Challenge
Organizations around the world host their most critical applications and their most sensitive data on Unix and Linux systems, making them high-value targets for external attackers and malicious insiders. The skillset required to manage Unix and Linux systems is very niche and can be difficult for organizations to obtain. Lack of expertise, combined with inadequate privilege management solutions, results in account sharing, providing unrestricted root access, and inadvertently leaving files and sessions open and unmonitored. These practices open the doors to threat actors, who are rapidly gaining the skills necessary to exploit them. And the risk only increases as attack surfaces expand, perimeters vanish, and compliance pressures mount.

How can you limit who has root privileges to reduce the risk of compromises as well as financial losses resulting from data breaches?
How can you collect audit data and session recordings in a centralized, protected location?
How can you achieve zero trust for your Linux estate?

Many organizations turn to open-source tools like sudo to manage privileged access. Although sudo and sudo-wrapped tools can offer some degree of privileged access management, they can’t meet the granular privilege management and compliance requirements that today’s Linux deployments demand. Utilizing sudo to manage root privileges can be a cumbersome process, with the potential to create increased risk exposure for your organization, especially if it is large and diverse. With no efficient centralized administration, potential compliance issues, and no support for immutable auditing or session recording, it’s clear that sudo’s many shortcomings make it an inadequate privilege management solution for most organizations.

Solution
BeyondTrust Privilege Management for Unix & Linux is an enterprise-class, market-leading privilege management solution that enables customers to effectively manage and control privileges across their Unix and Linux systems and achieve zero trust. With the largest install base in the market, our solution helps customers eliminate credential sharing, limit root access, and prevent and contain breaches – without hindering productivity and without relying on sudo or custom tools. Robust auditing capabilities, including keystroke logging and session recording, along with centralized management, allow for streamlined compliance and protection.
Privilege Management for Unix and Linux was conceived in the early 1990s by engineers that included the top data scientists from MIT and the US Department of Defense. By 1994, some of the world’s largest banks were standardizing on the solution.

Privilege Management for Unix & Linux is the most reliable and trusted privilege management solution available. Today, customers include:

- 8 of the top 10 banks
- 4 of the top 5 telecommunications companies
- Government agencies
- Leading tech giants

**Powerful Auditing for Simplified Compliance**
Centralize the capture and management of event logging, including logs of privilege elevation events and full session recordings. Logs are securely stored in a protected, immutable format.

**Fine-Grained Least Privilege**
Allow for fine-grained, policy-based control of privilege elevations, eliminating the need for root sessions and sudo.

**Script-Based & Dynamic Access Policy Controls**
Provide limitless options for policy and integration with script-based policies. Dynamic access policies utilize factors such as time, day, and location to make intelligent privilege elevation decisions.

**Remote System & Application Control**
Enable users to run specific commands and conduct sessions remotely based on rules – without logging on as admin or root. Use of bastion hosts is fully supported, with the full input and output of all sessions recorded.

**File & Policy Integrity Monitoring**
Audit and report on changes to critical policies, systems, applications, and data files.

**Centralized Management**
Centralize the management of all policies, upgrades, updates, and deployments, including audit data and session recordings, for Unix and Linux servers and Linux desktops.

**Integrations & Scalability**
Leverage the REST API to facilitate task automation and seamless integration with various systems and tools, including SIEM, ITSM, and orchestration utilities. The architecture is designed to efficiently scale from a handful of systems to tens of thousands.

**Benefits**

**Increase Security**
Limit the attack surface by dynamically elevating privileges for standard users and preventing the use of the root account, based on flexible role or script-based policies.

**Ensure Compliance**
Streamline forensics and simplify compliance by providing an unimpeachable audit trail of all user activity.

**Improve Efficiency**
Streamline management and operations and enhance user productivity by simplifying processes that can be complex with sudo or custom tools.

** Prevent and Contain Breaches**
Detect suspicious user, account, and asset activity in real time with monitoring of all logs and sessions.
Use Cases

Manage Privileges and Audit User Actions

Traditionally, a Linux user or administrator uses a root shell or sudo to perform privileged actions. This approach leaves the organization wide open to attacks of many kinds and is not consistent with the principle of least privilege. That’s because it’s an all-or-nothing approach – either the user has full administrative privileges or they have nothing – and it doesn’t control what privileged actions that user may execute.

Furthermore, logging of privileged actions is not easily centralized, and audit records are subject to modification by malicious actors.

Privilege Management for Unix and Linux provides a more secure, more effective approach to managing privileges, monitoring user actions, and protecting your organization. In this example of a basic configuration of Privilege Management for Unix & Linux, there are a handful of Linux endpoints on the same network. The BeyondTrust Endpoint Privilege Management client is installed on the endpoints and a policy and logging server is stood up. Next, the BeyondInsight user interface is used to deploy role-based policies to the endpoints and disable unfettered use of root and sudo.

Now the user has limited entitlements. The user may still elevate privileges, but the elevation is subject to policy-based controls and is fully recorded on the protected logging server. Additionally, Privilege Management for Unix and Linux captures a full recording of the user’s session so all input and output that occurred during the privileged session can be viewed. All of this audit data is centrally managed on a protected host, making it practically impossible for malicious actors or software to tamper with the audit data.

"Rather than looking at Privilege Management for Unix/Linux like you’re doing a bunch of draconian policies trying to lock everyone down, think of it more like you’re enabling your users; how quickly can I get that person online, get them [access] to the things that they need to do, and let them fix the system? That’s what we do with Privilege Management for Unix/Linux."

- Chad Erbe, Sr. Staff Engineer, ServiceNow
Privilege Management for Unix and Linux (PMUL) is designed to scale from supporting a handful of endpoints to hundreds of thousands in an enterprise estate. ServiceNow, for example, uses Privilege Management for Unix & Linux to control privileged access, help achieve compliance, and prevent and contain breaches on over 13,000 Unix and Linux endpoints. This example shows how Privilege Management for Unix & Linux can be deployed at an enterprise scale, similar to ServiceNow’s, by splitting functionality onto multiple servers and by adding additional servers for load balancing and redundancy, as well as the solution’s support for cloud environments.

The use of bastion hosts, as shown in the example, is fully supported by the BeyondTrust solution. Since Privilege Management for Unix & Linux can be configured to allow commands to be submitted from one host and run on another, the need for users to log in to protected hosts is eliminated. Both privileged and non-privileged operations can be configured to be launched from bastion hosts.

Supported Platforms

UNIX Systems
- HP-UX 11i v3
- IBM AIX v7.1 TL5, v7.2, v7.3 (POWER 64-bit)
- Oracle Solaris 10 & 11 (SPARC, x86 32-bit, x86 64-bit)

Linux Systems
- Debian GNU/Linux 9.x, 10.x (x86 64-bit)
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS (x86 64-bit)
- Centos 6.x, 7.x, 8.x, 9.x (x86 64-bit)
- Red Hat Ent Linux 6.x*, 7.x*, 8.x*, 9.x* (x86 64-bit)
- Red Hat Ent Linux Workstation 7.x*, 8.x*, 9.x* (x86 64-bit)
- Oracle Linux 6.x**, 7.x**, 8.x**, 9.x** (x86 64-bit)
- SUSE Linux Ent Server 12, 15 (x86 64-bit), Red Hat 6.x, 7.x (PowerPC Big Endian 64-bit)
- Red 7.x, 8.x (PowerPC Little Endian 64-bit), IBM zSeries RHEL v7.x, v8.x (s390x 64-bit)
- ARM64/Gravitron2 – Amazon Linux 2 in AWS, ARM64/Gravitron2 – Red Hat 8 ARM Gravitron2 in AWS

Compliance
Achieve regulatory requirements such as PCI DSS, HIPAA, GDPR, ISO27001, NIST, CIS, SOX, and more

Integrations
Supports REST API architecture to enable task automation and integration with a variety of systems and tools, including SIEM (Splunk, Elastic, and others), ITSM (ServiceNow), Password Management (BeyondTrust Password Safe), and more.
Policies in Privilege Management for Unix & Linux can support complex integrations with ticketing systems, which would allow an organization to gatekeep privileged actions based on the assignment of a ticket to a specific user. All of this audit data is centrally managed on a protected host, making it practically impossible for malicious actors or software to tamper with the audit data.

Privilege Management for Unix & Linux’s powerful script-based policy language allows for complex integrations and business logic to be built into policy, allowing for practically any kind of customization that may be required for determining how to handle an elevation, based on practically any criteria. As an example, a policy could be built to integrate with a ticketing system such as ServiceNow. This would allow an organization to gatekeep privileged actions based on the existence of a ticket assigned to a specific user.

Additional Resources

**DEMO**  Privilege Management for Unix & Linux

**BLOG**  Unix & Linux Server Security: 10 Best Practices

**CASE STUDY**  Investec “Journey to Zero Trust: From Theory to Practice”

BeyondTrust is the worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners.

beyondtrust.com