BeyondTrust

Control Root Privileges & Streamline Compliance with Endpoint Privilege Management for Linux

Linux servers are high-value targets because privileged access often provides direct control over critical infrastructure, cloud workloads, and sensitive data.

Traditional Linux administration often relies on shared root access, sudo, and standing privileges. While sudo provides basic command delegation, it can leave organizations with broad access, limited policy granularity, and insufficient visibility into privileged activity—creating excessive risk that attackers, ransomware, and compromised workloads can exploit.

BeyondTrust Endpoint Privilege Management for Linux (EPM-L) enables organizations to remove standing root privileges, enforce least privilege, and elevate only approved commands and processes—helping administrators remain productive without granting unrestricted root access.

The solution combines granular privilege management, command control, and comprehensive auditing to strengthen Linux security, streamline compliance, and improve visibility into privileged activity across on-premises, private cloud, and public cloud environments.

CUSTOMER SUCCESS

ServiceNow

"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 Security Engineer

- **Privilege Hardening**
  Enforce least privilege across Linux servers by removing standing root-level privileges and limiting elevation to approved commands, applications, and processes. Reduce the risk of unauthorized access, privilege escalation, and lateral movement, while maintaining administrator productivity.
- **Prevent Misconfigurations**
  Control the execution of privileged commands and processes to reduce the risk of unauthorized changes, privilege escalation, and server misconfigurations. Constrain risky scripts, interpreters, and child processes commonly abused in ransomware and fileless attacks.
- **Comprehensive Auditing**
  Gain centralized visibility into privileged activity through detailed logs, session monitoring, and audit trails across Linux environments. Accelerate incident investigation, support forensic analysis, and streamline compliance reporting with full accountability for privileged actions.
- **Unified Management**
  Centrally manage and enforce privilege policies across Linux servers, cloud workloads, and hybrid infrastructure from a unified console. Maintain consistent security controls, while simplifying administration and reducing operational complexity at scale.