BeyondTrust

Busting the 6 Myths of PAM

Privileged Access Management:
Sorting Fact From Fiction

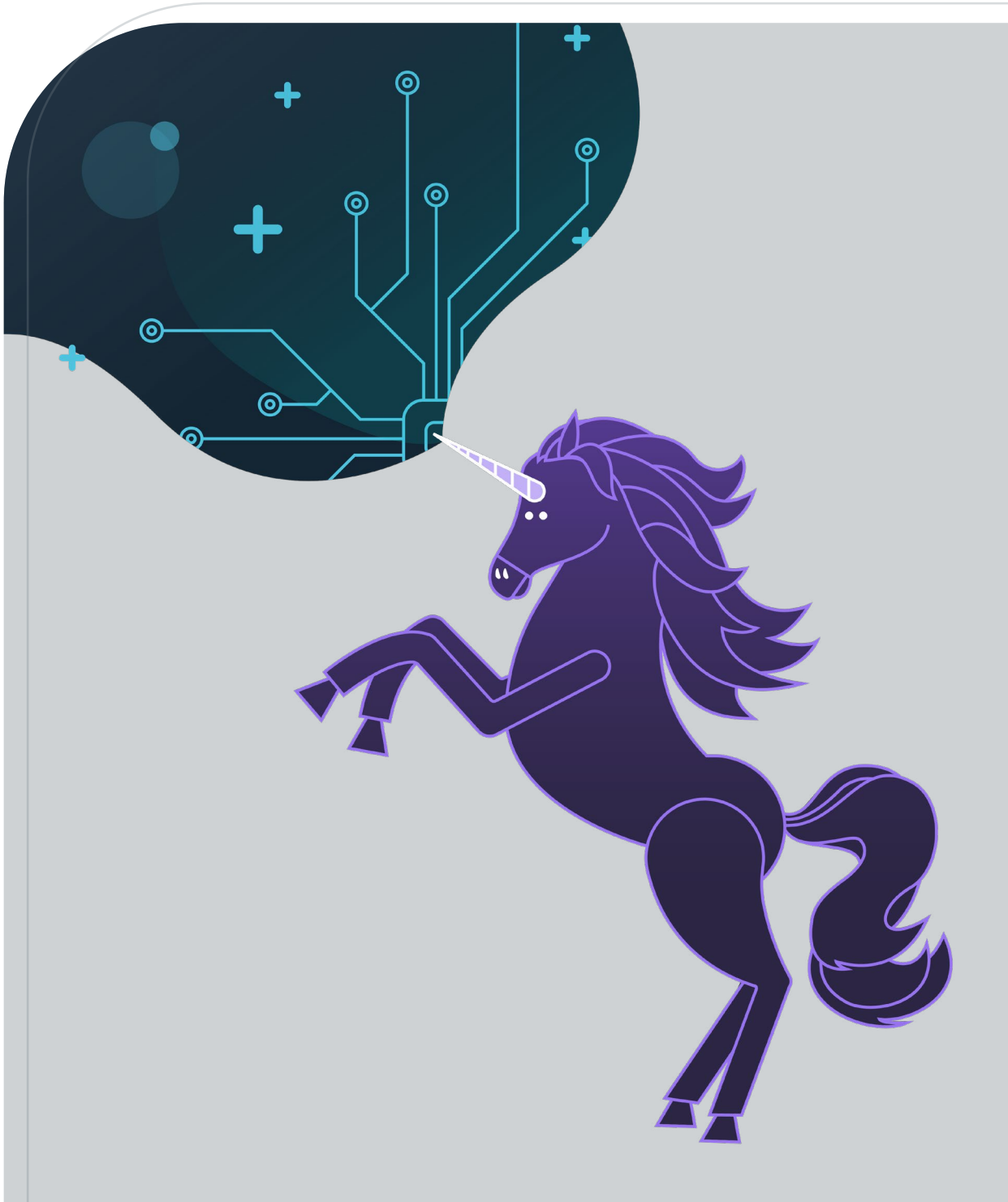
TABLE OF CONTENTS

INTRODUCTION

Myths are curious things, aren't they? Widely held, false beliefs that gain momentum over time, they can grow and spread quickly. The line between myth and fact soon becomes blurry – and many choose to believe a myth because it's often a 'nicer' or more appealing reality, or simply because it's heard enough times.

Here at BeyondTrust, we've tried *and tried* to believe in unicorns, yet they're still eluding us. And while we're refusing to write them off as make-believe just yet (along with Bigfoot), there are some myths we do want to dispel.

In this whitepaper, you'll discover six popular beliefs about Privileged Access Management (PAM) that are, in fact, wrong. We'll explain why, shed some light on the truth, and provide you with actionable takeaways to develop your journey to a more secure, folklore-free organization.



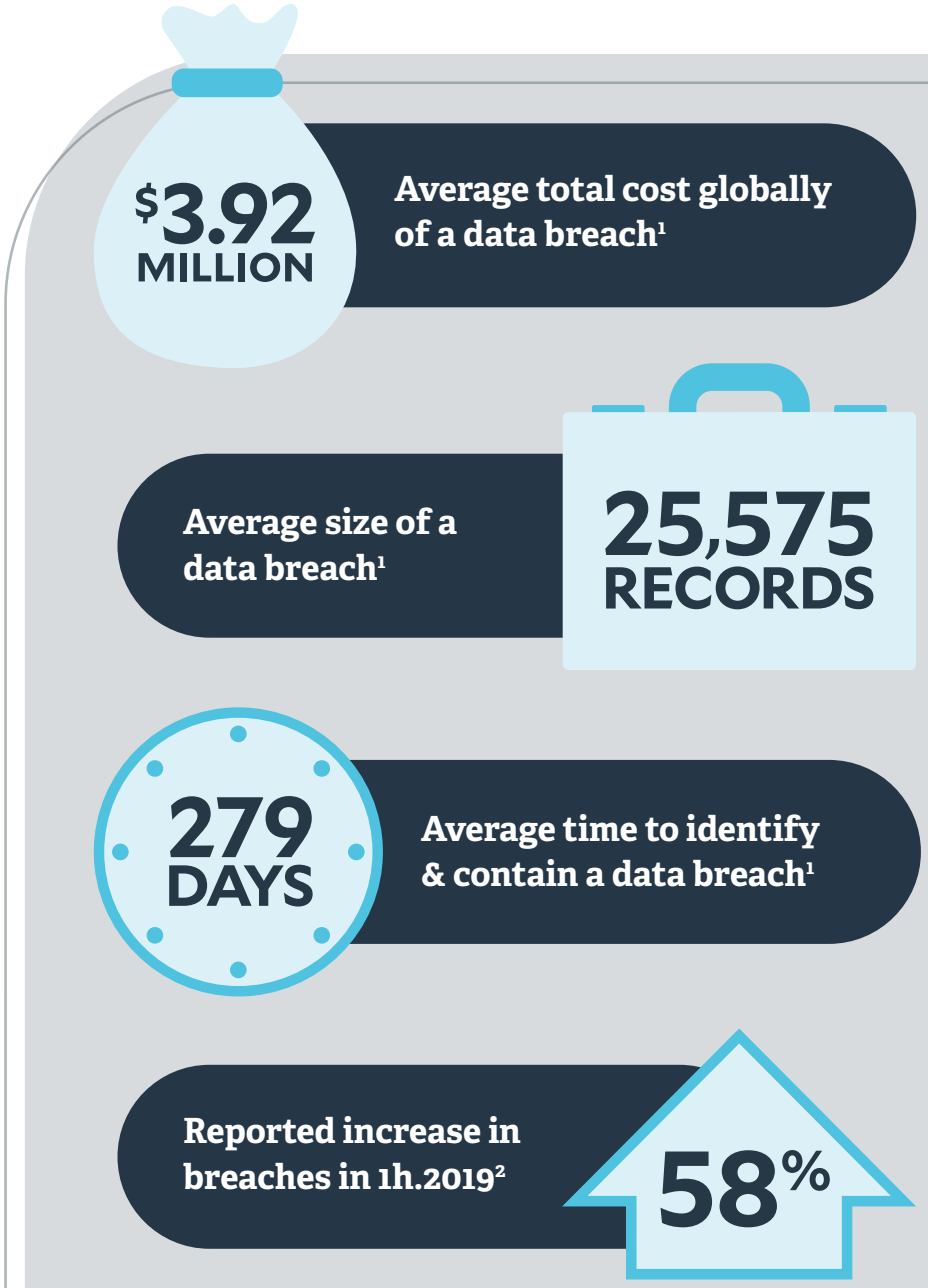
THE INCREASING THREAT OF A DATA BREACH

Before getting to the myths, let's start with some facts. Data breaches are not slowing down. It seems with every passing month a new, high-profile breach occurs. And hundreds more take place every month that don't make the headlines. As a business, it's become a case of when, rather than if, security gets compromised – which is why having a strategy in place to address this risk is important and, increasingly, top-of-mind.

Below is an overview of key statistics from recent reports published about data breaches.

Ponemon Study: 2019 Cost of a Data Breach

The recent Cost of a Data Breach Report conducted by the Ponemon Institute and sponsored by IBM Security reveals some harrowing statistics around what cyber breach victims face in the way of losses. Currently, the global average total cost of a data breach sits just shy of $4 million, with around 25,575 records being the average size of a breach. With the average time to identify and contain a breach being almost 10 months, it's obvious that a solution is needed, and fast.



Sources: 1. 2019 Cost of a Data Breach Report, Ponemon Institute;
2. 2019 MidYear QuickView Data Breach Report, Cyber Analystic, Aug 2019

HACKER'S DELIGHT: MORE NETWORK PATHWAYS THAN EVER BEFORE

A major reason why so many breaches are occurring is simply because the attack surface has grown exponentially over the last 20 years. Whereas IT networks used to consist primarily of on-premise assets, the number of accounts and endpoints has exploded. IT organizations must learn how to manage human identities as well as shared admin accounts, servers, desktops, IoT, and machine credentials across diverse environments that can include on-premise, cloud, and hybrid, as well as DevOps. Cyberattacks and scams leveraging AI are also increasingly perceived as making the jump from science fiction to a present day reality.

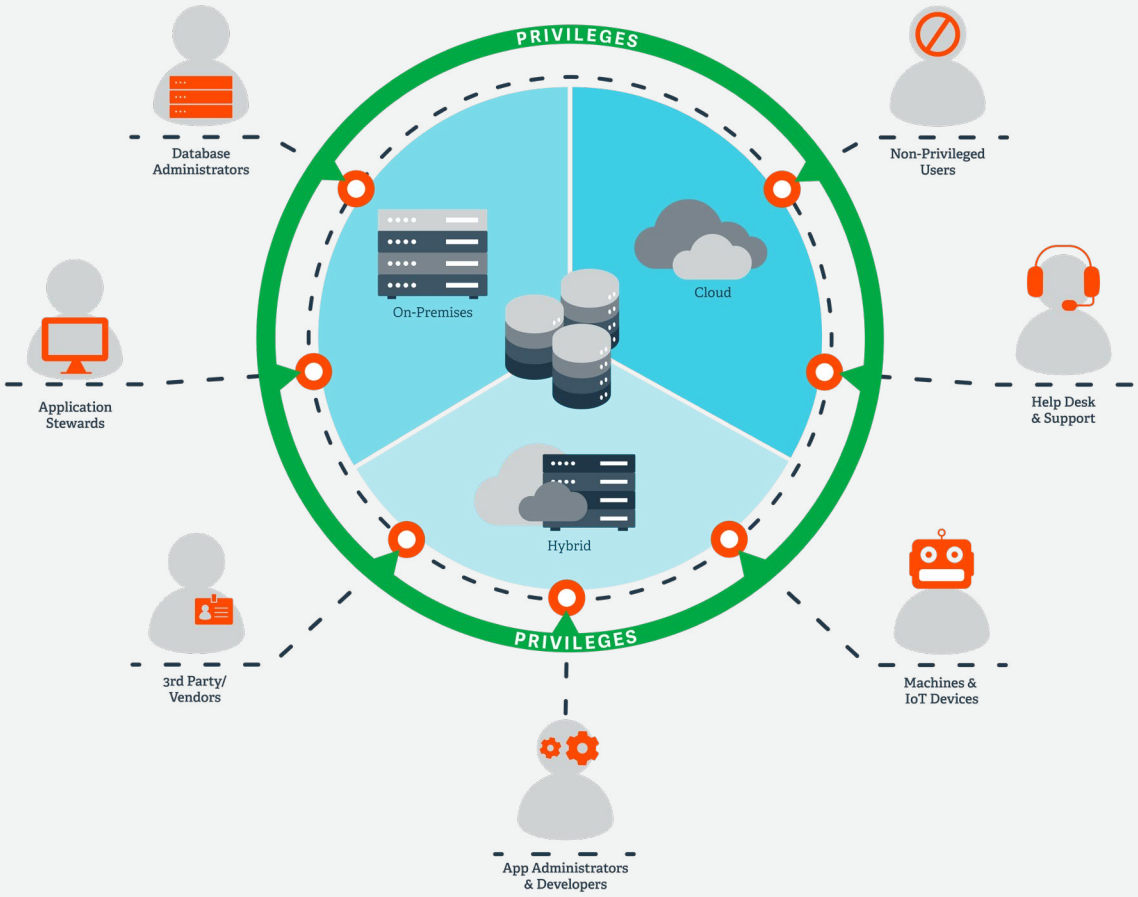
Add all of this together and the problem is widespread, complex and potentially difficult to solve. The hacker's playground is forever growing and, while keeping up may mean new security investments and an evolution of your strategies, losing ground could ultimately be catastrophic for your business.

A problem correlated with the expanding attack surface is the need for productivity. As the number of as applications, systems, and new technology grows, so does the need for privileged access.

The employees of modern enterprises require dynamic a company's critical IT assets and valuable data. And depending on their job role, location or operating system, giving them the necessary access without creating risk often seems impossible.

Since many IT teams are fearful of negatively impacting productivity, they give out administrator rights and over-provision privileges without addressing the related security risk.

How Are Your Networks Being Accessed?



BROWSE UP VS. BROWSE DOWN SECURITY MANAGEMENT

Browse Up Security

Browse Up security is a concept whereby IT systems are administered from 'low trust' devices that are at heightened risk of being compromised, such as a personal home computer. This is, unfortunately, a typical scenario today, proving that common practice isn't always good practice. An end-user device used by an administrator can be one of the easiest paths into the target system.

In computer systems where data integrity is important (such as cloud storage services, which handle personal data or payments, or industrial control systems), if you don't have confidence in devices that are being used to administer or operate a system, you can't have confidence in the integrity of that system.

Browse Down Security

On the other side of the spectrum, Browse Down security is the best practice for mitigating risk in your environment. Browse Down security involves having dedicated workstations for remote administration that live on a segregated network with the OS locked down, along with email and web browsing blocked.

The idea is that if the "dirty", less trusted workstation/environment gets compromised, then it's not directly underneath the clean environment, and it would be difficult for the malware operator to gain access to your clean environment, as it lives on a separate workstation.

However, this approach comes with a number of drawbacks. Although very secure, it's impractical. Imagine a remote worker – do they typically have access to a secondary system on an isolated VPN?

A much better alternative is Privileged Access Management (PAM).

As stated by the National Cyber Security Centre (NCSC part of GCHQ), "Browse up is a bad security model, but is often used as it makes administration easier for staff to manage. **Privileged Access Management (PAM)** helps mitigate some of these risks. Browse down is better, and coupled with privileged access management, can really help you gain confidence in your management interfaces."

> **"Browse Down Security Management alone isn't scalable and doesn't mitigate risk enough on its own."**

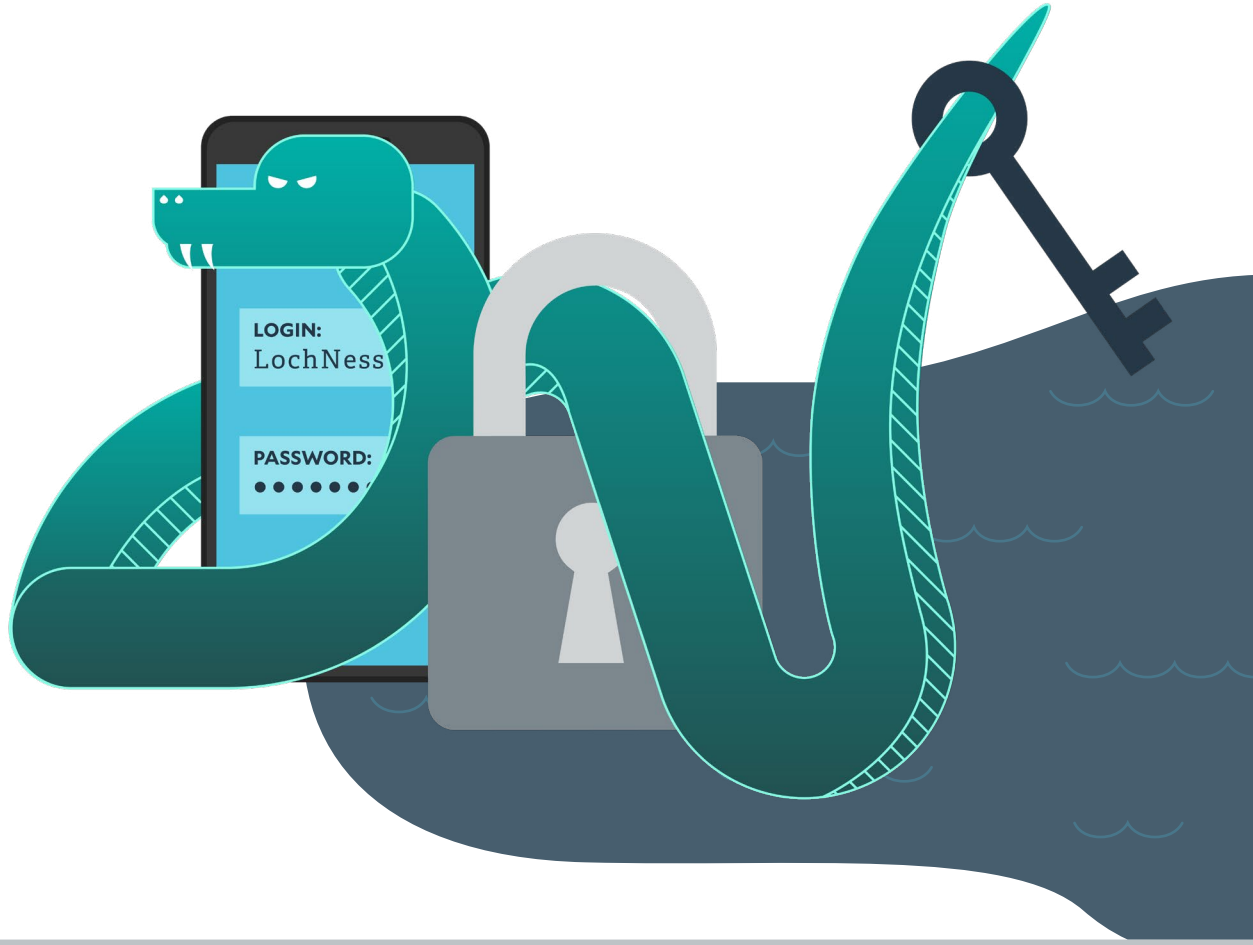
PAM: THE NUMBER ONE SECURITY PROJECT FOR 2019

Why did Gartner name PAM as their number one security project for the year? Because implementing PAM not only has a strong (positive) business impact, but also significantly mitigate the risk of a data breach..

Privileged Access Management helps organizations manage and control privileged access, without compromising on productivity. PAM can ensure a high level of security by managing privileged credentials via a centralized password store, controlling privileged activities and access, and monitoring for any suspicious activity.

At the end of 2018, Gartner released their first-ever Magic Quadrant for PAM. The report evaluates the privileged threat landscape, delivers a thorough analysis of 14 PAM providers, and highlights which privileged access management capabilities are indispensable.

However, misunderstandings around PAM abound. BeyondTrust has identified six of the biggest myths about Privileged Access Management and debunked them to make your life easier when it comes planning your security strategy.



> **By 2022, 90% of organizations will recognize that mitigation of PAM risk is a fundamental security control, which is an increase from 70% today.**
>
> *— Gartner, "Best Practices for Privileged Access Management Through the Four Pillars of PAM," January 28, 2019*

MYTH #1: ZERO TRUST IS ACHIEVABLE

What Is The Zero Trust Model?

First coined in 2010 by John Kindervag, Principal Analyst at Forrester Research, it's become a very popular concept with many organizations seeking to reduce the risk of a data breach.

The principle behind zero trust is that it requires strict verification measures for every device and person accessing resources on a private network, regardless of whether they are within the perimeter of the network. There's no specific technology associated with zero trust, rather several technologies (with multi-factor authentication, or MFA, being a core tenet) in order to reach the ideal state of security. It's therefore considered a holistic approach and an ideal that many companies work towards.

Three Reasons Why Zero Trust is an Unrealistic Ideal

While zero trust has become a trendy catchword in IT, in practice, this model is generally impractical and unrealistic to implement. Though Forrester has provided a five-step roadmap to achieving zero trust, and while many of the recommended approaches have merit and seem logical, a number of unrealistic assumptions are made due to the following issues facing almost every organization:

1 Technical Debt

If your organization develops its own software for consumption, and the applications are more than a few years old, you have technical debt. Redesigning, recoding, and redeploying internal applications can be costly and potentially disruptive. There needs to be a serious business need to undertake these types of initiatives. Adding security parameters to existing applications to make them zero trust-aware is not always feasible. It's extremely likely that your organization utilizes existing applications that have no ability to accommodate zero trust.

2 Legacy Systems

Legacy applications, infrastructure, and operating systems are unlikely to be zero trust-aware. They may lack the concepts of least privilege and lateral movement, and they may not possess authentication models that dynamically allow for modifications based on contextual usage. Any zero trust implementation requires a layered approach to enable these systems. However, a layered approach entails wrapping the external access to the resource and rarely can interact with the system itself. This defeats the premise of zero trust.

3 Digital Transformation

Even for organizations that are in a position to build a new data center, implement a role-based access model, and embrace zero trust 100%, the digital transformation considerations can make the theory difficult to embrace. The digital transformation driven by Cloud, DevOps, and IoT does not inherently support the zero trust model as it requires additional technology to segment and enforce the concept. For large deployments, this can be cost-prohibitive, and may even impact the ability for the solutions to interact correctly with multi-user access.

"Reality"

One model that can help bridge the gap is Just-In-Time Privileged Access Management (JIT PAM). The 'JIT' part originates from within the manufacturing industry and is a strategy that minimizes costs by reducing the in-process inventory level. It is driven by a series of signals that tell the production line to make the next piece for the product and when it is needed.

JIT PAM can help drastically condense the privileged threat surface and reduce risk enterprise-wide, ensuring that identities only have the appropriate privileges when necessary, and for the least time necessary. This process can be entirely automated so that it is frictionless and invisible to the end user.

According to Gartner in their 2018 Magic Quadrant for PAM, "By 2022, more than half of enterprises using privileged access management (PAM) tools will emphasize just-in-time privileged access over long-term privileged access, up from less than 25% today."

Read a more in-depth overview of Just-In-Time Privileged Access Management.

MYTH #2: SHARED ACCOUNTS ARE NEEDED TO ENABLE PAM

Many IT organizations use shared accounts for privileged users, administrators or applications so that they can have the access they need to do their jobs. If managed incorrectly, this practice presents significant security and compliance risks from intentional, accidental, or indirect misuse of shared privileges.

Even for the savviest IT teams, the task of managing shared accounts introduces complexities and risks.

Shared Accounts are Hard to Audit

According to a recent Monitor Report by ICS-CERT, shared accounts "make it difficult to identify the actual user and they allow malicious parties to use them with anonymity. Accounts used by a shared group of users typically have poor passwords that malicious actors can easily guess and that users do not change frequently or when a member of the group leaves."

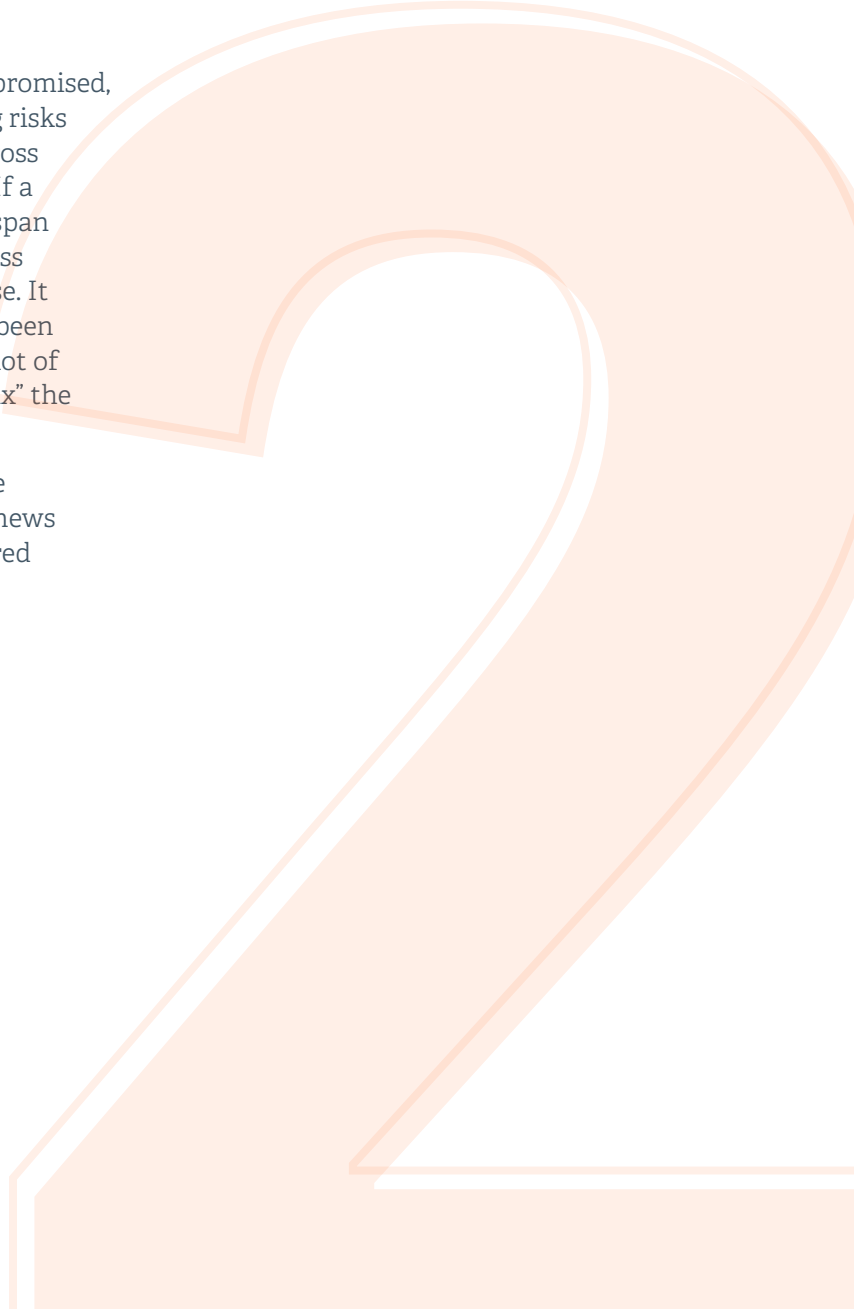
Ingrained Employee Habits are Hard to Change

Even extensive security training and awareness won't always be enough, and hackers prey on our human nature. Social engineering continues to be a popular and successful technique when it comes to gaining access to important systems and data. All it takes is one employee to click a phishing link or visit an insecure site to open a door for hackers. The employee might even be savvy to these kinds of attacks, but if they're caught in a busy moment or are targeted by a sophisticated phish, they can become a victim. And if a superuser account is compromised, the hacker may have instant access to the crown jewels.

"Reality"

If a shared privileged account is compromised, then it carries potentially devastating risks as shared accounts are often used across multiple applications and resources. If a breach occurs, the attacker is able to span multiple employee accounts and access multiple locations across an enterprise. It makes it harder to pinpoint who has been compromised and usually requires a lot of systems that need to be touched to "fix" the problem.

A compromised shared account is like Christmas day to a hacker. The good news is that you don't need to move to shared accounts in order to enable PAM.



MYTH #3: PAM ONLY MANAGES PRIVILEGED ACCOUNTS

PAM Does More Than Manage Your Privileged Accounts

Managing privileged accounts is the tip of the proverbial PAM iceberg. Privileged Access Management comprises of several components, each serving a purpose in the path to achieving the optimal balance between security and productivity. A central goal is the enforcement of least privilege, defined as the restriction of access rights and permissions for users, accounts, applications, systems, devices (such as IoT), and computing processes to the absolute minimum necessary to perform routine, authorized activities.

Alternatively referred to as privileged account management, privileged identity management (PIM), or just privilege management, PAM is considered by many analysts and technologists as one of the most important security projects for reducing cyber risk and achieving high security ROI.

"Reality"

A comprehensive PAM platform includes far more than just privileged account and session management (PASM), though this remains a key component. PAM also consists of privileged elevation and delegation management (PEDM)—also known as endpoint privilege management, secure remote access (for vendors and employees), and more. Some key PAM capabilities include:

- Discovering privileged accounts/credentials on systems, devices and applications and onboarding for ongoing management.
- Automatically randomizing and storing passwords for both human and non-person privileged identities.
- Eliminating administrator and root privileges and simplifying enforcement of least-privilege policies
- Securing remote access pathways for vendors and employees
- Integrating vulnerability data to make informed privileged elevation and delegation decisions based on real-time risk
- Logging all privileged access for auditing and reporting
- Providing privileged user behavior and threat analytics

Integrating with identity governance solutions for seamless visibility and management of privileged and non-privileged identities enterprise-wide

Simply put, PAM covers a much larger area of security controls and threat mitigation than people might think.

- The MITRE ATT&CK framework
- The Top 20 Critical Controls

PAM Components

Password Storage		Password Management		Session Management		Privileged Management	
Asset & Account Discovery	Shared Password Storage	Standard Op Prodcedures	Password Check In/Out	Session Monitoring & Logging	Session Launching (Windows & *nix)	Endpoint/Least Privileged Management	Application Control
	Strong Encryption & Auto Population	Ad-hoc Password Mgmt	Automated Password Mgmt				
System Integration		**PAM Governance**		**Analytics & Reporting**		Application Risk Management	Advanced Control & Audit (ACA)
Help Desk & Ticketing	SIEM	PAM Standards & Policies	Privileged Acct Ownership	Reoprting on KPI's & KRI's	Audit		
SSO & MFA	Access Certification		Privileged Acct Reconciliation		Forensics	User Behavior Analysis	Platform Agnostic

MYTH #4: PAM HELPS YOU MANAGE & CONTROL ACTIVE DIRECTORY

Privileged access management addresses far more than your Active Directory (AD) accounts. Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

"Reality"

However, in 2018, 52.2% of internet traffic came from **mobile devices** and is predicted to rise to 63.4% by the end of 2019. The cocktail of increasing BYOD challenges and expanding cloud services are all part of the multi-platform movement towards which IT environments are shifting. It's also worth noting that enterprises utilizing DMZ networks (which often sit outside the walls of AD) have additional security risks which PAM can also assist in mitigating.

Another high-value target for attackers are Unix and Linux systems, since they host your most critical data and applications. Without complete protection and control of privileged credentials and accountability over user actions, organizations could be exposed to risky gaps in security.

A comprehensive PAM solution for Unix and Linux mitigates all of these risks by securing, auditing, and monitoring all privileged accounts and activities across your most critical systems. Active Directory is just one of many considerations organizations should have in their security strategy.

Additionally, PAM also helps in other, less conventional areas of risk across your organization, such as corporate social media accounts. Passwords to your corporate Facebook, Twitter, or LinkedIn accounts should be considered privileged; if the credentials fall into the wrong hands, misuse could lead to significant, long-term brand and reputational damages.

MYTH #5: VENDOR ACCESS CAN BE SECURED USING THE SESSION MANAGEMENT CAPABILITIES OF YOUR PASSWORD MANAGER

The Role of Password Managers

Password managers are helpful tools for users overwhelmed by the volume of passwords they need to know to access the myriad of systems, portals, and countless other applications existing in the typical organization. So, the idea of having an encrypted digital vault that can store all of this information for you, as well as generate unique and strong passwords for different services, is often an essential (and sometimes free) tool many people leverage.

But consumer-oriented password managers, such as LastPass, 1Password, and Dashlane have significant limitations. Many mistakenly believe these types of password managers will offer session management capabilities that can secure vendor access. That just isn't the case.

The Limitations of VPN

VPN access is not the same as session monitoring. Knowing a VPN session has been initiated does nothing to tell you if the actions in the session are appropriate. For the sake of security and auditability, IT teams need to go above and beyond VPN management capabilities, which means session monitoring with keystroke logging, indexing, and command filtering for truly secure remote sessions.

"Reality"

Session management alone does not secure the protocols used for vendor access. A gateway, proxy, bastion host, or jump point is needed as a middleware to ensure that the session is not used as a beachhead for additional malicious activity.

Solutions such as Privileged Remote Access not only secure, manage, and audit vendor and internal remote privileged access without a VPN, but it also works across hybrid environments and enables you to meet more complex compliance requirements through its comprehensive audit trails and session forensics.

It's important to stress that free tools (such as RDP) just aren't robust enough – for an in-depth analysis, review the white paper: The True Cost of Free Remote Support Software.

MYTH #6: PAM REQUIRES A LARGE IT TEAM & EFFORT TO IMPLEMENT & MANAGE

The concept of implementing privileged access management can be daunting for many – especially if your environment is made up of a variety of operating systems, legacy software, and far-flung global locations. Or, maybe you have a small IT team that is already stretched to the limit. However, a good PAM solution will be simple to deploy and maintain over time. Implementing PAM is easier than you might think.

"Reality"

PAM is comprised of three primary components, with different efforts required for each, listed below from lowest to highest effort and maintenance:

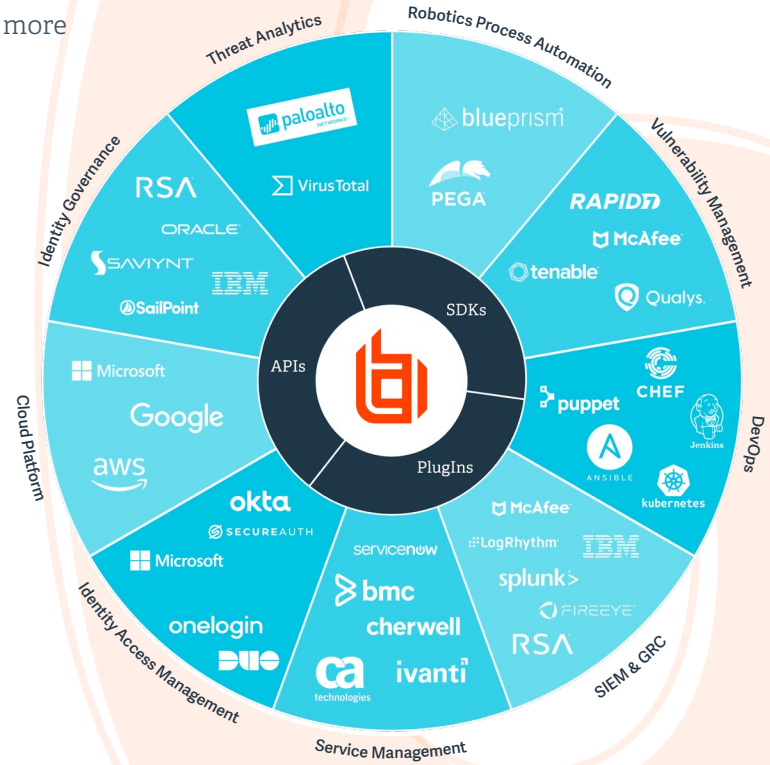
- Secure Remote Access (SRA): secure, manage, and audit vendor and internal remote privileged access without a VPN. Little to no maintenance required.
- Endpoint Privilege Management (EPM): eliminate unnecessary privileges and elevate rights to Windows, Mac, Unix, Linux and network devices without hindering productivity. Limited maintenance required when environmental or application changes occur.
- Privileged Account and Session Management (PASM): discover, manage, audit, and monitor privileged accounts of all types. Medium-level maintenance needed, when changes to procedures, environment, or personnel occur.

Once the environment is installed for each component, internal automation (including database maintenance), are all provided in a leading PAM solution.

Implementation Made Easier Through Integrations

In terms of implementation, you should consult the experts from partners, vendors, and system integrators (SI's). They have experience installing PAM and can turn a potentially steep learning curve into a very manageable project. Leading PAM providers will provide an extensive set of integrations, meaning you can benefit from technologies working together straight out-of-the-box, maximizing your existing IT investments and making the entire process even more seamless and efficient. For example, BeyondTrust integrates with a wide range of third-party solutions. See the figure below for an overview of our partner ecosystem.

For less overhead and infrastructure requirements, PAM solutions can be deployed in the cloud using SaaS (software as a service) or a hosted solution such as AWS or Azure. Managing credentials in the cloud can make managing privileged access easier and more cost-effective. For organizations looking to reduce privileged access risks, while facing ongoing staffing and resource shortages, PAM cloud solutions provide reduced administrative burdens along with rapid deployment.



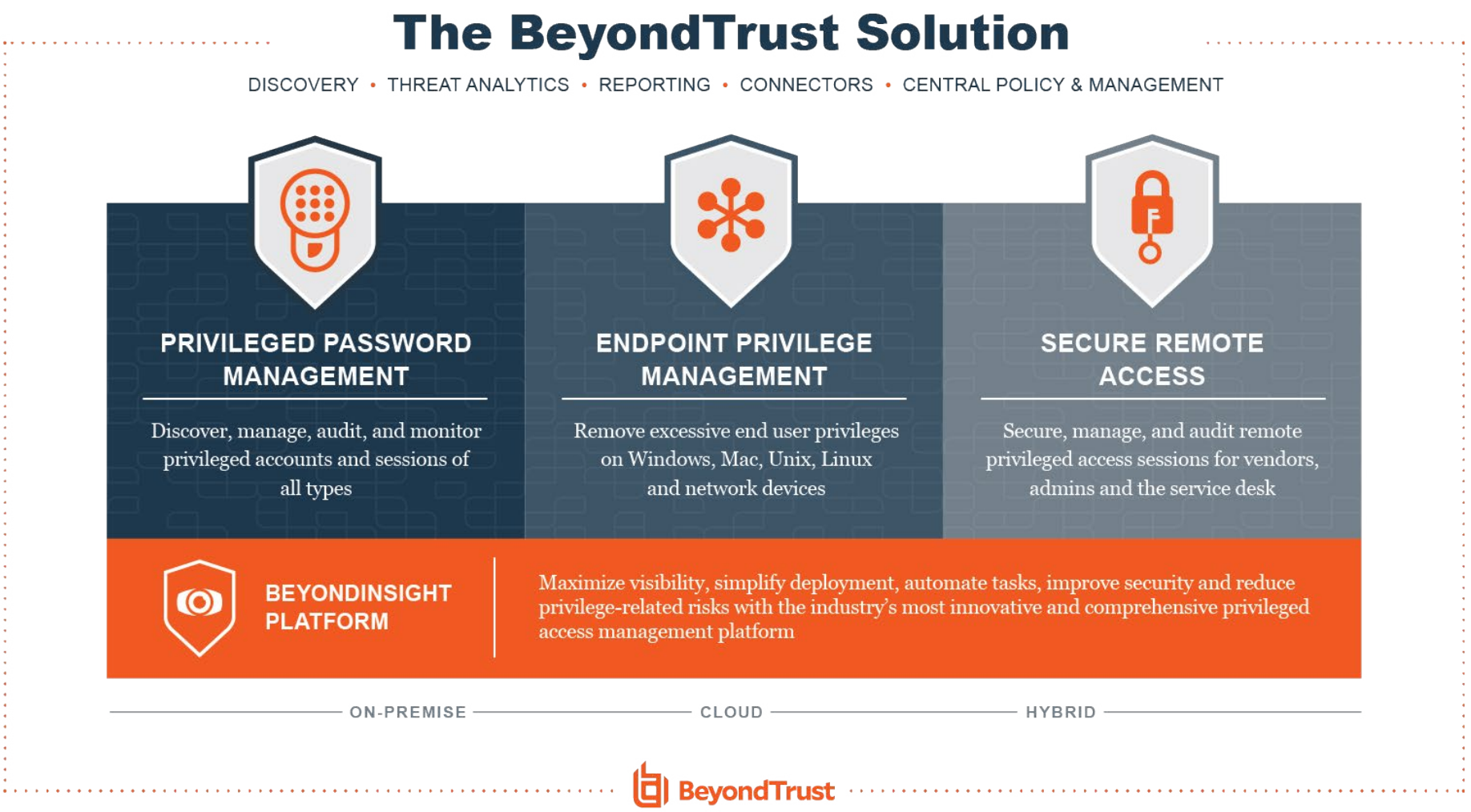
CONCLUSION

It's important to be able to sort myths from facts when determining your organization's approach to mitigating the risks of a cyber breach. Understanding the true benefits and use cases of privileged access management is a key step you can take to significantly enhance your organization's security strategy.

The comprehensive Buyer's Guide for Complete Privileged Access Management from BeyondTrust provides more detailed guidance on selecting the right PAM solution for your business. In it, you'll discover how to holistically assess your privileged access security needs and map them to modern privilege management solutions. It will help you identify where to begin your privileged access management project, how to progress to a better IT security posture, and what business outcomes to expect.

THE BEYONDTRUST PLATFORM

The BeyondTrust Privileged Access Management platform is an integrated solution to provide control and visibility over all privileged accounts and users across all enterprise platforms. By uniting best of breed capabilities that many alternative providers offer as disjointed tools, the BeyondTrust Privileged Access Management platform simplifies deployments, reduces costs, improves system security, and closes security gaps to reduce risks.



About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.

About Endpoint Privilege Management

BeyondTrust Endpoint Privilege Management combines privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices without hindering productivity.

About Privileged Password Management

BeyondTrust Privileged Password Management solutions enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities.

About Secure Remote Access

BeyondTrust Secure Remote Access solutions enable organizations to apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.

beyondtrust.com

V2020_03_ENG