

INDUSTRY SOLUTIONS

# OIL + GAS

Premiere Identity and Access Management Software for Linux and UNIX Servers

## TAKE CONTROL OF IDENTITY AND ACCESS MANAGEMENT

BoKS<sup>®</sup> ServerControl is a comprehensive, all-in-one product that provides multiple IAM solutions for your Linux and UNIX environment.

- ▶ Account Provisioning
- ▶ Group Management
- ▶ Granular Access Control
- ▶ Active Directory Bridging
- ▶ Web Services Interface
- ▶ Centralized Sudo Control
- ▶ Switch User Control
- ▶ Compliance Reporting
- ▶ Keystroke Logging
- ▶ Pluggable Authentication
- ▶ Password Management
- ▶ SSH Client for Windows

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

FoxT BoKS<sup>®</sup> 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.

## DESIGNED FOR OIL AND GAS ORGANIZATIONS

### User & Group Administration

BoKS<sup>®</sup> 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 by 40% while providing a more secure computing environment.

### Centralized User, User Role, Host and Host Role Access Management

Oil and Gas infrastructures can be widely spread geographically, requiring secure access with centralized policies, and delegated mitigated local administration linked to your Risk Register. BoKS<sup>®</sup> ServerControl utilizes a highly efficient matrix-style access management model. This proven design scales to tens of thousands of hosts, and hundreds of thousands of user accounts. Based on customer experiences, you can grow your infrastructure by 100% without additional operations staff.

### Privileged Access Management

Linux and UNIX based operating systems have critical operational vulnerabilities. Their simplistic security model allows you to transition (Assume Privilege) by changing sessions to another more privileged account (like "root" or "oracle", or execute commands) as that more privileged account without changing sessions. With widely spread server infrastructures, the risks of inconsistency in access management are removed by using BoKS<sup>®</sup> ServerControl.

### Technical Innovation and Long Term Platform Support

Upstream infrastructures may often be in place for 10-20 years of operation before replacement, including control servers and software stacks. Having been in this market for thirty years, we have deep experience protecting critical infrastructures maintained under custom support arrangements. Please ask for further information on how we can tailor for your specific requirements.



## SOLVE YOUR KEY SECURITY ISSUES WITH BOKS

### M&A activity in Upstream exploration and production sector

At well over USD 300 billion annually in M&A activity getting control of acquisition assets is a challenge. BoKS® ServerControl allows you to apply common security policies immediately over separate infrastructure domains, with separate sources of identity until consolidation can occur.

### Shared Ownership in diverse geographies

Joint ownership, often with regional or national government development agencies is common. Applying common security policies consistently over multi-national boundaries can be both an operational and regulatory nightmare. BoKS® ServerControl's multi-dimensional Host and User Role grouping model allows you to share as broadly as possible common Roles, and also be as specific and granular to meet local HR and joint-ownership conditions.

### Fraud Control

BoKS® ServerControl's multi-dimensional Role model prevents local administrators' from "walking around" your infrastructure, both at local exploration and production sites, and the wider corporate assets. When disconnected from the corporate network, local servers operate under a restricted local policy set, as mandated by your risk profile definitions, not the whim of local system administrators

## ABOUT FOXT

Fox Technologies is a global security company that helps organizations centralize Linux and UNIX identity and 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](http://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](http://www.foxt.com) | [info@foxt.com](mailto:info@foxt.com)

