silverlake
SYMMETRY AT WORK

masterSAM

Privileged Access Management and Solution Value to End users

An ROI ANALYSIS FOR PAM USERS

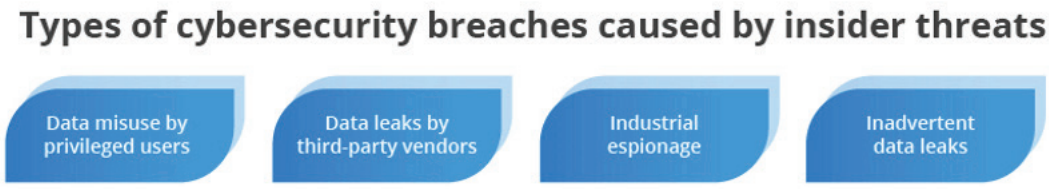
Executive summary

In an ideal world, a security organisation would be designed and built from scratch, with processes, people and technology chosen to support business outcomes. In reality, however, security organisations adapt and develop in response to changing business priorities, regulatory standards requirements, or recommendations from auditors or consultants.

In today's business climate, businesses are affected by both external threats and insider attacks. While external threats such as individual hacktivists, state actors, etc., are difficult to control, managing insider threats can be far more effectively addressable with the right security frameworks in place and this largely entails Privileged Access Management (PAM).

By ensuring your systems are monitored and the right accesses are given to the right people for the right amount of time, organisations can largely mitigate potential breaches that can lead to reputational and financial damages.

Insider Threats can be largely detrimental if left unaddressed



Privileges must be granted on a need-basis and hinge on the Least Trust Policy or Zero Trust Model. Fundamentally, Zero Trust Network Access (ZTNA) means enabling precision ("just in time" and "just enough"), least-privilege access for named users to specific applications only after an assessment of the user identity, device identity and hygiene (highly encouraged), and context has been made. When privileged users have elevated access rights, they tend to have more opportunities to leak data by mistake, misuse data or steal data. The best practice is therefore, to prevent and mitigate data misuse by limiting number of privileged users, monitoring user actions and controlling the access to sensitive data.

Executive summary

External Threats, largely unexpected and difficult to control, can have far more impact on businesses

According to an annual report on global cyber security, there were a total of 304 million ransomware attacks worldwide in 2020. This was a 62 percent increase from a year prior, and the second highest figure since 2016. (Business Insider, 2021) The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020.

The key to reduce the impact of a ransomware attack is by ensuring attackers do not have privileged account access. Organisations can do this with privileged access management strategy and related automation technology to manage privileged access controls and store user credentials in secured vault instead of typical excel spreadsheets.

To prevent or reduce improper use of privileged access accounts, organisations employ Privileged Access Management strategy to. A comprehensive PAM solution will help to:

- Identify the scope of their privileged access risk
- Protect and monitor access to privileged accounts, credentials
- Automate privileged access controls
- Control privileged access to critical assets
- Monitor privileged access activity

ROI for privileged access management (PAM) projects

Now that we established the need for PAM, businesses may struggle to justify the implementation and deployment of the solution, by convincing their board of directors and senior management on how PAM can bring quantifiable value.

We at MasterSAM, believe in ensuring our customers aspiring to deploy PAM, fully understand the value it brings to their organisation.

Goals and objectives of deploying PAM solution:

- Reduce or prevent incidence of a Data breach
- Manage Insider threats
- Record user sessions to ensure accountability and transparency
- Fulfill Regulatory compliance and audit
- Cover hybrid IT infrastructure

Quantifying the customer value of MasterSAM's PAM solution:

Lowering costs by improving productivity

MasterSAM PAM monitors user activity and provides real-time alerts when it detects unusual session activity or malicious activities. All command line and windows activities will be kept in the repository and archive to meet audit and compliance mandates.

With the 360-degree surveillance engine, there is no requirement for both internal labor and external audit. Typically, the average labor savings can be one FTE (full-time equivalents) annually, and possible external audit savings annually due to recording of sessions and automation.

Auditors expect to see clear audit reports to show how a firm grants access to sensitive and privileged credentials, such as for systems and database administrators, and what these administrators do with the system. With PAM implementation, this entire process can be pain-free as the process, rules, activities are transparent, monitored and recorded with playback functionality.

MasterSAM PAM helps reduce the time required to gather evidence to show compliance by simply generating customisable audit reports that show adequate compliance and adherence to the regulatory standards that mandate effective management of passwords and monitoring of privileged users and accounts.

Thus, we can say, with less operational effort, there is an automated function to ensure malicious activities are monitored while every session is recorded and audited. With this solution, one is able to meet multiple regulatory standards, some of them being PCI-DSS, HIPAA and ISO27001, among others.

Process automation to reduce labor costs

This calculation based on the cost of FTEs (full-time equivalents) can be based on the time IT admins spend on tasks that will be automated by PAM solution. Labor costs can be anything from IT help desk for helping with privileged accounts, to discovering, managing and rotating passwords, to providing detailed reports and audit information to internal and external audiences.

The equation for calculating cost savings from productivity gains looks like this:

Cost Savings = ((# FTEs* x % Time To Do This Task x Average Annual Salary) x % Savings from your solution) + Cost of other resources

*FTEs is a way to express the total number of people that adds up partial contributors. For example, if 10 people are using half of their time to do something, it would equal five FTEs (10 people x .5 time/person).

Example:

Resources required for task	No. of FTEs doing this task	5
Average annual salary	Local currency	$100,000
Time to do this task	Average % of time per person	15%
Time saved by product	% of cost product saves	50%
Cost of other resources	Local currency	$20,000

Quantifying the customer value of MasterSAM's PAM solution:

Avoiding Risk

With PAM, less time and effort will be needed in managing and mitigating breaches, which in turn leads to reduction in cost of triggering the Organisation's incident response team and external cybersecurity consulting services and potential saving annually.

Below are both internal and external roles of an organisation's incident response team, where incident activation costs can be avoided.

- IT security, information and infra staff.
- Legal and communications representatives
- Business and operation representatives.
- External security consultant and investigators.

According to the 2019 Cost of a Data Breach Study: Global Overview from IBM Security Institute report, the global average cost of a data breach is $3.92 million, up from $3.86 million in 2018. A key finding is that the average total cost of a data breach is 95 percent higher in organisations without security automation deployed;

Avoiding non-compliance fines and costs

Depending on the industry and compliance regulation, fines vary. One should understand each regulation and the associated fines for non-compliance, as well as how PAM solution mitigates risk related to non-compliance.

The effects from privileged user breaches could be devastating, causing the company to lose revenue, market reputation, and competitiveness. MasterSAM PAM helps avoid such security breaches.

The equations for calculating costs avoided and revenue saved to quantify Risk Avoidance are:

Cost Avoided = Fines Avoided + Incident Activation cost avoided
Revenue Saved = Total Annual Revenue x % Revenue Not Lost

Conclusion

With implementation of PAM, the business initially incurs the cost of deployment. This is an investment the business has to make to reap long term benefits. There is clearly a financial incentive that will immediately get a CFO's attention – operational efficiency. PAM facilities removal of tedious business processes by digitising workflows, thus reducing wasted employee time (and therefore money) carrying out manual tasks. For more information, please write to mastersam.info@silverlakeaxis.com