Deloitte.

cyber 101

An introduction to privileged access management

March 2020

Privileged access management

What is it?

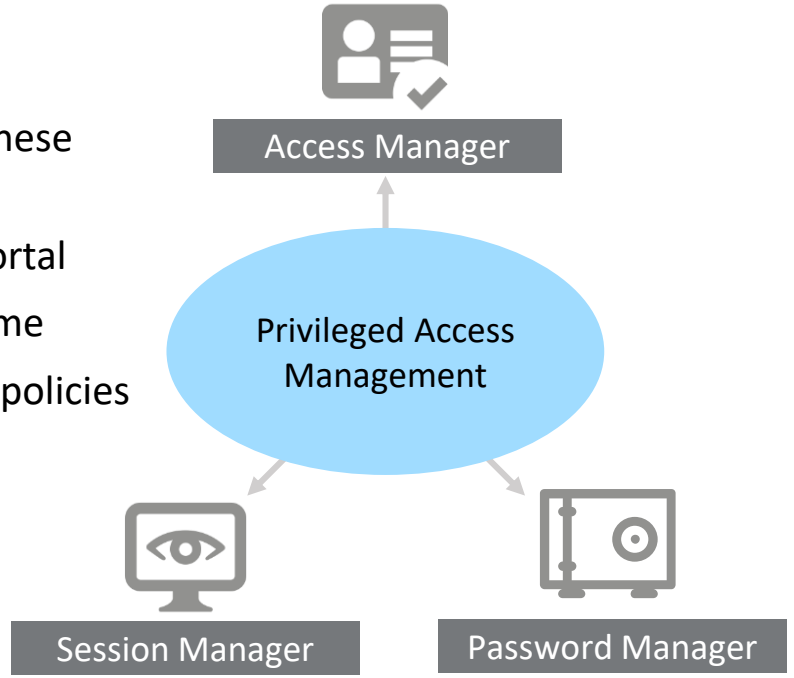
Gartner has named privileged access management the **#1 cyber security priority** for organisations. But what exactly does privileged access management entail?

'Privileged access' encompasses access to critical systems - computers, networks and network devices, software applications and other digital assets. Privileged access management (PAM) is thus, the combination of tools and technology used to **secure, control and monitor access** to an organisation's **critical information and resources**.

What does it comprise?

While PAM solutions vary in their design, most of them consist of these three components:

- **Access Manager** – Manage all employee access from a single portal
- **Session Manager** – Monitor all privileged user actions in real-time
- **Password Manager** – Protect passwords and enforce password policies



https://www.netprotocol.net/gartner-privileged-access-management-is-the-1-cyber-security-priority/

http://blog.wallix.com/what-is-privileged-access-management-pam

http://blog.wallix.com/privileged-access-management-features-pam-features

https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

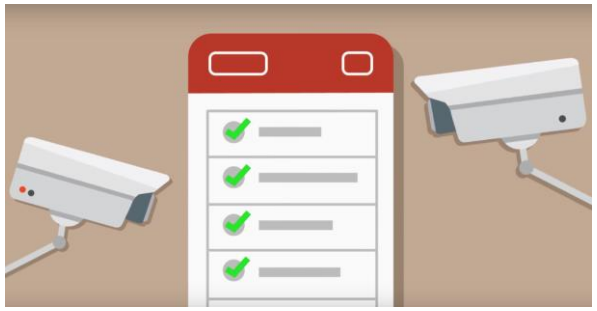
Key components of PAM

An overview

The **Access Manager** helps security teams to manage all employee access on a single portal, from which:

- Privileged user can request access, and
- Administrators can disable a privileged user's access

The **Session Manager** provides real-time monitoring of privileged users to prevent and detect suspicious activity. It tracks and creates an audit trail of actions taken during a privileged account session.



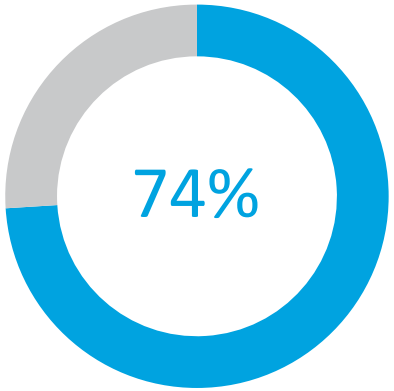
The **Password Manager** helps with controlling passwords and enforcing password policies. This allows regular rotation and revocation of passwords while maintaining them in a centralised and encrypted vault.

http://blog.wallix.com/privileged-access-management-features-pam-features

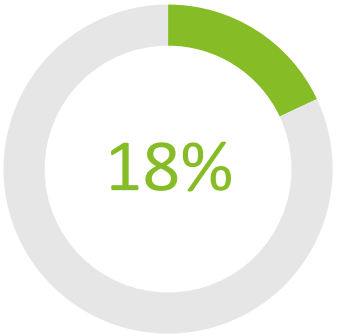
Why do organisations need PAM?

Overview

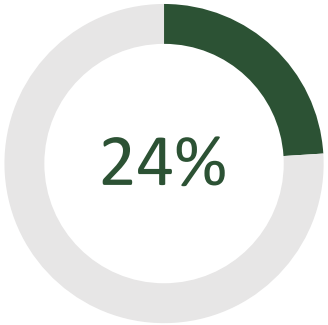
A standard data breach can cost and organisation an average of **USD3.92 million**. Enterprises that prioritise privileged credential security are able to ensure that their operations will not be interrupted by a breach, hence by creating a formidable **competitive advantage** over their peers in time and costs.



of data breaches start with privileged credential abuse
(Source: Centrify)



of healthcare employees would sell confidential data for just USD500 to USD1000
(Source: Accenture)



of employees know of someone who has sold privileged credentials to outsiders
(Source: Accenture)

Why do organisations need PAM?

Benefits of PAM

Powerful security solution

- PAM is a powerful security solution that can be used to improve insights into vulnerability assessments, IT network inventory scanning and identity governance, among other things. This enhancement of cyber security serves as a deterrence to many cyber criminals.

Saves time and money

- Most cyber security solutions only reduce risk but bring no additional business value. However, employing the right PAM solution can increase productivity by giving employees access to systems and applications faster and more securely. This enables CISOs to get more done with the same budget.

Fast track to compliance

- With strong security control recommendations, PAM develops a good baseline of policies that can help to fast-track your compliance standards to align with industry and government regulations.

Quick recovery from cyber-attacks

- A PAM solution enables you to quickly audit privileged accounts that have been used recently, identify passwords that have been changed, and determine which applications have been executed.

https://www.netprotocol.net/gartner-privileged-access-management-is-the-1-cyber-security-priority/

How breaches could have been prevented with PAM

Case study: Capital One Bank

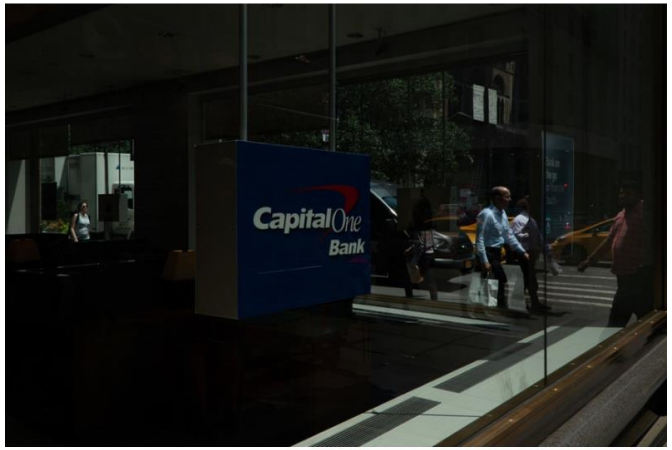
One of the most high profile cases of 2019 was the data breach of Capital One Bank, of which over 100 million customer accounts and credit card applications were exposed.

How the breach occurred:
Paige Thompson, former Amazon AWS employee (Capital One's cloud hosting service), took advantage of misconfigurations in Capital One's cloud services and firewalls. She bypassed the firewalls, used web application firewall credentials to obtain privilege escalation and gained access to more and more sensitive data.

Consequences:
As a result of the breach, the following were stolen from Capital One's database:

- More than 140,000 social security numbers
- 1 million Canadian Social Insurance numbers
- 80,000 pieces of banking and credit information
- Undisclosed number of names, addresses, credit scores, and more

Capital One Data Breach Compromises Data of Over 100 Million



Read more: The New York Times

How breaches could have been prevented with PAM

Case study: Facebook

In October 2019, global social media giant, Facebook, encountered yet another data breach when hackers took over a single account belonging to one of its biggest data partners.

How the breach occurred:
Hackers commandeered the personal account of a LiveRamp employee who had privileged access to advertising accounts on Facebook. Using that personal account, hackers gained access to the company's Business Manager account, allowing them to run ads with LiveRamp's customers' money.

Consequences:
Using that access, hackers ran a series of ads on LiveRamp's customer accounts on Facebook. They spent thousands of those victims' dollars to trick viewers into buying fake products.

One of the ads had been viewed more than 60,000 times and directed visitors to a page designed to steal people's credit card numbers.

Hackers infiltrated a big Facebook data partner to launch scams

Marketing giant LiveRamp has privileged access to advertising accounts on the social network. Hackers took notice.

Alfred Ng January 29, 2020 1:06 PM PST

LiveRamp is a major data partner for Facebook and suffered a hack, causing a domino effect of scam ads.

Read more: Cnet

How breaches could have been prevented with PAM

Case study: Marriott International

In late 2018, hotel chain Marriott International discovered unauthorised access within Starwood's reservation system, a subsidiary Marriott acquired in 2016.

Internal investigation determined that Starwood's network was compromised in 2014, which meant that there had been unauthorised access for 4 years into Starwoods' systems by the time it was found out.

How the breach occurred:
Attackers managed to take control of a user account with privileged access to make a database query.

The user credentials were stolen using a Remote Access Trojan (RAT) along with Mimikatz, a tool used to find out username/password combos in system memory, that were placed onto the server.

Consequences:
Up to 500 million guest records were stolen, including extremely sensitive information like credit card and passport numbers.

Read more: CSO Online

How breaches could have been prevented with PAM

How PAM might have helped

1. Real-time session monitoring could have caught and detected the suspicious activities of hackers, terminated such sessions, and alerted the security teams, preventing an incident from happening.

2. The segmentation of user privileges could have prevented hackers from bouncing from one resource to another.

3. Besides multi-factor authentication (MFA), PAM also checks for circumstances surrounding privileged access (e.g. time and IP location). If caught as unauthorised, access would be denied even if credentials were otherwise valid.

4. A strong PAM solution would have hidden the very existence of sensitive resources to users who do not have privileged access. If hackers were in the system with credentials that have no database access, they would not even be able to see personal information, much less query against it and retrieve it.

http://blog.wallix.com/biggest-data-breaches-2019

Deloitte.