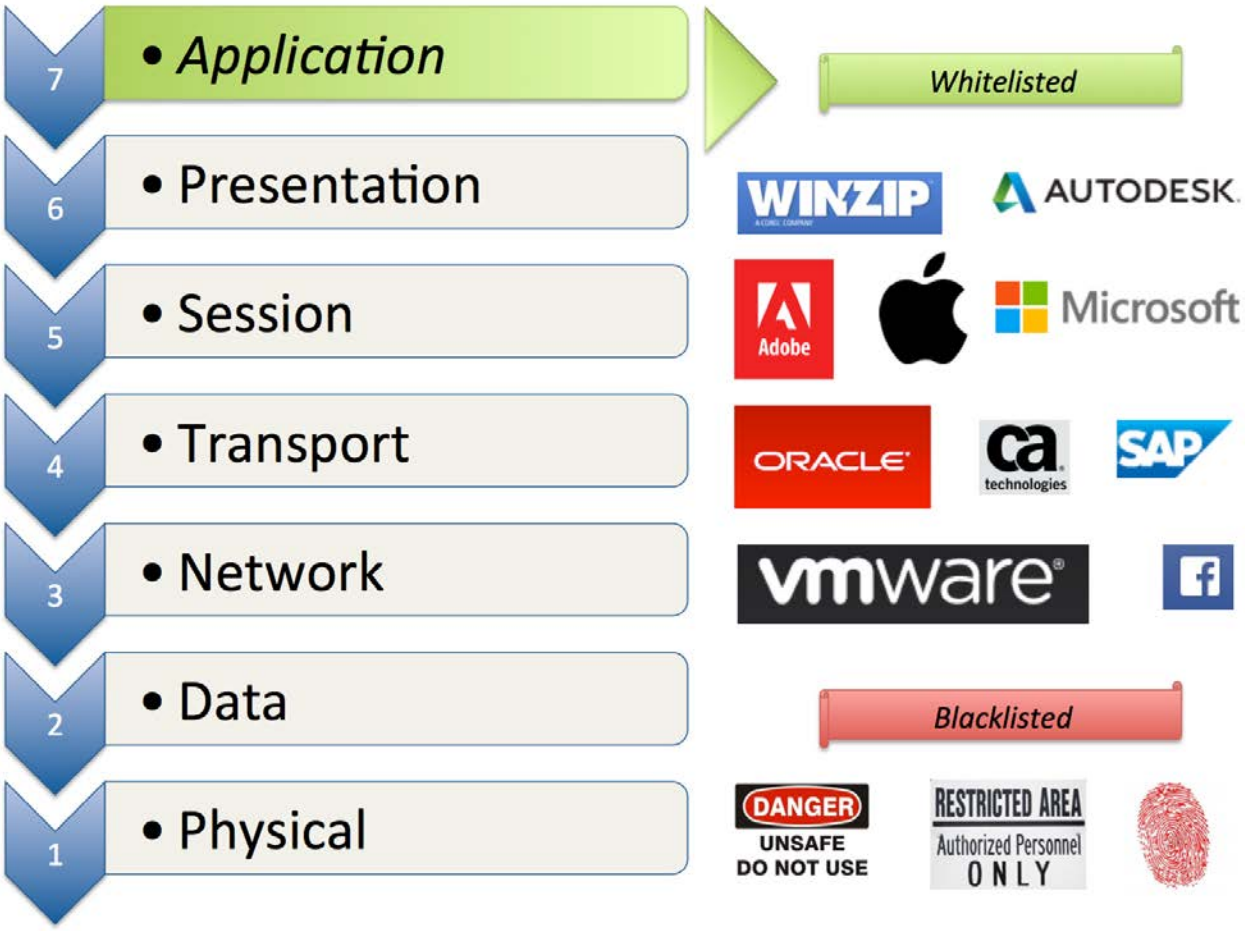
High-risk applications then require whitelisting to execute.



Application Control's Dependence on Whitelisting

Okena first introduced whitelisting via its StormWatch solution. The company was later acquired by Cisco, and StormWatch was renamed Cisco Security Agent (CSA). The technology whitelisted network traffic using application and system firewall rules. This required the agent to "learn" expected behavior and create vast rule bases for acceptable network behavior. In the early days, StormWatch was designed to stop the onslaught of network and service-based worms. Any unknown process or application was denied access to the network – and any modified programs were automatically corrected.

This approach extended the ISO model to the application layer, reflecting a natural technology evolution. The first generation of application control solutions required businesses to identify all trusted software, hence the name "whitelist." Maintaining the solutions called for significant staffing investments. A less intensive process was required.



Challenges stemming from labor-intensive whitelisting requirements spurred the birth of Application Control solutions with:

- Pre-defined whitelist libraries of millions of known and trusted applications
- Blacklist and reputation libraries of millions of malware and questionable applications
- Greylisting criteria for classifying unknown applications
- Management tools for to handle rule customization and the inclusion of business-unique applications.

It's also important to note that, in many cases, not all applications from a specific trusted vendor are suitable for all employees. Given this, the whitelisting approach is still inherently complex and flawed, and it raises the need to consider alternative solutions.

A Better Way to Reduce Application Security Risks

BeyondTrust PowerBroker® for Windows represents the next logical step beyond application control. Like traditional application control, PowerBroker for Windows enforces restrictions on software usage, installation, and operating system configuration changes. However, it does not require a default-deny mode enforced by a third-party agent to keep systems secure.

Instead, PowerBroker for Windows defaults all users to standard user privileges and leverages rules and policies to elevate applications to administrator privileges, enabling them to function correctly. By using a native operating system security model (from Windows XP and higher), PowerBroker for Windows essentially "default-denies" inappropriate user actions while elevating application and task permissions. PowerBroker for Windows therefore enables you to implement least-privilege best practices without obstructing productivity.

Rather than managing a complex whitelist with thousands of application signatures, PowerBroker for Windows customers usually only need to work with a few dozen rules. These rules, hosted in either Active Directory Group Policy or BeyondTrust BeyondInsight® Web Services, can be based on Publish, Path, URL, Active X Control, MSI, and a wide variety of other criteria. PowerBroker for Windows even ships with a Rule Library for the most common programs to expedite implementations.

Greylisting via Vulnerability-Based Application Management

So what about greylisting? As referenced above, application control solutions use thresholds for evaluating applications and do not necessarily require absolute rules. PowerBroker for Windows takes a similar approach and uses industry standards for guidance.

PowerBroker for Windows includes patented technology for Vulnerability-Based Application Management. Based on the BeyondTrust Retina Vulnerability Database, greylist rules can be created based an application's published vulnerabilities and filtered by:

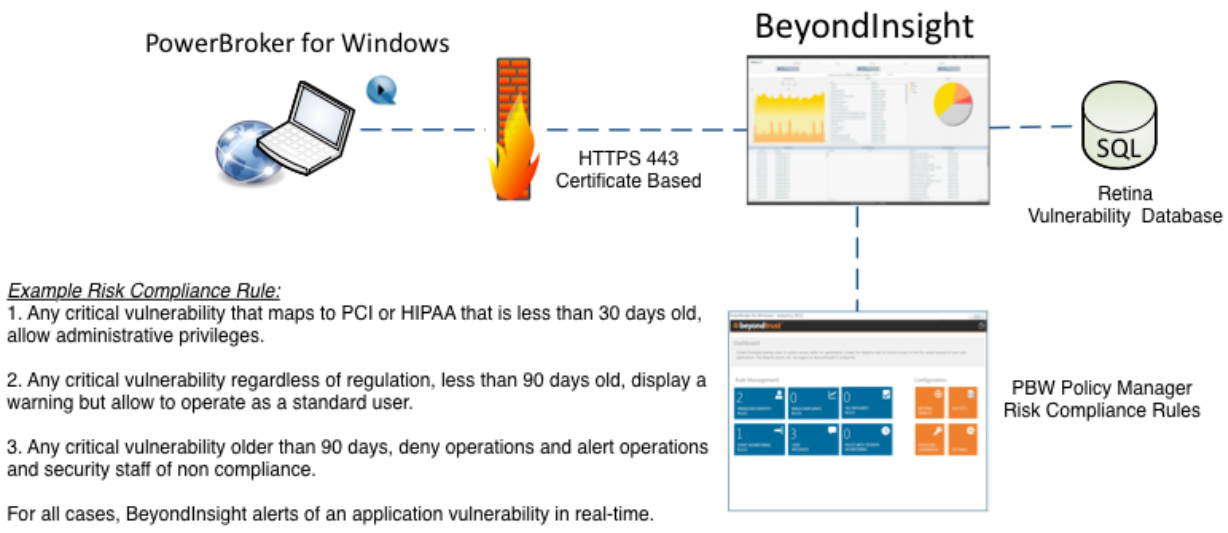
- Regulatory violations per PCI, HIPAA, HiTrust, NIST, ISO, SOX, GLBA, ITIL, etc.
- Vulnerability Severity from PCI and CVSS
- Age of the vulnerability since publicly released

These rules can be used to blacklist an application or even modify its privileges. Therefore, applications are controlled based on known vulnerabilities and advanced persistent threats per industry standards and regulations.

Example Use Case: Mitigating Acrobat Reader Risks

As a quick example, consider the first release of Adobe Acrobat Reader 10. In a traditional application control environment, this product is trusted. It is from a known vendor, is digitally signed, and can easily be installed as a part of another software package. The fact that it was installed, assumes you had administrative rights. Now, if you execute the program, it is

trusted and has the current user's permissions. Traditional application control solutions, as noted above, normally run on hosts where users are administrators or have administrator credentials. This version of Reader is highly vulnerable, has publicly available exploits, and is susceptible to malware easily purchasable in malware toolkits. So, why would you ever trust it, let alone give it administrative privileges? This is a huge, unnecessary risk. The diagram below represents how simple this is in the real world:



With PowerBroker for Windows, a simple Risk Compliance rule would flag the vulnerable version, deny it from executing, or even just strip its privileges so that it is not as susceptible to an attack. In addition, the BeyondInsight management console would be notified that an application with known risks has been executed in the environment; in real time. This helps to verify that desktop and server patch management policies are being followed – for almost all applications and operating system functions.

Beyond Application Risk Management

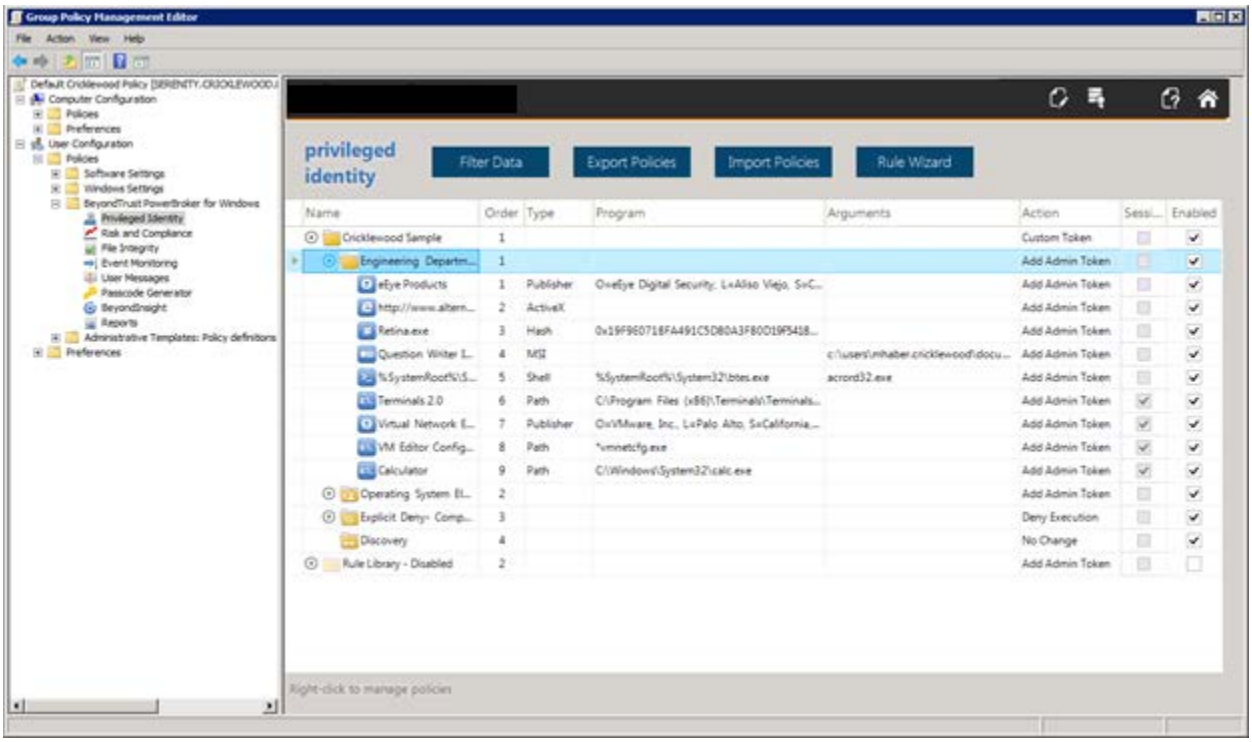
PowerBroker for Windows does more than just application risk management. It is a least-privilege solution that leverages the operating system's core components for application control. It can also document all privileged and application activity on a desktop or server using the BeyondInsight management console. You can therefore:

- Monitor UAC events, application rules, requested elevations, denied applications, etc.
- Monitor the Windows Event Log for events related to privileged or suspicious activity – and report on it
- Monitor the file system for unauthorized changes based on user or group – and even deny unauthorized changes
- Record the user's screen (multi-monitor aware) and allow playback with full keystroke logging and searching

- Report on user or rule activity using an integrated data warehouse with role based access and multi-tenant functionality

Application Control does not need to be a high-maintenance, unsustainable project for your organization. The Microsoft Windows operating system does a fantastic job of locking users down, but it unfortunately has no native tools for loosening the reins to ensure productivity.

PowerBroker for Windows allows applications to execute with necessary permissions, while maintaining the operating system's native level of security. Applications can therefore execute the way they were designed to, and security and operations teams have complete control over configuration, permitted software, and even the Active X controls.



With patented least-privilege technology, PowerBroker for Windows is the next-generation application security solution. When combined with the native security model of the Microsoft Windows operating system, PowerBroker makes it easy to maintain granular control over applications and privileges with just a few rules.

About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Account Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.