Achieve least privilege and streamline compliance with Endpoint Privilege Management for Linux

Challenge

Linux servers host essential services, store sensitive data, and power business-critical operations. Yet many organizations lack robust security measures to safeguard these high-value endpoints. As a consequence, Linux users may be granted unrestricted access to root, and what's more, this access may not be monitored and audited effectively.

Linux ransomware attacks increased 62% from 2022 to 2023[1].

External threats only make up one piece of the threat landscape. Insiders can pose just as much risk, whether by abusing their privileges deliberately or inadvertently committing errors that could compromise critical systems or sensitive data.

Without the right solution in place to manage and secure Linux endpoints, organizations struggle to control root access and monitor their Linux users' privileged activity. This lack of visibility makes it difficult to respond to audits to maintain compliance, to qualify for cyber insurance, or to track changes to business-critical endpoints.

- **How can you control root access to achieve least privilege without sacrificing user productivity?**
- **How can you collect privileged event logs and session recordings in a centralized location to streamline compliance?**
- **How can you centrally manage zero trust security controls for your Linux estate?**
- **How can you generate reports to understand your users' entitlements across your Linux estate?**

Many organizations try to use open-source tools like sudo to manage privileged access for their Linux estates. While sudo can offer some degree of privileged access management, it's not remotely adequate for addressing the granular privilege management and audit requirements that modern enterprise Linux deployments demand.

Utilizing sudo to manage root access can be a cumbersome, manually intensive process for IT and security teams, only growing in difficulty as the organization's deployment becomes larger and more complex. 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.

[1]The Linux Threat Landscape Report. Trend Micro. August 2023.

The Solution

BeyondTrust Endpoint Privilege Management for Linux is an enterprise-class privilege elevation and delegation management solution that enables customers to control root access, streamline compliance, enforce least privilege, and centrally manage zero trust security controls – without sacrificing productivity. Purpose-built for Linux, our solution empowers customers to extend capabilities far beyond sudo with centralized event logging, session monitoring and management, as well as child process control. Offered via SaaS, Endpoint Privilege Management for Linux deploys simply and can scale quickly.

Endpoint Privilege Management for 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.

With the largest install base in the market, Endpoint Privilege Management for Linux is the most reliable and trusted privilege management solution available. Today, customers include:

- Some of the largest banks in the world
- Telecommunications giants across the US, South America, Asia, and the Middle East
- Federal, state, and local government agencies
- Hundreds of small and medium-sized organizations

Key Features & Capabilities

Fine-Grained Least Privilege
Control root access and dynamically elevate privileges for standard users through fine-grained, policy-based controls, replacing sudo and eliminating the need for root sessions.

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.

Role-Based Policy Controls
Address your core security gaps quickly with lightweight, easy to implement role-based policies that can be created on a who, what, where, and when basis.

Centralized Management
Centralize the management of your Linux estate, including all user activity data, policies, upgrades, updates, and deployments.

Integrations & Scalability
Integrate with your other systems and tools such as SIEM, Elasticsearch, or BeyondTrust Active Directory Bridge to extend authentication across your hybrid environment.

Benefits

Harden Linux 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.

Streamline Compliance & Cyber Insurance
Ensure compliance with increasingly complex regulations and qualify for cyber insurance by providing an unimpeachable audit trail of all user activity.

Monitor & Track All Privileged Activity
Gain full centralized visibility into all privileged user activity, including full session recordings, so you can achieve and maintain change confidence and improve incident response times.

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

Gartner Critical Capabilities

BeyondTrust ranked the highest in the UNIX/Linux and macOS Privilege Elevation and Delegation Management of the September 2023 Gartner Critical Capabilities for Privileged Access Management report

Read the Report

Use Cases

Manage Privileges and Track Privileged User Activity

In many organizations, Linux users and administrators use 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.

Some organizations rely on access management solutions, such as identity governance and administration (IGA), to restrict access to their Linux servers. While these tools can offer basic functionality for managing access, they prove to be of little value in the event of a breach. Any organization following a defense-in-depth strategy should assume they will get breached at some point. If they're primarily relying only on an access management solution, when an attacker is able to compromise credentials and access their Linux environment, their last line of defense has been broken and the attacker can wreak havoc.

Endpoint Privilege Management for Linux provides a more secure, more effective approach to controlling root access, monitoring privileged user activity, and centrally managing your Linux servers and desktops, all in a simple-to-deploy solution. Below is an example of a SaaS deployment of Endpoint Privilege Management for Linux.

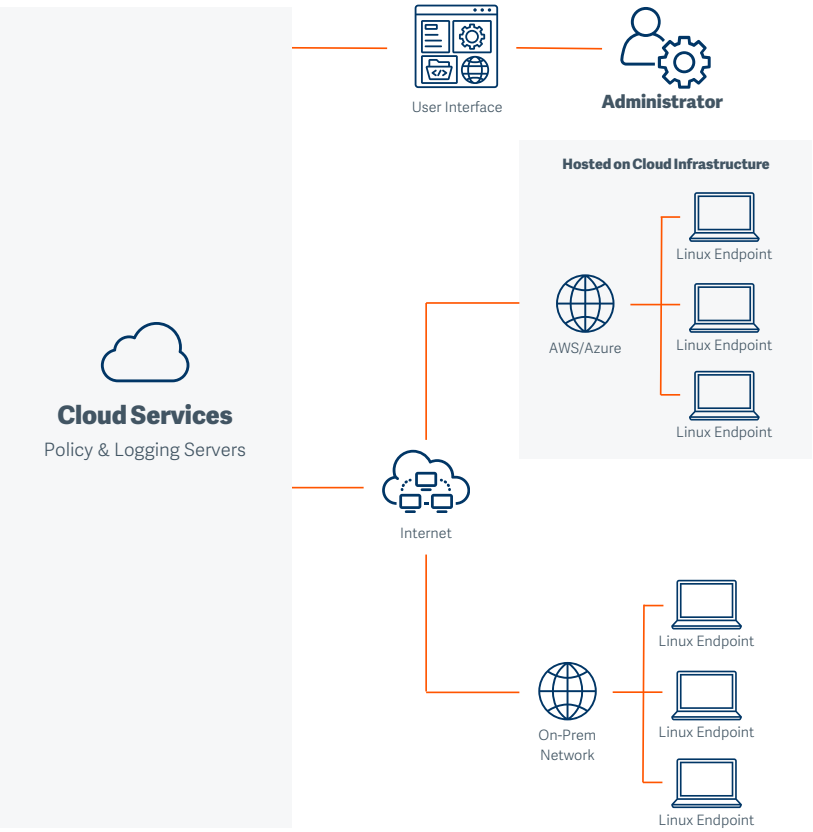

Figure 1. A SaaS-based deployment of Endpoint Privilege Management for Linux. Simply download and deploy endpoint agents to all of your Linux endpoints across environments. Policy management and auditing are performed via the cloud-based management console.

No servers or controllers are required to be installed to deploy Endpoint Privilege Management for Linux, freeing you up from the cost and hassle of managing, maintaining, and updating on-premises software.

Deployment is straightforward: simply download and deploy endpoint agents to all your Linux endpoints across on-premises, hybrid, and cloud environments. Endpoint Privilege Management agents periodically communicate with the cloud-based policy and logging servers to verify privilege elevations against policy and collect audit data and session recordings. Policy management and auditing are performed via the SaaS-based management console.

With Endpoint Privilege Management for Linux deployed, your Linux users will have limited entitlements. They may still elevate privileges, but the elevation is subject to policy-based controls and is fully tracked on the protected logging server.

Additionally, Endpoint Privilege Management for Linux can optionally capture a full recording of the user's session so all input and output that occurred during the privileged session can be viewed. All this audit data is centrally managed, making it practically impossible for malicious actors or software to tamper with the audit data.

Scale to Thousands of Endpoints in an Enterprise Setting
Endpoint Privilege Management for Linux is designed to scale from supporting small to medium-sized organizations with a handful of Linux endpoints, to deployments of thousands of Linux servers and desktops in a complex enterprise estate.

Robust, flexible policy controls are offered in Endpoint Privilege Management for Linux, enabling organizations of all sizes to get up and running quickly. Role-based policies allow organizations to quickly deploy foundational security measures on a who, what, where, and when basis that address core security gaps.

Specifications

Helps Ensure Adherence To

Regulatory requirements such as PCI DSS, HIPAA, GDPR, ISO27000, NIST CSF, CIS, SOX, and more.

Integrations

Supports integration with a variety of systems and tools, including SIEM (Splunk, Elasticsearch, and others), ITSM (ServiceNow), Password Management (BeyondTrust Password Safe), Identity Management and Access Control (BeyondTrust Active Directory Bridge), and more.

Cloud Security

Hosted in Amazon Web Services (AWS). All data centers used to support BeyondTrust's cloud environment have achieved certifications such as ISO/IEC 27001, ISO/IEC 27018, and have completed rigorous audits such as SOC 2 Type II and others.

Technical Documentation

Refer to our technical documentation for a detailed view of all technical aspects of Endpoint Privilege Management for Linux

Hear from Our Customers

"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

"When you're managing privilege at the server and application level, you're dealing with too many points of administration. BeyondTrust's Endpoint Privilege Management for Linux integrates with Active Directory to create a single touchpoint for managing privilege and access permissions. Instead of having hundreds of administrators dealing with segments of your network, or even with individual machines, you have a few people doing everything consistently across the enterprise."

-- Jeff Lundberg, Principle Consultant,
Fortune 100 Financial Services Company

"With Endpoint Privilege Management for Linux, we have better user engagement/experience for our customers, along with better security. After setting up roles for all the different user types, adding new users is easy."

-- Holger Bürger, Director of Site Operations,
XING

Aditional Resources

Gartner Magic Quadrant for Privileged Access Management
Cyber Insurance Checklist
Buyer's Guide for Complete Privileged Access Management (PAM)
A Guide to Endpoint Privilege Management
Investec's Journey to Zero Trust: from Theory to Practice
ServiceNow: Improving Security Posture for System Access and Authorization

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. Learn more at **www.beyondtrust.com**.