



PowerBroker for Desktops

Delegate Privileges with Certainty & Clarity
on Windows Desktops

 **beyondtrust**[®]
privilege. made simple

© 1985-2010 BeyondTrust Software, Inc. All rights reserved

BeyondTrust at a Glance



What We Do:

Empower IT to eliminate the misuse of privileges in physical, virtual and cloud environments

How We Do It:



Heterogeneous Platforms

- Desktops
- Servers
- Network devices

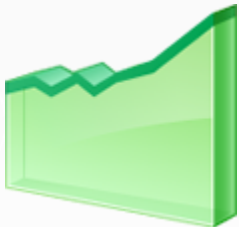
Virtualization

- Host OS
- Virtual guest
- Supports standard environments

Cloud Computing

- Private cloud
- Public cloud
- SAS 70 and ISO 27001 compliance

Business Value:



92% reduction
in exploited
vulnerabilities¹

\$113,000 savings
from insider
breaches²

\$1,237 savings
per desktop³

25% increase
in system
admin
productivity⁴

Compliant
with mandates
and audits

People Need Boundaries, Not Walls



- Control “virtual sprawl” on servers and desktops
 - Increase collaboration > without compromise: virtualization & cloud
 - Assign privileges > within guidelines
 - Root or admin passwords and access > to no one
-

“Organizations continue to struggle with excessive user privilege as it remains the primary attack point for data breaches and unauthorized transactions.”

~ Mark Diodati, Burton Group

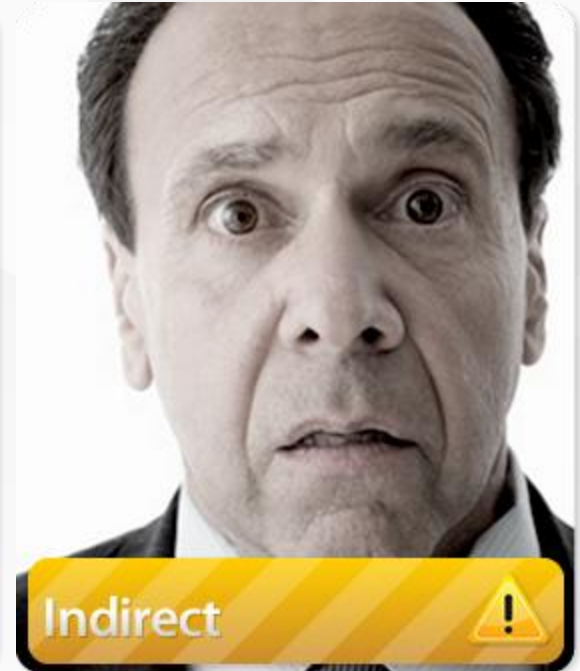
Privileges are Misused in Different Ways



Insider attacks cost an average **\$2.7 Million** per attack¹



Desktop configuration errors cost companies **\$120/yr/pc**²



Virtual sprawl and **malware** are ever-present realities

Source: ¹ Computer Security Institute and FBI Survey.

Source: ² IDC Report: *The Relationship between IT Labor Costs and Best Practices for Identity and Access Management with Active*

Desktop Catch 22: Security or Productivity



- **Countless line of business applications require admin privileges to run**
- **Software and ActiveX installs require admin privileges**
- **Employees need to self maintain certain system settings, and cannot without admin privileges**

Windows 7, UAC & PowerBroker for Desktops

“End users have been asking for Windows to provide a way to add arbitrary applications to the auto-elevate list since the Windows Vista beta... Windows 7, just like Windows Vista, doesn't provide such a capability.”

Mark Russinovich, Technical Fellow at Microsoft , Inside Windows 7 User Account Control,
<http://technet.microsoft.com/en-us/magazine/2009.07.uac.aspx>

“BeyondTrust PowerBroker for Desktops helps corporations that need to allow standard users to run applications that require administrative privileges on Windows Vista with UAC enabled without any prompts or input required from the user...”

The combination of elevating approved applications transparently with PowerBroker for Desktops and running UAC in no prompt mode with Internet Explorer in protected mode provides a best-of-breed solution to the least privilege problem.”

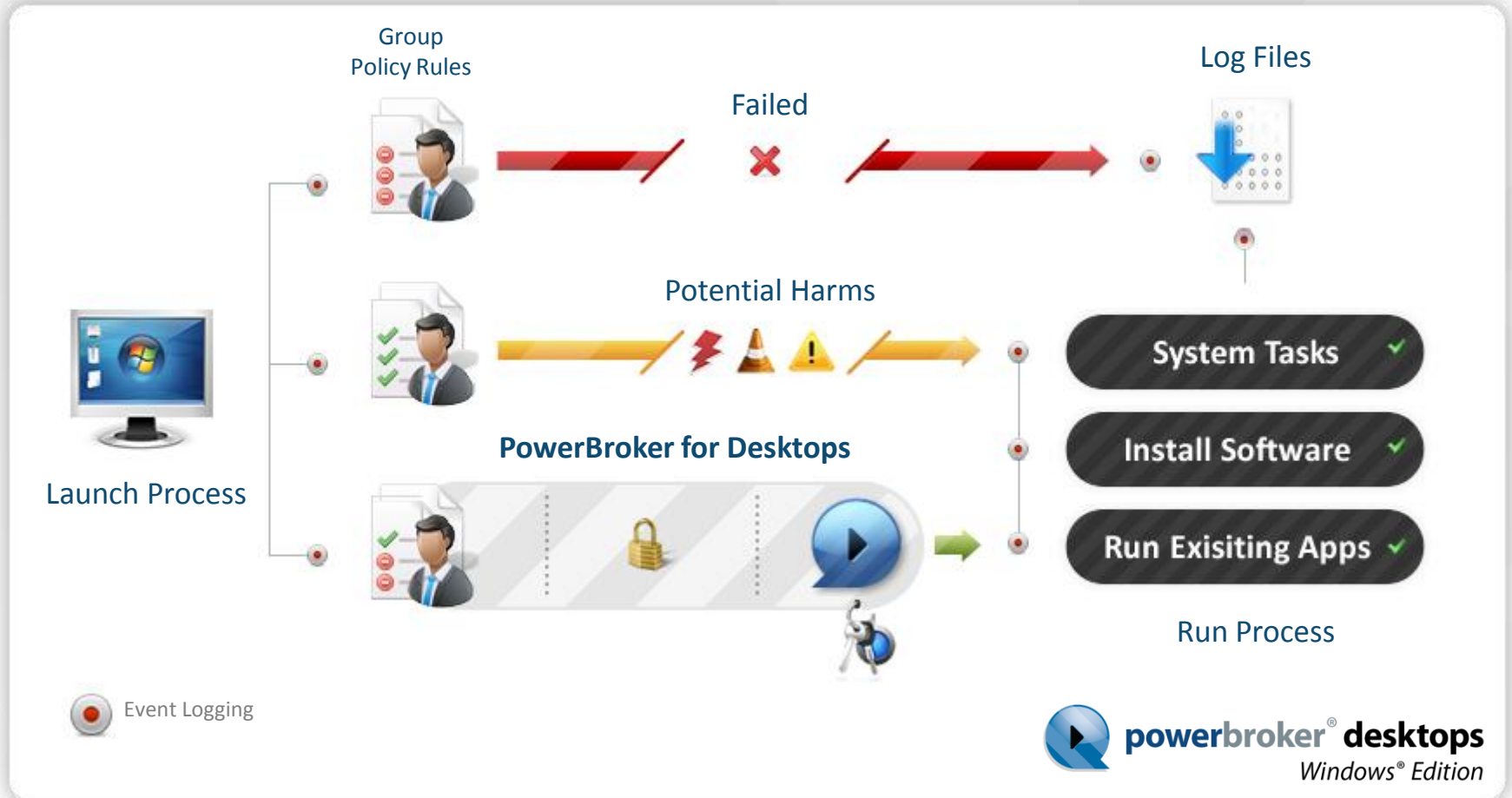
Austin Wilson, director, Windows Client Security Product Mgmt. at Microsoft eWeek,
<http://www.eweek.com/c/a/Windows/BeyondTrust-Reins-in-Vista-UAC-Prompts/>

Delegate Privileges with Confidence & Clarity



- No root or admin passwords or access
- Centrally and easily define policy for authorized tasks
- Monitor privileged access
- Physical, virtualized or cloud

BeyondTrust Unique Value: Desktop



PowerBroker Desktops

New Features

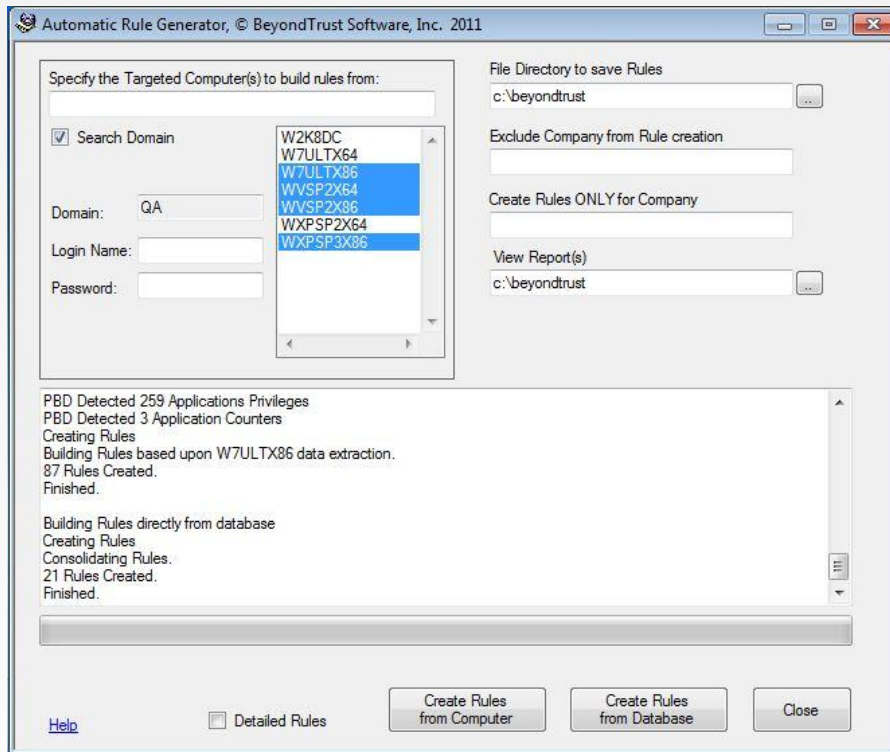
The screenshot displays the PowerBroker Desktops Windows Edition interface. At the top left is the logo and 'Windows Edition' text. To the right are social media icons (RSS, Facebook, LinkedIn, Twitter, YouTube) and the product version '5.0.0'. The main content is divided into two panels. The 'Getting Started' panel includes a 'CLOSE' button and two links: 'Getting Started' (Instructions and Samples) and 'More about PowerBroker' (Learn all there is to know and more). The 'Tools & Wizard' panel also has a 'CLOSE' button and four main sections: 'Create a New Rule' with an 'Enable Wizard' button, 'Automatic Rule Generator', 'Create Collection', and 'Edit Rules and Collections'. Each section contains a brief description of its function.

Improved Dashboard

The new dashboard in PowerBroker desktops consolidates key functionality into one location, improving ease of use and presenting key features in a more obvious place.

Links to documentation, social media, reports, and other tools are all featured prominently in the user interface.

PowerBroker Desktops New Features



Automatic Rule Generator

PowerBroker Desktops can be configured in passive mode to automatically detect the applications in an organization that require administrator privileges.

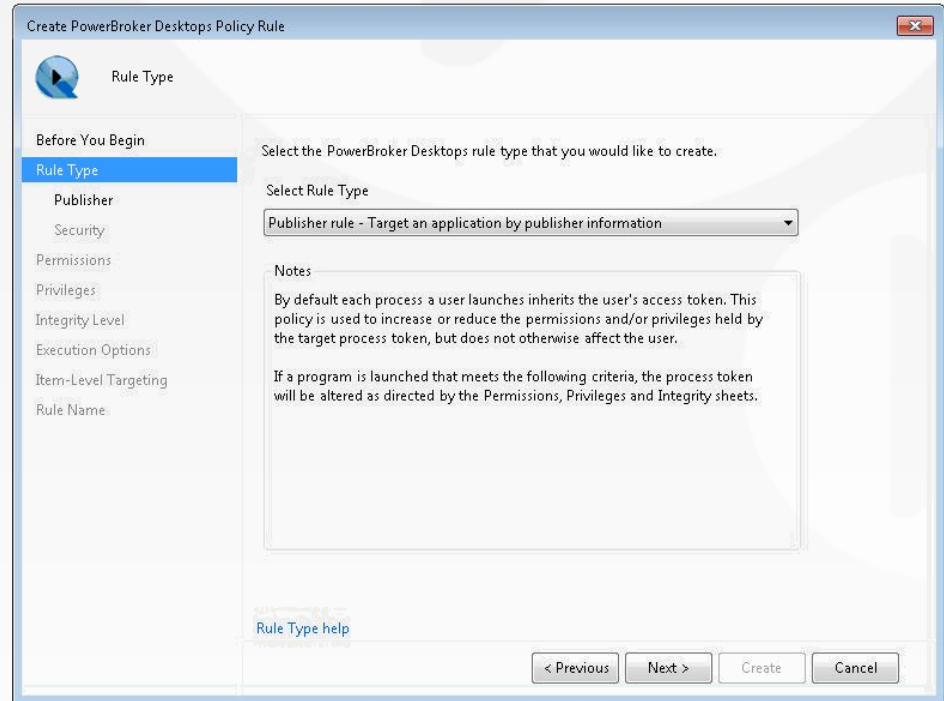
PowerBroker Desktops is the only end to end solution for eliminating administrator rights on the market today with such a high level of automation.

PowerBroker Desktops New Features

Rule Wizard

The new Rule Wizard walks admins through the process of creating new rules and exposes functionality that was previously not obviously accessible.

The wizard allows for rapid creation of rules and is the easiest way for new administrators to get started using PowerBroker Desktops.



PowerBroker Desktops New Features

Publisher Rule Type

The new Publisher Rule provides organizations with the same targeting mechanisms for application elevation that Microsoft's AppLocker uses for application white listing.

The Publisher Rule allows organizations to target applications for elevation based on the Publisher, Product Name, Original File Name and File Version.

The screenshot shows the 'Create PowerBroker Desktops Policy Rule' dialog box. The 'Publisher' rule type is selected in the left-hand navigation pane. The main area contains the following fields and options:

- Reference file:** A text box containing 'C:\Users\pb\Desktop\procxp.exe' and a 'Browse...' button.
- File Properties:** A list of fields with corresponding values:
 - Publisher: O=Microsoft Corporation, L=Redmond, S=Washingt
 - Product name: PROCESS EXPLORER
 - File name: PROCEXP.EXE
 - File version: 11.33.0.0 (with a dropdown menu set to 'And above')
- Use custom values
- Rule scope:** Applies to only the specified version of this file.

At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Create', and 'Cancel'. A 'Publisher rule help' link is also present.

PowerBroker Desktops New Features

Publisher Rule Type

The new Publisher Rule provides organizations with the same targeting mechanisms for application elevation that Microsoft's AppLocker uses for application white listing.

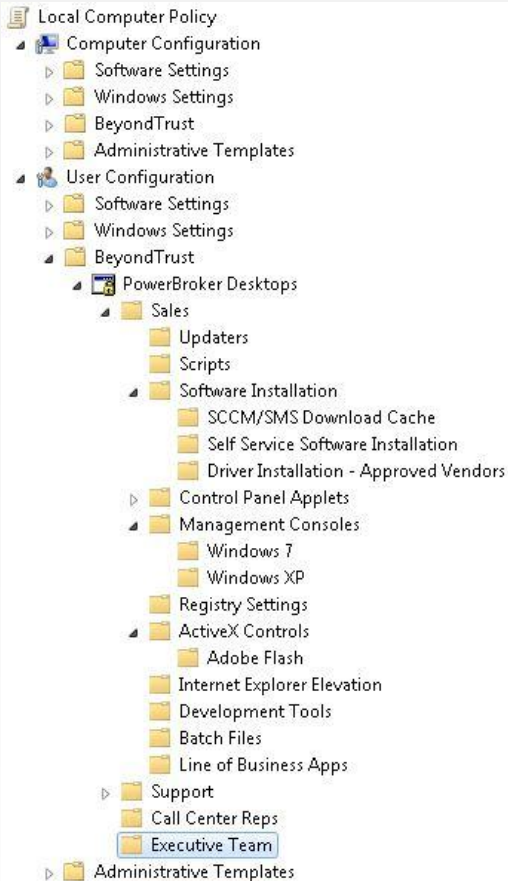
The Publisher Rule allows organizations to target applications for elevation based on the Publisher, Product Name, Original File Name and File Version.

The screenshot shows the 'Create PowerBroker Desktops Policy Rule' dialog box. The 'Publisher' rule type is selected in the left-hand navigation pane. The main area contains the following fields and options:

- Reference file:** A text box containing 'C:\Users\pb\Desktop\procxp.exe' and a 'Browse...' button.
- File Properties:** A list of fields with values:
 - Publisher: O=Microsoft Corporation, L=Redmond, S=Washingt
 - Product name: PROCESS EXPLORER
 - File name: PROCEXP.EXE
 - File version: 11.33.0.0 (with a dropdown menu set to 'And above')
- Use custom values
- Rule scope:** Applies to only the specified version of this file.

At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Create', and 'Cancel'. A 'Publisher rule help' link is also present.

PowerBroker Desktops New Features



Improved Rule Collections

Rules can be now grouped in a hierarchical fashion, similar to the Group Policy Preferences Registry Extension. Rules can be grouped in folders and targeting criteria can be applied to the entire collection instead of on each individual rule.

This streamlines the creation and organization of rules which was previously not possible in earlier versions.

PowerBroker Desktops Advantages

- The only complete end to end solution on the market, with automatic discovery, remediation and deployment
- Fastest and easiest path to removing administrator privileges from users
- Enhance Windows 7 deployments and drastically improve the UAC experience for end users
- Achieve compliance with regulatory mandates by configuring all users as standard user
- Prevent unlicensed software installation
- Reduce data theft
- Reduce the attack surface available to malware
- Ease the deployment of Windows 7



Key Considerations for Users



Security

- Users can do their job safely without exposing the enterprise to security risks



Productivity

- Users can perform all necessary tasks for their job role without interruption



Continuity

- No process required to request access to perform necessary tasks

Be Secure



- **Malware can no longer install on desktop**
- **Mitigate 92% of software vulnerabilities**
- **Your data remains safe**

Operate as a Standard User

- **No environmental changes**
- **User logs in as standard user**
- **Does their job as they always have**



Be Productive

- Necessary privileges to run all applications are provided transparently on an as-needed basis

The image displays two screenshots of software applications. The top screenshot shows a dashboard with various reports and charts. The bottom screenshot shows a patient list application with a table of patient information.

Dashboard Screenshot:

- How to customize dashboard:** You can customize dashboard to show the information you're interested in. Options include: Add or restore reports, Modify reports, Change layouts, Add additional pages, Get started now.
- Join the QuickBooks Community:** Connect with a host of Sales users and experts to find answers and share advice. Includes a link to the community.
- Recent comments:** Marketing down a damaged item (2), POS and ZIN CASE (1), Changing document numbers (1). Includes a link to check out the QuickBooks.
- Sales Year over Year:** Table showing sales performance over time.
- Department Sales Graph:** Pie chart showing sales distribution by department.
- Best Selling Items:** Table showing top-selling items.
- Bar Chart:** A bar chart showing data for three categories: 1 to 10, 20 to 30, and 30 to 40.

Patient List Screenshot:

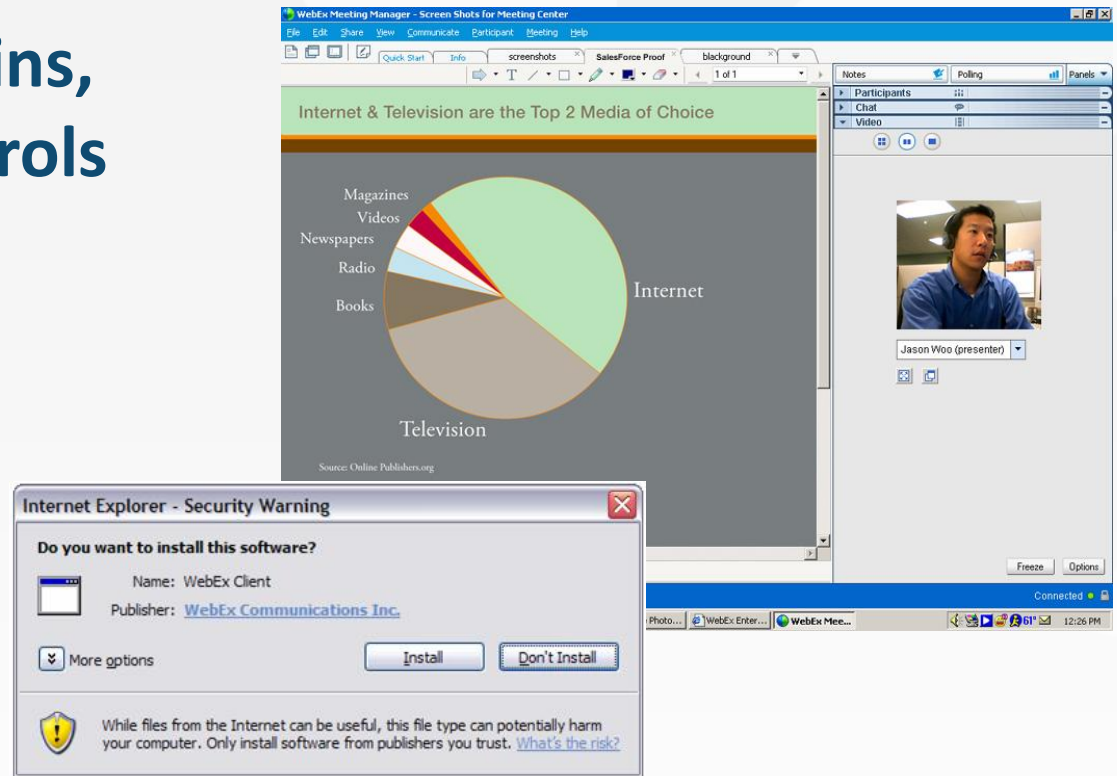
Paragon Clinical Coordination - Current User: DAWSON, PAT

Search Criteria: View ID: [dropdown], Patient Name: [input], Assigned Patients: [checkbox], Include Unknown Roundeds: [checkbox]

Alias	View ID	Patient Name	Location	Sex	Age	AA	CP	Inf	PS	MR	RS	RE
	3168170	BRACOPOL, MARGHERITA	3960307401	F	53	20	20	20	20	20	20	20
	3168172	BRONKH, ROBERT	3960307402	M	54	20	20	20	20	20	20	20
	3168089	BRUCE, JEROME	3960308401	F	26	20	20	20	20	20	20	20
	3168142	MICHELL, TANGIA	3960308402	F	45	20	20	20	20	20	20	20
	3168196	IRINA, LEONARDO	3960308401	M	54	20	20	20	20	20	20	20
	3168181	ONIL, ROBERTO	3960308402	M	37	20	20	20	20	20	20	20
	3168183	BURT, DONNA	3960310401	F	48	20	20	20	20	20	20	20
	3168184	SOUL, HELENA	3960310402	F	63	20	20	20	20	20	20	20
	3168191	PRICE, VICTORIA	3960311401	F	22	20	20	20	20	20	20	20
	3168185	COBB, DAN	3960311402	M	50	20	20	20	20	20	20	20
	3168182	MARNE, JAMES	3960312401	M	54	20	20	20	20	20	20	20
	000168306	MATHERS, MONA	3960312402	F	33	20	20	20	20	20	20	20
	3168193	CARRARA, CLAY	3960313401	M	39	20	20	20	20	20	20	20
	3168051	HILLS, SWANSON	3960313402	F	62	20	20	20	20	20	20	20
	3168171	SMITH, ALBERTA	3960314401	F	63	20	20	20	20	20	20	20
	3168198	MARNE, COCO	3960314402	F	29	20	20	20	20	20	20	20
	3168176	BOOTH, PENNY	3960315401	F	36	20	20	20	20	20	20	20
	316817000	BAILEY, JANE	3960316401	F	80	20	20	20	20	20	20	20

Be Collaborative and Creative

- Install web plug-ins, e.g. ActiveX controls
- Install approved software
- Update existing software



Be Self-Sufficient and Empowered

- **Self manage system tasks, e.g. connecting to a local printer**





Key Considerations for Administrators



Security

- Protect the enterprise from security threats
- Meet compliance objectives for security



Control

- Centrally manage privileges securely
- Provide audit-ready activity logs



Efficiency

- Enable the enterprise to remain productive
- Control IT costs and manage labor hours

Protect Critical Assets

- **Manage Resources**
 - Define policies that grant privileged access to IT resources and deploy through existing Active Directory infrastructure.
- **Enable Best Security Model**
 - Employ standard user model, no admin rights for end users
- **Achieve Compliance**
 - Full compliance with principle of Least Privilege

Maintain a Standard Desktop Image

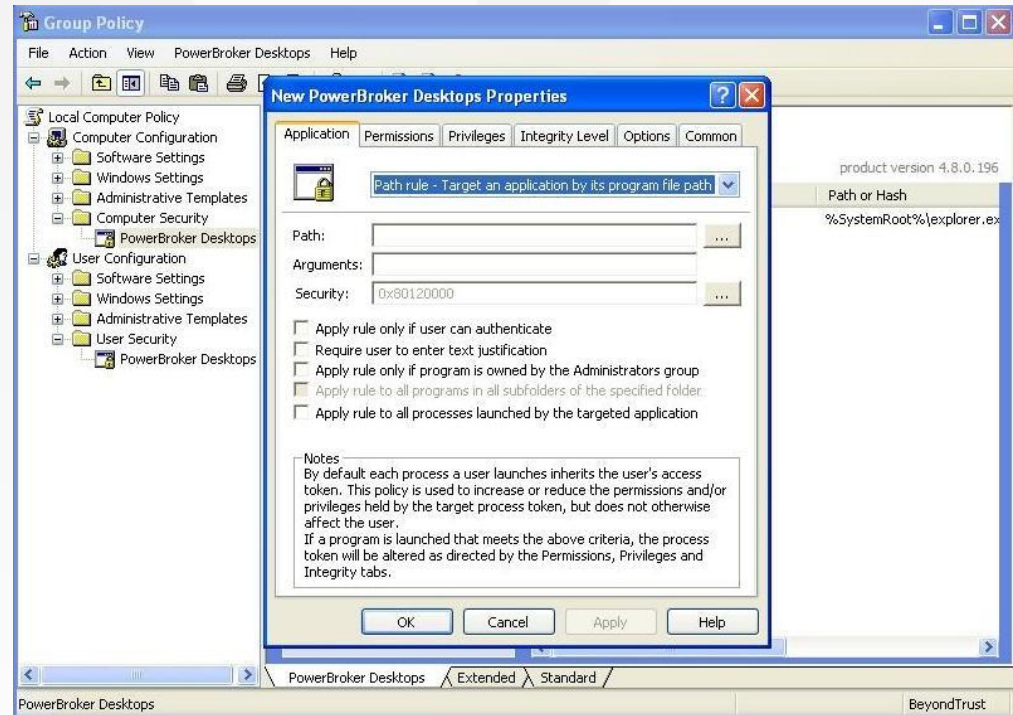
- **Maintain a standard desktop image**
- **Prevent users from installing whatever software they wish**
- **Stop users from altering security configurations**

Quickly Deploy to All Desktops

- **Deploy PowerBroker for Desktops Client Side Extension (CSE) to desktop**
 - Deployed as an .msi file using Group Policy or any software distribution solution (SMS, SCCM, Altiris, etc.)
 - As Microsoft adds functionality to Group Policy, they add CSE's to process added functionality delivered to desktop.
 - BeyondTrust adds a CSE per Microsoft specifications, does not install or run as a service
 - There is a small footprint with no performance impact

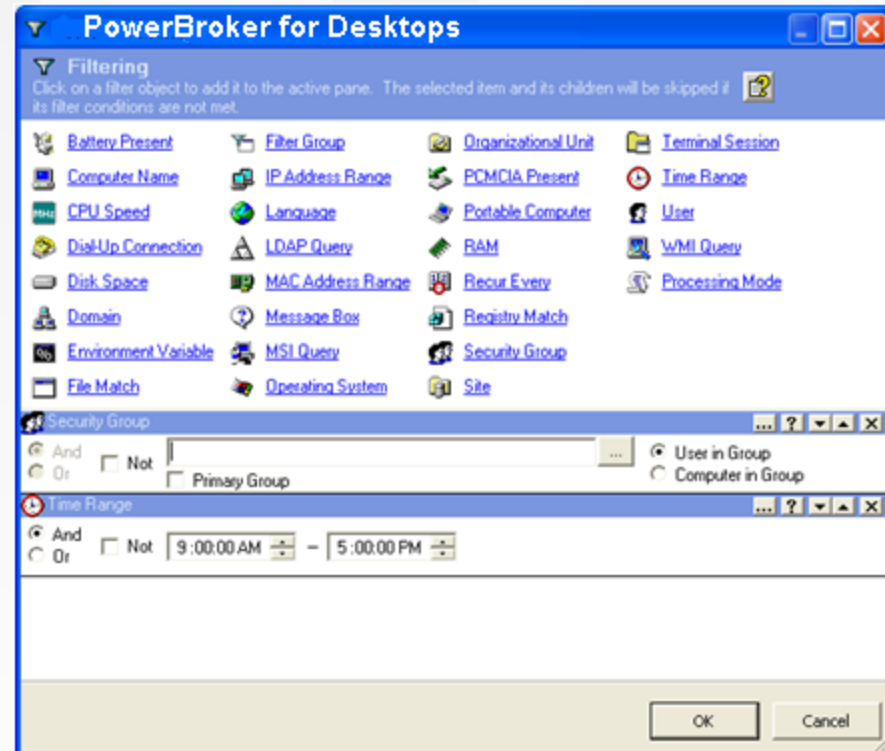
Easily Manage with Seamless GP Integration

- Editor snaps-in to Group Policy Mgmt Console and uses familiar interface
- Intuitive policy mgmt with no new UI to learn
- No changes to the Active Directory schema
- Simply target processes, and set privileges for execution



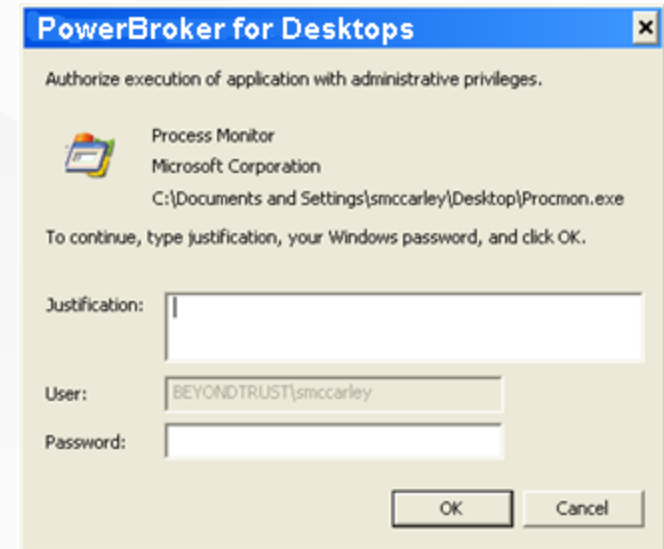
Adapt to Change

- Leverage existing OU structure and target policies with 25 powerful filters
- Create broad rules for laptops or groups like development or finance, as well as specific rules for individual users
- As changes are made in group policy, the existing rule structure will adapt without edits



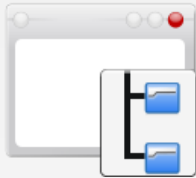
Reduce Helpdesk Calls

- As malware and user configuration errors are eliminated –complaints about “slow” desktops are reduced
- Policy rules enable users to run approved applications - no more visiting desktops
- Create rules to allow users to securely run applications on-demand - with audit logs





Key Considerations for Auditors



Identity

- Central policy control of all privileges
- Privileged identity is maintained by preserving the users logged in security context



Authorization

- Authorized users are provided access to approved applications



Reporting

- All privileged activity is logged for auditing and compliance

Achieve Compliance

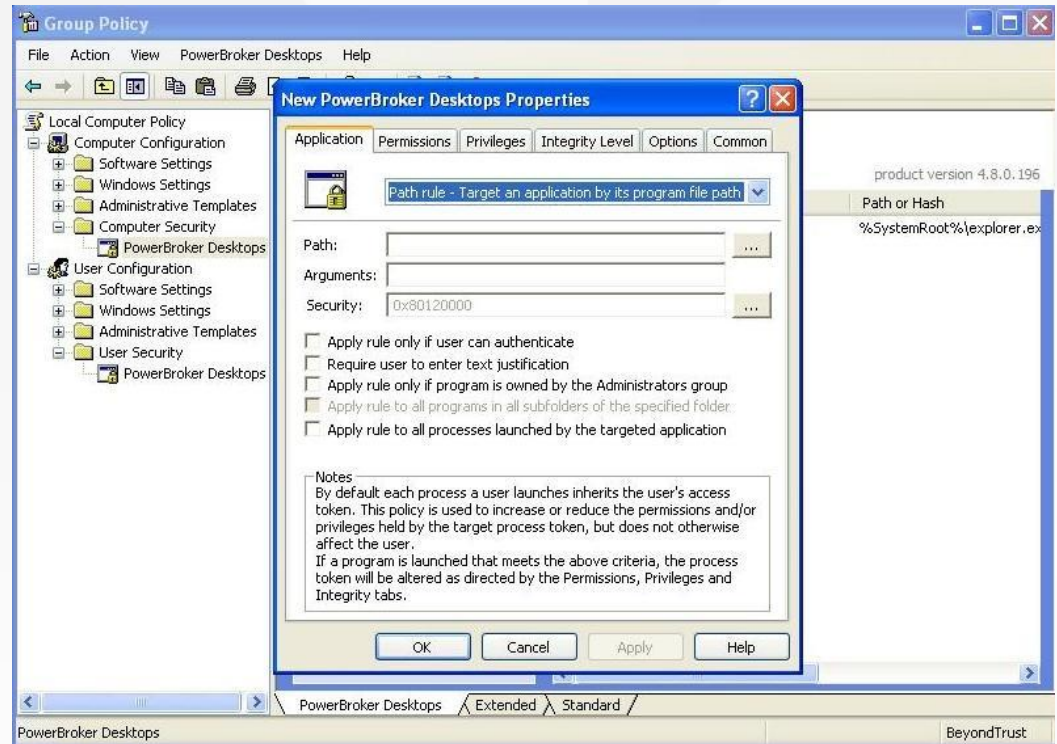
- **Comply with mandates including: FDCC, SOX, FISMA, HIPAA, PCI , NERC and GLBA**
- **Removing admin rights is key to maintaining Least Privilege and standardized security configurations**
- **Users only have privileges they need to do their job when they need it**

Protect Critical Assets

- **Access defined in Active Directory**
- **Employ standard user model, no admin rights for end users**
- **Policy to enable access to authorized privileged access**
- **Full compliance with principle of Least Privilege**

Control Scope

- Centralized policy to enable privileged access to resources



Know Who Has Access to Critical Assets

- Show users and roles that have access
- Show level of access privileges

Privileged Access Audit Report - 2/1/2010 5:20pm

User	Computer	Time	Rights	Resource	Privileges
Smith, John	Finance 1	2/1/2010 4:32pm	Standard	Quickbooks.exe	Admin privileges
Jones, Abigail	Support 22	2/1/2010 4:35pm	Standard	IPconfig.exe	Admin privileges
Richards, Tim	Support 22	2/1/2010 5:07pm	Standard	Polmon.exe	Debug

Perform Forensic Analysis

- **Centralized audit log of all privileged access performed by users**

Privileged Access Policy

User	Computer	Resource	Privilege Manager Policy	Rights	Privileges
Smith, John	Finance 1	Quickbooks.exe	Quick Books for Finance	Standard	Admin privileges
Jones, Abigail	Support 22	IPconfig.exe	Wireless Connection	Standard	Admin privileges
Richards, Tim	Support 22	Polmon.exe	Monitor Processes	Standard	Debug



PowerBroker for Desktops Customers

Office DEPOT



bmi

PAYCHEX

PCAOB[®]
Public Company Accounting Oversight Board

U.S. Census Bureau



U.S. AIR FORCE



UCSF Medical Center

PURDUE



UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

AMERICAN MUSEUM OF NATURAL HISTORY



Case Study: Fortune 500 Financial Services Company

Situation: Director Info & Risk management sees high risk from development environment because of skill concentration; mandate to implement least privilege

Complication: Developers often require administrator privileges to use certain developers tools. “Run as” being used currently to allow access; no accountability

Competition: Avecto and run-as

PowerBroker for Desktops differentiators: Depth of elevation parameters and configuration options for specific executables; group policy integration, native windows architecture (no relearning or proprietary risk).

Numbers: 5000 seats



PowerBroker for Desktops – Key Competitive Differentiators

Breadth of Coverage

Over 170 preconfigured rules in the current released version.

BENEFIT: Preconfigured rules provide out of the box support for many windows platforms and new Windows 7 rules / support in latest release

Ease of Deployment

Windows Group Policy integration. Easy to use rule editor. Policies are deployed via Windows Group Policy update (background process)

BENEFIT: No Dedicated server or additional services required.

Platform Options

Support for Windows 2000, 2003, 2008, XP, Vista, Windows7

BENEFIT: Flexibility to suit current and future environmental needs

Investment Protection

Part of full product suite for Privileged Access Lifecycle Management in heterogeneous environments.

BENEFIT: Customers have flexibility to deploy suite components aligned with their needs and budgets

Company Viability

Highly profitable company with ~\$40M bookings and ~30% Year over Year bookings growth from 2008 to 2009.



 **beyondtrust**[®]
privilege. made simple

Thank You

For more information visit:
www.beyondtrust.com

© 1985-2010 BeyondTrust Software, Inc. All rights reserved