A Solution for Managing Privileged Access

Today's threat environment demands a secure framework for remote access management

WHITE PAPER

TABLE OF CONTENTS

What problems do PAM solutions solve? 2

A necessity, not a luxury 2

Password management essentials 2

PAM help for the enterprise 2

PAM @work 3

Wresting order from chaos 3

A common PAM thread 3

If you are an IT or security specialist in a typical smaller organization, the following scenario will probably have a familiar ring.

A need arises to access some remote servers and virtual machines, each with unique passwords. These machines and the various domains stored on them are accessible by different privileged users. The IT sys-admin knows some of the passwords and some of the users, but not all of them. Emails are sent, phone calls are made, Excel spreadsheets and even yellow sticky notes are parsed. Eventually IT gains access to the remote servers, but not before a lot of valuable time is consumed. And perhaps more important, this process does not occur with the kind of military-grade security practices that today's hyper-dangerous threat environment demands.

This is the typical fire drill that so often arises today in small and medium-sized businesses lacking an effective, user-friendly privileged access management, or PAM, solution. And, as will be shown, there are a number of factors and dynamics at work, making it all the more important for SMBs to have just such a PAM solution in place.

Devolutions Remote Desktop Manager

TechTarget | Custom Media

In contrast, most enterprise-class organizations have had PAM solutions in place for some time, either of a homegrown variety or one of many purchased from leading PAM vendors. But these comprehensive PAM solutions, which are way beyond the financial means and technical expertise of most SMBs, have their own issues. Most notably, they often are complex and not user-friendly.

While there are specific PAM solution needs across all sizes of organizations, those needs differ. What organizations do share are the same drivers for PAM solutions, as well as the same security risks of not having a workable one in place.

WHAT PROBLEMS DO PAM SOLUTIONS SOLVE?

Hackers and the tools at their disposal are becoming increasingly sophisticated, making it easier for them to crack into networks and steal domain administration account credentials. These can be the keys to the data kingdom and the pathway to data destruction, data theft and, in general, a world of hurt for the organization attacked.

Simply put, the goal of PAM solutions is to make it very hard for hackers to get this prized access to privileged user accounts. PAM solutions further boost network monitoring while improving overall network visibility for sysadmins and providing more fine-grained controls at their fingertips. Such solutions offer real-time knowledge of just who the privileged users are and what they are doing across the entire remote computing environment.

The better PAM solutions also automate the process of randomizing passwords and then managing them in a highly secure vault, which also can house other credentials for various service and application accounts.

A NECESSITY, NOT A LUXURY

Seen this way, PAM solutions are an essential element of secure remote user and remote server environments. They allow organizations, including SMBs, to effectively monitor and manage privileged accounts and access, which not only enhances protection of critical data assets, but helps businesses meet compliance requirements as well.

Make no mistake, PAM is not a solution in search of a market. Rather, the fast-growing interest in PAM, particularly among SMBs that formally thought them unnecessary or too costly, is being driven by strong forces, including:

- The distinct uptick in the sophistication, frequency and destructiveness of cyberattacks on organizations of all sizes, including SMBs targeted by spear phishing and ransomware attacks.
- The belief by attackers that many SMBs have not adequately protected privileged account and remote server access.
- Increasing regulations and compliance rules that mandate better audit trails and proof of data security efforts, such as PAM solutions.
- The growing instance of third parties—such as contractors and cloud providers—being granted privileged user access.

PASSWORD MANAGEMENT ESSENTIALS

Remote access by definition involves usage and sharing of passwords. It is in this area that many SMBs fall far short in taking relatively simple steps to shore up gaping holes in security defenses. One major study found that 63% of confirmed data breaches involved weak, default or stolen passwords.[1] Another recent study determined that 20% of business users either use very weak passwords or routinely share passwords, both of which make such passwords relatively easy to hack.[2] The study also found that SMBs with higher than average percentages of compromised passwords similarly had higher than average percentages of shared passwords.

The remedy is a comprehensive password management system. **The better ones** generate random complex passwords and feature a secure vault that stores all passwords and credentials. Users need not remember any of these machine-generated passwords, and sysadmins using shared passwords for remote access never see the actual passwords, as they are brokered by the password management solution. Thus, these password management systems accomplish the dual task of syncing various passwords needed for remote access without getting in the way of overall productivity, all in a highly secure manner. As a side bonus, SMBs adopting password managers for the first time often find that help desk calls almost immediately are reduced, as users no longer phone in looking for forgotten passwords.

PAM HELP FOR THE ENTERPRISE

PAM solutions have been fixtures in enterprise-class organizations for years. Typically, they are comprehensive,

1 "2016 Data Breach Investigations Report," Verizon, 2016
2 "35% of LinkedIn Users' Passwords Are Weak Enough to Hack," TechRepublic, March 13, 2017

complex, expensive and often not particularly user-friendly. However, many of the makers of these enterprise-grade systems are now partnering with PAM providers targeting SMBs with more user-friendly solutions, seeking to integrate the best of both worlds. In looking at such integrations, enterprises should first check that the latter solutions integrate with a broad list of technologies, including virtual private networks (VPNs), credentials managers, Secure Shell (SSH) protocols, virtual network computing, Remote Desktop Protocol and all personal password managers.

PAM @WORK

The IT team at Siemens Building Technologies (SBT) in West Sacramento, Calif., was continuously facing problems associated with remote connection management for the 30 servers the team supports. It had no way of securely organizing and managing shared connections to customer sites, and sharing credentials with customers' servers was clumsy, difficult and therefore costly.

Fed up with the failings of an incumbent remote connection manager, the senior programmer on site downloaded **a free trial** of another PAM solution, which quickly led to purchasing a license for the solution. Today, the IT team at SBT can securely manage connections and credentials in a way that is easy to update, share and protect.[3] No longer do team members email connections or store them in a network location, or text credentials back and forth.

WRESTING ORDER FROM CHAOS

Meanwhile, a world away in Slovenia, engineers and the IT team at EM-Soft Sistemi had been storing credential data locally on a designated computer. That meant repopulating all credentials elsewhere in case the computer failed or needed to be replaced. They also could not access credential information away from the home office, and they were using a confusing hodgepodge of tools for different devices and connection types.

After trying various PAM tools, all with poor results, the team settled on a remote desktop manager solution that now securely stores credentials for different users in a centralized vault.[4] The credentials can be securely accessed via the cloud from any desktop or mobile device. IT now controls all firewalls, switches and services from a single console, and a single, user-friendly application is used for all types of connections.

A COMMON PAM THREAD

What these diverse companies **and many others** have in common is praise from strong results using PAM solutions from Devolutions, whose flagship **Remote Desktop Manager** is deployed today by more than 300,000 users in 130 countries. A hallmark of the Devolutions solutions is a highly secure vault for secure storage of passwords and credentials.

In addition, the Devolutions PAM tools are designed to work with the broadest array of VPNs, SSH tunnels and personal password managers. A veritable Swiss Army knife for security and IT professionals in both SMBs and enterprises, Devolutions' PAM solutions solve the central challenges surrounding secure privileged access.

To learn how remote desktop management solutions can help sysadmins do their job better and more efficiently, read Top Five Features to Look for in a Remote Desktop Management Solution.

3 "Case Study: Siemens Uses RDM to Sync Up Its New Connections Automatically in a Shared Database," The Devolutions Blog, Jan. 10, 2017

4 "Case Study: EM-Soft Sistemi Chose RDM as Their Centralized Repository Solution to Store Their Credentials," The Devolutions Blog, Oct. 26, 2016