CASE STUDY

CYBERARK®

Company: National Gypsum Company
Charlotte, North Carolina
www.nationalgypsum.com

National Gypsum Relies on the CyberArk
Privileged Access Manager Solution to
Get Privileged Accounts Under Control for
Improved Security and Compliance

Industry: Manufacturing
Employees: 1,900+
CyberArk Product & Services:
CyberArk Privileged Access Manager Solution
CyberArk Secrets Manager

> "We have thousands of privileged accounts managed by CyberArk. We have taken care to ensure that people only have the level of access that is needed. We deny by default, then allow based on needs, granted by approval."

Mike Brannon, Senior Manager of Information Systems at National Gypsum

National Gypsum Company is a fully integrated building products manufacturer and one of the leading gypsum board producers in the world. Headquartered in Charlotte, North Carolina, National Gypsum manufactures gypsum wallboard, cement board and related construction materials at 43 facilities in North America.

THE CHALLENGE

National Gypsum faced a turning point in its security program when its CFO and controller demanded that IT pass audits related to access control. However, National Gypsum had never set up any management or monitoring of privileged accounts, which would be essential to meet compliance requirements. As a result, National Gypsum faced significant database vulnerabilities and compliance weaknesses.

Shared administrative and embedded application accounts represent an enormous security risk. For example, the manufacturer used one "domain admin" level account across all its applications and servers, and passwords were not well documented or managed, and not often changed. This single embedded account and its password had become well known by IT personnel and some power users, and the password could not be changed without breaking the systems where it was embedded.

Recovery from a serious security compromise could be devastating to the business unless the compromised account(s) and credentials are left in place. For example, exploiting poorly managed accounts on privileged systems would have an impact on business operations far beyond a data breach.

Mike Brannon, senior manager of information systems at National Gypsum, used the results of penetration tests against privileged accounts that are not associated with a person to help make the case for an automated privileged identity management tool. "The only way to fix it would be to disrupt operation of all these systems almost as though we had a disaster without the building burning down," said Brannon. "If key privileged accounts were disclosed, changing their passwords would break the systems where they are used. If this ever happened in the real world (outside of an audit / penetration test), there's no way we could make this change without breaking production systems."

THE SOLUTION

One of the first steps was to make significant improvements in routine production systems access controls. In doing so, one of National Gypsum's goals was to make it easier to be secure, but more painful when users tried to do things they shouldn't. As part of National Gypsum's new security model, the team created more Active Directory accounts to accommodate roles in development, QA and production environments. They also set up new accounts for SYS and "firefighter" roles, instituting a least privilege strategy where users would be granted access on-demand only to the systems needed to perform a particular task, in a documented way.

Results & Key Benefits:

- Rapid time-to-value
- Improved workforce efficiencies
- Application passwords are generated for all new projects
- Developers manage Dev-QA (self-service)
- Regular password changes
- "Firefighter accounts" auditable production access
- Successful audit related to privileged and production account management

The manufacturer implemented the CyberArk Privileged Access Manager Solution, leveraging its Enterprise Password Vault® to better manage nearly 2,000 passwords, making sure they areautomatically updated, changed at regular intervals and fully auditable. The National Gypsum security team is now in charge of all the production accounts and can track who requested access to a system, and what was done once access was granted. Through its integration with Active Directory, the CyberArk solution alleviates the need for dual management and maintenance of roles, overall improving operational efficiency.

National Gypsum also integrated the CyberArk Secrets Manager™ solution with Opalis, a process automation system. Opalis is responsible for performing numerous IT automation tasks across the manufacturer's servers and applications.

Integrating with Secrets Manager allowed National Gypsum to remove sensitive (domain/server admin level) hard-coded passwords from the Opalis jobs and benefit from secure caching capabilities to ensure business continuity even in the case of a network outage.

THE RESULTS

Typically, employees are given a level of privilege that they can either apply incorrectly and do some damage to the privileged system to which they have been given elevated rights, or gain access to confidential information.

Brannon says, "We have taken care at National Gypsum to ensure that people only have the level of access that is needed. This prevents users from unwittingly bringing down production systems because they have access to data and/or processes outside of their routine needs. We deny by default, then allow based on needs, granted by approval."

Working with CyberArk also helped fuel new business initiatives, such as National Gypsum's SAP deployment, "which presented an opportunity to do things the right way," said Brannon.

For example, National Gypsum leveraged its SAP deployment in an external data center to set up stronger system controls and appropriate levels of access. According to Brannon, some internal people said that approach would not work at the company, and that National Gypsum did not have the staff.

"We knocked out the argument that all Windows environments require what we now regard as inappropriate access and privilege to operate efficiently," he said. "We built our new SAP applications with application roles and a Windows infrastructure that worked the right way – with limited privileges. We proved we can actually can set up systems that are very controlled, reliable and that don't inexplicably get changed or go down unexpectedly."

Even a good faith effort to control access according to need and based on the privilege quotient for the applicable accounts, assets and processes are daunting, to say the least. Organizations will typically use spreadsheets or similar artifices to control and track privileged access, but find it is impossible to keep up with demands for access and quickly fall behind and lose track.

"We have thousands of privileged accounts managed by CyberArk," said Brannon. He had been frustrated by the Excel approach to privilege management and had to deal head-on with the problem of embedded accounts when National Gypsum upgraded its SQL Server databases and a slew of dependent legacy apps as Microsoft wound down support for SQL Server 2000.

"Never in our wildest dreams would we have attempted the application integration, as well as the Windows local systems administrators and some of the Windows services accounts that we're managing this way. The new approach really improves our ability to manage all access to privileged accounts," concluded Brannon.

Perhaps one of the most tangible results of the CyberArk deployment was National Gypsum achieving a major compliance milestone, by passing a privileged and production account management audit for the first time.