Centralized Linux and Unix Access Management for on Premises and Cloud Environments

Powertech Identity & Access Manager (BoKS) transforms your multi-vendor Linux and UNIX server environment into one centrally managed security domain. It simplifies your organization's ability to enforce security policies, and control access to critical systems and information. With full control over accounts, access and privilege, IT and security teams can proactively prevent internal and external critical system attacks before they start.

Key Benefits

- Centralize user and group provisioning with management to save time and increase operational efficiency
- Centrally manage access control for over-the-network services such as SSH, telnet and ftp (only configured access is allowed)
- Single Sign-On, and strong authentication with public key technology and two-factor devices such as tokens
- Enforce a common password policy across the domain on diverse platforms
- Audit all network login, access and administration to meet auditor requirements
- Secure, encrypted access with SSH and telnet, enforceable for specified hosts and users
- Direct keystroke logging of user sessions for sensitive operations
- Non kernel-intrusive PAM-based solution, easy to deploy, does not impede kernel patching

Enhanced and Efficient Account Administration

Identity & Access Manager enables organizations to centralize the administration of users, improve the controls over how users are granted access to system resources, as well as enhance the auditability of Linux and UNIX servers.
By eliminating manual processes and inefficiencies, organizations can significantly improve administrator productivity while providing a more secure computing environment.

- Within minutes, centrally create, modify, and/or remove users and groups across server environment
- User password and group synchronization are pushed automatically
- Integration with external Directories - LDAPS/LDAP based
- Bridging with Microsoft Active Directory - making User and Host Groups visible in AD, reducing operational costs
- Integration with external Identity/ Role and Federation services as sources of identity using Web Services

**Granular Access, and Privileged Access Management**

IT security teams are challenged with protecting sensitive data, and enabling users across the organization to maintain productivity. You can bridge that gap between IT security and user enablement with Identity & Access Manager’s granular privileged access management solution. As a result, your organization will become more secure, meet (and simplify) compliance, and increase overall operational efficiency.

- Define and enforce who is granted elevated privilege, when, from where, and how
- Control which commands can be executed by privileged users, (“SUDO”) and audit privileged activity
- Granular assignment of who can switch sessions (“SU”)
- Assign groups of commands instead of giving open root access to all commands
- Define with policy which SUDO sessions are keystroke logged, based on risk and user
- Remove the need for distribution of sudoers files with configuration management solutions or scripts

**Increase Security, Simplify Compliance, and Become More Efficient**

**Security**

- Centralized management of accounts, access, and privilege to better control entire security landscape
- Defaults to least privilege to protect systems from the start
- Granular access control over who, when, where, and how someone can access systems
- Support for 3rd party 2-factor authentication
- Integration with sources of identity (LDAPS, Active Directory)
- Break-glass critical account access

**Compliance**

- Recording of all input and output of command ran on a Linux/UNIX system including raw input (including anything not actually shown on a screen)
- Supports access/authorization control regulations (HIPPA, PCI DSS, SOX, GLBA, FISMA, BASEL III, European Data Protection Directives)
- Provides Role-based Access Control (RBAC)
- Audit trail of ALL user sessions, and automated reporting

**Efficiency**

- Centralizes administration tasks for increased efficiency, and reduction in overhead costs
- Automates reporting for audit and compliance
- Reduce impact (50%) of exposure to reported CVEs for OpenSSH
- Deploys rapidly, is reliable, and scales easily with growing enterprise

**Get Started with Identity & Access Manager**

To learn more or request a demo, please visit [www.helpsystems.com/cta/request-live-demonstration-identity-access-manager](http://www.helpsystems.com/cta/request-live-demonstration-identity-access-manager)

---

**About HelpSystems**

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.