



Large Federal Credit Union Turns to Lieberman Software to Help Mitigate Security Risks

Think you've got challenges? One of the largest credit unions in the United States – with approximately 218,000 members and over 40 branches located throughout the United States and Puerto Rico – works to secure depositor assets while maintaining high levels of customer service. While this institution's IT infrastructure undergoes major improvements to handle growing workloads and keep costs under control, the organization faces near-continuous, in-depth financial auditing that scrutinizes virtually every aspect of its IT operations.

"We are incredibly audit-driven," said the institution's Information Security Analyst. "We have many types of audits each year. They all touch IT in some way because of how deeply involved IT is in all of our business operations."

The Situation

To pass these frequent audits - whether it's the National Credit Union Administration, external financial audits, vulnerability assessments, or internal auditors - the credit union needs to demonstrate that it has secured the powerful privileged account passwords that exist on almost all of the institution's IT resources.

"We're proactive about closing any open audit issues," said the analyst, "and knew we needed something to get our privileged passwords under control."

Part of meeting this requirement was to secure the hard-to-manage service accounts that may not belong to specific users but still have privileged rights. These accounts exist in corporate email services such as Microsoft Exchange Server, database and line-of-

Customer Profile

The credit union was founded in the 1930's and has branches located throughout the U.S. and Puerto Rico with approximately 218,000 members.

Situation

To pass frequent financial and regulatory compliance audits, the credit union needed a privileged identity management solution that could locate and update all privileged account passwords and also manage service accounts.

Solution

Enterprise Random Password Manager was deployed to the credit union's cross-platform enterprise.

Result

The credit union has full control over its service account passwords and remains in compliance with its audits.

business applications, network management frameworks, and numerous others.

The credit union had relied on scripts to update some of its privileged passwords but the process had many limitations. Scripted changes could only be applied to known accounts, and it was nearly impossible to update service accounts using scripts because service interruptions could result if scripted changes failed to account for every service account dependency.



“The service accounts were too intertwined across the enterprise for us to even consider updating the credentials by hand,” the analyst said. “You’re talking about a lot of servers that each have multiple service accounts. You can change the passwords on those accounts, but the scripts can’t synchronize those changes everywhere they’re needed in the network. If you’ve got one service dependent on four others that are all running on the same password you’ve got to stop them all, change the password, and then restart them in the correct order. So the service accounts were essentially untouched. And the auditors noticed.”

The credit union needed an efficient solution, especially since it was in the midst of a significant datacenter redesign. The organization was transitioning to a virtualized environment encompassing the entire network of dozens of branches with a mixture of Windows Server, UNIX, and Citrix linked by Cisco network devices.

The Solution

The IT staff at the credit union began a search for a solution assuming that they would need multiple products from different vendors to change and store privileged account passwords and manage service accounts running in their virtualized environment. After researching the privileged identity management marketplace, the IT staff decided to evaluate Enterprise Random Password Manager™ (ERPM) from Lieberman Software. ERPM automatically discovers, updates, stores, and securely stores local, domain, and process account passwords in the cross-platform enterprise.

The credit union began its evaluation by deploying ERPM in its test environment. The IT group discovered that while ERPM was one of several products capable

of changing local account passwords, it is the only solution that can also reliably manage service accounts. Additionally, the staff confirmed that ERPM not only secures user, administrator, and process ID passwords, but also meets their requirement of securing sensitive files and documents in an encrypted data store using FIPS certified AES encryption. When the evaluation also demonstrated that ERPM – which is certified for Microsoft Windows Hyper-V – is fully functional in virtual environments, the credit union halted its evaluation and proceeded with a production deployment of ERPM.

“We looked at other products, but we weren’t willing to bring something in that didn’t manage service accounts,” the analyst said. “A lot of products change the local administrator passwords, but that’s only one part of the picture. When you add up ERPM’s service account management with its vaulting technology and virtualization capabilities, this was an easy decision for us. We needed something that could handle all of those requirements, and ERPM was the only product that qualified.”

***“Without ERPM, if someone were to crack one computer they’d essentially get the keys to every system.*”**

The fact that we can change those passwords frequently, and make each of them different, is huge.”

The Result

Following the test deployment, ERPM was put into production to manage cross-platform servers and workstations. The credit union chose Microsoft SQL as the ERPM back-end data store, though Oracle 11g is also available as an option.

“Every security professional will tell you that password security can keep them up at night,” the analyst said. “Without a privileged identity management solution, your systems will continue to share common local passwords because you can’t manually maintain or secure a list of all the passwords that would be required.”

The credit union is now frequently updating its privileged accounts, including the service accounts, with unique and complex passwords. As a result, the organization has strengthened its security significantly is also meeting its audit requirements.

“Not only are we now changing our privileged account passwords on a regular basis, but if someone – by some stretch of the imagination – were to crack a password, they would only get access to a single box. They wouldn’t be able to go anywhere else in our environment. Without ERPM, if someone were to crack one computer they’d essentially get the keys to every system. The fact that we can change those passwords frequently, and make each of them different, is huge.”

As for managing the organization’s service accounts, the analyst says, “The dependencies are no longer an issue. With ERPM we no longer have to manually stop and restart each service when we update the passwords.”

The IT staff also described how ERPM brings benefits of improved productivity and subsequent cost savings. For example, they estimated that without ERPM it took at least 10 minutes per system to change local administrator account passwords on each server in the datacenter. And the estimated total time of more than 10 IT staff hours for each change does not account for changes in service accounts that were required but rarely implemented.

“To find where all service account passwords exist and update each of them would take a good two to four weeks per change – and that’s assuming that you succeeded in locating them all,” the analyst said. “It’s like painting the Golden Gate Bridge – starting at one end, working your way to the other end, and then starting all over. Essentially by the time you were done changing service account passwords, you would have to start it all over again. ERPM automates that tedious, error-prone process for us.”

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.liebssoft.com.