Case Study

World's leading virtualization platform provider relies on Password Manager Pro to consolidate and secure privileged accounts

Instant Productivity Gains Through Easy-to-Use Password Security:
The R&D division of the virtualization platform vendor deploys ManageEngine Password Manager Pro to solve virtual security challenges by controlling access to hundreds of physical devices and thousands of VMs and vApps.

Solving the Security Challenge

Automated password management assures virtually unbreakable password security

With over 300,000 customers, the virtualization platform vendor stands tall as the global leader in virtualization and cloud infrastructure solutions helping customers reduce capital and operating expenses, improve agility, ensure business continuity and strengthen security. The success of such a huge portfolio of virtualized solutions relies on finely honed and integrated Research & Development effort.

The R&D division of the organization is tasked with the responsibility of modeling and managing virtualized applications, which, in turn, requires a strong IT infrastructure base. The R&D division's IT environment is vast and includes hundreds of physical devices, virtual machines virtualized applications, and mobility-enabled virtual workloads that traverse the network from one physical server to another. Just like any other complex IT environment, physical devices and VMs are accessed and controlled by administrative accounts that grant unlimited access privileges.

Fast Facts

Organization:
Virtualization Platform Provider

Industry:
Technology

Location:
United States of America

Business Challenge:
Proliferation of complex, hard-to-remember administrative passwords. Consolidate and secure them in a centralized vault and establish access controls.

Solution:
ManageEngine Password Manager Pro

Why Password Manager Pro?

- Simple, secure, reliable, enterprise-ready, scalable and operationally efficient
- Part of ManageEngine's broad suite of products
- Comprehensive auditing capabilities

VMs and other virtualized applications are organized as sets of gear stacks, which are virtual centers in a cluster. Many such virtual centers run in a centralized Management Stack. Each stack gear has a unique, 16-digit password. Naturally, such lengthy passwords are nearly impossible for the members of the R&D team to remember.

"Putting Password Manager Pro to work was a breeze. We set it up and deployed in our production environment in about just two hours".

The manual approach to storing, accessing and managing these administrative passwords was cumbersome, time consuming and labor intensive and also highly insecure. Determined to be proactive in ensuring security at all levels, the IT team of the R&D division clearly needed an automated password management solution.

“Our immediate requirement was to consolidate and secure all the administrative passwords in a centralized vault and establish access controls. Tracking ‘who’ has access and determining ‘when’ passwords are accessed were equally important to ensure accountability for access and actions,” explains the Director of the division.

The Solution: ManageEngine Password Manager Pro

The IT team of the R&D division had several key imperatives in mind while evaluating alternative approaches to address and solve their password management and security challenges. They expected the solution to be simple, secure, reliable, enterprise-ready, scalable and operationally efficient. Provision for integration with Active Directory for user management and authentication was another important consideration. After researching various tools, they chose ManageEngine Password Manager Pro.

"All the passwords for our devices, including those for networking gear, storage devices, and service management processes are all maintained in Password Manager Pro"

“ManageEngine was specifically chosen because of its broad suite of products. Password Manager Pro satisfied all our requirements and we decided to deploy it immediately,” says the Director.

Putting Password Manager Pro to work was a breeze. “We set it up and deployed in our production environment in about just two hours,” he recalls.

The Password Manager Pro Difference: A 'Must Have' Tool

ManageEngine Password Manager Pro has rapidly become one of the Division's favorite IT management solutions as it has brought a welcome and long-awaited end to once convoluted, manual and insecure password management practices.

"During one of the conferences in 2011, Password Manager Pro maintained password access to over 15,000 vApps"

"All the passwords for our devices, including those for networking gear, storage devices, and service management processes are all maintained in Password Manager Pro. Whenever passwords are required, our administrators just login to Password Manager Pro and get secure access to the required passwords through a simple, intuitive web interface," says the Director.

By eliminating password fatigue, Password Manager Pro has improved productivity by protecting privileged identities and bolstering overall security. "Whenever someone retrieves a password, I immediately receive an email notification from Password Manager Pro," he says. "The audit trails help track 'who' accessed 'what' and 'when'. This is where we get both productivity benefits and high security."

ManageEngine Password Manager Pro at Global Conference Venues

Apart from proving highly effective in securing the in-house privileged identities in day-to-day operations, Password Manager Pro has been playing a significant access control role at the broadly attended and highly visible global conference organized by the virtualization platform provider.

"At the sessions and labs in the conference venue, students and attendees are granted access to thousands of virtual applications," says the Director. "The access activities at the conference are transient, but mandate security."

Prior to the selection of ManageEngine Password Manager Pro, easy-to-remember static passwords were used to grant access at the conferences. Password Manager Pro has altogether changed that scenario by maintaining access to privileged passwords and providing users with secure and managed access to vApps. During one of the conferences in 2011, Password Manager Pro maintained password access to over 15,000 vApps. "For us, Password Manager Pro has proved to be a 'must have' tool," he says. "Given all of Password Manager Pro's many useful features, we are at present only using it in simplistic mode. However, we are

planning to leverage advanced features like remote password synchronization, application-to-application password management, access control workflows and other features soon. We are very pleased with ManageEngine and Password Manager Pro and intend to expand its usage in addition to deploying other ManageEngine products as well."

Real-Time IT and ManageEngine Password Manager Pro

ManageEngine serves more than 55,000 established and emerging enterprises - customers with IT infrastructures that are far more dynamic, flexible and elastic than ever before. The net result is what ManageEngine calls real-time IT.

> "For us, Password Manager Pro has proved to be a 'must have' tool"

Real-time IT calls for IT to make the most of today's game-changing technologies and deliver immediate services to organizations that are operating at an ever-increasing pace.

Industry experts assert that the overall security level of an enterprise is the sum of many security foundation elements: strong perimeter defenses, the proper configuration of system resources and effective controls for resource access. Protecting application and data resources requires, among other things, authenticating the people that access those resources. In turn, the integrity of the authentication process depends on uncompromised, secure passwords. Administrative and privileged passwords introduce the potential for security breaches everywhere in the enterprise. Servers, databases, switches, routers, firewalls and any other hardware or software can have large number of administrative passwords. Often, passwords are insecurely stored in spreadsheets, text files and even as printouts and are shared by a group of administrators. With ManageEngine Password Manager Pro, passwords are no longer the weak link in your security strategy.

ManageEngine Password Manager Pro is a web-based, shared account Password Management Solution for enterprises to control the access to shared administrative passwords of any enterprise resource, such as servers, databases, network devices, applications etc. Password Management Pro enables IT managers to enforce standard password management practices such as maintaining a central repository of all passwords, usage of strong passwords, frequent changing of sensitive passwords and controlling user access to shared passwords across the enterprise. www.passwordmanagerpro.com