WHITE PAPER

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Closing the Privilege Gap on Mac Desktops

July 2015

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.

Table of Contents

End users are increasingly emerging as an insider threat

Organizations today face challenges when it comes to managing their IT infrastructures. Outside of keeping up with the latest trends and hardware, the constant wish lists from users, and trying to manage a never-ending list of projects, keeping all of this running securely is more difficult than ever.

Hackers and scammers outnumber IT and security professionals. Breaches resulting from insider misuse are increasing. Look no further than the 2015 Verizon Data Breach Investigations Report for confirmation of this. This year's data shows that 10.6% of confirmed data breaches resulted from insider misuse, up from 8% in 2013. The percentage of incidents that came from insider misuse was 20.6% up from 18% in 2013.

But here is the rub. Breaches involving the end user are increasing, yet those from system administrators are decreasing. A whopping 37.6% of insider abuse incidents involved the end user in 2014, up from 17% last year. On the upside, however, only 1.6% of incidents were attributed to system administrators this year, down from 6% last year.

While breaches – especially those from insider misuse – are increasing year over year, all of the tools, process and technology put in place to control and manage administrator access to systems and data might actually be delivering on their intended purposes. However, this focus has come at a cost – end users are increasingly emerging as a greater insider threat. Organizations must tackle this challenge immediately. But how?

Desktop least privilege reduces risks

One way to close end user security gaps while ensuring that the user population still maintains the access they need to do their jobs (and IT to maintain their sanity), is to implement least privilege. The challenge, though, for many organizations is that most do not have the same level of least privilege management applied across their heterogeneous environments. Because of the preponderance of these platforms, you may have some controls in place for Windows, Unix and Linux machines, but very little for Macs. Inconsistency reigns supreme.

Why Macs can be an unknown – and growing – risk

The use of Mac devices at the enterprise level has increased dramatically over the past few years, with a reported 11% of all devices shipped in 2014 being Mac OS. In addition to companies purchasing these devices for their users, Bring Your Own Device (BYOD) is growing at a fast rate, and many of these users opt for Macs in their personal lives. The increased use has put a spotlight on the lack of security controls realistically available for Macs.

Historically, Mac devices have been the exception when it comes to security policies. Yes, you can install anti-virus tools, enforce a common configuration, and deliver an acceptable use policy to your workforce. These are all necessary components, but are they enough?

Just as in Windows, a user on a Mac OS machine can be a privileged or non-privileged user, or root or standard. In a properly configured security model, most users would be non-privileged users. Unfortunately, when doing so, you also severely limit those users from performing routine tasks that are

part of their job. You could hire an army of techs who do nothing but respond to privilege requests, but that is not financially sustainable.

How to close the privilege gap on Mac desktops

A more appropriate option is to introduce a solution that can authorize an approved application to run with administrative access or as root, without providing the user with full root access to their machines. That is exactly what BeyondTrust's PowerBroker for Mac does. PowerBroker for Mac is the first and only solution available that provides a centralized, graphical system to manage the rights of applications launched on the Mavericks, Yosemite, or El Capitan operating systems.

Users of our PowerBroker for Windows solution will already be familiar with this concept. A small client is delivered to Mac clients. These clients can then relay information about what actions are being done that require additional authorization to run properly to the included BeyondInsight IT Risk Management Platform. Based on an approval workflow, Policy Rules are delivered through Web Services and can be set for Mac System Preferences, Application Launches, Application Installers or Upgrades, thereby allowing the user to carry out the roles of their respective job. The target functionality now works without the need for an administrative or secondary account, authenticate for every elevated action they take, or have any requirements for a Sudoers file. See Figure 1 below. This is a first for Mac security, and only BeyondTrust offers this.

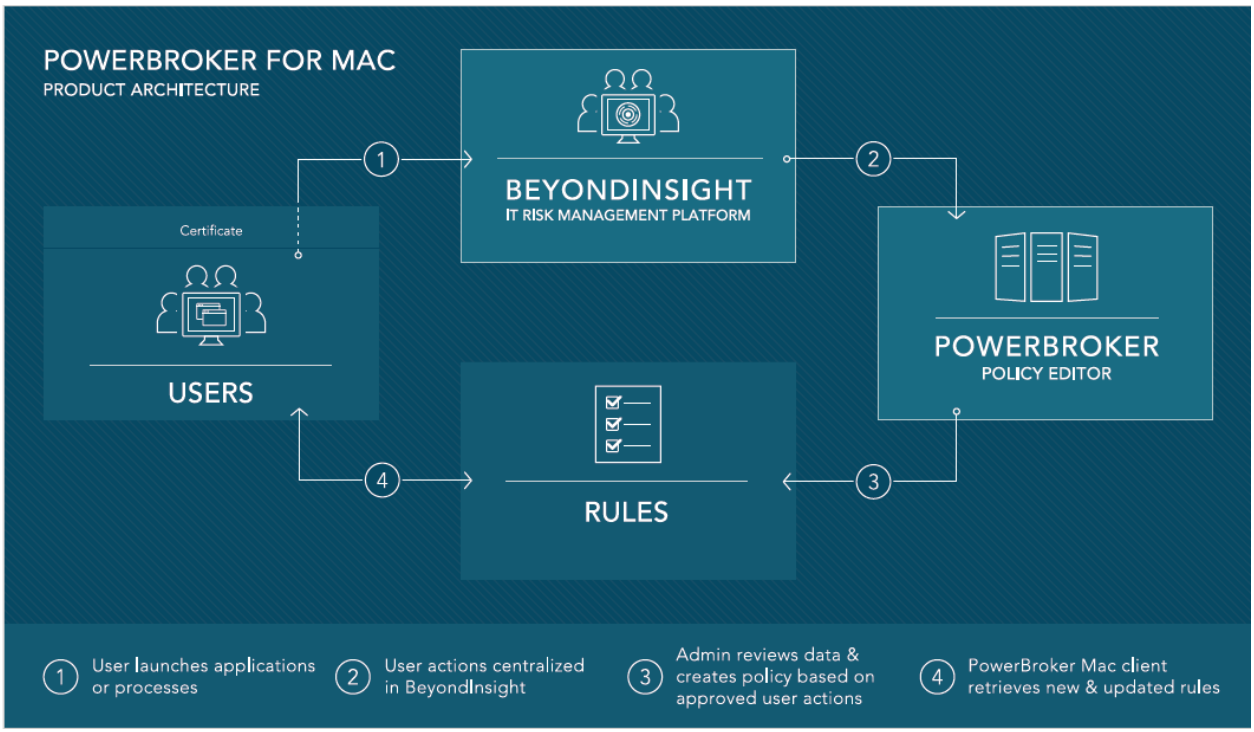

Figure 1. PowerBroker for Mac enables standard users to perform administrative tasks without entering elevated credentials.

Key capabilities in Mac least privilege management

Simplified Client for Easy Least Privilege Management

The PowerBroker for Mac client processes centrally managed rules for least privilege elevation on an Apple Mac®, Macbook®, Macbook Pro®, Macbook Air®, or Xserve®. The client monitors application launches and elevates them to the proper permissions (administrator or root) in order to operate correctly without prompting for system administrator credentials. All rule interactions are logged for complete visibility into privileged usage on OS X assets. The client removes the need for Mac users to have administrator credentials, or a second account that has administrative access, to perform basic updates and changes to the device and applications. See Figure 2 below.

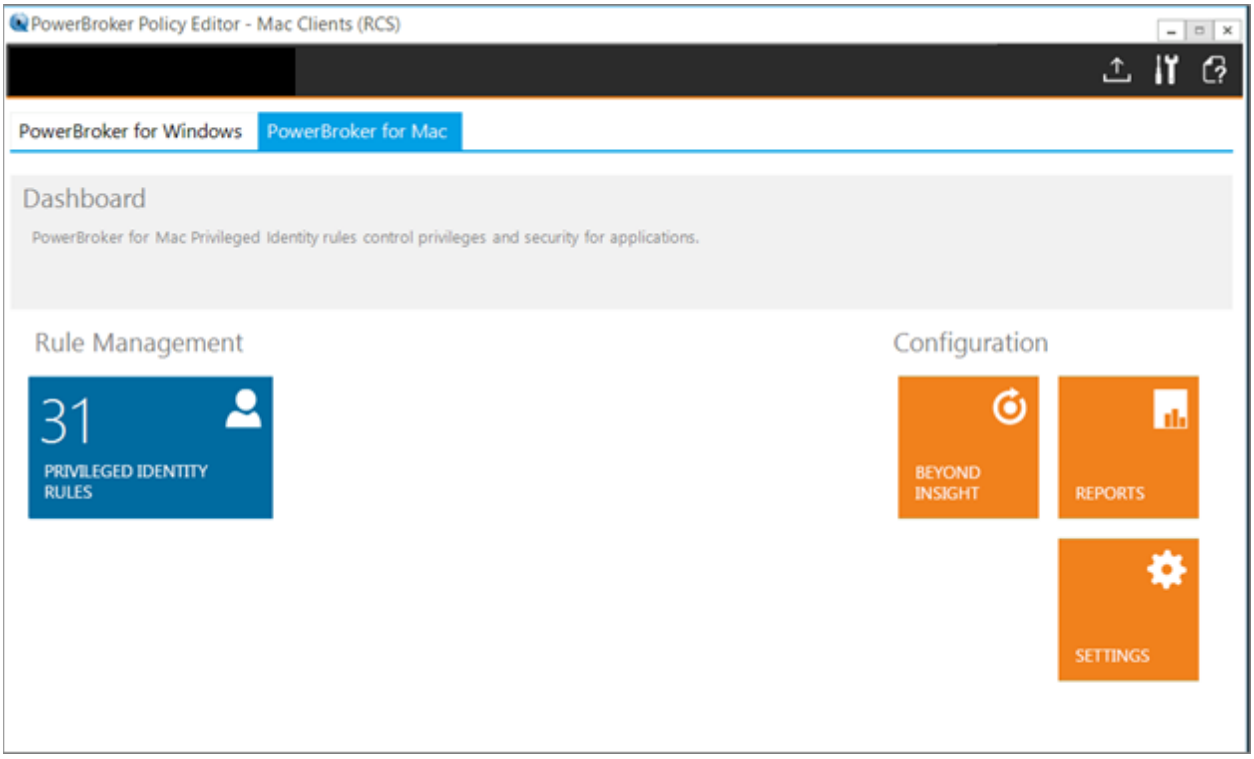

Figure 2: PowerBroker for Mac dashboard.

Extensive Rule Library to Speed Results

PowerBroker for Mac ships with an extensive rule library that contains more than 40 of the most popular applications that require privileges from Microsoft®, Adobe®, Apple® and VMware®. This enables organizations to rapidly begin using least privilege on OS X assets and reduce risk immediately. PowerBroker for Mac enables users to define custom rules based on application and path, or Shell Rule. These two rule types allow for virtually any additional application, or custom solution, to be elevated to meet business needs including specifying specific arguments and application publisher information. All policies can be centrally managed via web services and BeyondInsight or hosted locally for air-gapped implementations. See Figure 3 below.

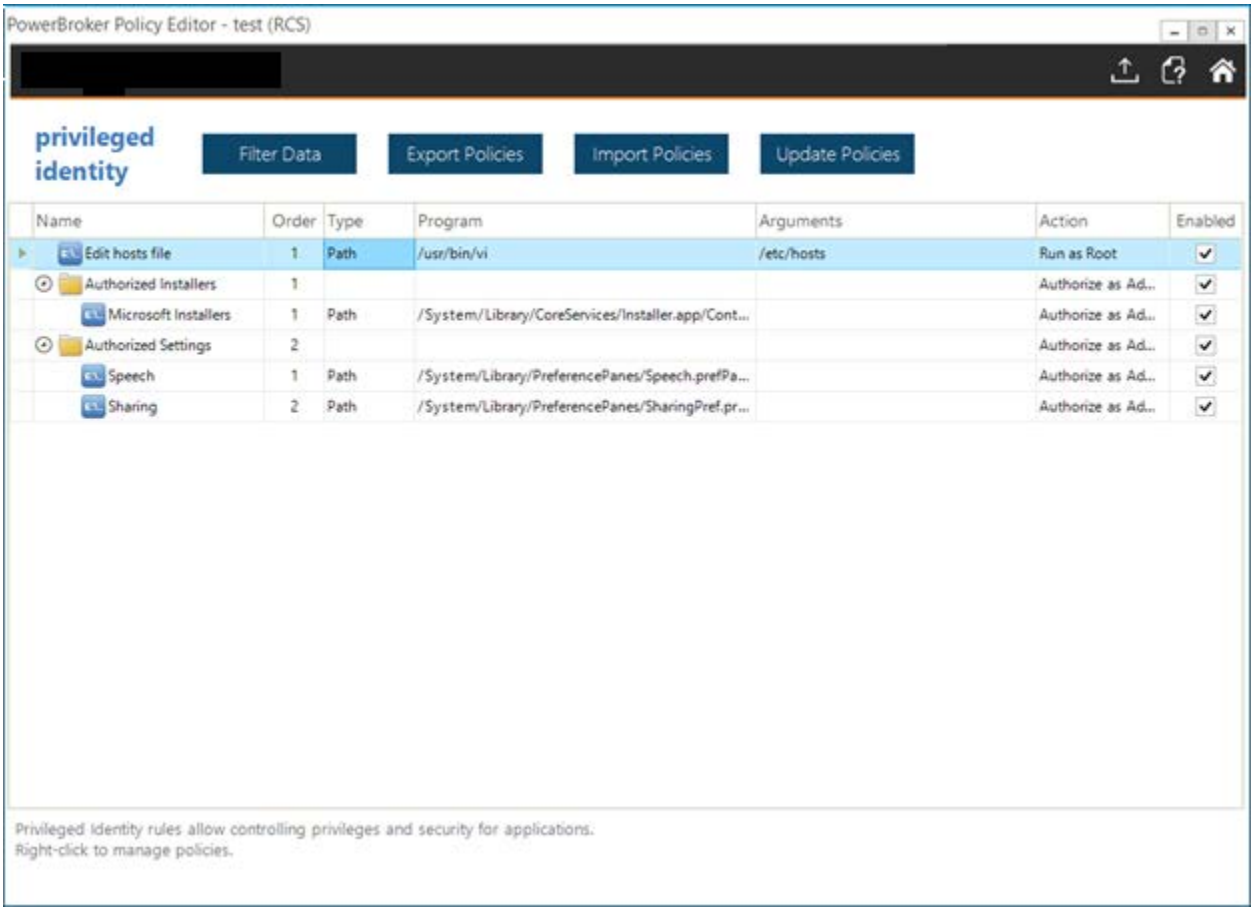

Figure 3. PowerBroker for Mac features an extensive rule library.

Policy Editor for Windows and Mac Enhances Productivity

PowerBroker for Mac leverages mature existing technology for developing new rules using the PowerBroker Policy Editor. Using the same editor in use by PowerBroker for Windows, desktop administrators can define and manage rules for both operating systems from a single location. This capability minimizes the number of products needed to perform least privilege across all endpoints and enhances productivity by providing the same user experience for both operating systems. See Figure 4 below.

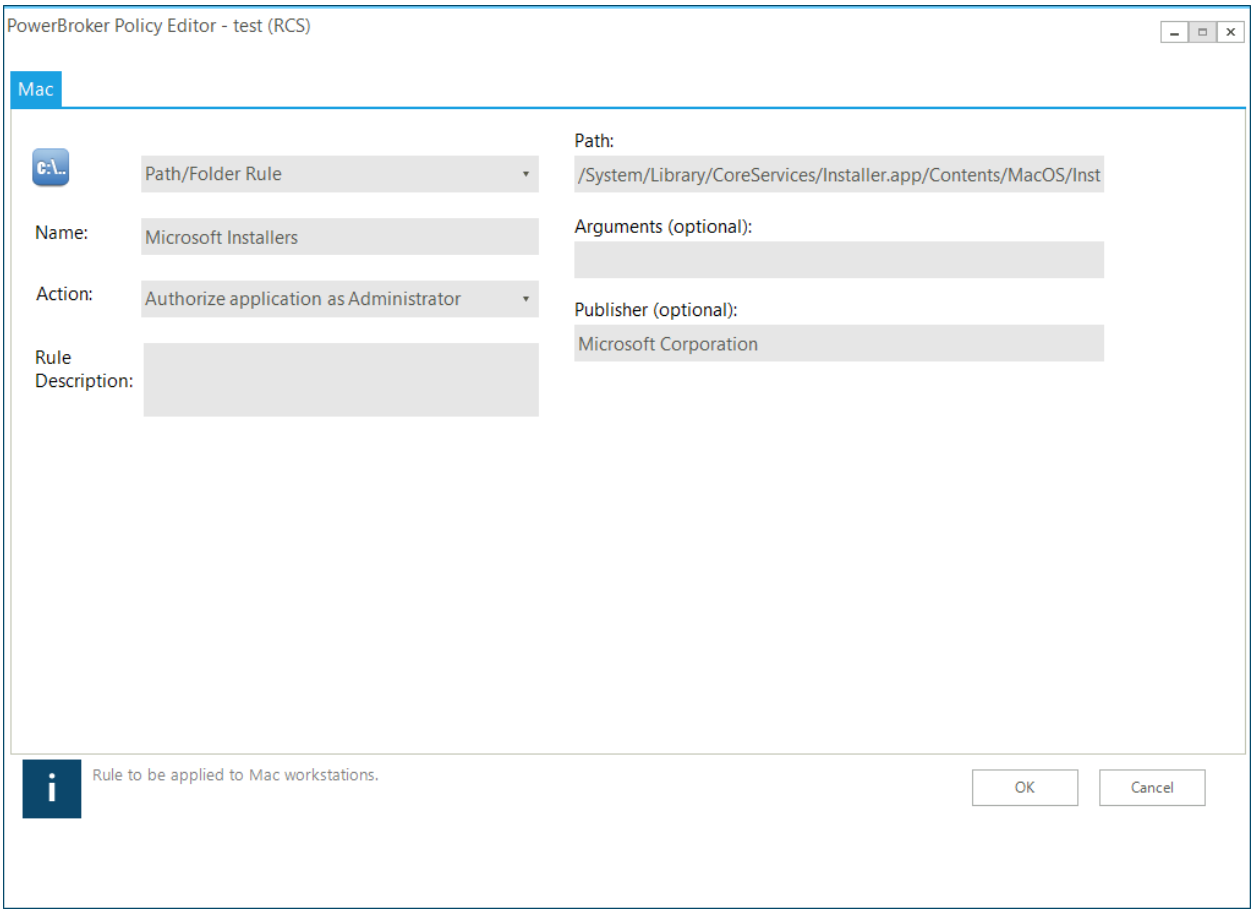

Figure 4. PowerBroker for Mac Policy Editor supports Run-As Root and Authorize Admin.

Enforce Least Privilege across a Heterogeneous Environment

PowerBroker for Mac is fully integrated into the BeyondInsight IT Risk Management Platform, providing a single platform to manage least privilege across heterogeneous environments including Windows, Mac, Unix and Linux. With PowerBroker for Mac, IT organizations can deploy hosting policies via web services for PowerBroker for Mac clients (and PowerBroker for Windows); deliver dedicated asset views for asset inventory and privilege event detection and elevation; take advantage of extensive reporting for complete visibility into privileged activity and usage patterns; and leverage smart rules for alerting and grouping of OS X devices and events. See Figure 5 below.

Figure 5. BeyondTrust enables least privilege management across the environment.

Who benefits from Mac least privilege management?

There are several high level functions within any company that can use and benefit from least privilege management on Macs.

Chief Security Officers (CSOs) will be assured that their entire desktop environment is controlled, not just their Windows or Linux desktops, but also Mac, closing potentially unknown security gaps and helping them achieve an acceptable level of risk.

Directors of Security will be assured that access policy is enforced across the environment, that users will have only the rights they need, that there is a secure audit trail of user and administrator activity, and there is a single pane of glass for reporting and privileged analytics.

IT Ops/ Help Desk will see fewer help desk calls for system tasks, less complexity, fewer products to manage and less time spent in enforcing least privilege across their environments, and a lower total cost of ownership.

Compliance Auditors will be able to quickly see areas that need to be remediated through complete reporting and analytics.

Why PowerBroker for privileged account management?

We believe our differentiation in the privileged account management market lies in the breadth and depth of our solution offering, the value you gain from analytics and reporting insights, and the context you gain with our solutions. Each differentiator is explored below.

Differentiator #1: Breadth and depth of our solution lowers total cost of ownership

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged account management solutions available in the market. From establishing and enforcing least privilege on Windows, Mac, Unix and Linux systems; to automating password and session management; to integrating Unix, Linux, and Mac OS X systems with Microsoft Active Directory; to auditing user and administrator activity, BeyondTrust unifies these capabilities into a single, integrated platform that acts as a central policy manager and primary reporting interface.

In its Market Guide for Privileged Account Management, research firm Gartner recognizes BeyondTrust as a representative vendor for all solution categories in the PAM market. What differentiates us from other vendors in this space is that BeyondTrust is the only company that offers these capabilities from a single, integrated reporting and management platform.

This comprehensive model delivers maximum insights, simplifies management, and lowers total cost of ownership. As well, BeyondTrust embraces a modular, integrated approach for customers with existing point solution investments.

Differentiator #2: Value gained from deep analytics and reporting insights

BeyondTrust solutions help security and IT operations teams make informed decisions. Since a privilege problem tends to involve more than one department, our solutions satisfy the reporting, auditing and management needs of multiple stakeholders from operations to security to compliance.

The BeyondInsight IT Risk Management Platform provides security and IT operations teams a single view of all assets and user activity. With behavioral analytics to understand anomalies, reporting to satisfy security, operations and auditors alike, and the ability to export data to other security solutions, BeyondInsight reduces risks while helping to maximize the value of existing security investments.

Differentiator #3: Better understanding of threats in context from experience

The last thing we think you need is another siloed security point solution. BeyondTrust provides a complete understanding of the modern threat landscape across both internal and external risk. Our solutions incorporate relevant security data – available exploits, risky privileged activity, vulnerable

systems and applications, compliance requirements, mitigations etc. – to help our customers drive better, more informed security decisions.

Analysts and experts agree

BeyondTrust's approach to solving privileged account management challenges has been validated by the industry as well as by our customers. Read what some of the most influential industry experts have to say:

BeyondTrust is a **"representative vendor" for all five key feature solution categories**.[1]

"Deploying the BeyondTrust PAM platform … provides an **integrated, one-stop approach to PAM**… one of only a small band of PAM providers offering end-to-end coverage."[2]

"BeyondTrust is a **pure-player** in the Global Privileged Identity Management market and holds a **significant position in the market**."[3]

"**Frost & Sullivan endorses PowerBroker Password Safe**."[4]

"**Leverage a solution like BeyondTrust's PowerBroker for Windows** to transparently remove administrator privileges."[5]

BeyondTrust is a **"Major Player" in Privileged Access Management**.[6]

"**BeyondTrust is a vendor you can rely on**… PowerBroker Auditor suite is an **impressive set of flexible and tightly integrated auditing tools.**"[7]

BeyondTrust is "**one of the elder statesmen of the industry**."[8]

[1]Gartner, Market Guide for Privileged Access Management, May 27, 2015.
[2]Ovum, SWOT Assessment: BeyondTrust Privileged Identity Management Portfolio, June 11, 2015.
[3]TechNavio, Global Privileged Identity Management Market 2015-2019, 2014.
[4]Frost & Sullivan, PowerBroker Password Safe – a Frost & Sullivan Product Review, 2014.
[5]Forrester, Introducing Forrester's Targeted Hierarchy of Needs, May 15, 2014.
[6]IDC, IDC MarketScape: Worldwide Privileged Access Management 2014 Vendor Assessment, March 2015.
[7]Kuppinger Cole, Executive View: BeyondTrust PowerBroker Auditor Suite, March 2015.
[8]451 Research, BeyondTrust looks to platform plan to make the most of its privileged management assets, June 18, 2015.

Conclusion: Delivering Business Value

End users are increasingly emerging as a greater insider threat, with Mac desktops an area where the fewest controls exist. Close the privilege gap on Mac with a solution that is easy to use, will not affect end user productivity, features the flexibility to create custom rules, and is comprehensive across the desktop environment. BeyondTrust PowerBroker for Mac meets and exceeds these criteria.

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.