



BeyondTrust PowerBroker[®]: Root Access Risk Control for the Enterprise



Table of Contents

Abstract.....	3
Poor Controls on Privileged Access: IT Risk at its Most Fundamental.....	3
Commodity Controls are Too Often Incomplete.....	4
Closing the Gaps: BeyondTrust PowerBroker for Server.....	4
EMA Perspective.....	5
About BeyondTrust.....	6

Abstract

Compliance efforts and security concerns have driven businesses to make substantial investments in threat control. Too often, however, these efforts pay far too little heed to the risks posed by poorly controlled access to administrative privilege in IT, which can have a hugely disproportionate impact on the business. Without putting more effective controls on high-privilege access such as Unix or Linux root account, enterprises not only expose the most business-critical IT assets to the most fundamental level of risk, they also expose trustworthy administrators to the consequences of privilege abuse by others. Commodity tools such as sudo often have gaps in the level of control, scalability and support the enterprise realistically needs. In this paper, ENTERPRISE MANAGEMENT ASSOCIATES[®] (EMA[™]) analysts examine BeyondTrust PowerBroker, a more comprehensive solution designed to close these gaps for the enterprise with provable control.

Poor Controls on Privileged Access: IT Risk at its Most Fundamental

Two of the biggest challenges facing the enterprise today are the management of security, and the management of compliance. The two are often interrelated, since compliance mandates frequently seek to bring regulated businesses to at least a minimum standard of security and risk control.

Compliance, however, does not necessarily mean security. This disconnect was seen, for example, in early 2008, when New England grocery chain Hannaford fell victim to a data security breach despite having validated compliance with the Payment Card Industry (PCI) Data Security Standard.

On the other hand, effective security can directly support compliance, particularly when the intent of compliance is to foster better security. Too often, however, efforts focus on the overwhelming growth in external threats, without sufficient regard for the fact that a highly knowledgeable insider with privileged access to the most sensitive IT resources—and the knowledge of how and where to exploit them—can have a vastly disproportionate impact. This has been evidenced in a number of cases, from French bank Societe Generale, where the bank's exposure to internal fraud at the hands of a sole individual was greater than the GNP of oil-rich Qatar, to the rogue technologists that have exploited administrator-level access with highly visible impact. These incidents have exposed the vast majority of trustworthy professionals to suspicion—but only because organizations that implicitly trust the extreme exposure of administrative-level access without adequate proof of control subject them to this doubt.

The irony of these cases is that while organizations are limited in what they can do to combat external threats, where spending on defense is too often open-ended and potentially infinite, internal threats are often something that the enterprise *can* address.

The root account presents one of the highest-impact opportunities for exploit, fraud or information theft.

The “root” account used to administer Unix and Linux systems offers one such example. Root privilege often means the highest and broadest level of control over the most fundamental level of IT—the operating system itself. Access to filesystems as well as functionality means that the root account presents one of the highest-impact opportunities for exploit, fraud or information theft.

Compounding this risk is the fact that root accounts are typically shared among a group of administrators, which limits the ability to define workable controls on the actions of *each individual* having root access. It also limits visibility into precisely who did what with root access in any specific case. The integrity of dedicated professionals should be better protected from this risk. This can only be achieved when access and actions can be credibly demonstrated and controlled, with minimal impact on the latitude these professionals need to do their work.

What is needed to address these gaps is a solid foundation of *provable* controls to assure these priorities. Such a foundation must offer tighter granularity of control over *who* can do *what* to *which* systems under *which* conditions. It

must provide a higher level of user-specific visibility into all the actions of those with access to root—not just which commands were entered, but outputs and results as well. This control must be matched with assurance

of the confidentiality and privacy of highly sensitive root-level actions, particularly when access is enabled via a network. This level of assurance is, in fact, the only way to *demonstrate* effective control, which, after all, is the only way to substantiate compliance.

Commodity Controls are Too Often Incomplete

Commodity controls such as sudo are often used to limit root-level access to specific actions on the basis of an individual user's identity—but when it comes to enterprise requirements for security or compliance, sudo is often incomplete.

When it comes to enterprise requirements for security or compliance, sudo is often incomplete.

Sudo controls on access to root-level privileges may be incomplete when sudo fails to control the consequences of allowed actions. While sudo may restrict privilege to the execution of specific commands or utilities such as the vi text editor, for example, vi may in turn enable the user to launch an interactive shell from the vi interface. This shell may have unrestricted root privileges not subject to the controls of sudo.

The visibility into activity enabled by sudo may be similarly incomplete. Sudo keystroke logging may be limited only to the commands invoked—but sudo may not capture all I/O, including stderr as well as stdout, which means that the outcomes of actions may not be fully recorded. This leaves gaps that would reveal when, for example, an illicit executable or Trojan is launched by invoking what seems to be a harmless or routine command.

Assurance may be incomplete when tools such as sudo expose log information to unauthorized eyes, or do not natively protect log records from alteration, enabling the malicious to cover their tracks. Sudo's use of the standard syslog facility presents the possibility that log data can be read as it is entered into syslog, or that the syslog facility could be redirected to somewhere other than the expected log file. Without complicating deployment with additional tools, this would allow a third party to gain unauthorized access to log data with the potential for unauthorized alteration, or stop their actions from being recorded in the intended logs.

Third party tools may also be required to secure commodity controls such as sudo and protect the privacy of communications when root access is enabled across a network. Without them, an eavesdropper may be able to directly obtain authentication credentials and other sensitive information used to exploit system control at the most fundamental level.

Together, these gaps raise what may be the most significant concern of all: that commodity controls may not truly be enterprise-ready. Tools such as sudo are often designed to run on only one system at a time. Their deployment may not take into account the scalability needed for the control of root privilege throughout the enterprise. They may have limited ability to integrate with enterprise identity management systems, which may be required to correlate individual user identity with root-level actions. Their ability to detect and report activity is often not intuitive to non-technical individuals in business management or audit roles. This can cause problems when these individuals are most directly responsible for policy enforcement, and may lead to situations where the business must depend on the very technologists supposedly managed by the tool in order to understand what the tool does or how it reports on activity, which may raise concerns about adequate separation of duties.

Closing the Gaps: BeyondTrust PowerBroker for Server

When root privilege control must be consistent and supportable throughout the enterprise, or when more truly comprehensive security and compliance controls are needed to close these gaps, businesses will want to consider commercial alternatives such as BeyondTrust PowerBroker for Servers.

When root privilege control must be consistent and supportable throughout the enterprise, businesses will want to consider commercial alternatives such as PowerBroker for Servers.

PowerBroker for Servers closes gaps such as the ability to invoke shells with uncontrolled privileges from approved commands. Its highly flexible policy language offers open-ended possibilities for policy definition, enabling its use across a wide variety of targets and use cases, even when distributed across multiple operations throughout the enterprise. This extensibility is enhanced by support for a wide range of systems, including versions of Apple Mac OS X—an increasingly visible factor at the desktop.

In addition to expanding the range and completeness of control, PowerBroker for Servers also offers more complete visibility into actions than commodity alternatives, with more comprehensive and reliable reporting. PowerBroker's in-depth detail in reporting is enhanced by the ability to report on user entitlements, addressing one of today's more significant issues for enterprise compliance and control. Its keystroke logging capabilities include the ability to capture all session I/O, including stderr as well as stdout, which reveals the outcomes of actions in addition to commands entered. PowerBroker's real-time replay capability enhances this visibility with the sequence of events that reveals actions and outcomes more fully. This not only supports security and compliance requirements, but also aids in troubleshooting root cause issues when human actions impact business-critical performance, availability, or resource integrity. PowerBroker complements these values with an advanced search capability that improves the efficiency of visibility when needed.

Most importantly of all for many organizations, PowerBroker for Servers is designed for the enterprise. It allows users to perform tasks across multiple targets simultaneously, and is readily deployed with rapid time to productivity. Its non-intrusive architecture requires no change to the Unix or Linux kernel, which significantly lowers barriers to deployment. There is no need to shut down servers or force a reboot in order to deploy, which eliminates impact on resource availability.

PowerBroker's distributed and reliable architecture includes consolidated reporting, which reduces the impact on record-keeping and record-gathering for the enterprise. It integrates with a wide range of enterprise identity management resources, from LDAP, NIS, NIS+ and other identity stores to local accounts, smoothing the ability to correlate actions with individual users, and leveraging resources such as PAM to enforce policy across concurrent sessions. Its native secure remote access capabilities help keep root privilege confidential. Perhaps most valuable to the business and audit professionals directly charged with responsibility for privilege control, its use and reporting capabilities are significantly more intuitive than commodity tools whose functions are often obscure. This enables more actionable visibility for these groups, and eliminates the need for extensive programming expertise on the part of PowerBroker users.

EMA Perspective

Rarely has there been a more significant need for the control of root-level privilege than in the current economic climate, with business consolidation and substantial personnel changes sweeping through virtually every industry. Without enterprise-class tools such as BeyondTrust PowerBroker, businesses may not only risk the loss of visibility essential to protecting trustworthy professionals as well as the business, they may also quite literally lose control of business-critical IT resources at their most fundamental level.

Rarely has there been a more significant need for the control of root-level privilege than in the current economic climate, with business consolidation and substantial personnel changes sweeping through virtually every industry.

BeyondTrust PowerBroker for Servers is such an enterprise-class solution, recognizing the real scope of the challenge. It closes many of the gaps exposed by commodity controls such as sudo, without inhibiting the ability of highly skilled professionals to do their job. It offers a more comprehensive scope of provable control, simultaneously helping the business to assure security as well as compliance priorities, and delivering verifiable protection against one of the highest-impact risks in the enterprise.

About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in Carlsbad, California. For more information, visit beyondtrust.com.

CONTACT INFO

NORTH AMERICAN SALES

1.800.234.9072
sales@beyondtrust.com

EMEA SALES

Tel: + 44 (0) 8704 586224
emeainfo@beyondtrust.com

CORPORATE HEADQUARTERS

550 West C Street, Suite 1650
San Diego, CA 92101
1.800.234.9072

CONNECT WITH US

Twitter: [@beyondtrust](https://twitter.com/beyondtrust)
Facebook: facebook.com/beyondtrust
LinkedIn: linkedin.com/company/beyondtrust
www.beyondtrust.com