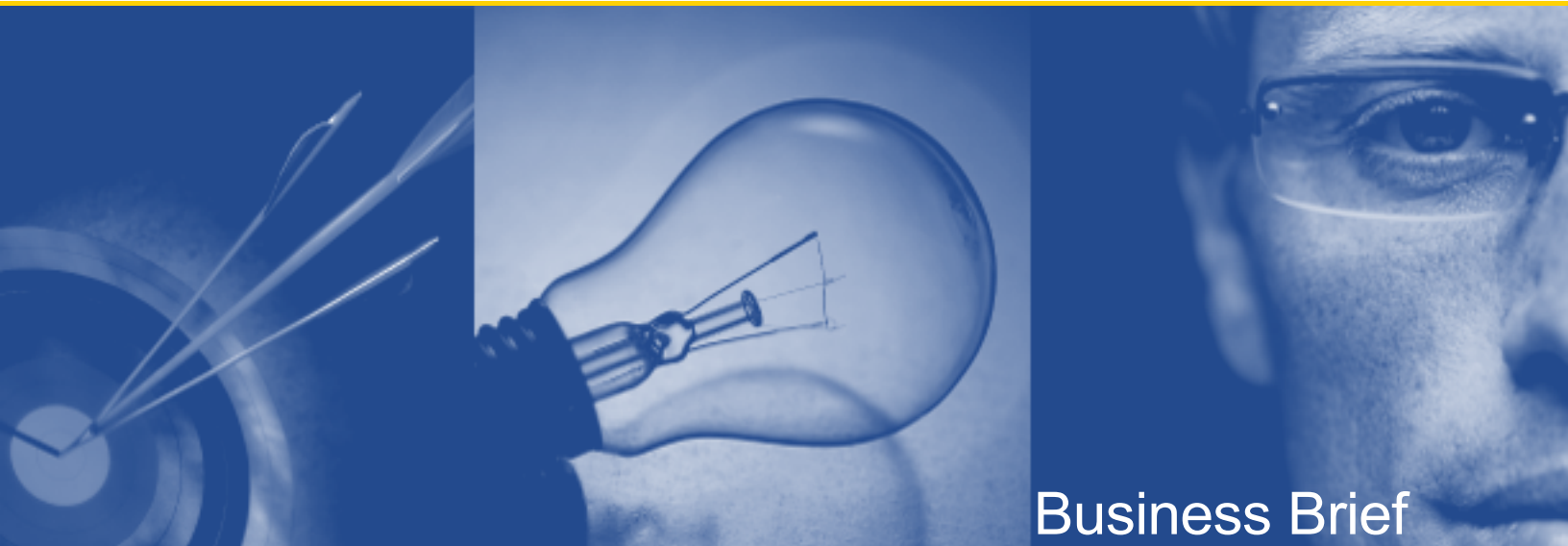


Protecting Your IT Systems from Attack

How Quest Can Help You Comply with FISMA

*Written by
Quest Software, Inc.*



Business Brief

**© 2009 Quest Software, Inc.
ALL RIGHTS RESERVED.**

This document contains proprietary information, protected by copyright. No part of this document may be reproduced or transmitted for any purpose other than the reader's personal use without the written permission of Quest Software, Inc.

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters:
5 Polaris Way
Aliso Viejo, CA 92656
e-mail: info@quest.com

Please refer to our Web site (www.quest.com) for regional and international office information.

Updated—May 2009

CONTENTS

- INTRODUCTION 1**
- CRITICAL CONTROLS THAT PROTECT YOUR SYSTEMS FROM ATTACK,
AND HOW QUEST CAN HELP 1**
- CRITICAL CONTROL 2: INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE;
ENFORCEMENT OF WHITE LISTS OF AUTHORIZED SOFTWARE 1
 - Quest Solutions: QMX for Configuration Manager, Policy Authority for UC,
InTrust, Reporter, SecurityManager and Storage Horizon 2*
- CRITICAL CONTROL 3: SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE
ON LAPTOPS, WORKSTATIONS, AND SERVERS 2
 - Quest Solutions: Desktop Authority, vWorkspace and SecurityManager 3*
- CRITICAL CONTROL 5: BOUNDARY DEFENSE 3
 - Quest Solution: Policy Authority for UC and Defender 3*
- CRITICAL CONTROL 6: MAINTENANCE, MONITORING, AND ANALYSIS
OF COMPLETE AUDIT LOGS 4
 - Quest Solutions: InTrust, ChangeAuditor for Active Directory,
ChangeAuditor for Exchange and ChangeAuditor for File Systems 4*
- CRITICAL CONTROL 8: CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES 5
 - Quest Solutions: ActiveRoles Server, Privilege Manager for Unix,
InTrust, Quest Defender and SecurityManager 5*
- CRITICAL CONTROL 9: CONTROLLED ACCESS BASED ON "NEED TO KNOW" 6
 - Quest Solutions: Authentication Services, ActiveRoles Server,
Access Manager, Privilege Manager for Unix, and Policy Authority for UC 6*
- CRITICAL CONTROL 11: DORMANT ACCOUNT MONITORING AND CONTROL 7
 - Quest Solutions: ActiveRoles Server, Authentication Services, Reporter,
and MessageStats, Access Manager, InTrust, InTrust Plug-In for Active
Directory, InTrust Plug-In for Exchange, InTrust Plug-In for File Access 7*
- CRITICAL CONTROL 13: LIMITATION AND CONTROL OF PORTS, PROTOCOLS, AND SERVICES ... 8
 - Quest Solutions: SecurityManager 8*
- CRITICAL CONTROL 15: DATA LEAKAGE PROTECTION 8
 - Quest Solutions: InTrust, InTrust Plug-In for File Access, Archive Manager,
Policy Authority for UC and Storage Horizon 8*
- CRITICAL CONTROL 18: INCIDENT RESPONSE CAPABILITY 9
 - Quest Solution: InTrust 9*
- CRITICAL CONTROL 19: DATA RECOVERY CAPABILITY 9
 - Quest Solutions: Recovery Manager for AD, Recovery Manager for
Exchange, Recovery Manager for SharePoint, LiteSpeed, SharePlex,
Policy Authority for UC, vReplicator, and vRanger Pro 10*
- SUMMARY 11**
- ABOUT QUEST SOFTWARE, INC. 13**
- CONTACTING QUEST SOFTWARE 13
- CONTACTING QUEST SUPPORT 13

INTRODUCTION

The Federal Information Security Management Act (FISMA) requires federal agencies to protect their information infrastructures against vulnerabilities and attacks and implement automated monitoring of their information security measures and controls.

To help agencies comply with FISMA, a team of cyber-security experts from Defense, Energy, Homeland Security's US-CERT, GAO, Transportation, HHS, and other organizations have published the [Consensus Audit Guidelines](#), which identifies 20 security controls that are important for blocking attacks. This document explains how Quest Software can help you meet the requirements of 11 of these controls.

CRITICAL CONTROLS THAT PROTECT YOUR SYSTEMS FROM ATTACK, AND HOW QUEST CAN HELP

Critical Control 2: Inventory of authorized and unauthorized software; enforcement of white lists of authorized software

Creating and enforcing a white list of authorized applications makes a system less vulnerable to attack in several ways. First, having a white list ensures that a system runs only the software needed for business purposes. This prevents the introduction of security flaws from extraneous applications.

A system with a white list of authorized applications also makes it more difficult for attackers to run their own unauthorized software. Preventing this infiltration is critical, because once a single machine is exploited, the attacker can collect sensitive information from the compromised location and all systems connected to it. It can even use the compromised machine as a launching point for movement throughout the network and any partners; one compromised machine can turn into many.

Finally, creating an inventory of authorized and unauthorized applications makes it easier to detect attacks. Organizations that do not have complete software inventories of their systems may not be able to detect that they have been compromised.

Quest Solutions: QMX for Configuration Manager, Policy Authority for UC, InTrust, Reporter, SecurityManager and Storage Horizon

Microsoft System Center Configuration Manager 2007 (SCCM) is a powerful solution for managing software inventory and white lists on Windows systems. [Quest Management Xtensions—Configuration Manager 2007 Edition \(QMX for Configuration Manager\)](#) extends SCCM to Unix, Linux, Mac OS X, and VMware ESX systems, enabling organizations to efficiently inventory and control application use across the enterprise. All Unix, Linux, VMware, and Mac OS X system software packages appear automatically in Add/Remove Programs and software inventory includes file collection, file details, and product detail collections. Advanced options capture additional data.

[Policy Authority for Unified Communications \(UC\)](#) controls access to instant messaging (IM) and other real-time communications. Policy Authority provides some of the most advanced peer-to-peer (P2P) controls available on the market—far more sophisticated than most firewalls—that can block Skype, FastTrack (used by Kazaa), BitTorrent, OpenNapster, IRC, Gnutella, and other P2P protocols.

[InTrust](#) tracks software installations through events in the Windows event log.

[Reporter](#) provides a quick list of installed software and can create exception reports.

[SecurityManager](#) allows administrators to specify which Active Directory (AD), Exchange, and member services must run or cannot run on monitored platforms, and provides active and passive remediation for policy violations.

[Storage Horizon](#) maintains system availability by helping storage administrators map and inventory which department has deployed what amount of data storage, what type, who is using it, and alerts administrators if storage limits are at a critical level endangering application functionality.

Critical Control 3: Secure configurations for hardware and software on laptops, workstations, and servers

Automated computer attack programs constantly search for systems with default configurations that are vulnerable to exploitation. The proper way to defend against these attacks is to install and regularly update computer and network components with secure configurations.

Quest Solutions: Desktop Authority, vWorkspace and SecurityManager

ScriptLogic [Desktop Authority](#) centralizes control over the desktop, providing all of the functionality usually achieved with a combination of logon scripting, group policies, user profiles, and security solutions. Desktop Authority 7.8 is certified as compliant with the Federal Desktop Core Configuration (FDCC) standard, and provides tools to help enforce FDCC compliance. Desktop Authority allows agencies to use a single set of policies in their network, without disrupting critical processes, by enabling administrators to open exceptions for users or computers that require mission-critical but non-compliant applications. This dynamic exception management is outlined in a free whitepaper, "[Effective Desktop Management Under the Federal Desktop Core Configuration Standard](#)."

[vWorkspace](#) ensures centralized configuration management for virtualized desktops. vWorkspace automates time-consuming configuration tasks; for example, it can dynamically create desktop and Start menu program shortcuts, configure background and color settings, connect to shared network folders and printers, execute scripts, configure user registry settings and environment variables, and lock down the user's workspace using standard Explorer shell policies.

[SecurityManager](#) allows administrators to specify which AD, Exchange, and member services must run or cannot run on monitored platforms, and provides active and passive remediation for policy violations.

Critical Control 5: Boundary defense

Internet-facing systems and extranets are ripe for attack, and organizations must take special measures to defend these boundaries. Strategies include: requiring all internet and extranet traffic to pass through managed, authenticated proxies; employing a DMZ that is separated from internal systems either physically or through tightly monitored filtering; deploying securely configured firewalls and intrusion detection systems at each gateway and requiring all remote access to use two-factor authentication.

Quest Solution: Policy Authority for UC and Defender

[Policy Authority for Unified Communications](#) provides security for instant messaging (IM) and other real-time communications. It also protects systems against known and zero-day virus infections using automatically-updated filters and heuristic analysis, including bot-defeating technology, through integration with Sophos and Symantec.

[Quest Defender](#) enhances security by enabling two-factor authentication to network, web, and applications-based resources. It bases administration and identity management on an organization's existing investment in Active Directory, eliminating the costs and time required to set up and maintain proprietary databases. Defender works with any OATH-compliant hardware token, allowing organizations to select the most appropriate token for their users.

Critical Control 6: Maintenance, monitoring, and analysis of complete audit logs

Some organizations maintain audit logs purely for compliance purposes, and do not regularly examine them carefully. Attackers may control their systems for months or years without being detected, even though evidence of the attack has been recorded in the unexamined log files.

Maintaining and analyzing complete audit logs is critical to detecting and preventing successful and unsuccessful attack attempts. Audit logs also track all activity after a successful attack, enabling organizations to take appropriate steps to control the damage.

Quest Solutions: InTrust, ChangeAuditor for Active Directory, ChangeAuditor for Exchange and ChangeAuditor for File Systems

[InTrust](#) delivers real-time alerting and granular auditing across heterogeneous networks, including Windows, Unix, and Linux systems. It automatically audits access to critical systems and immediately provides alerts to inappropriate or suspicious access-related events. With InTrust, a cached location can be created on each remote server for real-time log duplication. This prevents a rogue user or administrator from tampering with the audit log evidence.

[InTrust Plug-In for Active Directory](#)

[InTrust Plug-In for Exchange](#)

[InTrust Plug-In for File Access](#) These solutions provide object-level alerts and auditing to ensure sensitive groups and objects cannot be changed when unauthorized individuals are mistakenly or maliciously added.

[ChangeAuditor for Active Directory](#)

[ChangeAuditor for Exchange](#)

[ChangeAuditor for File Systems](#) These solutions support real-time granular auditing for Active Directory, Exchange and file systems. It immediately provides alerts to critical configuration changes, including changes to Group Policy Objects, DNS, server configurations, and nested groups. A secure audit trail records who made each change; when, where and why the change was made; and the original and current configuration values for fast troubleshooting. ChangeAuditor can also automatically generate in-depth forensics for auditors and management.

Critical Control 8: Controlled use of administrative privileges

Properly controlling administrative privileges greatly reduces the risk of unauthorized access. The first step is to limit the use of administrative privileges on end-user workstations. If a workstation user with administrative privileges opens a malicious e-mail attachment or a file from a malicious web site, the attacker can take over the victim's machine and install keystroke loggers, sniffers, and remote control software to find administrator passwords and other sensitive data.

Attackers may also gain access to a server through a vulnerable service or guessed password. If administrative privileges are loosely and widely distributed, the attacker may find many accounts that lead to full control of the server.

Organizations can take a variety of steps to control administrative privileges. They need to ensure that administrative passwords are strong, and access requires two-factor authentication. Use of administrative access should be monitored and limited to system administration activities. Password re-use should be controlled. Advanced organizations should segregate administrative accounts using role-based policy.

Quest Solutions: ActiveRoles Server, Privilege Manager for Unix, InTrust, Quest Defender and SecurityManager

[ActiveRoles Server](#) provides complete, practical user and group lifecycle management for the Windows enterprise. It enhances the security controls inherent in Active Directory by automating the provisioning process and providing role-based administrative privileges. ActiveRoles Server provides easy-to-use web interfaces for self-service, making strong passwords more feasible.

[Privilege Manager for Unix](#) helps organizations enhance security through fine-grained, policy-based delegation and auditing for Unix administrated privileges. In addition, Privilege Manager audits all activity, tests security policies and provides graphical analysis of system activity while highlighting anomalies. This enables organizations to improve efficiency, enhance security and achieving and sustaining their compliance objectives, ultimately resulting in reduced organizational costs.

[InTrust](#) sends an automatic alert if an administrative account performs an inappropriate interactive login.

[Quest Defender](#) enhances security by enabling two-factor authentication to network, web, and applications-based resources. It bases administration and identity management on an organization's existing investment in Active Directory, eliminating the costs and time required to set up and maintain proprietary databases. Defender works with any OATH-compliant hardware token, allowing organizations to select the most appropriate token for their users.

[SecurityManager](#) assists with both security policies and AD monitoring rules.

Critical Control 9: Controlled access based on “need to know”

By limiting the access of individual users to what each needs to know, an organization limits the amount of critical data can be accessed if the account is compromised by an attack.

Quest Solutions: Authentication Services, ActiveRoles Server, Access Manager, Privilege Manager for Unix, and Policy Authority for UC

[Authentication Services](#) extends the native access control capabilities of Active Directory to Unix, Linux, and Mac platforms and enterprise applications. By unifying identities and directories and providing true single sign-on, Authentication Services enables organizations to control the access rights of each user.

[ActiveRoles Server](#) provides complete, practical user and group lifecycle management, including temporary access control based on a user’s roles within the organization.

[Access Manager](#) provides a single console that enables administrators to identify and control user and group access to resources such as files, folders, and shares throughout the enterprise. This strict control and granular visibility enables organizations to easily understand and manage each user's access rights across the network, enforce business policies, and quickly create, change, or delete access as needed.

[Privilege Manager for Unix](#) enables organizations to define security policies which determine exactly what privileged actions a user can perform once they have logged in. Such policies can be based upon user, group, command, host, day, or time. In addition, Privilege Manager audits all activity, tests security policies and provides graphical analysis of system activity while highlighting anomalies.

[Policy Authority for Unified Communications](#) prevents unauthorized communication between functional roles based on any directory attribute ensuring that ethical walls are maintained between people who should not be communicating for compliance or operational reasons. Policies can be created granularly, can differentiate between internal, inbound and outbound users, and can apply to multiple modalities (i.e., text, file transfer, VoIP, video). Policies can be set independently by provider. Policy Authority provides content filtering and captures file transfers for OCS/LCS and Public IM improving security and reducing risk by preventing potentially sensitive data from being sent to the wrong recipients.

[Reporter](#) provides null and policy reports to ensure user passwords are strong.

Critical Control 11: Dormant account monitoring and control

Attackers, including malicious former employees, can impersonate legitimate users by using inactive user accounts. Because the accounts are legitimate, discovering and stopping this unauthorized access is difficult. Therefore, organizations must regularly monitor the use of all accounts and automatically log users off after a standard period of inactivity. They must also quickly disable and deprovision user accounts that are no longer needed. Organizations should also profile each user's typical account use, including normal time-of-day access and access duration, and monitor for atypical use that might indicate an attack.

Quest Solutions: ActiveRoles Server, Authentication Services, Reporter, and MessageStats, Access Manager, InTrust, InTrust Plug-In for Active Directory, InTrust Plug-In for Exchange, InTrust Plug-In for File Access

[ActiveRoles Server](#) provides complete user and group lifecycle management, including automated provisioning, deprovisioning, and deletion of accounts.

[Authentication Services](#) extends the user and group lifecycle management of Active Directory identities available through ActiveRoles Server to also include Unix, Linux, and Mac identities. When a user account is deactivated in Active Directory, it is also automatically deactivated across all integrated platforms and systems.

[Reporter](#) provides reports that identify inactive accounts. There is a report that highlights user accounts that were created but never used, for example, an account created for a new hire who declines the job offer or for a consultant whose start date is postponed. Another report lists user account lockouts (instances when an account password is entered incorrectly several times in succession), indicating an attempt to use someone else's account.

[MessageStats](#) tracks use of mailboxes, public folders, distribution lists, and contacts, and provides reports that identify dormant Exchange mailboxes and Blackberry accounts.

[Access Manager](#) identifies every point of access of a specified user across the Windows network enabling easy cleanup of unresolved user IDs.

[InTrust](#) provides automated alerts when individuals are mistakenly or maliciously granted access to critical data.

[InTrust Plug-In for Active Directory](#)

[InTrust Plug-In for Exchange](#)

[InTrust Plug-In for File Access](#) These solutions provide object-level protection to ensure sensitive groups and objects cannot be changed when unauthorized individuals are mistakenly or maliciously added.

Critical Control 13: Limitation and control of ports, protocols, and services

The installation process for many software packages automatically installs and enables services (such as web servers, mail servers, file and print services, and DNS servers). Because the users often are not aware that the services have been enabled, they are unlikely to disable or patch these services, making them targets for attack.

Quest Solutions: SecurityManager

[SecurityManager](#) proactively prevents accidental or unauthorized modifications or deletions to critical objects in Active Directory with object-locking policies and instant notification of unauthorized access.

Critical Control 15: Data leakage protection

To prevent the loss of sensitive data, organizations must carefully monitor the movement—both electronically and physically—of data across network boundaries.

Quest Solutions: InTrust, InTrust Plug-In for File Access, Archive Manager, Policy Authority for UC and Storage Horizon

[InTrust](#) delivers real-time alerting and granular auditing across heterogeneous networks, including Windows, Unix, and Linux systems. It automatically audits access to critical systems and provides immediate alerts to inappropriate or suspicious access-related events.

[InTrust Plug-In for File Access](#) monitors and prevents data movement and unauthorized access through file protection and change auditing.

[Storage Horizon](#) delivers real time alerts and monitors storage utilization across all data centers to the LUN level—mapping where sensitive data is stored, by storage type, how much is being used by an organization or department, and alerts administrators if storage limits are at a critical level. The solution also monitors and forecasts where data usage is growing across data centers. Through predictive analysis, the solution informs administrators where data demand is growing and where additional storage deployment will be required to ensure no loss of sensitive data occurs.

[Archive Manager](#) captures, indexes, and archives all messaging data into a scalable and secure repository, enabling faster e-discovery and strict compliance with regulations.

[Policy Authority for Unified Communications](#) provides content filtering (utilizing regular expressions and MOD-10 credit card filtering) and tagging for IM conversations to help prevent the loss of sensitive data and protects against abusive or inappropriate language. Policy Authority captures file transfers for OCS/LCS and public IM, preventing potentially sensitive data from being sent to the wrong recipients. Policy Authority also prevents unauthorized communication between functional roles based on any directory attribute. Policies can be created granularly, can differentiate between internal, inbound and outbound users, and can apply to multiple modalities (i.e., text, file transfer, VoIP, video). Policies can be set independently by provider.

Critical Control 18: Incident response capability

To limit damage from incidents, organizations need to have written response procedures in place, with defined roles for personnel and standards for timely incident reporting.

Quest Solution: InTrust

[InTrust](#) delivers real-time alerting and granular auditing across heterogeneous networks, including Windows, Unix, and Linux systems. It automatically audits access to critical systems and provides immediate alerts to inappropriate or suspicious access-related events. Automatic responses can be assigned to InTrust alerts, for example, offending users can be automatically disabled or the change can be reversed.

Critical Control 19: Data recovery capability

When attackers compromise a machine, they may make significant or subtle changes to its configuration, software, and data. Organizations need a trustworthy data recovery capability to restore compromised systems to their proper states. Regular backups are part of the solution, but they need to be complete and encrypted. In addition, organizations need to be able to quickly determine what needs to be restored and easily recover the data.

Quest Solutions: Recovery Manager for AD, Recovery Manager for Exchange, Recovery Manager for SharePoint, LiteSpeed, SharePlex, Policy Authority for UC, vReplicator, and vRanger Pro

[Recovery Manager for Active Directory](#) provides granular and scalable online recovery. Comparison reports highlight changed and deleted objects and attributes in Active Directory, enabling a fast and accurate recovery.

[Recovery Manager for Exchange](#) provides a complete search of backup media for granular recovery of individual, message-level items—without the need for dedicated recovery server.

[Recovery Manager for SharePoint](#) provides complete backup and granular recovery of SharePoint sites and individual documents.

[LiteSpeed](#) is a fast and flexible backup and recovery solution for Oracle and SQL Server databases. LiteSpeed's low-impact, high-performance compression technology reduces the size of backups and the length of the backup window, enabling organizations to take backups regularly. Multiple levels of encryption, up to AES 256-bit, keeps data secure. And LiteSpeed's flexible, granular recovery options accelerate recovery times by up to 70 percent.

[SharePlex for Oracle](#), the leading database replication solution, provides log-based, high-speed replication for Oracle, preventing downtime or loss of critical data.

[Policy Authority for Unified Communications](#) archives IM conversations to an archive system and can restore its own logging database if the database becomes compromised.

Vizioncore, Quest's server virtualization management subsidiary, offers an extensive management solution for today's leading virtual server environments. [vReplicator](#) supports disaster recovery strategies with affordable replication of the entire virtual machine, including configuration settings, patches to the OS, the application, the data, and all other OS-level changes. [vRanger Pro](#) provides fast image-level hot backups of the entire virtual machine or just the differential.

SUMMARY

The following table summarizes the key controls for preventing and responding to infrastructure attacks and lists the Quest solutions that can help achieve FISMA compliance:

CONTROL	QUEST SOLUTIONS
2: Inventory of authorized and unauthorized software; enforcement of white lists of authorized software	Quest Management Xtensions – Configuration Manager 2007 Edition Policy Authority for Unified Communications Reporter SecurityManager Storage Horizon
3: Secure configurations for hardware and software for which such configurations are available.	Desktop Authority vWorkspace SecurityManager
5: Boundary defense	Policy Authority for Unified Communications Quest Defender
6: Maintenance, monitoring, and analysis of complete audit logs	InTrust InTrust Plug-In for Active Directory InTrust Plug-In for Exchange InTrust Plug-In for File Access ChangeAuditor for Active Directory ChangeAuditor for Exchange ChangeAuditor for File Systems
8: Controlled use of administrative privileges	ActiveRoles Server InTrust Quest Defender Privilege Manager for Unix SecurityManager
9: Controlled access based on need to know	Authentication Services ActiveRoles Server Access Manager Privilege Manager for Unix Policy Authority for Unified Communications
11: Dormant account monitoring and control	ActiveRoles Server Authentication Services Reporter

Protecting Your IT Systems from Attack

CONTROL	QUEST SOLUTIONS
	MessageStats Access Manager InTrust InTrust Plug-In for Active Directory InTrust Plug-In for Exchange InTrust Plug-In for File Access
13: Limitation and control of ports, protocols, and services	SecurityManager
15: Data leakage protection	InTrust InTrust Plug-In for File Access Archive Manager Policy Authority for Unified Communications Storage Horizon
18: Incident response capability	InTrust
19: Disaster recovery capability	Recovery Manager for Active Directory Recovery Manager for Exchange Recovery Manager for SharePoint LiteSpeed SharePlex for Oracle Policy Authority for Unified Communications vReplicator vRanger Pro

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Visit www.quest.com for more information.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at <http://support.quest.com>

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: [http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)