Leiberman RED Identity Management [EOL]

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

Leiberman RED Identity Management [EOL]

Read 1 reviews of Leiberman RED Identity Management [EOL]

Review by a Real User

Verified by IT Central Station

Cyber Security Engineer at a recruiting/HR firm with 51-200 employees

CyberSecurity33

WHAT IS MOST VALUABLE?

Randomizing local accounts on all endpoints ERPM's greatest ability is that it can easily randomize ALL local accounts on almost any endpoint. One of biggest security risks that occur within a company is the ability of an attacker to compromise one system and then use similar local accounts to slide horizontally through an environment. Many organizations will use group policy to change the local admin account and even change the password as well. The problem with this is that every Windows system will have the same name for their local admin account and most likely, have the same password for every one as well. If an attacker is able to compromise one system, then there is a high likelihood that they will be able to compromise multiple systems within the environment as well from these local accounts. By randomizing local accounts, ERPM is able to keep local account passwords from becoming stale. Depending on the company's policies, it might be required to change all passwords every 30 days, 90 days, 180 days, etc... Without a tool to randomize all of these accounts, then trying to do this manually or remotely would be extremely difficult and time consuming. By setting up jobs to do this within ERPM, I do not have to do anything other than check a report to make sure all of my systems are being randomized. Service accounts normally have heightened permissions on servers, workstations, and throughout a company's environment. However, service accounts are also forgotten about and do not have their passwords changed very often. Before we started to crack down on service accounts in my environment, we had passwords for service accounts that were several years old. The only caveat to this is that for ERPM to change the password of the service account and then push it to the locations that it is being used, the service account must be available via a COM object, service, a task or other Windows functions. If the account is embedded within a program, either an API must be written to change the password from within the program, or the password must be manually changed. Using ERPM to change ALL Service Account passwords is not ideal or always possible, but it does help with many accounts; and can give an auditor insight into how old a password is and where it is being used within your environment. Randomizing accounts that have elevated privileges in the domain: Since most IT administrators must have the ability to perform maintenance, install programs, and other tasks on servers or sensitive systems, they normally have admin rights on these systems or domain admin for an entire domain. This makes the IT group a VERY high target for attackers since most company's IT admins use their normal computer account to access servers as well. In order to have a clear segregation of a 'user' account and a 'server' account, we removed ALL permissions for a user's account from all servers, appliances, or sensitive systems and created 'server' accounts to access these sensitive systems. In order for an admin to access a server, sensitive system, or appliance, they must 'check out' the daily password for their server account and then use that account to perform their daily duties. If an attacker were to compromise an IT admin's normal account, they would only have access to that computer and would not be able to navigate through the environment with heightened permissions. Even if an attacker were to get local admin on one server and tried to dump the hashes to try and grab stored accounts for other users, these passwords would be no good since the password gets randomized every 24 hours. This has actually saved us during one of our third-party penetration tests where the tester was able to get onto a server using a compromised service account that ONLY had rights to that one server. Even though the tester dumped the hashes from the

registry, all of the account's passwords were old and were not able to be used. This kept the tester from obtaining domain admin within our environment. Now, the tester could have sat on the server and possibly grabbed credentials from memory from a user that logged on later using mimikatz or another tool, but this would have taken more time and resources.

HOW HAS IT HELPED MY ORGANIZATION?

RDP Admin Checkouts Removing hard-coded credentials from most of our built-in Apps

WHAT NEEDS IMPROVEMENT?

One of the features that ERPM is capable of providing is giving users the ability to 'request' admin credentials on their machines for a specific purpose (provided you have removed all users from local admin on their machines). You can force them to put in descriptions or ticket numbers for logging when they want to check out an admin password but keeping the backend configured properly, so that users can ONLY see their assigned computers is rather difficult. My company is only around 600 users, so manually assigning users to specific computers is not too difficult but if my company was larger with several thousand endpoints, it would be almost impossible. Fortunately for me, we have spent time so that our CMDB is up-to-date. I can export the active computers in my network with the users who are assigned, and then import them into ERPM. I know some ERPM admins have to compromise by allowing users to see a 'group' of computers so that assignments can be by a group of computers instead of one to one but, to do it properly, you only want the user to have the ability to see ONLY their computer and nothing else. Also, you want to make the checkout experience as seamless as possible for the end user, so having only their computer show up makes it easier for them to navigate the web program. This is not a huge issue, but something that would be nice in future releases.

FOR HOW LONG HAVE I USED THE SOLUTION?

I have been using it since February 2013.

WHAT WAS MY EXPERIENCE WITH DEPLOYMENT OF THE SOLUTION?

If you have multiple domains, DMZ's, or segregated subnets that cannot talk to the ERPM server, then setting up Zone Processors will be necessary. This has become easier to deploy but making sure the proper ports and permissions are given to the system that the Zone Processor exists can be a little time-consuming. Also, if the server that the Zone Processor exists has any issues, this can/will cause the Zone Processor to have communication issues with the ERPM Server. If the Zone Processor is not communicating, then any job that needs that Zone Processor will not work. To help avoid this, we added the 'Restart Service' to every Zone Processor Service and we also monitor these Services using Solarwinds. If any of the Services restart or fail all together, then we are alerted via Solarwinds. This has helped our ability to have confidence that the Zone Processors are always up and operational.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

Stability is not necessarily an issue since your purchase comes with a DR license for another management server. However, I have never had an issue with the program causing issues alone. The only actual issue I have had is, when the jobs run to randomize accounts, it can get stuck on a system and the job never completes. However, this is able to be mitigated by the Heartbeat setting that will allow forcing a job to stop scanning a specific system if it has not finished or shown any changes over x amount of time. Also, we use High Availability (HA) for every aspect of the program. The ERPM solution can sit entirely on one server, which is absolutely what you DO NOT want to do. So, we set up two web servers that use a load balancer to redirect incoming requests to the server with the least amount of work. Both of the web servers talk back to two separate application servers; which gives us not only HA but also redundancy if one of the servers goes down. The application servers then point to what could be considered a ‘single point of failure’, which is the SQL Server Database. However, we have active mirroring to our DR site that allows ERPM (which has to be configure in the ERPM DB Setup) to automatically switch to the DR database if the primary SQL Server is unresponsive for a certain amount of time. We also have our DR instance of ERPM that the load balancer will automatically switch to if both of the primary web servers are down.

Leiberman RED Identity Management [EOL]

Read 1 reviews of Leiberman RED Identity Management [EOL]

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

We encounter little scalability issues. The biggest issue was setting up the Zone Processors so that I could minimize latency in our remote locations and also use the ERPM solution to randomize endpoints in other domains. The process for setting up Zone Processors is simpler than it used to be, but you must have everything mapped out and know where you need every item before you start deploying ERPM to every endpoint.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Customer Service: I would give a 9/10. Whenever I have had any questions or issues with licenses or renewals, the Lieberman team has always assisted and fixed any issues extremely quickly and professionally. Technical Support: Technical support is 9/10... I have never had an issue with their support. Anytime I have had an issue, they have responded to my emails within minutes, which is faster than the call times for many vendors. If my issue is critical, then I will call and escalate the issue as quickly as possible.

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

This was our first PIM solution.

HOW WAS THE INITIAL SETUP?

For Windows-based systems, the setup is relatively straightforward. You will need an account that has the ability to change passwords or manage any endpoint that you want controlled by ERPM. For accessing other operating systems, it can be a little more challenging. It took some configuring, but we are also randomizing the built-in accounts for our IDRACs, ESXi Hosts (which they just started offering), and some of our more prominent printers. We do not do ALL of our printers because every printer requires a different Response File to do the call to randomize the password. However, if you can annotate how any system authenticates into the underlying OS, then you can build a Response File that can do the randomization call.

WHAT ABOUT THE IMPLEMENTATION TEAM?

Make sure to scale implementation before purchasing any licenses. Know what systems and endpoints you will use this solution for and the location of those endpoints; so, the proper number of licenses is purchased and the number of Zone Processors is known beforehand. The Zone Processors are used to randomize systems that are in different locations (another country and you want to minimize latency) or in a DMZ. As long as you open the proper ports for the Zone Processor to talk back to the ERPM application, a Zone Processor can be placed almost anywhere and does not have to be a member of the ERPM application's domain.

WHAT WAS OUR ROI?

Unknown. It was a significant upfront cost but I believe that the amount of malware that has been blocked and possible infections that have been avoided due to randomizing the accounts truly outweigh the cost of the product and yearly maintenance renewals.

Leiberman RED Identity Management [EOL]

Read 1 reviews of Leiberman RED Identity Management [EOL]

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

Make sure you know exactly what endpoints will be utilized for the solution. The only difference in price is between Standard Endpoints (Windows workstations, Linux, Cisco, etc...) and Servers (Microsoft Server 2008, 2012, etc...). Make sure you know if you are going to use this on just servers and workstations or if you will also include network devices, printers, IDRACs/ILOs, VMware ESXi and others.

WHICH OTHER SOLUTIONS DID I EVALUATE?

Cyber-Ark

Learn more: Read 1 reviews of Leiberman RED Identity Management [EOL]