

Cloud-Based Analytics Provider Uses Lieberman Software Privileged Identity Management Solution to Secure Confidential Customer Data

Customer Profile

Based on the east coast of the United States, this company performs cloud-based analytics for Global 2000 corporations.

Situation

The company struggled with securing and managing password lifecycles for service accounts, as well as shared privileged accounts such as domain administrator. There was no quick and easy way to audit who was using privileged credentials and what actions were being performed with them.

Solution

Lieberman Software's Enterprise Random Password Manager was deployed to systems across multiple sites in the company's enterprise.

Result

Privileged accounts throughout the environment are now continuously located, tracked and secured; access to these accounts is audited and monitored; control over customers' sensitive data is maintained.

Look around your hometown and you're certain to find a favorite national retailer, restaurant chain, or financial institution that relies on cloud-based services from this leader in analytics. More than 75 of the world's largest corporations depend on this cloud service provider (CSP) to make more efficient use of corporate resources, improve the success rates of new product and service initiatives, and foster better customer relationships.

"Given that we're hosting confidential data on behalf of our clients, our reputation is everything to us. Anything we can do to enhance our security profile is highly critical. But we also have to think in terms of the future. How can we scale the business to thousands more servers?"

Such are the challenges that face the Senior Vice President (SVP) of Technology at this analytics CSP. Because when you're the analytics provider for many of the world's best-known consumer brands, protecting customers' proprietary data is an absolute imperative. Maintaining a reputation for leadership requires the CSP to employ automated, proactive security practices to help ensure the uninterrupted growth of its dynamic, rapidly expanding cloud service environment.

The Situation

For this CSP, securing and managing the password lifecycles for service accounts, as well as the many shared privileged accounts on the network, used to be a struggle.

Unless the organization took control of its powerful privileged accounts, its proprietary data was at risk of being breached through new, automated exploits that compromise shared privileged passwords. Meanwhile cumbersome, time-consuming manual processes to mitigate the threats were diminishing IT productivity.

"We were attempting to use a manual process that involved storing privileged passwords on two encrypted spreadsheets," said the SVP. "It was a management headache and it didn't give us fine-grained control over who was accessing the spreadsheets and how they were using the stored passwords."

The Solution

Aware that they needed an enterprise-level solution that could manage all of the privileged accounts on both physical and virtual systems in the company's multi-site network, while auditing access to these critical accounts, IT management began a search for a privileged identity management product. Their research led to Lieberman Software's Enterprise Random Password Manager™ (ERPM).

ERPM automatically discovers privileged accounts throughout the cross-platform enterprise, and then continually tracks and secures them. It helps protect an organization's most sensitive data by fully auditing administrative access to systems and applications in the IT infrastructure. ERPM specifically shows who had access to systems with critical data, at what time and for what stated purpose.

The CSP deployed ERPM to its internal test network for evaluation.

"The evaluation of ERPM was very impressive," the SVP said. "It seemed to be the perfect fit for us. In fact, we abandoned our evaluation of all other products based on how quickly we were able to get ERPM up and running."

Following the evaluation, the IT group rolled ERPM out to its production network.

"We ended up going with a VM architecture, realizing that having ERPM on a secure hypervisor was probably best for us from a resiliency standpoint," the SVP said. "We could go ahead and virtualize it and then deal with hardware needs as they arose. The VM approach also gives us a lot of security options as far as how we lock it down on the systems."

"With ERPM, we as an executive management team now have an understanding of what's occurring on our network, ensuring that people are taking the proper course of action."

The Result

The IT group immediately began using ERPM to change all of its service account, local administrator account and domain administrator account passwords.

"We chose ERPM for its ability to reach out and discover all of the privileged accounts on the network," said a systems administrator at the company who regularly uses the product. "So as soon as it was operational we could tell, for example, that these service credentials are in these locations. And, this local administrator account is running this scheduled task."

"But the other part is that once ERPM finds the privileged accounts, it then changes all of the credentials across the board very quickly. We have several dozen servers, so it would be miserable doing that by hand, he said.

The SVP went on to praise the time-savings advantages of ERPM. "For time and accuracy we pride ourselves on using automation to simplify the lives of our IT staff. We're very much opposed to manual processes if they can be avoided. The key point of ERPM for us is that it automates what would otherwise be days of work into a single click of a button."

Now that ERPM has accomplished all of the company's initial IT security and management objectives, the SVP envisions the product becoming an important part of the company's strategic business operations.

"ERPM adds significantly to our ability to monitor and maintain all of the systems in our enterprise," he said. "For example, we can now understand that system admin John Doe accessed a certain password. We can see what he did with that credential - if he modified or installed something. With ERPM, we as an executive management team now have an understanding of what's occurring on our network, ensuring that people are taking the proper course of action."

About Lieberman Software Corporation

Lieberman Software provides privileged identity management and security management solutions to more than 1000 customers worldwide, including 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.liebssoft.com.



LIEBERMAN SOFTWARE

www.liebssoft.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.