CyberQP

The Future of Authentication for MSPs

How to Build a Cybersecurity Program Designed for Today's Identity-Based Threats

cyberqp.com

The Future of Authentication for MSPs

As threat actors continue to develop and exploit new vulnerabilities to launch increasingly destructive cyber attacks (whether it's part of a nation state's activities or for the sake of exfiltrating critical data for extortion), cybersecurity remains a major concern for both businesses and individual clients alike.

Unfortunately, there aren't enough security professionals in the cybersecurity landscape to protect every organization or individual. According to industry reports, there are over 3.4 million vacant cybersecurity roles worldwide. [1] And while the unemployment rate in the cybersecurity industry has continued to hover around zero percent for the past six years, it's incredibly difficult for Managed Service Providers (MSPs) to find and hire talent from today's cybersecurity workforce. [2]

The cybersecurity landscape also faces a major experience gap. Even if an MSP had the money and the resources to assemble the infrastructure and talent for a cybersecurity program, they would struggle to find a candidate with ten years of experience or the knowledge base necessary to build and properly manage a cybersecurity program and team.

Simply put, the cybersecurity landscape cannot keep up with the constant growing, unsatisfied demand for qualified workers.

Risk

	2000	2007	2014	2022
Device	Desktop/Laptop	Mobile	IoT (Internet of Things)	IoE (Internet of Everything)
Applications	Client/Server	Web	Agile	Automation
Data	1 Exabyte	1/4 Zettabyte	1 Zettabyte	100 Zettabytes
Mobile Device Speed	2G	3G	4G	5G
Communication Platform	Instant Messenger	Facebook	Twitter	TikTok, Instagram
Hackers	Script Kiddies	Criminal Ecosystem	Hactivists	Other Non-state Actors
Perimeter	Controlled Access	Wide Access	Hybrid Cloud	No Perimeter
Attacks	Intrusive	Disruptive	Destructive	Cyber Armageddon?

Market Opportunity

To make matters worse, enterprise-level firms frequently get to qualified talent first or poach promising candidates from the small-and-medium sized business (SMB) level. Even if an MSP is able to properly train someone for a cybersecurity program, or to gain expertise in cloud systems to be a Tier 3 or Tier 4 technician, an enterprise firm can hire them away with better pay and better benefits.

[1] ISC2 Cybersecurity Workforce Study 2022
[2] The State of Pentesting 2022: How Labor Shortages are Impacting Cybersecurity & Developer Professionals

This leaves SMBs with little recourse in the event of a breach. There's no 911 for cybersecurity, and software alone cannot secure the amount of data and devices that an organization needs to protect.

That's why MSPs are the **only solution** to today's cybersecurity problems. This community of IT and security professionals can offer SMBs a human element to their cybersecurity, a helpful guide and support system for major issues, actually helping people when they have a cybersecurity problem.

Q: What is a Privileged Account?

A privileged account is a user account that has more access and privileges than average users. Examples include local admin accounts, domain administrators, service accounts and Azure AD/O365 tenant admin accounts.

However, this means that MSPs need affordable, scalable solutions purpose-built for their mission. And in the face of threat actors rapidly pivoting to target SMB Active Directory and Azure AD instances, hoping to compromise peoples' identities for their ulterior goals, CyberQP is dedicated to stepping up and building the solutions that MSPs need to prevent threats to SMBs' end users, privileged accounts, and credentials.

How to Decode the Acronym Soup of Cybersecurity Acronyms

As enterprise cybersecurity vendors squabble and create too many acronyms to establish their own verticals and industry-leading categories, it can be difficult for business leaders to understand what piece of jargon represents a solution or something that a company is trying to protect.

And as major acronyms (such as MSSP, XDR, and SOC) achieve wider recognition, newer acronyms to reflect solutions to protect privileged accounts and credentials are emerging, such as:

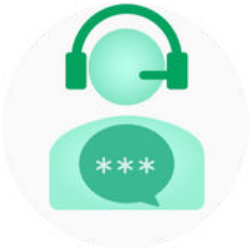
IAM:
Identity and Access Management

JIT:
Just-in-Time Accounts

PAM:
Privileged Access Management

PIM:
And Privileged Identity Management

What is Identity and Access Management?



Identity and Access Management solutions ensure that the right people have access to the resources appropriate to their position within an organization, for the right reasons, at the right time. This is the broadest category we'll discuss today, encompassing all forms of identity and authentication, including employees' privileged accounts and end users' accounts alike.

What is Privileged Access Management?

Privileged Access Management tools offer a set of tools and best practices to safeguard privileged accounts, whether they are local admin accounts across a client's endpoints or Azure AD/Office 365 tenant admins, the metaphorical keys to the kingdom.

Privileged Access Management enables MSPs to discover, monitor, and manage these privileged accounts using a variety of products including:

- A secure password vault
- Products that regularly rotate privileged credentials
- Temporary privilege escalation products
- Privileged account discovery tools

Where your services come from when you buy other PAM

VAULT	✓
ROTATION	X
TEMPORARY PRIVILEGE ESCALATION	✓
DISCOVERY	X

Where your services come from when you buy CyberQP

VAULT	✓
ROTATION	✓
TEMPORARY PRIVILEGE ESCALATION	✓
DISCOVERY	✓

What is Privileged Identity Management?

While Privileged Identity Management has several similarities to PAM, this category of cybersecurity products is rapidly emerging to form its own category of solutions designed to **assign** privileged resources and **auditing** access history.

These solutions allow MSPs to assign start and end dates to account access for both employees and contractors. These include accounts that expire after a certain day by rotating credentials to lock out users, or even **Just-in-Time (JIT)** accounts, which are only active for the exact amount of time that they need to be used for.

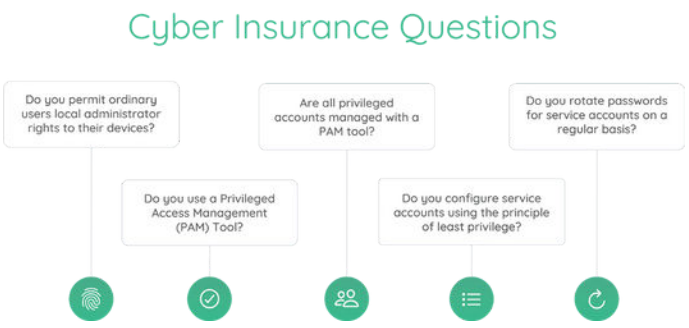
PIM also encompasses session recordings for privileged accounts, giving people clearer visibility with a full audit trail starting from when an employee can access sensitive resources and ending when they lose access.

Microsoft has also recognized the need for a Privileged Identity Management solution by introducing Azure PIM. However, MSPs need a PIM solution purpose-built for their use cases.

PAM vs. PIM

Because of these two terms' similarities, many people assume that PAM and PIM are two distinct IAM subcategories. But while PIM and PAM are both under IAM, PIM solutions should actually be considered part of a subcategory beneath PAM. PIM and PAM solutions specialize in administrator accounts and credentials, while Identity and Access Management specializes in protecting general user accounts.

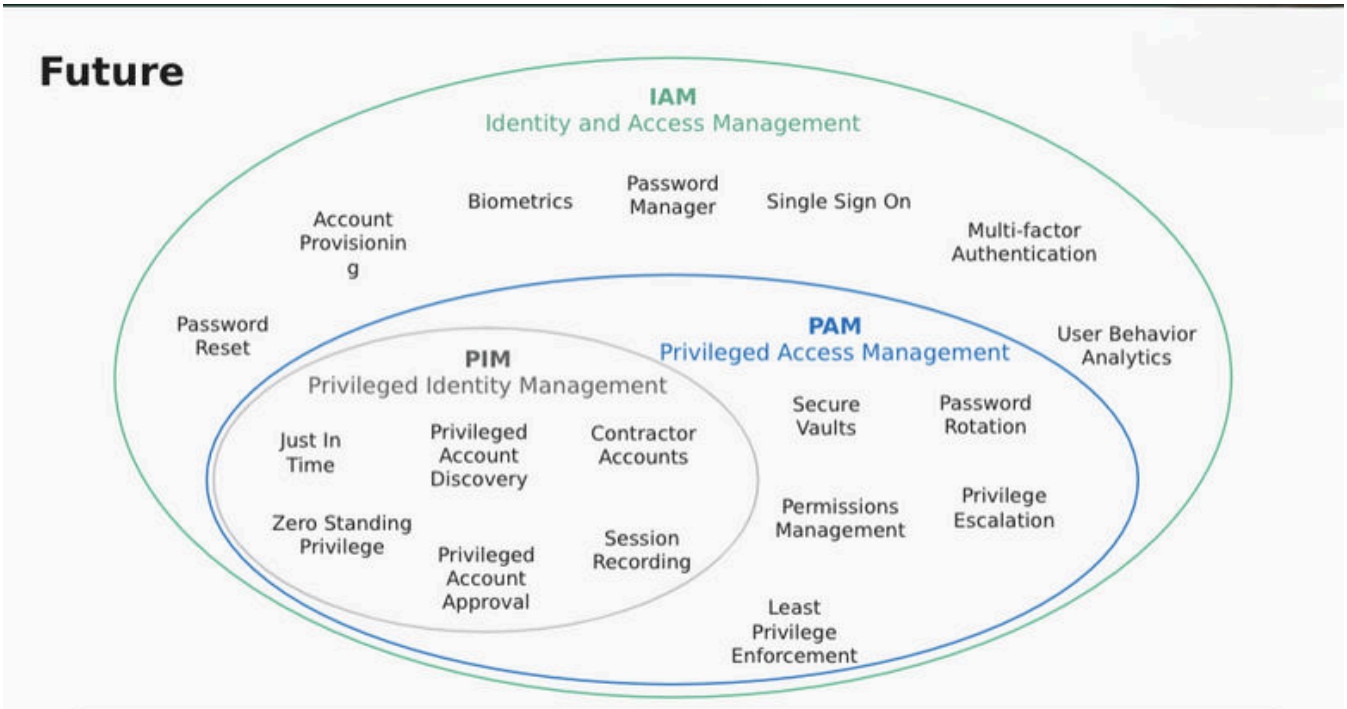
What's Next?



Privileged Access Management tools are becoming a prerequisite for cyber insurance policies, redefining what makes for a strong cyber health posture.

In preparation for the future of the cybersecurity landscape, CyberQP is dedicated to developing solutions to support MSP help desks expanding their security programs to account for IAM, PAM, and PIM. We specialize in the PAM needs that help desk technicians care about, such as password rotations, account provisioning, and biometric authentication, and offer a rapidly growing list of robust PAM and PIM capabilities to MSPs, with more on the way.

To learn more about how CyberQP can give you one platform to accelerate your MSP's workflow for privileged account and identity-focused tickets, you can learn more here.



Get CyberQP Today

To learn more about how CyberQP can provide one platform to accelerate your MSP's workflow for privileged account and identity-focused tickets, you can learn more here.