Financial Services Company Turns to Automation to Mitigate Emerging Security Threats

Heartland Financial Deploys Enterprise Random Password Manager from Lieberman Software to Maintain Control

How do you keep customers' financial data safe from network intruders while protecting your organization from internal users who might unintentionally leave you vulnerable to attack? This was the challenge faced by Shane Nicely, VP of Information Services, and his team of IT professionals at Heartland Financial USA, a diversified financial services company.

Nicely oversees a group that is charged with maintaining operations and security for servers, workstations and thin clients spread across an enterprise with 73 sites. A pressing concern for the team is ensuring that the billions of dollars in customer assets are protected against unauthorized access.

Determined to be proactive in its approach to security, Nicely's team took the initiative to gain control over the powerful privileged account passwords that could allow network intruders or malicious programs to access financial records, change configuration settings, and run applications on virtually any system in the enterprise.

"The last straw for us was when one of our administrators went to a user's desk to help with a problem and noticed that a helpdesk employee had given him the administrator password," said Nicely. "The user had it written down on a scrap of paper at his desk. This was especially troublesome since so many of our computers shared that same password."

Profile: Heartland Financial

Heartland Financial USA, headquartered in Iowa, is a publicly traded financial services company that provides banking, mortgage, wealth management, insurance and consumer finance services across 73 locations. Visit www.htlf.com.

Situation

Heartland Financial required a solution to secure and manage privileged account access in order to comply with regulatory mandates, including Sarbanes-Oxley

Solution

Enterprise Random Password Manager was acquired and deployed to all branches in the network.

Result

Heartland Financial maintains secure control over its privileged account passwords, continues to prevent data breaches and complies with all audits.

The Situation

"As a financial institution we're challenged with security and compliance concerns that organizations in many industries don't face," Nicely said.

And as a public company Heartland Financial faces extensive IT audits. The organization is subject to Sarbanes-Oxley, FDIC and state exam audits that run almost non-stop throughout the year. Nicely's team believed that securing privileged accounts could help the institution pass its audits more easily.

To accomplish its goals, Heartland Financial looked for a solution to regularly update each of its privileged accounts with unique, cryptographically strong credentials. Privileged accounts exist in almost all IT hardware and software assets and hold elevated permission to access files, run programs, and modify configuration settings.

"Like many organizations, all of our machines were originally set up with the same administrator password," Nicely said. "This was done as a convenience to IT, but it unintentionally creates a huge security hole. For example, if a worm were to infect one computer then other machines on the network with the same password would be jeopardized as well. Frequently randomizing the passwords on individual systems can prevent that."

Heartland Financial first turned to scripts in an attempt to randomize administrator passwords, but soon determined that the approach was not reliably changing privileged accounts on all systems. The result was that some of the organization's mission-critical systems were left vulnerable.

The Solution

Nicely's team immediately began researching privileged identity management products and decided to evaluate Lieberman Software's Enterprise Random Password Manager (ERPM). ERPM continuously discovers, updates, stores, and enables secure recovery of privileged account passwords in the cross-platform enterprise. It automatically detects each location where privileged account credentials are used, including services, tasks, applications, and more. ERPM then secures these credentials and propagates the changes everywhere they exist in the enterprise.

"ERPM definitely fits our needs," Nicely said. "Its ease of use is a nice factor. We also like the flexibility of being able to schedule the frequency of password changes. Another feature that's very important to us is the ease of recovering our current passwords."

Passwords are secured in ERPM's encrypted data store using FIPS certified AES encryption. When authorized IT personnel need to perform routine tasks or emergency fire call repairs, ERPM quickly grants credentials through a web-enabled console, according to policies predefined by the organization.

Following the evaluation, Nicely decided to roll ERPM out to servers throughout the company.

> ***"Our biggest advantage is that our systems are now much more secure.***
>
> ***Controlling our privileged identities helps protect us against threats like malicious software. Another benefit with ERPM is the time savings and increased productivity compared to scripting."***

The Result

Heartland Financial is now regularly changing its privileged passwords on a scheduled basis – more frequently even than regulatory compliance mandates dictate.

”Our biggest advantage is that our systems are now much more secure,” Nicely said. “Controlling our privileged identities helps protect us against threats like malicious software. Another benefit with ERPM is the time savings and increased productivity compared to scripting.”

ERPM also assists Nicely and his staff with meeting the control and auditing requirements of its many compliance mandates. And now that ERPM is in production throughout the Heartland Financial enterprise, the organization can move to its next planned stage of deployment – managing service accounts.

“If there’s one thing that auditors look for it’s managing service accounts that have non-expiring passwords. This is a very complex task because of the difficulty involved in locating all of the service accounts dispersed throughout a large enterprise, as well as the potential for downtime to mission-critical applications if changes don’t account for every service dependency. But, ERPM will help us get there.”

About Lieberman Software Corporation

Lieberman Software provides privileged identity management and security management solutions to secure the cross-platform enterprise. By automating time-intensive administration tasks, Lieberman Software increases control over the IT infrastructure, reduces security vulnerabilities, improves productivity, minimizes business disruption, and ensures regulatory compliance. Lieberman Software pioneered the privileged account security market, having developed its first product to address this need in 1999. The company is headquartered in Los Angeles, CA with a support office in Austin, TX. For more information see www.liebsoft.com.

www.liebsoft.com | P 800.829.6263 (USA/Canada) P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152 | 1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067