FORTRA

DATASHEET (Compliance and Audit Reporting)

Core Privileged Access Manager (BoKS)

Critical Systems and Data Access Management Software for Linux and UNIX

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

Core Privileged Access Manager (BoKS) transforms your multi-vendor Linux and UNIX server environment into one centrally managed security domain. BoKS simplifies your ability to enforce security policies and features a simple configuration framework for streamlined, robust administration. Easily control access to critical systems and information with straightforward deployment. Ensure full control over accounts, access, and privilege, so your IT and security teams can prevent internal and external attacks on critical systems 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)
- Deploy quickly with native packages for all server agent platforms and master & replica platforms
- Enhance security with support for sudo and sudoedit, and automated renewal for node keys
- Leverage Single Sign-On and strong authentication with public key technology and two-factor devices
- 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 kernal-intrusive PAM-based solution, easy to deploy, does not impede kernal patching
- Enhance failover performance with intelligent downloading of database tables

INCREASE SECURITY

Centralize privileged security for better control and visibility -- while ensuring regulatory compliance.

DRIVE EFFICIENCY

Automate IT Administration and processes to optimize current staff, and reduce cost of business operations.

ACCELERATE GROWTH

Securely scale your hybrid environment 10x faster, with less impact on IT operations processes and applications.

Enhanced and Efficient Account Administration

Core Privileged 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 Core Privileged 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 Core Privileged Access Manager

To learn more or request a demo, please visit www.coresecurity.com/products/core-privileged-access-managerboks/demo

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.