Global charitable organization streamlines its password lifecycle management processes across 80 locations using Securden

A renowned charitable organization having IT establishments in over 80 locations across the globe secures the sensitive passwords of its complex IT infrastructure using Securden. Streamlines its password lifecycle management processes and achieves complete control.

Background and the Business Challenge

Engaged in poverty alleviation, women and children welfare, and rebuilding human lives in disaster-hit areas across the globe, the charitable organization commands respect for rendering yeomen service for the past several decades. The organization has a huge IT infrastructure with hybrid devices - physical, virtual, and cloud - and the teams are spread across multiple locations.

The teams, working from over 80 locations, many of them remotely, were keeping their own password databases to access the IT resources. The password databases varied from homegrown tools, spreadsheets, and text files. This approach led to various issues ranging from unnecessarily granting full access to everyone, having to refer to multiple files to locate the credentials, system lockouts due to outdated passwords, and much more.

IT Environment

- A mix of physical, virtual, and cloud instances. Geographically distributed teams.

Problems Faced

- Passwords were scattered across and teams dealt with data silos. No centralized control or visibility on who had access to what resulting in difficulty in ensuring password management best practices.

Securden Deployment

- Self-hosted on VMs on Azure

Results

- Secure, centralized, monitored, fully managed, and highly available password management system
- Granular access control to critical IT systems with complete control and visibility over IT access.
- Automation of password management best practices

There was no track on who had access to what systems and it made things difficult when an IT staff member left the organization - they had to manually change the passwords. There was no centralized control over the data. Teams were dealing with data silos.

The IT department realized that their password lifecycle management involved manual approaches and was creating security holes. They wanted to streamline the entire process before things went out of control.

> We've been using Securden for more than a year now and are absolutely loving it

The Solution

The team realized that they needed an intelligent password management system that could help efficiently handle the sensitive passwords belonging to various types of IT assets accessed by a geographically distributed team.

The infrastructure management team started evaluating the password management and Privileged Account Management (PAM) solutions available on the market. They had certain critical considerations:

- They strongly preferred a self-hosted solution as they were not willing to store their data on third-party systems
- The solution has to integrate with Active Directory for user provisioning and management
- Support integrating with multiple active directory systems
- The solution should be highly scalable capable of managing thousands of IT assets distributed across locations
- Should have high availability provisions inbuilt in addition to a robust disaster recovery mechanism
- Should be very easy to set up and maintain
- Highly intuitive to end-users
- Suit the stringent IT budget allocation typical of non-profit organizations

The IT infrastructure team shortlisted a few competing vendors and commenced a PoC. Soon they found Securden satisfying all the requirements and considerations.

"Other solutions we evaluated did not fit our requirements. Some solutions looked an overkill and some others lacked vital features. A few others had clunky interfaces making it difficult to use. Securden presented a refreshing look and we realized that it was the perfect solution for our needs," says the IT infrastructure specialist.

The team went ahead and deployed Securden in no time on a virtual machine on Azure and the instance is accessible to the IT team members belonging to the 80 locations via a web-browser and mobile apps both internally and externally.

> Securden team has always gone above and beyond in assisting with our queries right from the presales time to till date. We are happy customers.

The Result

Today, the organization has a secure, centralized, monitored, fully managed, and highly available password management system in place. Access to passwords is granularly controlled, which in turn controls access to the critical IT systems. The IT team is enforcing its policy for password management. Securden has fully automated the process with reports on compliance status, identification of weak passwords and tips to make them strong.

“Securden has brought intelligence to the process by identifying the passwords that are reused for many accounts. It also sends timely alerts on expiring passwords, thus helping us easily adopt all best practices. The provision to grant access without revealing passwords has made the process very secure,” says the Infrastructure Security Manager.

The IT department now closely tracks all access to password records. This gives them complete control over the entire process. “The AD integration is super helpful in that we allow access to password records based on the AD group membership, which mirrors in Securden,” says the IT specialist.

Having derived solid benefits by streamlining the process, the organization is planning for larger adoption.

“We've been using Securden for more than a year now and are absolutely loving it. In fact, we're looking at expanding it for wider use in the organization beyond the IT management teams in several other locations. Securden team has always gone above and beyond in assisting with our queries right from the presales time to till date. We are happy customers.”