BeyondTrust

PRIVILEGE MANAGEMENT FOR UNIX & LINUX

PROTECT PRIVILEGED ACCOUNTS AND ACHIEVE COMPLIANCE

Limit Root Access

Provide fine-grained privilege elevation rules to execute only specific tasks or commands.

Audit All User Activity

Protect against unauthorized changes to files, scripts, and directories.

Monitor Logs & Sessions

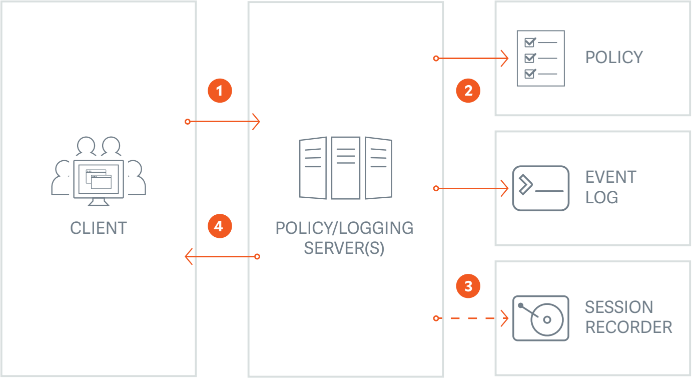
Detect suspicious user, account, and asset activity in real-time.

BeyondTrust Privilege Management for Unix & Linux is an enterprise-class, gold-standard privilege management solution that gives you unmatched visibility and control over complex server environments.

Features and Capabilities

- **Auditing & Governance:** Analyze user behavior by collecting, securely storing, and indexing keystroke logs, session recordings, and other privileged events.
- **Fine-Grained Least Privilege:** Elevate privileges for standard users on Unix and Linux through fine-grained, policy-based controls.
- **Dynamic Access Policy:** Utilize factors such as time, day, location, and application/asset vulnerability status to make 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.
- **File & Policy Integrity Monitoring:** Audit and report on changes to critical policy, system, application, and data files.
- **Privileged Threat Analytics:** Correlate user behavior against asset vulnerability data and security intelligence from best-of-breed security solutions.

HOW IT WORKS



1. User requests are sent to the policy servers
2. Requests are checked against central policy
3. Request is written to central event log, with optional session recording
4. Policy decision is sent back to the user

Supported Platforms

BeyondTrust Privilege Management for Unix & Linux supports more than 100 platforms, including Debian GNU, HP-UX, HP Tru 64, Red Hat Enterprise Linux, Sun Solaris, SuSE Linux Enterprise, VMware ESX, IBM AIX, and others.

> "The Privilege Management for Unix and Linux implementation was very successful. All server access is limited – even via SSH. The auditors can easily see that procedures are being followed, and our IT employees are able to remain productive."
>
> **SVP SYSTEMS / RECOVERY, CTO, DCI**

BUSINESS BENEFITS

Ensure Compliance

- Provide an unimpeachable audit trail of all user activity.
- Enable compliance through the compartmentalization of IT tasks that require privileged accounts.
- Ensure that critical files and policies have not been tampered with.

Secure Critical Systems and Files

- Limit attack surfaces by providing just enough access to complete a task.
- Prevent the use of the root account.
- Enable only approved applications/commands to be executed.
- Eliminate workarounds or gaps that could lead to exploits.
- Make privilege decisions based on context and risk.
- Protect critical files from malware and misuse.

Improve Efficiency

- Streamline processes that are complex with sudo.
- Simplify management and speed deployments with a central management console.

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing privilege-related breaches. Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. We are trusted by 20,000 customers.

beyondtrust.com