BoKS ®ServerControl

Critical Systems and data Access Management Software for Linux and UNIX

foxtechnologies.

CENTRALIZED LINUX AND UNIX ACCESS MANAGEMENT FOR ON-PREM AND CLOUD ENVIRONMENTS

BoKS® ServerControl 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 kernal-intrusive PAM-based solution, easy to deploy, does not impede kernal patching

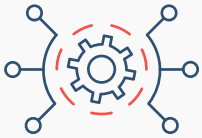
ENHANCED AND EFFICIENT ACCOUNT ADMINISTRATION

BoKS® ServerControl 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

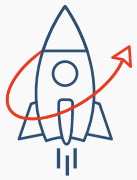
INCREASE SECURITY

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



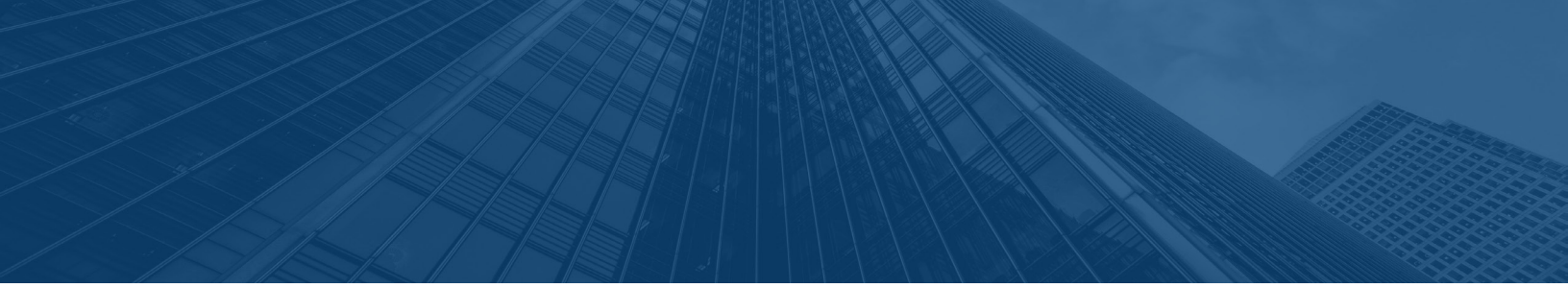
DRIVE EFFICIENCY

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.



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 BoKS® ServerControl'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

ABOUT FOXT

Fox Technologies is a global security company that helps organizations centralize Linux and UNIX access management across hybrid IT environments. Enterprises world-wide rely on FoxT to enforce granular security controls, simplify compliance, and increase over-all IT department efficiencies. Proactively prevent internal and external critical system attacks before they start by empowering IT and security teams with control over security. Fox Technologies has been a leader in the data security industry for over 30 years. We are trusted by some of the world's top fortune 500 companies, and protect over 20 trillion dollars in assets.

To learn more about Fox Technologies, please visit us at:
www.foxt.com

CONTACT INFO

North America
3300 Eagle Run Drive NE, Suite 202
Grand Rapids, MI 49525
+1 877 818 3698 (Toll Free)

Sweden
FoxT Sweden AB
Kungsängsgatan 18A
SE-753 22, Uppsala
+46 18 16 00 00 (Main)

United Kingdom
400 Thames Valley Park
Reading , Berkshire RG6 1PT
+44 1189 637 681 (Main)

www.foxt.com | info@foxt.com

foxtechnologies.