

Case Study: DSM

Customer Profile

DSM is active worldwide in nutritional and pharma ingredients, performance materials and industrial chemicals. The company develops, produces and sells innovative products and services that help improve the quality of life. DSM's products are used in a wide range of end-markets and applications, such as human and animal nutrition and health, personal care, pharmaceuticals, automotive and transport, coatings and paint, housing and electrics & electronics. DSM Nutritional Products, formerly Roche Vitamins and Fine Chemicals, is the world's leading supplier of vitamins and carotenoids to the feed, food, pharmaceutical and cosmetic industries.

DSM has annual sales of over €8 billion and employs 18,000 people worldwide. The company is headquartered in the Netherlands, with locations in Europe, Asia, Africa, Australia and the Americas.

Business Challenges

DSM was working on an internal project to migrate 18,000 desktops from Windows NT4 to Windows XP. A new group was created to design the XP desktop environment to be as secure as possible. The group identified a critical component to improving security was to remove local administrator rights from end users and to enforce a Least Privilege environment. To achieve this, DSM set a policy that all end users must log on as standard users without elevated privileges.

In order to retain leadership position in many different fields, DSM knew that productivity could not be sacrificed. The new desktop environment not only had to be secure, but also it had to ensure that it did not prevent people from doing their job. Like many large companies DSM relies on a long list of applications that require administrative privileges to do business. If end users no longer had administrative rights, these applications would not work. Additionally, given DSM's worldwide presence, DSM's sales force must be able to manage certain settings, such as connecting to local printers and configuring an IP address when connecting to a new wireless network. Without administrator privileges, end users would not be able to make necessary system changes when they traveled.

“ A company like DSM cannot be successful if it is forced to choose between security and productivity. BeyondTrust Privilege Manager allows us to maintain the critical security policy of having users log in without administrative rights, while still allowing the users to run all required applications and manage all necessary computer settings. Without this product our 18,000 users would still be running as administrators.”

– John Penris, Design Manager Global Desktop, DSM



CHALLENGES

- Enforce a Least Privilege environment for all 18,000 end-users
- Allow restricted end users to run all required applications
- Permit travelling laptop users to manage certain computer settings
- Allow restricted end users to self-install approved ActiveX controls
- Centrally manage policy changes

SOLUTION

BeyondTrust Privilege Manager™

BENEFITS

- All 18,000 end users log on without admin privileges
- End users can securely run all approved applications as standard users
- End users can self install authorized software and ActiveX controls
- Decreased malware and help desk calls
- Centralized and granular policy control.

Making the Decision

As DSM was moving to a new Active Directory environment with 18,000 end users running XP, BeyondTrust Privilege Manager was the solution to their problems and it required no additional infrastructure. BeyondTrust Privilege Manager would allow DSM to remove administrator rights from all end users, while still allowing users to run critical business applications that required administrative privileges. Additionally, laptop and traveling users would be able to make authorized system changes despite not having administrative privileges.

Solution

DSM deployed BeyondTrust Privilege Manager enterprise wide to all 18,000 users. BeyondTrust Privilege Manager has allowed DSM to meet their goals of creating a secure, Least Privilege desktop environment while allowing end users to continue to run all required applications. It has exceeded expectations by reducing the number of help desk calls and increasing end user and administrator productivity.

At DSM the majority of users need access to applications that require elevated privileges. Using BeyondTrust Privilege Manager end users who do not have local administrator rights can run these applications while remaining a locked down user. Users also need to install software and ActiveX controls. BeyondTrust Privilege Manager allows users to self install approved software and ActiveX controls, reducing IT support costs. By permitting users to only install approved software security is greatly enhanced.

BeyondTrust Privilege Manager also provides a solution to the issues faced by DSM's 4000 laptop users. DSM's laptop users travel worldwide often visiting different subsidiaries. While traveling these users need to adjust some of their own computer settings. Privilege Manager allows restricted users to maintain authorized computer settings such as, connecting to local printers, IP configuration settings to connect to a wireless networks, and changing time zones.

Benefits

BeyondTrust Privilege Manager has enabled DSM to enforce the security best practice of Least Privilege for all of their 18,000 end users. By doing so, DSM has increased security. End users no longer know or need to know the local administrator password, reducing the potential of any malicious activity.

In addition to security, DSM has also realized several productivity gains. End user computers have significantly less malware as result of running with administrative privileges, while still being able to run all required applications, connect to local printers and install approved software. These benefits have resulted in fewer help desk calls.

BeyondTrust Privilege Manager™

BeyondTrust Privilege Manager was the first product to enable the security best practice of Least Privilege in Windows environments by allowing administrators to assign end users permissions to required or selected applications.

With BeyondTrust Privilege Manager, end users can run all required applications, processes and ActiveX controls without administrative privileges. By removing the need to grant end users administrative rights, IT departments can eliminate what is otherwise the Achilles heel of the desktop – end users with administrative power that can be exploited by malware and malicious users to change security settings, disable other security solutions such as anti-virus and more.

For more information, contact us:

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

www.beyondtrust.com
+1 603-610-4250

© 2007 BeyondTrust Corporation

All rights reserved. BeyondTrust and BeyondTrust 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