

# Financial Services Firm Fully Automates Privileged Account Management with Lieberman Software

## Customer Profile

Founded more than a century ago, this investment and wealth management firm has nearly \$90 billion in assets under supervision.

## Situation

The firm needed to manage its service accounts to increase security, prevent lockouts and comply with GLB and other regulatory mandates.

## Solution

Lieberman Software's Enterprise Random Password Manager was deployed to systems on the company's cross-platform network to automatically find, track and secure privileged accounts - including service accounts.

## Result

The company is now fully automating all privileged identity management operations - significantly increasing security and easing regulatory compliance audits.

When you're a century-old financial services firm managing billions of dollars in customer assets, your IT staff faces the dual challenges of securing customer data and meeting strict regulatory compliance mandates. For this asset management company, that means complying with the Gramm–Leach–Bliley Act, among other regulations, while controlling access to clients' private financial information.

## The Situation

"Finance is probably one of the most heavily regulated industries from a compliance perspective," said the Vice President, Senior Information Security Analyst at the financial services firm. "The internal and external pressure to comply with Gramm–Leach–Bliley and other benchmarks like Sarbanes-Oxley are paramount. In fact, we hold ourselves to a higher standard than we are legally obligated."

A major part of meeting regulatory compliance requirements is the ability to secure and audit all of the powerful privileged accounts on the network. Privileged accounts grant the highest level of access in an enterprise because they can allow users to install hardware and software, configure systems, and maintain the IT infrastructure.

Included among these privileged accounts are difficult to manage service accounts. Service accounts cause a particular problem for IT because each credential can be referenced in multiple places. And, a password change on a service account can potentially cause lock outs and system failures if performed incorrectly.

The Vice President explains: "Like most companies, we have literally hundreds of service accounts. They run services on our Windows servers, and can be hard-coded into systems. According to agreements with our internal IT audit personnel, we are obligated to change the password on all of these accounts on an annual basis. When you add up several hundred of these accounts, the time and coordination needed to change a single password is overwhelming. We were drowning. And that's before even considering the security ramifications of having certain people know the password of accounts with elevated privileges. We needed a solution to limit that risk."

For a while the IT staff at the firm attempted to write scripts to manage their privileged accounts, including service accounts. However they soon realized that the many types of systems present in the environment, and the skill sets needed to write reliable scripts for each, were so varied that scripting was impractical.

The Vice President began searching for a commercial solution that would work on nearly 700 servers, 1500 workstations, and an assortment of SQL Server, Oracle, ESX and Linux accounts spread across the 15 physical sites at his company.

## The Solution

While attending a security conference, he learned about a privileged identity management product that seemed to meet the company's criteria. The product — **Enterprise Random Password Manager™ (ERPM) from Lieberman Software** — continuously discovers, tracks and secures all privileged accounts 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.

To learn if ERPM could achieve the organization's requirements, the Vice President arranged a product evaluation.

"We built a list of what we wanted ERPM to accomplish and how we wanted to test it," he said. "We then spent two days putting ERPM through its paces. It fit the bill perfectly. Service account management was the main selling point."

Another contributing factor in the purchasing decision was ERPM's ability to work across all types of accounts in large and complex enterprise environments.

"ERPM is very easy to use. The way it's designed, it doesn't really matter what type of account you're managing. If you understand the concept you can manage a SQL ID, an Oracle ID, and Active Directory account, or an IIS application pool. There's no real difference."

## The Result

Once ERPM was deployed to the production environment, the Vice President's staff immediately placed all privileged accounts — including service accounts — under the management of ERPM by default. Today no one, including IT personnel, knows the passwords for these accounts without first submitting an audited request.

"Let's say I deploy a server and I need a service account named 'security service'," the Vice President explained. "I don't know the password for security service. Only ERPM knows it. As an authorized user, I can access the password if I'm in a situation where I need to recover it to make repairs or configuration changes. ERPM will audit my use of the account. It then re-randomizes the password after use, so it really makes every service account a one time password."

In addition to controlling access to privileged accounts, the financial services firm's IT staff also relies on ERPM to regularly change all privileged account credentials.

"Before we had ERPM, our privileged password changes could easily take a couple hours," he said. "Now they just take a few minutes. Once we set up the password change job, we just make a copy of the job and schedule it to run. We're confident that ERPM is going to update the passwords for our privileged accounts, and all the places where the accounts are being used."

There was initially some hesitation among the IT staff about entrusting the management of all of its powerful privileged accounts to a new product, the Vice President said. But ERPM is now used on a daily basis throughout the company.

"At first people were scared to have a product hold 'the keys to the kingdom'," he said. "However, ERPM is now used heavily in our environment for many different things. For example, one of our groups had about 12 passwords they needed to store on a spreadsheet. So with the Password Spreadsheet Manager component of ERPM we uploaded those passwords as a management set. Now we can audit who recovered which passwords and why they needed them. That capability was unavailable to us before ERPM."

*"Before we had ERPM, our privileged password changes could easily take a couple hours. Now they just take a few minutes... We're confident that ERPM is going to change the passwords for our privileged accounts, and all the places where the accounts are being used."*

The ability to control and audit access to privileged credentials — and subsequently increase security and meet regulatory requirements — have been impactful at the financial services firm.

"By implementing ERPM, not only have we gained control from a privileged access perspective, we've also removed a good amount of local administrative privileges on our servers," the Vice President said. "With ERPM we can provide an authorized user with access to a privileged account when required, but without having to be a local administrator most of the time. We've really reduced our risk that way."

## Moving Forward

Now that ERPM is an integral element of his company's IT security and management processes, the Vice President is ready to expand the use of the product.

"We've already gotten more than our ROI out of ERPM. But there's more we want to do. There are still a lot of places in our company where passwords are stored in files, whether it be XML files or text files. We want to modify our code so that all passwords going forward are stored in the ERPM encrypted store. The code will have the ability to go to ERPM's encrypted store, grab the password it needs and continue."

He went on to say that a solution like ERPM should be a security imperative for any enterprise.

"If I left this company, no matter where I went, if they didn't have a privileged identity management product, that would be the first thing I'd implement."

## About Lieberman Software Corporation

Lieberman Software provides privileged identity management and security management solutions to more than 1200 customers worldwide, including more than 40 percent of the Fortune 50. By automatically discovering and managing privileged accounts everywhere on the network, Lieberman Software helps secure access to sensitive systems and data, thereby reducing internal and external security vulnerabilities, improving IT productivity and helping ensure regulatory compliance. The company developed the first solution for the privileged identity management space, and its products continue to lead this market in features and functionality. Lieberman Software is headquartered in Los Angeles, CA with an office in Austin, TX and channel partners throughout the world.

For more information, visit [www.liebsoft.com](http://www.liebsoft.com).



**LIEBERMAN**SOFTWARE

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  
© 2013 Lieberman Software Corporation.  
Trademarks are the property of their respective owners.