QUEST SOFTWARE

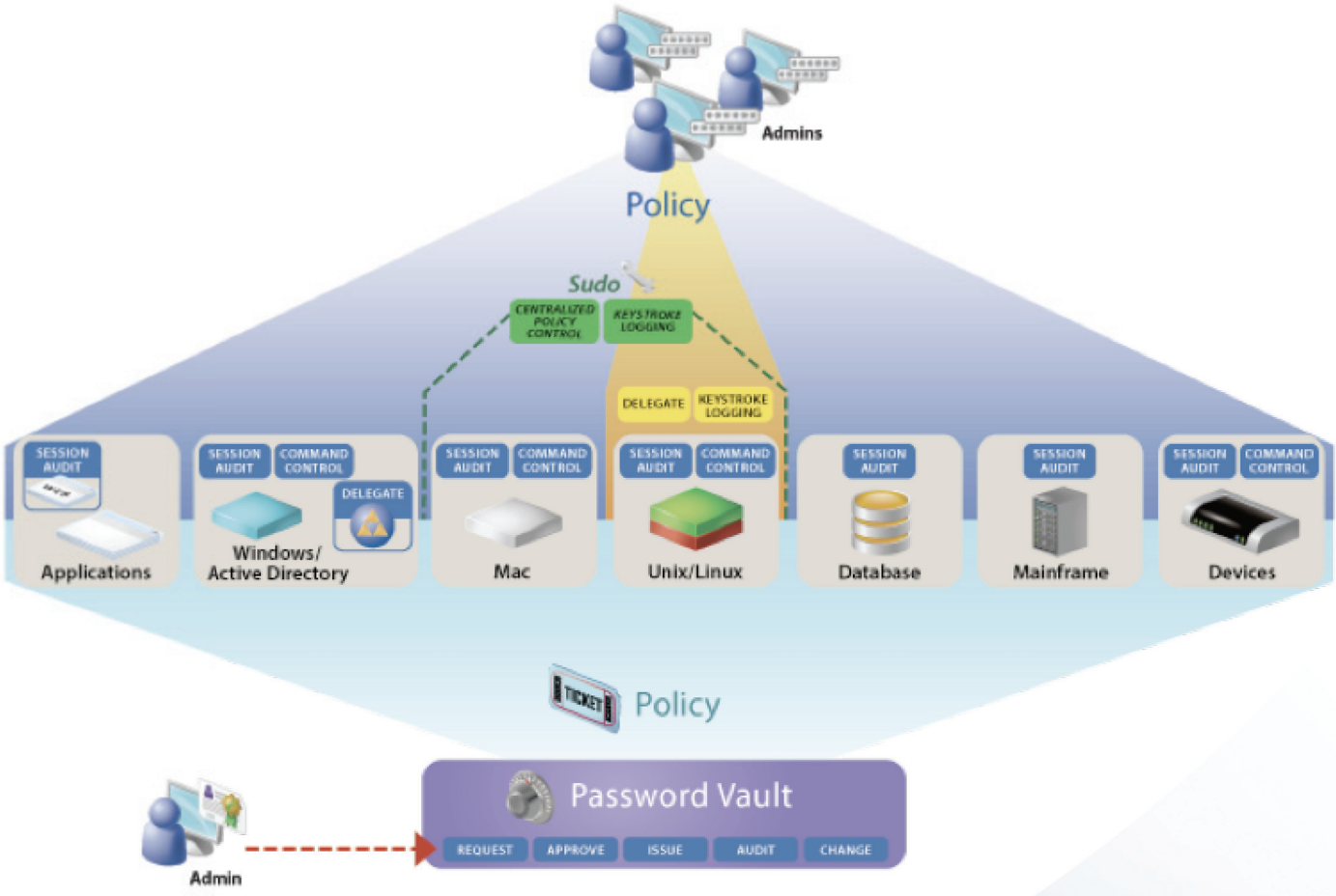
PRODUCT SUITE BROCHURE

Quest® One Identity Solution

Privileged Account Management

Eliminating the "Keys to the Kingdom" Problem

The Quest One Identity Solution empowers you to control administrative access enterprise-wide. Quest One solutions for privileged account management improve efficiency while enhancing security and compliance: administrators are granted only the rights they need—nothing more, nothing less—and all activity is tracked and audited. Specifically, Quest One solutions include granular, policy-based delegation for superuser credentials; command control; session audit and replay; keystroke logging; and secure and automated workflows for issuing privileged credentials to administrators and in application-to-application and application-to-database scenarios.



The Quest One Identity Solution enables you to secure, delegate, control, and audit access for superuser accounts and shared administrative credentials—across a variety of platforms and systems.

The Quest One suite of privileged account management solutions includes both network-based and host-based solutions:

Network-based solutions: These powerful solutions provide "password vault" functionality, session audit and replay, and command control from a single, secure, hardened appliance that maximizes economy, ease of deployment, and system coverage.

Quest® One Privileged Password Management

Privileged Password Management provides secure storage, release control, and change control for privileged passwords for individual accountability across highly diverse deployments of systems, devices, and applications. Privileged Password Management ensures that when administrators require elevated access (typically through shared credentials such as the Unix root or Windows Administrator account), it is granted according to established policy, with appropriate approvals, that all actions are fully audited and tracked, and that the password is changed immediately upon its return. It's a secure, compliant, and efficient solution to the age-old "keys to the kingdom" problem.

Quest® One Privileged Session Management

Privileged Session Management provides session control, proxy, audit, recording, and replay of high-risk users such as administrators and remote vendors. It provides a single point of control from which you can authorize connections, limit access to specific resources, view active connections, record all activity, alert if connections exceed pre-set time limits, and terminate connections.

Quest® One Privileged Command Management

Privileged Command Management provides command control for daily administrative tasks that require elevated credentials. Privileged Command Management provides control over access to specific programs, granularly delegated tasks, and specific commands. It is ideal for those Unix-based or Windows systems that require advanced security beyond native capabilities and would benefit from a network-based proxy model of command control.

Quest® One Application Password Management

Application Password Management replaces hard-coded passwords with programmatic calls that dynamically retrieve the account credential—eliminating this often overlooked exposure. It completes the Quest One suite of network-based tools running from the same appliance by securing application-to-application and application-to-database access.

Host-based solutions: These powerful solutions deliver maximum security and control through agents deployed on target systems. For those systems with the heaviest compliance burden, Quest One's host-based options provide the depth, granularity, and "forensics-ready" visibility your auditors require.

Quest® Privilege Manager *for Unix*

Privilege Manager for Unix protects the full power of root access from potential misuse or abuse. Privilege Manager helps you to define a security policy that stipulates who has access to which root functions, as well as when and where individuals can perform those functions. It controls access to existing programs as well as any purpose-built utilities used for common system administration tasks. In addition, Privilege Manager provides comprehensive auditing of all activities performed through the solution, down to the keystroke level.

Quest™ Authentication Services

Authentication Services is the pioneer in the now ubiquitous "Active Directory bridge" space. It enhances Privilege Manager for Unix by unifying Unix/Linux identities into AD, enabling you to use a common management interface and policy set to control delegation of the Unix root account.

Quest® ActiveRoles® Server

ActiveRoles Server is the most popular and most powerful Active Directory security and management solution on the market today. It provides granular delegation of the Active Directory Administrator account and central control of administrative access using a single, well-defined set of roles, rules, and policy.

About Quest Software, Inc.

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest solutions for application management, database management, Windows management, virtualization management and IT management, go to **www.quest.com**.

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | EMAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.