SILVERLAKE MASTERSAM INDUSTRY SOLUTIONS HEALTHCARE

Revised 2020

This paper aims to explore how Privileged Access Management solutions from Silverlake MasterSAM can effectively address the Cyber threats faced by Healthcare industry

PAM for Healthcare Industry

Contents

Executive Summary 2
An Overview of PAM 3
Influence of Government in PAM Implementation 3
Support in Partners in PAM Implementation 3
What are the Challenges to Healthcare Services? 4
Highly Regulated Compliance requirements 4
IT Outsourcing 4
Privileged Users Are Unavoidable 5
Financial Impact 5
Tracing The Cyber-attack Chain 5
Key drivers of PAM 6
How Silverlake MasterSAM helps 7
Sample Use Cases 9
Use Case 1: Privilege Access 9
Use Case 2: Password Retrieval 9
Use Case 3: Surveillance, Review and Alert 9

Executive Summary

Hospitals have increasingly become a prime target for cyberattacks, often likened to the “dinosaurs of cybersecurity.” The vast and open infrastructure of healthcare organizations, coupled with the rapid adoption of connected medical devices, has left significant gaps in security. Despite the shift to electronic medical records (EMRs), cybersecurity has not always been prioritized, exposing healthcare systems to heightened risks.

The healthcare industry now accounts for over 34% of identity theft breaches, making it one of the most vulnerable sectors, second only to the business industry. The need for robust Privileged Access Management (PAM) solutions is more critical than ever. By implementing PAM, healthcare organizations can:

1. **Protect Sensitive Data**: Safeguard patient information and medical records from unauthorized access.
2. **Mitigate Insider Threats**: Limit access to critical systems and ensure accountability through detailed activity monitoring.
3. **Streamline Compliance**: Meet stringent regulatory requirements such as HIPAA, GDPR, and other healthcare-specific standards.
4. **Secure Connected Devices**: Provide enhanced protection for the growing ecosystem of IoT and medical devices.

In an era where cyber threats are becoming increasingly sophisticated, adopting a comprehensive PAM strategy is essential to safeguard patient trust, ensure operational resilience, and maintain compliance with regulatory mandates.

An Overview of PAM

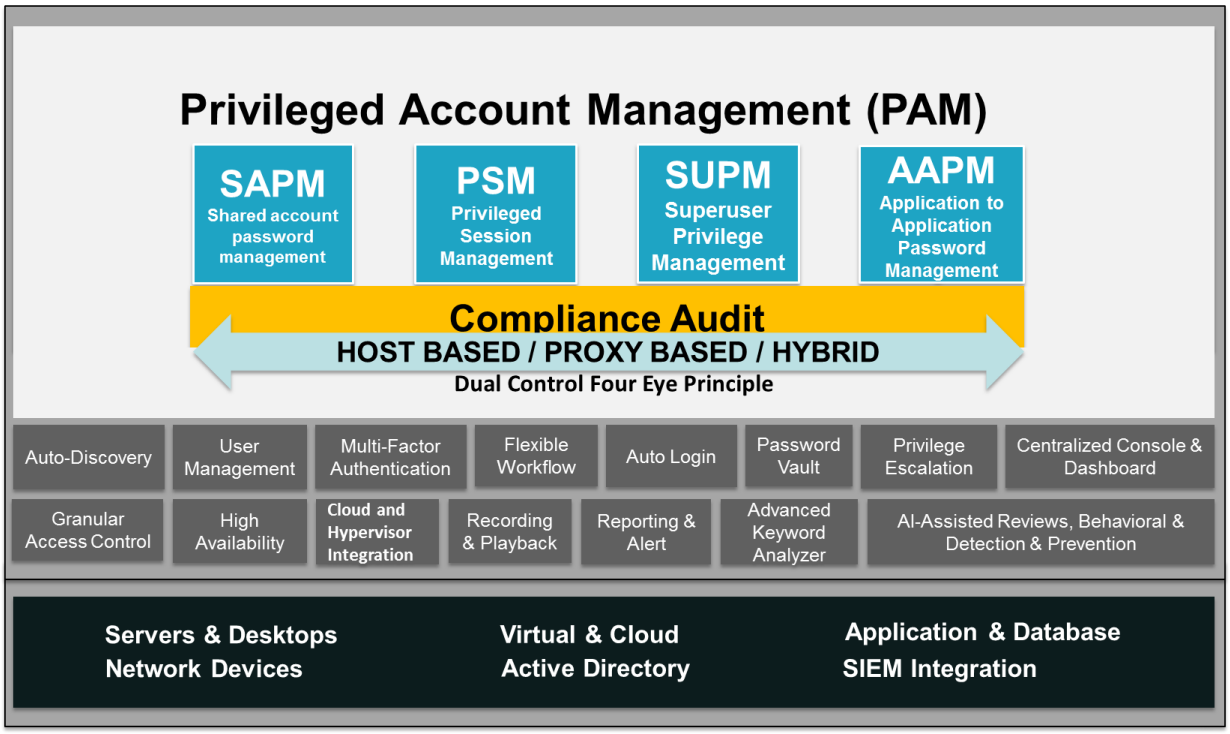
Privileged accounts are valid credentials used to gain access to systems containing sacred, proprietary information. Unlike non-privileged accounts, they also provide elevated access to the underlying platform normally restricted to standard users.

INFLUENCE OF GOVERNMENT IN PAM IMPLEMENTATION

Industry expert Gartner predicts that by 2017, more stringent regulations will lead to a rise of 40% in fines and penalties imposed by regulatory bodies. In addition, by 2018, 50% of organizations will use authentication methods other than passwords for administrative access, up from 20% in 2015. On the other hand, limited regulatory requirements in developing regions are slowing down the adoption of PAM in these regions. The influence of the government is never one to be underestimated and is set to grow.

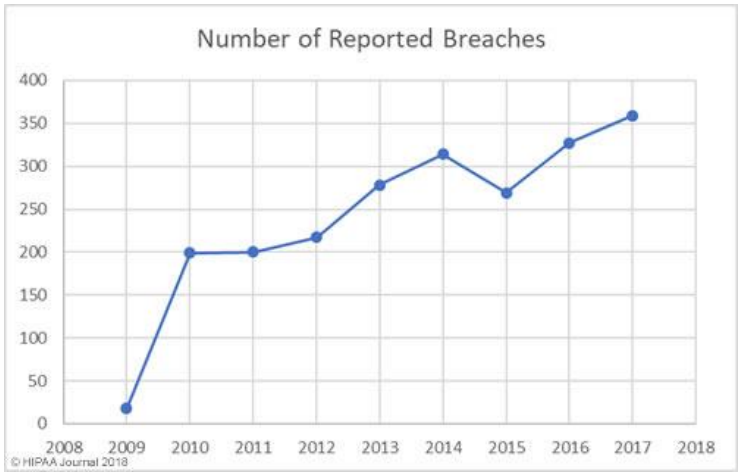
SUPPORT IN PARTNERS IN PAM IMPLEMENTATION

Partners of PAM vendors enable expertise from both parties to pool their offerings and meet greater customer needs within a short period of time. This is increasingly becoming more relevant as the PAM market matures, existing PAM customers are looking to more scalable solutions as the organization expands and offer integration with help desks and cloud support to increase productivity. Examples of partners include: resellers, distributors, managed service providers and technology partners.



What are the Challenges to Healthcare Services?

Healthcare industry are always under cyber threats. The scale of potential losses from data breach are high. According to HIPAA journal, between 2009 and 2017 there have been 2,181 healthcare data breaches involving more than 500 records. Those breaches have resulted in the theft/exposure of 176,709,305 healthcare records. That equates to more than 50% of the population of the United States (54.25%). Healthcare data breaches are now being reported at a rate of more than one per day.



On top of that, the industry is also subject to overlapping compliance requirements enforced across the globe. Responding to cyber threats can be tricky as well as a regulatory compliance complexity.

Healthcare is a business, but it is unlike most businesses. The industry's "product" is the health of the patient. Healthcare provider who supports them, have a duty to the well-being of the patient and also the patient's right to privacy. The fact that protecting patient confidentiality is the ultimate goal of IT security in healthcare, not just ticking security compliance boxes.

HIGHLY REGULATED COMPLIANCE REQUIREMENTS

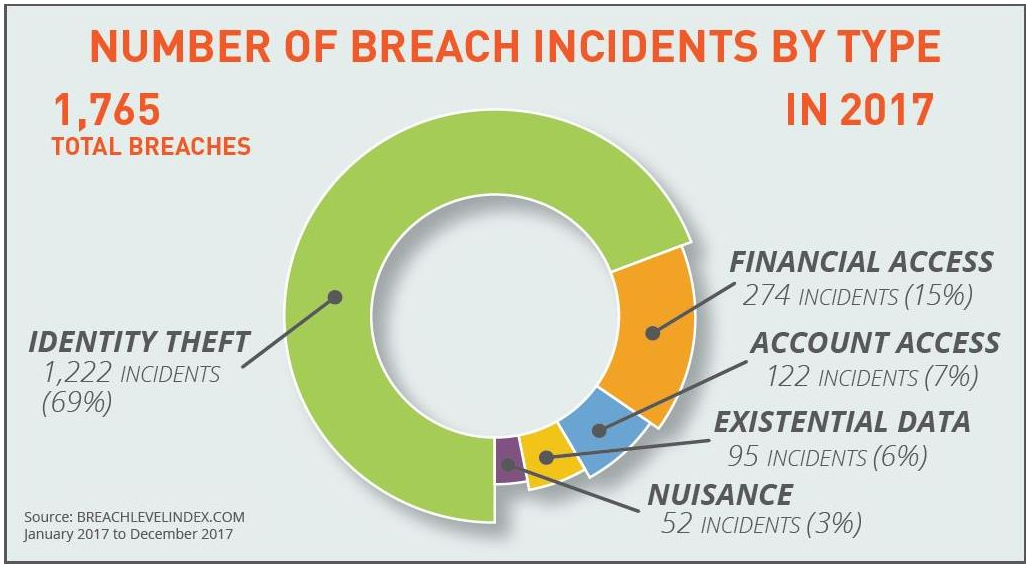
Healthcare industry has tight compliance regulations such as HIPAA-HITECH, GDPR/PDPA, ISO 27001 and etc. Each of these compliance standards have its own security requirements and audit processes. For example, GDPR and PDPA governing the data protection, may be similar but each has its own controls over the personal data. Healthcare industry need to implement these controls and demonstrate to auditors that these are being followed. Non-compliance shall incur hefty penalties.

IT OUTSOURCING

Due to increased competition, many healthcare institutions have outsourced their IT services to achieve cost reduction and expertise. Employees of outsourced companies will thereby require privileged access to healthcare systems. Threat actors can take advantage of an IT outsourcing company's access to get over the boundary of the healthcare companies.

PRIVILEGED USERS ARE UNAVOIDABLE

For an attacker, privileged accounts are the main target as they provide the direct pathway to access the IT infrastructure-server, database, application, network and security devices and etc. While it can take few days for the attackers to attack, it may take months or years to discover the breach and by then, it could have wreaked havoc on your organization's data network.



Privileged user is the center of all healthcare industry security and compliance. The larger the healthcare companies the more complex the systems are, the more privileged user are required. They may be employees, external contractors, remote users and etc. Hence, effective control over privileged users and full control of their activities are essential for security.

FINANCIAL IMPACT

The increasing number of high profile data breaches such as WannaCry's worldwide cyber-attack plastered on the headlines have recently captured the attention of many organizations. Besides, 80% of these incidents are due to privileged credentials but majority took over a week to detect implying huge financial losses involved. While many might buy into the misconception of breaches affecting larger organizations, unfortunately, 61% of the incidents occurred to companies under 1,000 employees.

TRACING THE CYBER-ATTACK CHAIN

The attackers would initially spend large amount of time researching a list of potential targets, gathering information about the organization's structure, clients, etc. Next, they would start hunting for system admins where internal networks are compromised. When an employee or third-party accidentally installs malware, cyber perimeters are breached. The hacker then observes the system and uses their legitimate VPN login to look for their opening. Once hackers gain a foothold by passing-the-hash, they execute lateral movement under the guise of authorized privileged users. Privileged accounts are often targeted as they are the direct pathways to access highly-guarded infrastructure containing proprietary information. Examples of privileged accounts include system accounts, administrative accounts, shared accounts and service/application accounts. At last, the hacker would be able to obtain the keys to the

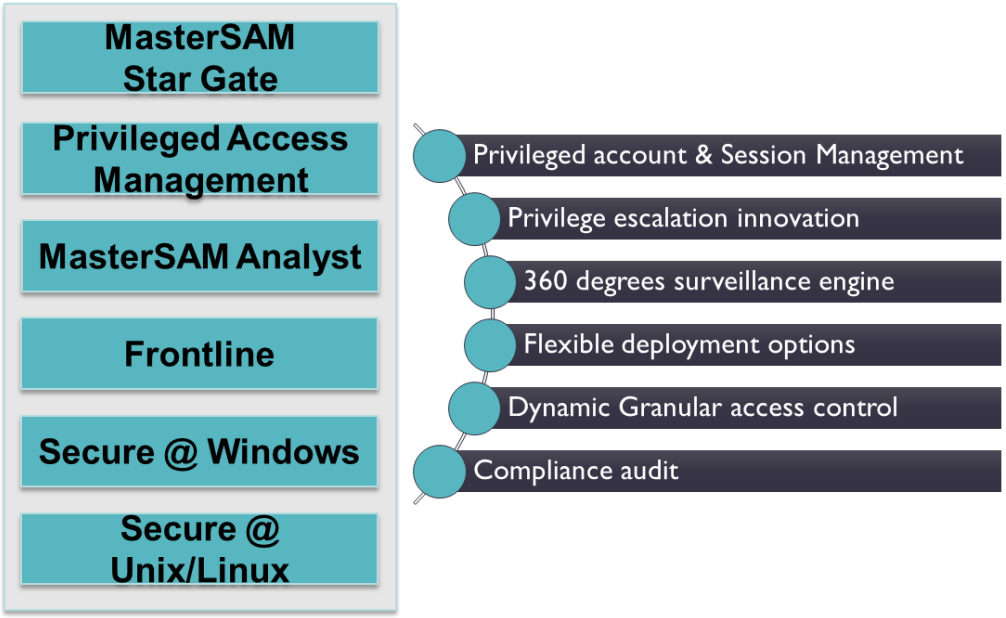
crown jewels and locate desired data. The system is then compromised. However, such threats could have also brewed from within known as “Inside Threat” caused by inadvertent employee behavior.

KEY DRIVERS OF PAM

Besides the heightened cyber security threats and increasing sophistication of hackers and breach incidents, other forces are also accelerating the implementation of PAM solutions such as regulatory compliance and productivity. Regulatory bodies and auditors have recognized the role of insiders and compromised accounts and credentials in security incidents, they have focused added attention on the controls and process organizations implement to mitigate these risks. Failure to address these concerns can result in costly penalties and critical findings to remediate. This is evident in the previous section on the role of the Government.

How Silverlake MasterSAM helps

Established in 2004, Silverlake MasterSAM is an innovative Privileged Access Management Solution company focused in helping organizations secure and manage privilege access from a complete lifecycle perspective. With a trusted and proven track record, Silverlake MasterSAM empowers privileged access management to businesses across the globe.



Silverlake MasterSAM presents itself as a premier solution provider that aims to disrupt this chain of cyber-attacks. To reduce the attack surface to limit exposure of privilege accounts to insiders and external hackers, access to privileged accounts is brokered for human users, services and applications. These passwords and other sensitive credentials are vaulted securely and automatically with restricted access to the vault under Credential Protection & Management. Granular least privilege access control policy is enforced by promoting minimal access - sufficient to perform his/her role. On the other hand, under Privileged Elevation and Delegation Management, administrator privileges can be controlled and elevated on-demand based on the task at hand. Finally, to combat attackers disguised as authorized insiders, monitoring and compliance recording feature would be able to track anomalies in privileged users' behavior to indicate in-process attacks.

Meeting audit and compliance requirements are no longer complex with Silverlake MasterSAM's PAM solution. Healthcare can effectively deploy the PAM solution and with ease, meet audit and compliance requirements of the regulations such as HIPAA-HITECH, GDPR/PDPA, ISO 27001, etc. through session management and password management.

The below is a look at HIPAA Security standards and how Silverlake MasterSAM helps to comply with all mandates.

Section	Description	Help to Comply
164.308(a)(1)	Security Management Process	Yes
164.308(a)(3)	Workforce Security	Yes
164.308(a)(4)	Information Access Management	Yes
164.308(a)(5)	Security Awareness and Training	Yes
164.308(a)(6)	Security Incident Procedures	Yes
164.312(a)(1)	Access Control	Yes
164.312(b)	Audit Controls	Yes
164.312(d)	Person or Entity Authentication	Yes

Sample Use Cases

USE CASE 1: PRIVILEGE ACCESS

Objective – To control and restrict administrator access

How to do it:

Administrator login to Silverlake MasterSAM platform with daily privilege access. Whenever a higher privilege credential is needed to perform specific task, administrator will go through approval request workflow to submit a ticket. Upon request approved, administrator will be able to access system with higher rights going through Silverlake MasterSAM.

USE CASE 2: PASSWORD RETRIEVAL

Objective – To safe keep and monitor password usage

How to do it:

All privileged account password will be check in and safe keep in Silverlake MasterSAM password vault. Whenever a request is needed to release the password, requestor will need to submit for approval in order to retrieve password. All the usage of the password will be log for audit purposes in Silverlake MasterSAM.

USE CASE 3: SURVEILLANCE, REVIEW AND ALERT

Objective – To record, playback, review and alert on user activities

How to do it:

All access sessions to target system through Silverlake MasterSAM can be recorded in text and video format. Reviewer can playback user access sessions to check on activities being performed. With security policy in place, officer will be alert when violating action happen.