

Avoiding “Game Over” by Securing the Server via Privilege Management

By Dr. Eric Cole

Sponsored by BeyondTrust



 ecole@secureanchor.com

 www.secureanchor.com

Secure Anchor is All Cyber Defense, All the Time

PREVENT | DETECT | RESPOND

Table of Contents

Are You Making the Attacker’s Job Easier?	3
Three Current Approaches – and Why They Are Failing	4
Making root or admin access a right, not a privilege	4
The principle of <i>most</i> privilege – user equals adversary	4
Using sudo and run-as controls	5
Why a New Approach is Needed	5
Top Use Cases for Server Privilege Management	5
Flexible policy language for command elevation	5
Advanced control and audit of commands down to the system level	6
Session monitoring, logging and reporting	6
Fine-grained control over stored credentials	6
Centralized account access and privilege control	7
Enterprise scale	7
Conclusion	8
Appendix: How BeyondTrust Helps with Server Privilege Management	9
Control and Audit Unix, Linux and Windows Server User Activity with Fine-Grained Policy Controls	9
Gain Visibility into Unix, Linux and Windows System Security	9
Understand Password, User and Account Behavior	9
Simplify Deployments with a Single Platform	10

Avoiding “Game Over” by Securing the Server via Privilege Management

Eric Cole

Are You Making the Attacker’s Job Easier?

Many organizations struggle with information security because they try to do too many things and they do not focus on the things that really matter. While defense in depth is important, in these types of reactive organizations quantity—instead of quality—of controls is too often the answer.

Nowhere is the quantity/quality disparity more evident than in an organization’s response to data breaches. Today’s security reality should not be about *preventing* a breach, but *controlling the damage caused by* the breach. Compromises are inevitable; thinking that an organization is never going to have a breach is as naïve as thinking that a person will never get sick. The focus needs to be on limiting the frequency and impact which directly ties to controlling the damage.

Therefore, the most appropriate question to ask when building, designing and implementing a plan for information security is, “What would allow an attacker to cause the most damage?” The answer is actually quite simple: Not controlling privileged access to critical information – information that is often housed in tier 1 systems.

In looking at the security of a server, the question that needs to be answered is whether the approach an organization is taking is offensive-friendly or defensive-friendly. Meaning, whose job are you making easier and whose job are you making harder? As ironic as it sounds, most organizations have servers with large amounts of critical information and minimal controls around privileged access which makes it very easy for the offense to cause harm and very difficult for the defense to protect, secure and detect attacks.

What would allow an attacker to cause the most damage? Not controlling privileged access to critical information.

While it might sound like an over simplification (it really is not), by focusing in on managing privileged access, an organization is joining the winning team by changing the rules so that the offense no longer has an unfair advantage. If a server gets compromised by an adversary but their access is limited, the amount of damage they can cause is also limited and controlled. On the other hand, if an adversary has unlimited or uncontrolled privileged access (i.e. root or administrator access), the game is over very quickly.

This white paper will explore the necessary elements of server privilege management – command elevation and delegation, session monitoring and logging, privileged account management, account consolidation and measuring risk to target systems. When used in concert, these capabilities will better secure access to critical systems and data.

Three Current Approaches – and Why They Are Failing

The approach most organizations take to security is to focus on building a robust perimeter with extensive emphasis on network traffic. Preventing and detecting adversaries at the packet level is the approach of choice. Unfortunately, the adversary has figured out ways to bypass all of those controls and gain access directly to the server where minimal to no security exists. Therefore, to properly defend an organization today requires focusing in on controlling and managing access to the key servers that contain the critical data that will cause the most damage. If an adversary has limited access, the impact is minimal. If they have full access the impact is extreme. But there are three primary shortcomings in how organizations currently seek to limit privileged access to their tier 1 servers.

Making root or admin access a right, not a privilege

The first major short coming in the approach that organizations take is that many users feel that root and admin access is a right, not a privilege. They think that it is a requirement to be able to have full control of a server, regardless of their job and control is often handed out like candy at Halloween to anyone who asks for the access. There is a reason it is called “privileged” access – because it can be removed, controlled and/or minimized at any time. In most organizations, very few individuals – if anyone – should have privileged access and instead the principles of separation of duties and rotation of duties should be implemented and put in place.

To properly defend an organization today requires focusing in on controlling and managing access to the key servers that contain the critical data that will cause the most damage.

The principle of *most* privilege – user equals adversary

The second major shortcoming faced in securing their servers is that many organizations implement a principle of *most* privilege by giving users the most access they need to do a given job. The problem with this approach is that any account on a network can and will be compromised. Therefore, user equals adversary. If an organization is giving users the most access or privileged access, they in turn are actually giving adversaries full access to their servers. By recognizing that a user account will be compromised, thus making user and adversaries equivalent, a principle of least privilege must always be implemented with regards to access. See figure 1.



Figure 1 – Microsoft’s approach to least privilege by controlling privileged access and escalation

Using sudo and run-as controls

The third major shortcoming with how organization manages access is through the use of “sudo” and “Run as” controls in Unix and Windows. While these controls do have some value in implementing effective security, they are limited in what they control, often not implemented correctly and are a single point of failure.

Why a New Approach is Needed

These flawed approaches 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. Deployments 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 too 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.

*The most significant concern of all -
That commodity controls may not
truly be enterprise-ready.*

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
- 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
- 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.

Top Use Cases for Server Privilege Management

When 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, organizations will want to consider commercial alternatives. The core benefits of such solutions include automation, visibility and proactive response to both traditional and advanced threats. Following are several common use cases where such solutions offer advantages over other insufficient methods mentioned above.

Flexible policy language for command elevation

A highly flexible policy language offers open-ended possibilities for policy definition, enabling its use across a wide variety of targets and use cases — such as the ability to invoke shells with controlled

privileges from approved commands – even when distributed across multiple operations throughout the enterprise. This extensibility is enhanced by support for a wide range of systems.

Advanced control and audit of commands down to the system level

Auditing and controlling activity inside scripts and third-party applications in Unix and Linux systems has been difficult for many companies to achieve, especially when it is easy to “cheat” the system by pointing shortcuts to unapproved applications. A solution is needed to enhance system level control and audit capabilities over any application – regardless of how the application is initiated. This approach would help organizations control actual commands being processed and the actions at the system level removing the ability of command spoofing or altered key sequencing.

Look for capabilities to provide a secure container for all applications at the very lowest system level, providing fine-grained control over interactions between the operating system and the user. This results in a faster and more secure way of providing root access for individual controlled applications or administrative tasks. This closes loopholes that exist in least privilege.

Session monitoring, logging and reporting

In addition to expanding the range and completeness of control, commercial solutions also offer more complete visibility into actions than commodity alternatives, with more comprehensive and reliable reporting. In-depth detail in reporting should be enhanced with the ability to report on user entitlements, addressing one of today’s more significant issues for enterprise compliance and control.

Keystroke logging capabilities should 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. 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.

Fine-grained control over stored credentials

Traditional enterprise password management solutions provide limited privilege delegation capabilities. The controlled accounts often have excess privileges which are more susceptible to misuse and creates a larger attack surface should those accounts be compromised. Regardless whether an account password has been checked out or the session proxied via SSH to a Unix/Linux host, organizations need to closely control what a user can and cannot do once logged on is critical.

To overcome this challenge, look for a solution that offers a centralized policy that can be used to provide tight controls and additional auditing capabilities for accounts checked out from a password storage solution. This allows for the credential with the least amount of rights possible to be stored in the store, but allows for the added flexibility of one off, custom and edge case type commands to be run at any privilege level.

Not only can the commands themselves be controlled, but so can user and system runtime environment

settings along with any parameters or arguments passed during a command request. Session recording down to the keystroke that is fully indexed and searchable may also be created.

Centralized account access and privilege control

When users and administrators need access to a system, a user account needs to be created on each host in order to provide system access for the user. Rights for these user accounts are often bloated and clean-up of accounts, along with their associated rights, often goes unchecked when an employee changes role or leaves an organization. Organizations need a way to reduce the number of accounts being created, control which server those consolidated accounts can logon to, and what rights that user has after they have been authenticated.

Consider using a server privilege management solution for consolidation of account and system access rights to control user rights post login. This way, user accounts can be created in one location, say, AD, with a user's AD group membership controlling what servers that user can access and a centralized policy to tightly control and audit that user's activities during each authenticated session.

Enterprise scale

Look for a solution that can perform tasks across multiple targets simultaneously, and is readily deployed with rapid time to productivity. There should be no change to the Unix or Linux kernel required, which would significantly lower the barrier to deployment, meaning no need to shut down servers or force a reboot in order to deploy, which eliminates impact on resource availability. For a sample architecture, see figure 2.

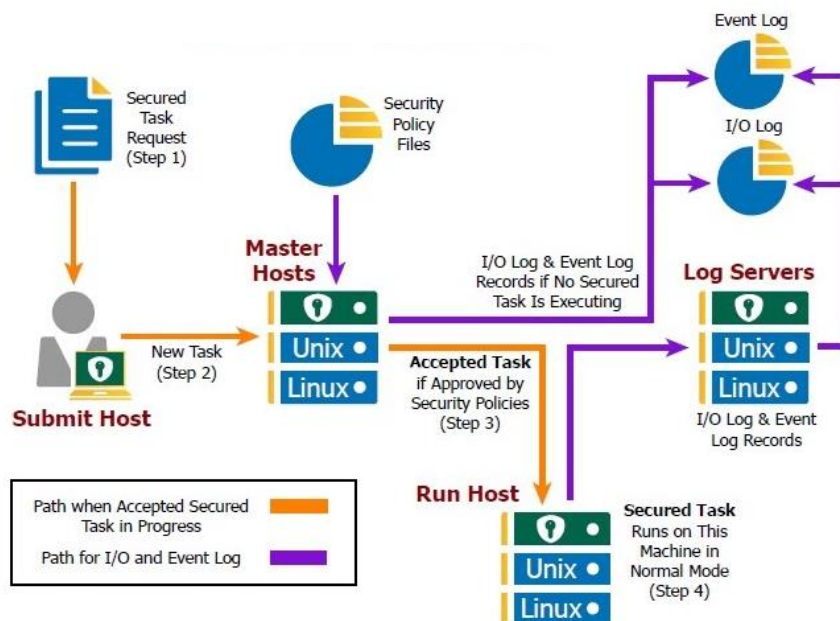


Figure 2 – Architecting a least privilege solution at enterprise scale.

Conclusion

Rarely has there been a more significant need for the control of privileged access than in the current threat climate, with business-impacting data breaches regularly dominating the headlines.

Without enterprise-class solutions to control and audit privileged access on critical servers, organizations may not only risk the loss of visibility essential to protecting trustworthy professionals, but they may also quite literally lose control of business-critical IT resources at their most fundamental level – a true “game over” moment.

Enterprise-class solutions exist that close many of the gaps exposed by commodity controls such as sudo, without inhibiting the ability of highly skilled professionals to do their job. These commercial solutions offer 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.

Appendix: How BeyondTrust Helps with Server Privilege Management

Lack of control over root or admin passwords, super-user status or elevated privileges could lead to a damaging breach or negative audit finding, especially if organizations are running their critical systems on tier-1 servers such as Unix and Linux. Although least privilege enforcement is important to preventing such activity, organizations typically aren't able to control what their users can do and what they have access to once they are authenticated by a system. Legacy approaches to solving this problem are siloed and not integrated: a password storage tool for access, sudo or a least privilege delegation tool for policy enforcement, no user behavior analysis to help identify anomalies. To help, security and IT teams are forced to cobble together point tools from multiple vendors resulting in unnecessary complexity and cost.

BeyondTrust solves this problem by:

- Discovering, storing and rotating privileged account passwords and SSH keys automatically, controlling access to tier 1 servers
- Providing fine grained policy controls over what Windows, Unix and Linux users can do once they are logged on to a system, reducing risk
- Enabling single sign-on and unifying policy across the environment, simplifying access for users
- Providing risk visibility into privileged activities and assets, reducing risk from known vulnerabilities
- Analyzing, recording and reporting on privileged password, user and account behavior, reducing risk from anomalies and helping to achieve compliance
- Delivering an integrated platform, speeding implementations and reducing costs

Control and Audit Unix, Linux and Windows Server User Activity with Fine-Grained Policy Controls

PowerBroker stores user accounts, and when a user checks out a password to invoke a command, fine-grained policy controls what the user can execute on the Unix, Linux or Windows box. This integrated approach limits the exposure of systems by combining password management and privileged user auditing. For organizations managing heterogeneous server environments, PowerBroker bridges Unix and Linux systems into Active Directory for simplified authentication and greater visibility over user activity.

Gain Visibility into Unix, Linux and Windows System Security

PowerBroker leverages vulnerability data from BeyondTrust Retina and other 3rd party vulnerability assessment tools to provide a complete picture of privileged application and asset security—including for network, cloud and virtual assets. Retina leverages PowerBroker to handle the command elevation for system scanning, eliminating the need to be the root or admin account. Having this zero-gap coverage reduces risk by ensuring that no assets are left unprotected, and that privilege decisions are made with insight into the risk profile of the user, system, applications, and asset.

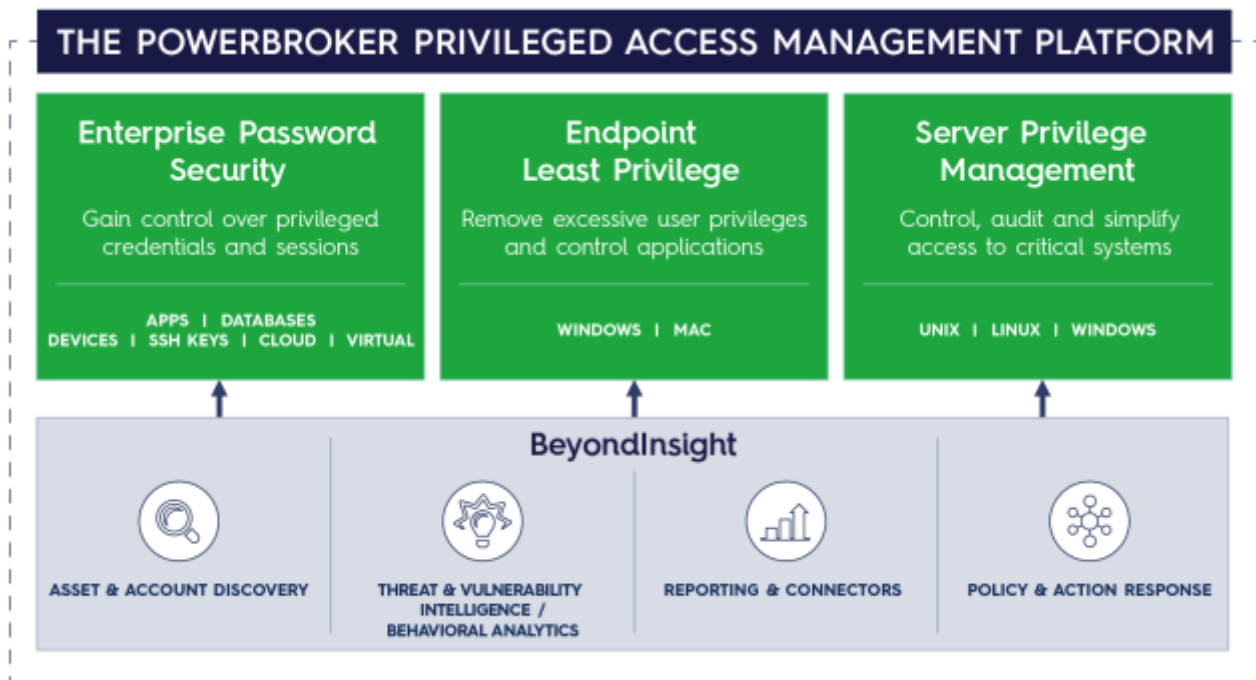
Understand Password, User and Account Behavior

PowerBroker analyzes privileged password, user and account behavior and augments it with additional threat attributes to assign a Threat Level—a key indicator of elevated risk—to each event based on the

user, asset, and application launched. This capability makes it easier for security teams to uncover emerging risks in the organization, pinpoint specific at-risk systems, report on the findings, and take action to eliminate the threat before the potentially damaging effects of a breach.

Simplify Deployments with a Single Platform

With PowerBroker, security and IT operations teams have a single pane of glass to manage their privileged access management policies and deployment, and provide reporting to multiple stakeholders. BeyondTrust delivers the PowerBroker Privileged Access Management Platform as a modular, integrated set of solutions united by common components. This approach greatly simplifies deployments, helps to control costs, and provides a foundation to reduce the evolving risks of privileged access.



For more on how BeyondTrust solves this problem, visit: www.beyondtrust.com/solutions/server-privilege-management/