ManageEngine
Password Manager Pro

Australia's Leading Retail Giant Streamlines Remote Vendor Access to IT Assets Using Password Manager Pro

The IT division of a trusted household appliance retailer in Australia consolidates privileged accounts and achieves fully controlled, closely monitored privileged access by using Password Manager Pro.

Background

The household appliance retail chain has been delivering quality consumer household appliances at competitive prices across Australia for over half-a-century now and commands the trust of its clientele. With retail stores at multiple locations along with a strong online presence, the organization has emerged the most-trusted retail icon. It still continues its winning pace, both across its store network and online, by maintaining a high level of service, brand promise, lowest prices, and a wide product range.

Business Challenge

In retail, keeping pace with industry trends is vital in consistently providing an exceptional shopping experience, which will in turn ensure customer retention. When the industry gravitated towards e-commerce, the retailers had to reposition themselves with an efficient IT infrastructure to retain their market share. IT frameworks in modern retail firms are typically used to connect the corporate network with the stores, data centers, and third parties; handle online payments as well as debit or credit card transactions at POS systems; hold scores of personal data collected from customer loyalty programs; and manage other back-end IT operations.

Responding promptly to market trends, the retail chain leveraged IT optimally and now, commands a sturdy IT framework. Its network infrastructure consists of 300-odd resources - a mix of servers, databases, switches, routers, and hubs. As the number of stores continues to grow, more IT assets get added to the network to continue giving the best service. With improved technology comes increased risks and the organization had to handle a few security challenges.

To any retailer, a strong supply chain is necessary, and it was no different for this retailer. The company worked with a number of third-party contractors, which included supply agents, payment gateway providers, and point of sale (PoS) vendors. These third parties required frequent access to the internal network to fulfill their contractual duties. Moreover, the vendors were geographically apart, which meant they usually accessed the IT resources remotely through VPN.

> **Especially, we hoped to get a clear picture by maintaining a centralized record of the IT assets in production and non-production deployments and track access permissions provided to each vendor**

The biggest challenge that the IT division faced was provisioning the required privileged access to the vendors based on their needs. Granting remote access included exposing the credentials of privileged accounts, which were shared with the contractors by email. Moreover, whenever the administrator changed the passwords, an email with the new passwords had to be sent out again. With the passwords, there was a slight chance the contractors could gain privileged access beyond their requirements. "Eventually, we found it difficult to track 'who' had access to 'which' passwords and 'what' they were doing," says the security specialist at the organization. At that point, the team realized the need to control and monitor vendor access.

In addition, the team dealt with a few minor challenges such as controlling employee access to critical resources, periodically resetting old passwords, ensuring uninterrupted access to IT assets, and complying with IT regulations. Being a retail giant, a normal day involved processing of massive amounts of financial data from its multiple stores spread across multiple states. To ensure the safety of the cardholder data during payment transactions, the firm had to take measures to comply with PCI-DSS as a part of its security best practices.

The Solution

When the security challenges started getting bigger, the IT team realized that KeyPass, the online password management tool they were then using did not provide the features they were looking for. What they needed was an integrated, all-in-one security solution that would secure their privileged accounts and establish strong controls to manage remote vendor access as well as internal access. They expected the solution to provide the vendors with access only to the resources that are necessary for their work and also, enable them to log on to the resources without getting to know the actual passwords. "Especially, we hoped to get a clear picture by maintaining a centralized record of the IT assets in production and non-production deployments and track access permissions provided to each vendor," explains the security specialist. With their security requirements straightened out, the team began scanning the market for an apt solution.

> **Since we run mainly on Solaris and IBM AIX,Password Manager Pro had to be installed on Linux. Though the installation process proved to be a bit of challenge, the support team at ManageEngine aided us throughout in deploying the solution smoothly**

While experimenting with the evaluation trials of various solutions, they chanced upon ManageEngine's Password Manager Pro, a privileged access management solution. A quick evaluation of the product made them understand that Password Manager Pro was the instant answer to all their security woes.

Password Manager Pro Difference

After the team evaluated Password Manager Pro, they decided to deploy the solution in their environment. "Since we run mainly on Solaris and IBM AIX, Password Manager Pro had to be installed on Linux. Though the installation process proved to be a bit of challenge, the support team at ManageEngine aided us throughout in deploying the solution smoothly," recalls the security specialist.

> **Password Manager Pro with Active Directory has made user management extremely simple and effective. It gives us a good picture of 'who' has access to'what', which we weren't able to see before**

Today, management of remote vendor access at the retail chain has become smooth. With Password Manager Pro as their security stronghold, the IT team has achieved the following:

- The contractors requiring access to the same resources are grouped together and assigned limited permissions on need-basis.
- They are allowed to launch remote RDP, SSH, and Telnet sessions with a single click, without seeing passwords in plain text.
- The privileged sessions launched by the contractors are video-recorded and archived for forensic analysis.
- Comprehensive audit trails provide the internal IT team with a transparent picture of privileged access details. "It gives us a good picture of 'who' has access to 'what',which we weren't able to see before," adds the security specialist.

This has enabled the organization to efficiently collaborate with its third-party contractors in a secure way. In addition, Password Manager Pro has benefitted the retail firm in a number of other ways.

Routine password management is now carried out with a centralized password vault where data gets stored in fully encrypted form. Employees requiring access to sensitive information are granted access after being subject to an access control workflow, based on their role in

the firm. Administrative passwords are automatically reset at pre-determined intervals with the 'Scheduled Password Reset' feature.

> It does what it needs to do & it does it well. Password Manager Pro is easy to use for the administrators as well as the end users to administer the passwords

The provision to integrate Password Manager Pro with Active Directory has made user management extremely simple and effective. Furthermore, the High Availability feature in Password Manager Pro ensures uninterrupted access to passwords. Altogether, the IT team is very happy with the way Password Manager Pro single-handedly addressed their challenges in a flash.

"It does what it needs to do & it does it well. Password Manager Pro is easy to use for the administrators as well as the end users to administer the passwords," declares the security specialist.

About Password Manager Pro

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, and applications.

Password Manager 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. It is available at costs affordable to SMBs.
www.passwordmanagerpro.com

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower IT teams to meet organizational needs for real-time services and support. Worldwide, established and emerging enterprises - including more than 60 percent of the Fortune 500 - rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corporation with offices worldwide, including the United States, India, Singapore, Japan and China.

ManageEngine

Zoho Corporation
4141 Hacienda Drive, Pleasanton,
CA 94588, USA
Phone: +1-925-924-9500
Email: sales@manageengine.com