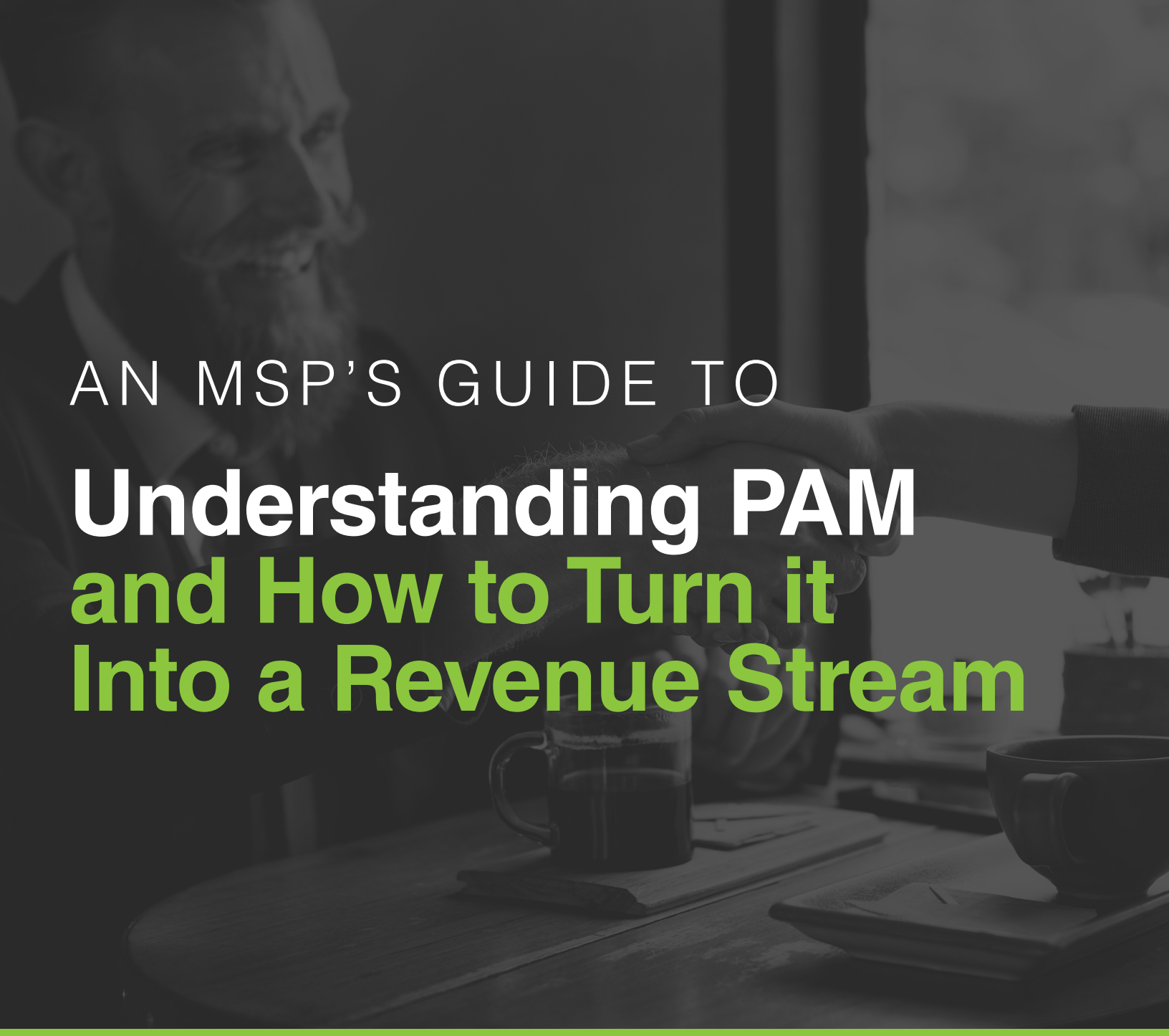

AN MSP'S GUIDE TO

Understanding PAM and How to Turn it Into a Revenue Stream

thycotic

An MSP's Guide to Understanding PAM and How to Turn it Into a Revenue Stream

$800 MILLION

Gartner estimates the current global PAM market to be $800 million to $1 billion, with around 40% of that market in EMEA

- 2016 Gartner Market Guide for Privileged Access Management

WHAT ARE PRIVILEGED ACCOUNTS AND WHAT THREATS DO THEY REALLY POSE?

Privileged accounts are how administrators and technicians log into servers, switches, firewalls, routers, database servers and the raft of other applications and devices that they need to manage on a daily basis. Importantly, they are also used for non-human operations like service accounts and system accounts.

Privileged accounts allow unrestricted management access to hardware and software and exist everywhere in nearly every connected device, server, hypervisor, operating system, database or application, both on-premises and in the cloud. This means an individual company could have hundreds of different privileged accounts within its network. Consequently, managed service providers (MSPs) will likely be handlings multiples of that.

To make things more complex, many of these accounts are for devices – such as network routers etc – that fall outside of the Windows domain and by default allow simple username/password combinations to log in. This all adds up to a serious headache for IT administrators and MSPs, and means that privileged accounts represent one of the most vulnerable aspects of an organisation's IT infrastructure if not managed properly.

PASSWORD BEST PRACTICE

As an MSP, the first thing you have to do when adding a new device or application to any of the networks you manage is to change the admin password. Once you've done that you then need to store that password somewhere so that it can be easily accessed when required. The most

common method for doing this is to list them all in an Excel spreadsheet – unfortunately, this is also the most insecure method, even if the file is encrypted.

You also need to ensure that all passwords adhere to the individual company security policy, not just in terms of strength but also in terms of the frequency with which they are changed. While many companies may follow protocol with regard to user passwords and server access passwords, the less obvious things like routers and switches too often get overlooked.

Not only can managing all these accounts be a full-time job, it can also leave you vulnerable to human error or abuse. And that's before you even get into tracking how they're actually being used.

PROTECTING PRIVILEGED ACCOUNTS IS CRUCIAL

If your (or your customer's) privileged accounts are compromised, malicious attackers with full administrative access are able to do much more serious damage to the business than with ordinary accounts. With administrative access, an intruder can move through a company's networks at will. They also have the ability to affect business-critical applications and infrastructure while doing so.

Ransomware also requires access to privileged accounts to enter networks and encrypt data. Without access to the wider network the malware can only encrypt a portion of the data that is native to the machine that has the infection. While this is not good, it's far better that having an attack spread across an entire network.

Understanding how a malicious user can obtain privileged access is the first step to protecting yourself. Most often, privileged account credentials are either accessed as the result of direct hacking or can be usurped from users by social engineering – attackers constantly target static, weak passwords that grant them elevated privileges.

DON'T JUST TAKE OUR WORD FOR IT...

Nine out of 10 participants at the Black Hat conference told us it is often very easy to find privileged account details[1] On top of this, the 2017 Verizon Data Breach Investigations Report (DBIR) found that 81% of breaches leveraged legitimate user passwords and other credentials to breach systems – up from 63% the previous year[2].

81%

OF BREACHES

leveraged legitimate user passwords and other credentials to breach systems – up from 63% the previous year

- 2017 Verizon Data Breach Investigations Report

30%

of new PAM purchases will be delivered as a service or run in the cloud

-2016 Gartner Market Guide for Privileged Access Management

This confirms that privileges are the primary method to conduct a successful attack and that the methods to get them are primarily through hacking techniques. The DBIR also highlights that 14% of breaches were the direct result of privilege misuse. Privilege misuse was also the third most popular attack vector, and the number two incident pattern in 20162.

Another stat from the same report indicates that 81% of privilege misuse breaches were carried out by an insider2. With misuse of privilege being one of the top ways attackers gain access to sensitive data, companies need to be proactive and get their privileged accounts under control.

If your own admins turn against you it is much more difficult to contain as they already have all the privileges they need. This is where a Privilege Account Management (PAM) system comes in.

HOW PROPERLY MANAGING PAM CAN MAKE A DIFFERENCE TO AN MSP

When looking at PAM, MSPs need to consider things from two distinct angles.

- Managing Privileged Accounts
- Offering PAM as a Service

Firstly, they should follow the right process within their own businesses. Each customer managed by an MSP may at any point ask the question: "how do we make sure that the people who manage our infrastructure and maintain our information are not abusing it?" This will become even more important to companies when GDPR (General Data Protection Regulation) comes into effect next year. **Under these regulations, if someone accesses data without authorisation this is considered a breach even if this was a privileged user trusted by organisation, and they have to declare it.** PAM can also be used to help organisations comply with regulations such as SOX, PCI DSS, HIPAA, Basel II, MASS Regulation 201 CMR 17 and ISO/IEC 27002.

By employing a PAM system, MSPs can ensure that they have the right level of access and authorisation to do their job. They can also use it to enhance the level of trust between themselves and the customer, through functionality such as the ability to automatically update and change passwords to make systems as secure as possible.

Secondly, MSPs can provide PAM as a Service to their customers. Businesses have a need to not only secure their privileged accounts, but also understand who is accessing their systems and when, as well as what they are doing while they are accessing it. PAM is the enabler for this level of insight and a crucial tool for accurate network auditing.

PAM removes the hassle of manual privileged access account management, by enabling networks to be scanned and privileged accounts to be uncovered automatically – once uncovered these accounts can have company security policies applied to them to ensure they are all compliant. The management and updating of these passwords can then be handled automatically. A full PAM system will also allow you to secure all these passwords within a vault so that admins/techs only need to access one system to gain access to the different system they use.

All information stored within the PAM system is encrypted, and role-based access controls can be put in place to ensure that only authorised people can access specific systems. All activity within the PAM system is tracked, so the company knows who has accessed what system and when. Within certain accounts, or to protect highly confidential information, video capability can be employed to record everything any users are doing while accessing those specific privilege accounts.

For both the MSP and the organisation this will also dramatically improve not only their security posture but also their performance – instead of taking 30 seconds to log into a server, admins/techs can gain access to the systems they need with a single click. This difference can be dramatically summarised across a year. One of our customers found that their admins were logging in 50-70 times a day, with a PAM solution in place they saved the equivalent of 4.5 full time employees.

There are also major cost savings to be made in relation to password management. In the event of a breach threat or a breach, an IT admin leaves or passwords on privileged accounts need to be changed for any other reason, this can be done automatically in a fraction of the time it would take for the process to be done manually by a technician.

VALUE OF PROPER PAM MANAGEMENT TO MSP'S:

- Ensure that they have the right level of access and authorisation to do their job
- Provide PAM as a Service to their customers
- Remove the hassle of manual privileged access account management
- Ensure admins/techs only need to access one system to gain access to the different system they use
- Securely encrypt all information in the PAM system

SELLING PAM TO YOUR CUSTOMERS

For some customers it may be enough to highlight the financial and transparency benefits, but if you need more ammunition, the following use cases will help bring home the importance of having a solid PAM system in place.

1. AN ADMIN LEAVES THE COMPANY

If one of the company's admins leaves and has access to the Excel spreadsheet or password vault that the company is using, they can easily take all their passwords with them. With a PAM system in place their access to the central access point can be immediately revoked and if necessary all passwords in the system can be automatically updated. Their supervisor can also view the admin's activity over the past six months to see if any suspicious activity has taken place, and appropriate action can be taken.

2. REDUCING COMPANY EXPOSURE

If a company admin has access to 50-100 privileged accounts, either stored in an Excel spreadsheet or a key vault, then that admin becomes a weak point within the organisation's security. The truth is some admins don't realise the power they have, they may manage servers but don't know how sensitive the data is on those servers. If the bad guys can figure out who has access they can target the admins through social engineering (or in really extreme cases kidnapping) in order to get access to privileged accounts and sensitive company data. A PAM system will ensure admins don't know all passwords, they just know their normal user password. So, if something were to happen they can only expose their own password, which reduces the company's exposure.

3. MANAGING SERVICE ACCOUNTS

Very often, service accounts don't have robust processes to change passwords. Often they are hardcoded into systems and difficult to change. This means they typically remain unchanged, leaving systems open to abuse. A PAM system can enable you to control access to these accounts in the same way you would all other accounts, removing this as a potential point of weakness within your network.

4. SECURING LOCAL ADMIN ACCOUNTS

Every single desktop has to have a local admin account. In many companies, due to the number of machines these accounts use the same password across the whole organisation – plus invariably this password is either guessable or easily hacked by someone using the latest password hacking technologies. PAM enables you to manage these accounts more effectively by running a scan across the entire infrastructure, identifying the individual desktop admin accounts and then setting unique and compliant passwords for each machine. This makes it extremely difficult for one infected or breached machine to become a single point of failure for an entire organisation.

5. PROTECTING EXTREMELY SENSITIVE DATA

Very often, companies will have certain servers that contain data that is more sensitive than others. These servers require additional controls to ensure integrity and security. They may trust their service provider, but occasionally service providers need to bring in additional third-party support. Using a PAM system means that all access can be controlled by a central supervisor – or group of supervisors – so that access can be granted on a case-by-case basis. Once approved access can be granted, removing the threat of people getting into the network who aren't supposed to be there, giving companies much greater visibility into who is doing what in their networks and where.

6. WHO'S WATCHING IT

With internal threats representing 81% of privilege misuse breaches, according to Verizon2, all companies would be wise to ask the question "who is watching IT?". Who does know exactly what admins are doing while they have access to systems. A PAM system will provide companies with peace of mind, as they can record each session and have video evidence of what is going on when admins are on their servers.

OPTIONS FOR MANAGING PAM

If you've managed to sell your customers the concept of PAM, the next step is to ensure they get the right deployment. This essentially amounts to two options:

ON-SITE STANDARD ARCHITECTURE

Here the company buys the PAM subscription, which is run on their individual servers. This is suitable if they don't want to share any passwords with anyone and want to have ultimate control over who accesses what on their server. The MSP can still manage their systems but ultimate control rests with the company itself.

OFF-SITE OR CLOUD-BASED ARCHITECTURE

This deployment allows MSPs to manage multiple customers from their own PAM system. The MSP PAM server is fully protected and each customer is isolated. The MSP simply installs a unique agent on its customer's server that enables the PAM system to run.

With our own system we focus on ultimate flexibility for the end customer, we can provide the service and technical architecture that the customer needs.

CONCLUSION

It's important to remember that PAM is not a simple vault where you store your passwords. There are a lot of products on the market that claim to offer PAM but actually just offer passwords storage. What sets a full PAM system apart is the management side; the ability to find passwords, change them, define them, apply workflow and video record sessions.

And the PAM market is growing. Gartner estimates the current global PAM market to be $800 million to $1 billion, with around 40% of that market in EMEA. According to The 2016 Gartner Market Guide for Privileged Access Management, by 2019, 30% of new PAM purchases will be delivered as a service or run in the cloud (up from less than 5% today)[3]. This growth suggests that the need for managed virtual infrastructure and cloud services will become more critical.

There are core pain points on both sides of the fence that need to be addressed...

FOR
MSPS:

- Ensure they can share passwords across teams to enable them to do their jobs more effectively
- Ensure only authorised people can access systems
- Ensure technicians' activity is logged and monitored
- Boost trust with customers

FOR
COMPANIES:

- Ensure whoever is managing infrastructure can provide audit controls
- Ensure good practices around privileged account management
- Ensure they know who has access to their infrastructure
- Ensure trust between suppliers

Growing businesses require a mature focus on protecting their network and data from crippling threats that take advantage of unmanaged privileged accounts to gain undetected access to the network. By implementing a PAM system you are helping your customers not only become more efficient but also dramatically improve their security posture.

Sources

1. Thycotic Black Hat Report https://thycotic.com/resources/black-hat-2017-survey/

2. 2017 Verizon Data Breach Investigations Report (DBIR) can be downloaded at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

3. The 2016 Gartner Market Guide for Privileged Access Management can be downloaded at https://www.gartner.com/doc/3398617/market-guide-privileged-access-management

To find out more about how Thycotic can help both your MSP business and your clients' business, visit www.thycotic.com or call +44 (0) 1777-712603