

Case Study: Quintiles Transnational

CUSTOMER PROFILE

Quintiles Transnational helps improve healthcare worldwide by providing a broad range of professional services, information, and partnering solutions to the pharmaceutical, biotechnology, and healthcare industries. Headquartered near Research Triangle Park, North Carolina, and with offices in more than 40 countries, Quintiles is a leading global pharmaceutical services organization and a member of the Fortune 1000.

Quintiles Transnational's competitive edge lies in its ability to leverage data, therapeutic expertise, and global resources through an integrated information technology network. Quintiles manages all phases of clinical trials for organizations seeking to gain FDA approval for their new products. Due to the high volume of information needed for clinical trials, no one collects and manages more data worldwide than Quintiles.

BUSINESS CHALLENGES

Quintiles Transnational manages over 13,000 end-user computers. The company wanted to remove the local administrative privileges from all end-user accounts and run a Least Privilege user environment. Running a Least Privilege environment would help Quintiles achieve compliance with the FDA's Title 21 Code of Federal Regulations, increase security, and better protect client and patient data.

While network security, regulatory compliance, and data protection are the primary focus of network administrators, they are also responsible for ensuring that users have access to appropriate computing resources and for improving overall productivity. With administrative privileges removed, end-users would no longer be able to run dozens of critical third-party, off-the-shelf software, as well as many in-house developed applications. End-users would also no longer be able to install local printers or any software on their own. No workaround that they had identified would allow applications that required administrator privileges to run, and writing custom install scripts or frequently visiting individual desktops to install software was not a secure or productive solution.

“ BeyondTrust Privilege Manager has played a critical role in our strategy to enforce the security principle of Least Privilege. We have over 13,000 non-administrator user accounts, and numerous applications that require elevated permissions. In addition to managing application privileges, we must be able to selectively allow our end-users to self-install certain software, such as printer drivers and authorized applications. ”

– Tom Powell, IT Architect, Desktop & Portable Tech., Quintiles Transnational



CHALLENGES

- Enforce a Least Privilege environment for over 13,000 end-users
- Prevent restricted end-users from making system level changes
- Allow restricted end-users to run all required applications
- Allow restricted end-users to self-install approved applications
- Centrally manage policy changes

SOLUTION

BeyondTrust™ Privilege Manager

BENEFITS

- All 13,000 end-users log on without admin privileges
- Increased compliance with regulatory mandates
- End-users can securely run all approved applications as standard users
- Reduced threat from malware and zero-day threats
- End-users granted access to install authorized software only
- Reduced downtime and help desk support
- Centralized and granular policy control.



MAKING THE DECISION

With Windows Active Directory installed and 13,000 end-users running Windows XP, BeyondTrust Privilege Manager was the perfect solution to the issues facing Quintiles. Security, compliance, and productivity were at the forefront of Quintiles needs, and running BeyondTrust Privilege Manager would enable them to create a Least Privilege environment while increasing their end-user productivity.

SOLUTION

Quintiles Transnational has now deployed BeyondTrust Privilege Manager on over 13,000 computers. It has met or exceeded all of Quintiles requirements and enabled end-users to access all required applications while running in a Least Privilege user environment.

Quintiles Transnational uses BeyondTrust Privilege Manager to elevate the permission level for the users who need to run authorized third-party and homegrown applications that require higher privileges than those to which the user is normally entitled. This eliminates the need to raise each user's privilege levels for all applications or to require that the restricted user be provided with a local administrator login to perform the tasks.

Additionally, network administrators can now allow only approved browser components to be installed by end-users. Using this functionality, Quintiles has improved security by only permitting end-users to run approved components such as the ActiveX controls for Quintiles' Learning Management System.

Finally, Quintiles will allow restricted end-users to self install XP SP2, as well as other authorized software. Using BeyondTrust Privilege Manager's self-service software feature, Quintiles will no longer have to write scripts to migrate and install authorized software, but rather can let the users install it at their own convenience without aid of an administrator.

BENEFITS

BeyondTrust Privilege Manager has enabled Quintiles to enforce the security best practice of Least Privilege for over 13,000 end-user accounts. By doing so, Quintiles has increased security and become compliant with the FDA Title 21 Code of Federal Regulations mandate.

In addition to security, Quintiles has also realized several productivity gains. End-user computers have significantly less malware as result of running without administrative privileges and experience less downtime, while still being able to run all required applications and install authorized software. These benefits have resulted in fewer calls being placed with the help desk, and when issues do arise they are easier to diagnose.

BeyondTrust™ Privilege Manager

BeyondTrust Privilege Manager was the first product to enable network administrators to enforce the security principle of Least Privilege on Windows desktops. With it, organizations can effectively run end-users as non-administrators, significantly reducing their exposure to malware and malicious end-users.

BeyondTrust Privilege Manager is incorporated into the Windows Group Policy system, allowing standardization on a single methodology and built-in infrastructure. This significantly reduces acquisition cost, training time, and management infrastructure while increasing security, reliability, and maintainability.

For more information, contact us:

BeyondTrust Corporation

125 Brewery Lane, Bldg. 320
Portsmouth, NH 03801 USA

www.beyondtrust.com
+1 603-433-5885

© 2006 BeyondTrust Corporation

All rights reserved. BeyondTrust and Privilege Manager are trademarks of BeyondTrust in the United States and other countries.

Microsoft, Windows, and other marks are the trademarks of their respective owners.

Microsoft®
GOLD CERTIFIED
Partner