

sudo or sudoesn't?

- Does sudo still have a place in today's highly regulated IT infrastructure?

Abstract

When it was first conceived in 1980, the idea of a “super-user do”, (or sudo) command for *nix environments made a great deal of sense. As a tool, it provided organizations a method to get specific types of jobs done. In the 30 years since its inception however, aggressive security, compliance and audit requirements have driven the need for more robust and manageable solutions with which to deliver proper access to enterprise systems. We’ve exceeded the capability of the tool, in enterprise settings.

Strict security and compliance requirements aren’t the only reason organizations are looking to enterprise-friendly sudo alternatives. Today’s IT infrastructure has become a dynamic fabric, where change and flexibility is an absolute requirement. Moving from sudo to a purpose-built solution for privilege authorization management provides a highly valued productivity enhancement, a force-multiplier that can be used to quickly corral the sprawl created by new technology adoption, such as virtualization and cloud computing.

This white paper will highlight certain situations where sudo has its place in IT. It will also show where it **sudoesn't**.



www.beyondtrust.com

2172 Salk Avenue
Carlsbad, CA 92008

800.234.9072

Table of Contents

When You're a Hammer, Every Problem Looks Like a Nail.....	3
Where Sudo es.....	4
Everybody Likes Free, Right?.....	4
Additional Layer of Protection to root.....	4
Simplified Process for Administrators	4
Upgrade in Auditing over Native Unix Systems	4
Time-Ticketing System	4
Where Sudo esn't.....	5
Sudo esn't Secure.....	5
Vulnerabilities Exist in Sudo	5
What Little Data that is Created is Insecure.....	5
Sudo esn't Comply.....	5
There's a Serious Lack of Institutional Control.....	5
Log Security and Compliance is Questionable at Best.....	5
Sudo esn't Scale Within the Enterprise	6
Hundreds of Releases, Countless Patches.....	6
There is No Official Support Available	6
Lacks Independent QA Testers.....	6
Sudo esn't Help You Move to the Cloud.....	7
Virtualization and Cloud computing.....	7
What's the Alternative?	7
PowerBroker Servers, by BeyondTrust	7
Reliable and Secure Operations across Complex Environments	8
Targeted Authorization with BeyondTrust PowerBroker Servers.....	8
Enterprise Intelligence, Not Just Metrics	9
Supported by Experts in Privilege Management	9
What's Next?	9
See For Yourself.....	9
About BeyondTrust.....	10

When You're a Hammer, Every Problem Looks Like a Nail

In most organizations, sudo is typically intended to only allow a certain set of people to run a very limited set of commands, as a different, elevated privilege user.

Unfortunately, given its easy access and liberal governance, system administrators often use the sudo command for everyday commands and tasks – bypassing corporate policy, network security and compliance requirements.



It goes without saying that IT pros require access to simple IT commands to remain productive and efficient.

Unfortunately, the proliferation of sudo has meant that these employees have been provided with passwords and IT access far above and beyond their actual needs. This has a direct impact on compliance and security.

For any organization where regulatory compliance, internal auditing and enterprise security is a way of life, the widespread access and availability of administrator privileges within the enterprise IT environment is a serious liability. But what is the alternative? In today's highly regulated and dynamic environments, organizations are often choosing to meter out this access through selective and programmatic delegation of root access – dictating permissions for users to the most granular levels. This separation of powers removes the need to disclose highly sensitive rootwords helps restore the balance between access/productivity and security/compliance.

Where Sudoes...

Everybody Likes Free, Right?

Shipping with countless *nix builds as an open source solution, sudo is hard to beat when it comes to a purely cost-conscious decision. However, it's important to remember that this is what an accountant would call your "up front" cost. As the UK government detailed in a recent study, *Total Cost of Ownership of Open Source Software*¹, many surveyed companies who had deployed open source software "needed to hire experts and look for support to meet their organization's ambitions including for control of code and configuration, and taking more direct control of their infrastructure to allow agile innovative responses to changing needs". In short, the software might have been free, but the customizations, support, control and continued development of the solution were not.



1.[https://www.acquia.com/sites/default/files/library/attachment/Total_cost_of_ownership_of_open_source_software_\(LSERO\)-1.pdf](https://www.acquia.com/sites/default/files/library/attachment/Total_cost_of_ownership_of_open_source_software_(LSERO)-1.pdf)

Additional Layer of Protection to Root

Too often, organizations fail to achieve necessary milestones in the control of root access to the heart of IT and its critical assets. Instead, they simply assign access to a shared account where activity may be difficult, if not impossible, to correlate to the actions of a single user. With sudo, the root account password does not need to be shared with everyone who needs to perform tasks on Unix/Linux systems.

Simplified Process for Administrators

Though this is often argued as a security and compliance risk, sudo can be configured in such a way that members of a designated group do not need additional authentication to become root, which results in higher productivity. At what cost to security?

Upgrade in Auditing over Native Unix Systems

Auditing in Unix/Linux was never a priority under the original intentions of these operating systems, since its origin of use was in Academic research programs and databases. Though sudo's logging functionality has serious security and compliance red flags, it is definitely a step in the correct direction to log what actions a user performed with privileged access.

Time-Ticketing System

When a user invokes sudo and enters their password, they are granted a "ticket" for five (5) minutes (default time). This time-ticketing system give some level of protection in situations where there is a danger of leaving a root shell open where others can physically use an administrator's keyboard.

Where Sudoen't...

Sudoen't Secure

Vulnerabilities Exist in Sudo

A well-documented example of a simple coding mistake within sudo that could have had catastrophic effects on network operations² highlights the challenges of relying upon an open source solution that is primarily responsible for doling out elevated privileges to your organizations most prized assets – your servers. As you'll read throughout this paper, these flaws also create a lack of control – institutional control – over the maintenance and upkeep of widely deployed sudo instances.

2.<http://nakedsecurity.sophos.com/2012/05/21/anatomy-of-a-security-hole-the-break-that-broke-sudo/>



What Little Data that is Created is Insecure

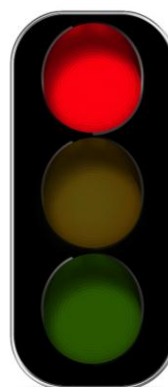
As security for sudo is provided through the binaries and configuration files, sudo lacks the necessary tools required to protect the integrity of generated security data. For example, log entries can easily be erased or tampered with – creating a potential auditing nightmare. The logs themselves are stored in syslog, which isn't natively secured. This significantly impedes an organization's ability to truthfully answer "who did what, when?"

Sudoen't Comply

There's a Serious Lack of Institutional Control

Amazingly, sudo has the ability to invoke a shell that has no control over itself whatsoever. This means that a user could obtain complete access over mission-critical systems and applications and perform whatever acts they please – copying, deleting or altering your data. As ITSecurity.com has reported, the #1 internal security threat isn't malware – it's your employees³ – "it's precisely this access that can endanger the security of mission-critical applications." This lack of institutional control is a good example of items auditors look for when it's compliance reporting time.

3.<http://www.itsecurity.com/features/the-top-5-internal-security-threats-041207/>



Log Security and Compliance is Questionable at Best

While sudo logs and tracks user activity over privileged accounts, it is very difficult to ensure safety of sudo's logs. It (sudo) does not natively protect log records from alteration, and

cannot provide remote logging to remote servers, which are best practices for security and compliance.

Sudoesn't Scale Within the Enterprise

Hundreds of Releases, Countless Patches

There have been well over 100 sudo version releases over the last few years alone⁴. This presents an enterprise challenge in a few ways. First, most companies have no idea which versions are installed on which servers – this makes cataloging sudo in an organization of size almost impossible. This is not only a management nightmare, but could also possibly create compliance failures if organizations are unable to disclose what types of access controls are in place on critical systems.

Second, managing the updates of these sudo deployments is troublesome. This not only speaks to the ability to harness new features within sudo, but also the requirement to patch the deployments that have security flaws resident. The act of patching and updating sudo across an organization of any size has real, hard dollar costs attached to it.

For most organizations, given the capabilities of sudo, this is too much risk to shoulder, considering the commercially supported a maintained options available to IT teams. This is also an excellent example of when “free” isn't really free.

There is No Official Support Available

Since sudo is open source, there is no directly accountable contact to call upon if an organization encounters technical problems with sudo. The unpredictability of researching and retrieving a correctable solution from the open source community, in a timely manner, translates to lower productivity and higher cost in managing privileged identities.

Lacks Independent QA Testers

When an organization is seeking to protect assets worth significant amounts of money, it would be prudent to ensure that the solution they are implementing has been tested and validated regarding the security and functional features. Though there are many contributors to issues and features, there is no dedicated group of QA testers to provide assistance and assurance that the product is enterprise ready.



4.<http://www.sudo.ws/sudo/changes.html>

Sudoesn't Help You Move to the Cloud

Virtualization and Cloud Computing

Virtualization and cloud computing introduce some new challenges to controlling access to privileged information and proving compliance. The use of virtual machines adds further complexity into the mix, since creating an identity for an individual virtual machine and tracking that virtual machine from creation to deletion can be challenging for even the most mature virtualized environments. Proving that the physical and virtual infrastructure of the cloud can be trusted becomes even more difficult when those infrastructure components are wholly owned and managed by external service providers. This far exceeds the intent of sudo and proves the need for a more robust solution for managing root access on critical systems, in both physical and virtual environments.



What's the Alternative?

Clearly, there is a need for elevated privileges as part of the ongoing operations around *nix systems. However, today's compliance realities – the regulations, guidelines and audit intensity – within the enterprise (both commercial and governmental) dictates the need for a much more rigorous approach to privilege management. This approach must be supportive of the overall goal of institutional control, the hallmark of compliance initiatives.

For all of its merits, the open source approach leaves a lot to be desired when it comes to control requirements. For those organizations who wish to mature their operational processes to better support the security and compliance requirements of the organization at large, BeyondTrust offers PowerBroker Servers.

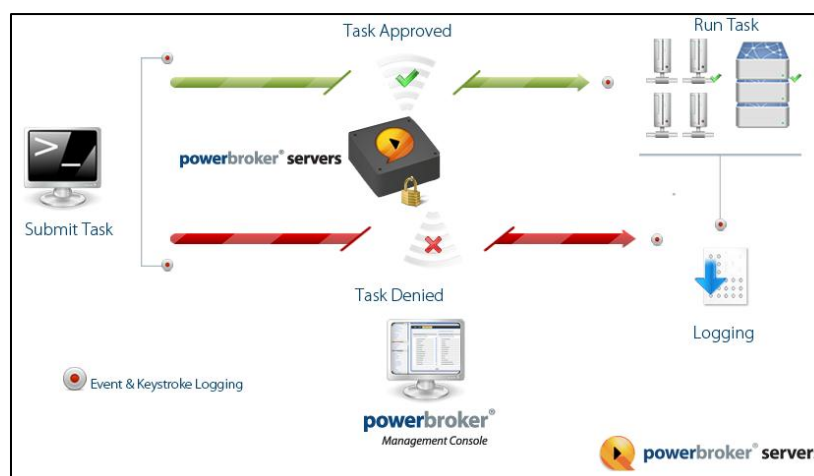
PowerBroker Servers, by BeyondTrust

PowerBroker Servers provides policy-driven access control and logging across UNIX and Linux platforms. Using a centralized policy server, every request for privileged access is evaluated by policy. In the policy processing, the request can be accepted or rejected, event and I/O logging turned on or off, and the request can be modified. This is the basis for a fully compliant privilege management solution, one that allows you to retain institutional control of your *nix systems.

With PowerBroker Servers, modifications could be as simple as removing an incorrect command-line parameter, or redirecting the request to run as a different user on a different host. Access can also be managed by day, date and time, user ID and group membership. PowerBroker's rich policy language provides the capability to address almost any conceivable business or compliance requirement for privileged access.

With regards to scalability and usability within the enterprise, PowerBroker has a clear advantage over sudo. In the specific case of patching/updating, in most cases, only the Master PowerBroker files need to be updated. For example, if a company updates their Master files every 1-2 years, the client endpoints can be updated approximately every 3 years, which translates into a real-world cost savings for operations teams.

Another customer-proven benefit of PowerBroker over sudo has to do with the sudo files themselves. Most organizations are faced with the reality of having individual sudoer files on each machine. In enterprise environments, this quickly becomes an administrative nightmare, in terms of maintenance and currency. Often, systems administrators are faced with the addressing each machine to add users or delete users from their sudo files. In fact, many organizations forgo the updates – creating a compliance and audit red flag - because of the significant amount of time it requires. Employee turnover adds to this issue, but again, the time required rectifying often means it goes un-updated. A single, centrally managed policy provided via PowerBroker, as shown below, solves this problem.



Reliable and Secure Operations across Complex Environments

PowerBroker Servers offers reliable, highly secure operations, which include a specialized client/server architecture that has fail-over servers that provide fault tolerance and load balancing for continual availability. As part of the highly secure functionality that PowerBroker Servers offers, key features include hardened shells, support for more than 30 encryption methods, indelible audit trails, checksum verification and the use of “forbidden keystrokes”.

Targeted Authorization with BeyondTrust PowerBroker Servers

Once users have logged into the UNIX/Linux network, BeyondTrust PowerBroker Servers minimizes security risks on the network by helping site administrators selectively delegate administrative privileges. It protects the root account, password and special accounts from potentially damaging misuse of administrative privileges by restricting authorization of UNIX/Linux tasks on a user-by-user basis, including:

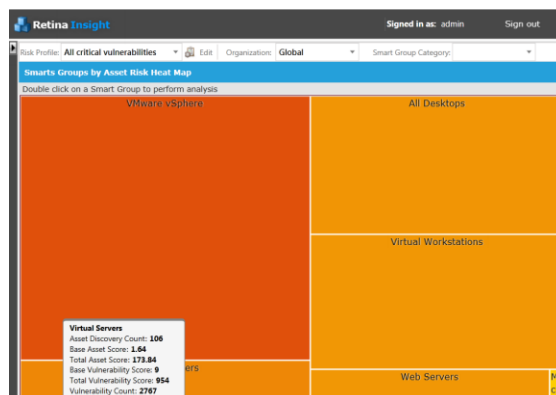
- Tasks that require root privileges
- Tasks that require other special account privileges such as access to databases, (Oracle) and applications (SAP)
- Tasks that may run only on specified hosts or at certain times
- Tasks not allowed to access certain directories or data

Enterprise Intelligence, Not Just Metrics

Managing root tasks and delegations for server systems is one thing.

Reporting on those activities is a completely different animal, especially when it comes to satisfying audit and compliance requirements. With BeyondTrust, you are able to centrally manage the reporting on your privilege management program, with both regulation-specific reporting packages, as well as a powerful, real-time analytics warehouse for ad-hoc

and custom reporting. In addition to reporting, our management console also provides the ability to perform regular vulnerability assessments of your server (and beyond) infrastructure. These capabilities help executive staff members understand the value and importance of replacing sudo deployments in highly regulated industries.



Supported by Experts in Privilege Management

BeyondTrust is the global leader in privilege authorization management, access control and security solutions for virtualization and cloud computing environments. BeyondTrust empowers IT governance to strengthen security, improve productivity, drive compliance and reduce expense. The company's products eliminate the risk of intentional, accidental and indirect misuse of privileges on desktops and servers in heterogeneous IT systems.

What's Next?

See For Yourself

Visit <http://go.beyondtrust.com/pbul-eval> to upgrade your environment with PowerBroker Servers and start managing privileged access in the most secure and compliance-driven way possible. Our solution experts can help you accelerate your migration from sudo, first by helping you discover all of your *nix servers and then by also identifying where sudo resides on those servers. Ready to get started?

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.