PowerBroker for Windows 7.5

New and Updated Features

The case for Windows privilege management is overwhelming. Consider the fact that 94% of critical vulnerabilities reported by Microsoft in 2016 could have been be mitigated by removing administrator rights from users. Whether hijacked by external attackers using phishing or ransomware, or simply misused by insiders, local and domain admin rights can facilitate devastating data breaches. Attackers prize these privileges because they can afford freedom of movement and access beneath the radar of detection. However, wholesale removal of administrator rights can bring productivity to a grinding halt and overwhelm your IT help desk. That’s where PowerBroker for Windows comes into play.

PowerBroker for Windows is a privilege management solution that gives you unmatched visibility and control over physical and virtual desktops and servers.

- **Reduce attack surfaces** by removing admin rights from end users and employing fine-grained policy controls for all privileged access, without disrupting productivity.
- **Monitor and audit sessions** for unauthorized access and/or changes to files and directories.
- **Analyze behavior** to detect suspicious user, account and asset activity.

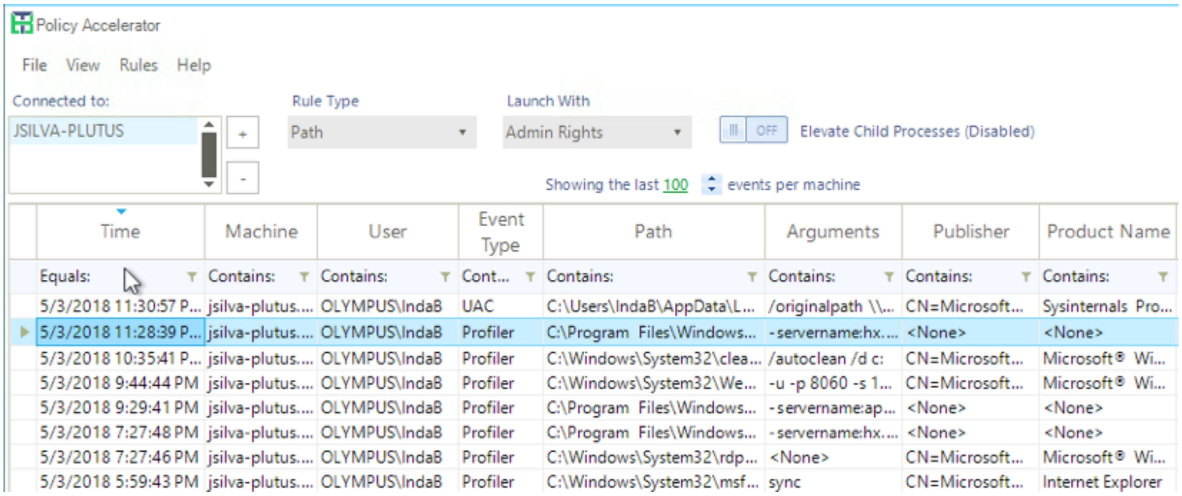
Whether you need simplified least privilege enforcement, patented application control, privileged activity logging, or file integrity monitoring, PowerBroker delivers the most comprehensive Windows privilege management capabilities available.

PowerBroker for Windows 7.5 adds several capabilities that further enhance management and usability. Please read below for a summary of new features.

New Feature Highlights

Quickly Build Rules for Processes Which Require Privilege Elevation with Policy Accelerator

The discovery, creation, and testing of policy based on what is used within an organization can be challenging. PowerBroker for Windows version 7.5 allows companies to quickly identify app launches and elevation requirements, then test and save required rules. This new feature allows customers and partners to evaluate privileges and see value faster, even in disconnected environments.



Connected to: JSILVA-PLUTUS

Rule Type: Path

Launch With: Admin Rights

OFF Elevate Child Processes (Disabled)

Showing the last 100 events per machine

Time	Machine	User	Event Type	Path	Arguments	Publisher	Product Name
Equals:	Contains:	Contains:	Cont...	Contains:	Contains:	Contains:	Contains:
5/3/2018 11:30:57 P...	jsilva-plutus....	OLYMPUS\IndaB	UAC	C:\Users\IndaB\AppData\L...	/originalpath \\...	CN=Microsoft...	Sysinternals Pro...
5/3/2018 11:28:39 P...	jsilva-plutus....	OLYMPUS\IndaB	Profiler	C:\Program Files\Windows...	-servername:hx....	<None>	<None>
5/3/2018 10:35:41 P...	jsilva-plutus....	OLYMPUS\IndaB	Profiler	C:\Windows\System32\clea...	/autoclean /d c:	CN=Microsoft...	Microsoft® Wi...
5/3/2018 9:44:44 PM	jsilva-plutus....	OLYMPUS\IndaB	Profiler	C:\Windows\System32\We...	-u -p 8060 -s 1...	CN=Microsoft...	Microsoft® Wi...
5/3/2018 9:29:41 PM	jsilva-plutus....	OLYMPUS\IndaB	Profiler	C:\Program Files\Windows...	-servername:ap...	<None>	<None>
5/3/2018 7:27:48 PM	jsilva-plutus....	OLYMPUS\IndaB	Profiler	C:\Program Files\Windows...	-servername:hx....	<None>	<None>
5/3/2018 7:27:46 PM	jsilva-plutus....	OLYMPUS\IndaB	Profiler	C:\Windows\System32\rdp...	<None>	CN=Microsoft...	Microsoft® Wi...
5/3/2018 5:59:43 PM	jsilva-plutus....	OLYMPUS\IndaB	Profiler	C:\Windows\System32\msf...	sync	CN=Microsoft...	Internet Explorer

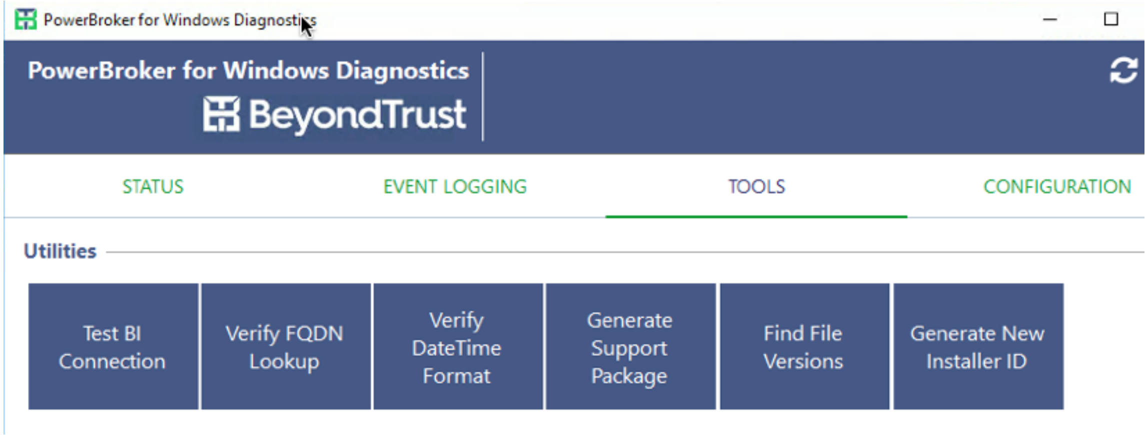
Policy Accelerator helps customers build rules quickly.

Support for Windows 10 April Update 2018 (1803)

PowerBroker for Windows v7.5 now supports Microsoft Windows 10 April Update 2018, allowing IT admins to remain up to date on the latest Windows OS.

Ensure Consistency with Enhanced Diagnostics

As an IT support person, you understand the importance of ensuring the software under your care is configured correctly and. In doing so, you often have to use Regedit, and navigate to various keys, or the file system, and navigate to various paths; just answer simple questions like is something on/off. PowerBroker for Windows version 7.5 provides a consolidated dashboard so that an IT administrator can pinpoint areas that need troubleshooting. It also reduces the number of places where an IT administrator needs to look to validate whether software applications are running as expected. The new feature saves time and ensures consistency across the environment.



Enhanced diagnostics in PowerBroker for Windows 7.5 saves time and ensures consistency.

Ensure Security on Scripts with Signature-based Powershell Rules

Many customers use scripts to manage IT processes. At times these scripts require elevation but are stored in a file location that many users have write access to— leaving open the possibility that a script could be changed and potentially used as a privileged attack vector. PowerBroker for Windows version 7.5 now allows companies to create a Publisher rule to target these scripts. So, if that script is changed, the signature is no longer valid. And with the signature no longer valid, the rule can no longer be triggered.

Customer-Requested Enhancements

In addition to the above new features, there are several customer-related fixes and enhancements available in PowerBroker for Windows 7.5. For a full list or to download the latest version, please visit the customer portal.

About BeyondTrust

BeyondTrust® is a global cybersecurity 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.