Best Practices:
PAM Security and Data Privacy

Chris Hills
Deputy Chief Technology Officer

BeyondTrust

Agenda

- Analyzing the Term “Best Practice”
- The Challenge
- Is My Organization Secure?
- Is My Cybersecurity and PAM Strategy Worth the Investment?
- Understanding Who has Access to What
- 10 Key Components for a Successful PAM Strategy
- Threat Landscape
- Busting the 6 Myths
- Key Takeaways

What Does Best Practice Really Mean?

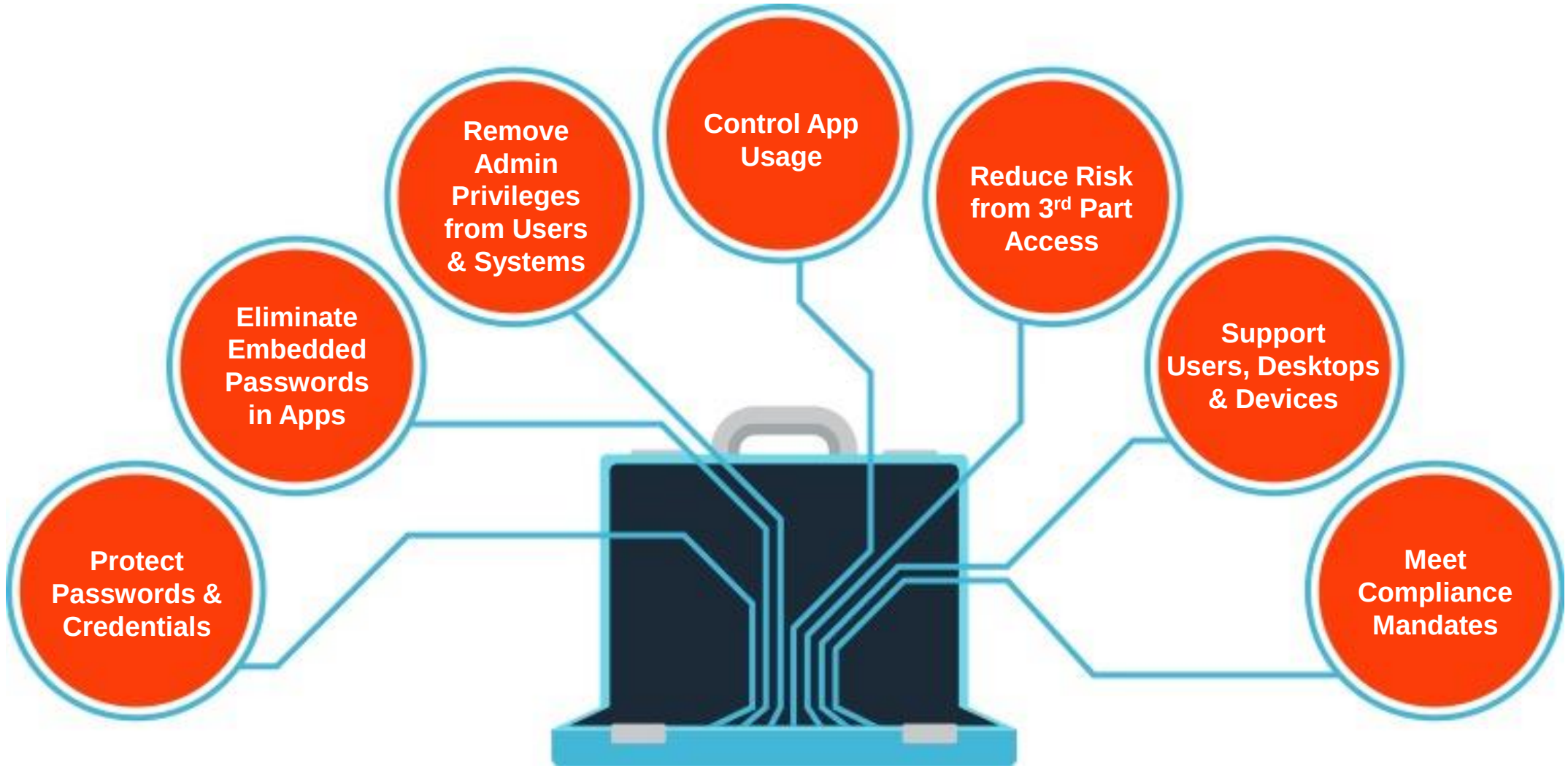
The Challenge

THREE MAIN QUESTIONS CISOs SHOULD BE ASKING

1	Is my organization secure?	Finding balance between Risk Appetite and Tolerance vs Mitigating Risk
2	Is my cybersecurity and PAM strategy worth the investment?	Finding balance between budgets, timelines and reducing risk
3	Who has access to what?	Understanding entitlements, controls, and compliance

Securing your Organization

HOW ARE YOU REMOVING RISK?



3 Pillars of Privileged Access Management

SECURING PRIVILEGED ACCOUNTS, ENDPOINTS, AND USERS

Data Breaches Are Not Slowing Down

VOLUME OF ATTACKS AND COST TO IMPACTED BUSINESSES CONTINUES TO RISE

Global average total cost of a data breach[1]

Average size of a data breach[1]

Average time to identify & contain a data breach[1]

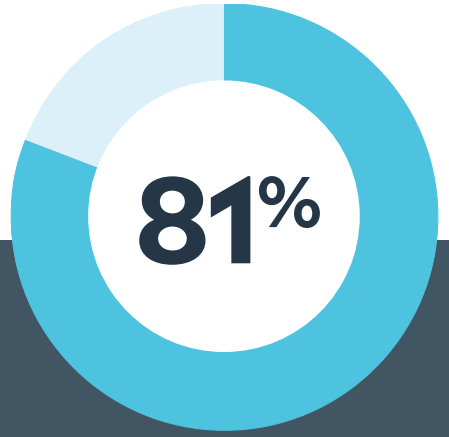
Reported increase in breaches in 1H.2019[2]

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

The Impact

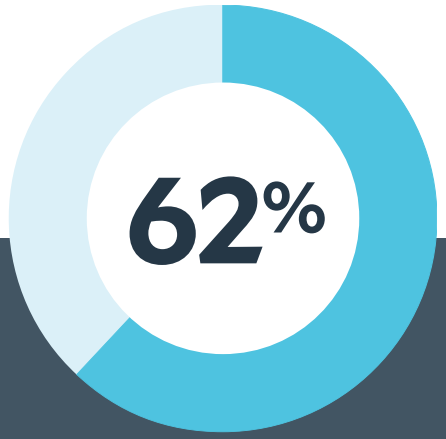
Unmanaged privileges and accounts leave the **door open for hackers**.

vulnerabilities are associated with **excess admin rights**[1]



of breaches start with **stolen and/or weak passwords**[2]

of breaches are the result of **privilege account abuse or misuse**[3]



of companies **aren't adequately tracking** privileged access[4]

Source: 1. 2018 Microsoft Vulnerabilities Report, BeyondTrust | 2. 2018 Privileged Access Threat Report, BeyondTrust
3. "The Forrester Wave™: Privileged Identity Management, Q3 2016 | 4. Forrester. "2017 Data Breach Investigations Report", 10th Edition, Verizon

Who Has Access To What?

ENTITLEMENTS, CONTROLS, AND COMPLIANCE

- **Entitlements**
- Validate and Review access
- 40% of Enterprises never bother to look for all Privileged Accounts
- **Controls**
- Ensure your controls align with Privileged Access and Risk Mitigation
- 62% of Enterprises fail to provision for privileged Access Accounts
- **Compliance**
- PAM provides a fast and flexible response to critical compliance factors
- GDPR – ISO 27001 – Access Rights, Data Privacy, Management, Audit

10 Key Components for a Successful PAM Strategy

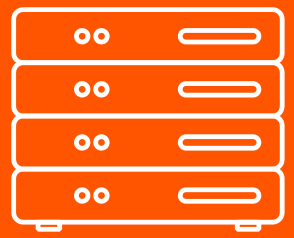
FRAMEWORK FOR PRIVILEGED ACCESS MANAGEMENT

1. Track and Consolidate all privileged accounts - Old and New – with an automated discovery mechanism.
2. Search for and Find Obtuse credentials in all corners of your organizations network
3. Define clearer roles aligned to Enterprise and Application based responsibilities.
4. Require multi-factor authentication and/or 2 Step Verification when possible.
5. Leverage shared accounts without revealing their password in plaintext, only when needed.
6. Remove excessive admins rights across all endpoints.
7. Mature access polices for Just-In-Time PAM.
8. Remove embedded credentials in scripts and applications processes.
9. Enforce strict policies Password rotations and intervals.
10. Ensure everything is tracked, audited, and reviewed.

Data Breaches Are Not Slowing Down

20 YEARS AGO

On-Premise



- Shared Admin Accounts
- Desktops (Windows, Mac)
- Servers (Unix, Linux, Windows)
- Industrial Control Systems
- Security Infrastructure
- Network Infrastructure
- Applications & Application Servers
- Databases & Database Servers
- Machine Credentials (AtoA)
- Hypervisors & Virtual Machine

10 YEARS AGO

Cloud & Hybrid

- Cloud Mgmt. Platforms (AWS, Azure)
- Virtualized Environments (VMWare, MSFT)
- Virtualized Machines (Unix, Linux, Windows)
- SaaS Apps (Facebook, LinkedIn, Custom)

TODAY

IoT & DevOps

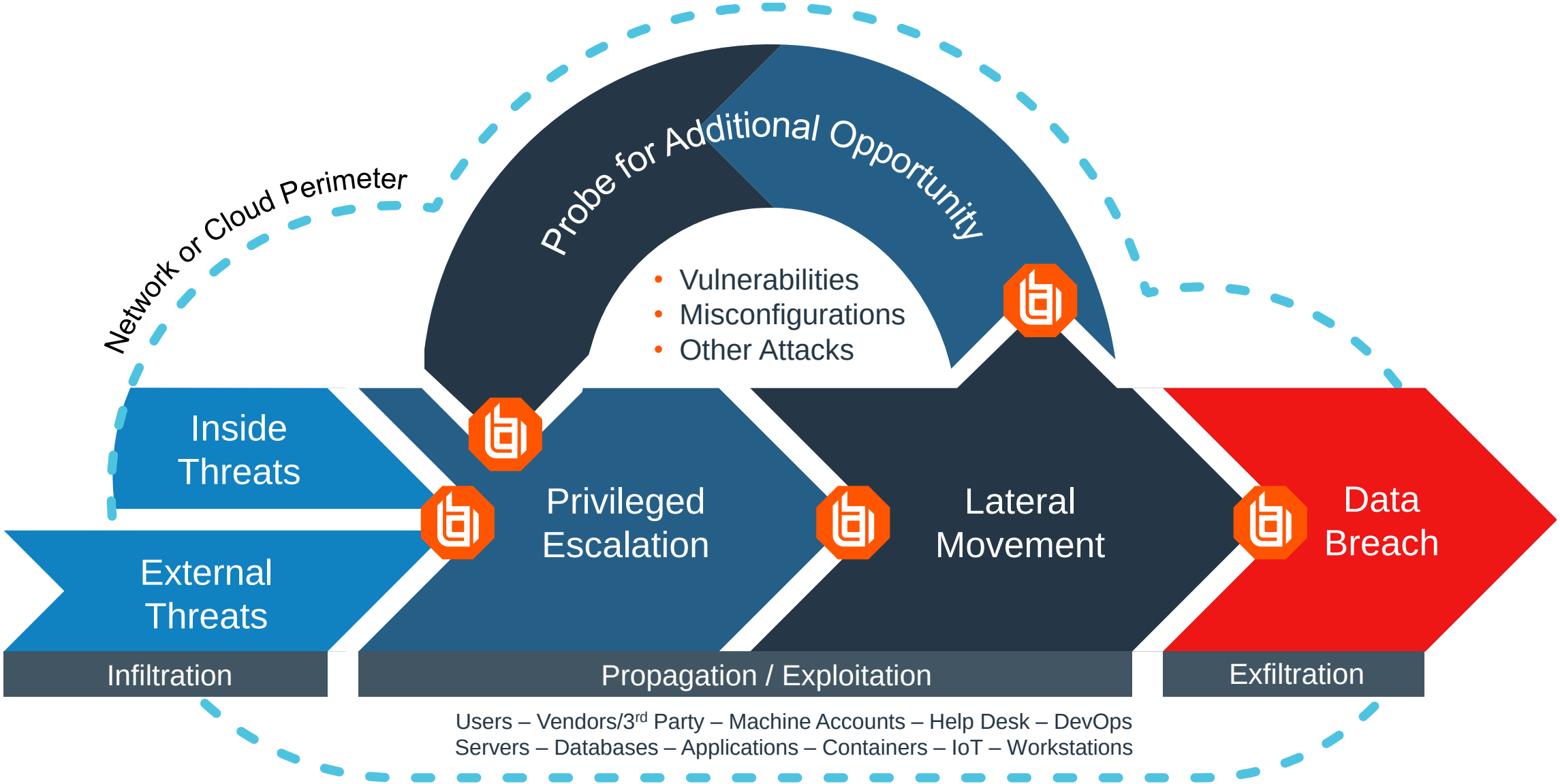
- Roaming workstations
- BYOD
- Cameras, Sensors, Printers
- DevOps & SecDevOps Tools
- Dynamic Virtual Environment
- Containers
- Microservices

NEAR FUTURE

Even More Priv. Accts

- SaaS Admins
- Cloud Admins
- Application Admins
- Privileged End Users
- Developers
- Machine Password & Keys

The Attack Chain



The Attack Vector

HIGHEST CHANCE OF SUCCESS

- The account is enabled (always on)
- The account is not monitored
- The account has root or administrative privileges
- The account can authenticate against multiple assets including critical and not critical resources
- The asset is not monitored for lateral movement or inappropriate activity
- An asset has multiple unmanaged accounts


Let’s Bust Some
PAM Myths!

MYTH #1

The Zero Trust Model Is Achievable

Myth #1: The Zero Trust Model Is Achievable

MYTH BUSTED

- While Zero Trust is a nice concept, it's also **unrealistic** for most companies to implement in a short space of time
- It would take a **lot of work to rearchitect entire networks**, and would be as fraught as changing a wheel while you're driving
- This is before considering whether employees will **adopt new practices** and change the ways they're used to working

Background on the "Just-In-Time" (JIT) Concept

Just-In-Time manufacturing is a strategy to minimize 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.

Gartner®

> 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.

- Gartner, Magic Quadrant for Privileged Access Management, December 3, 2018

MYTH #2

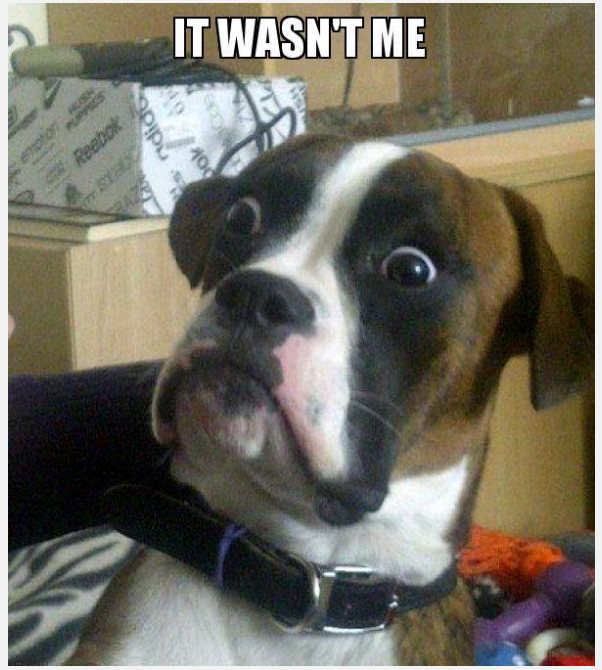
To Enable PAM You Must Move To Shared Accounts

Myth #2: To Enable PAM You Must Move To Shared Accounts

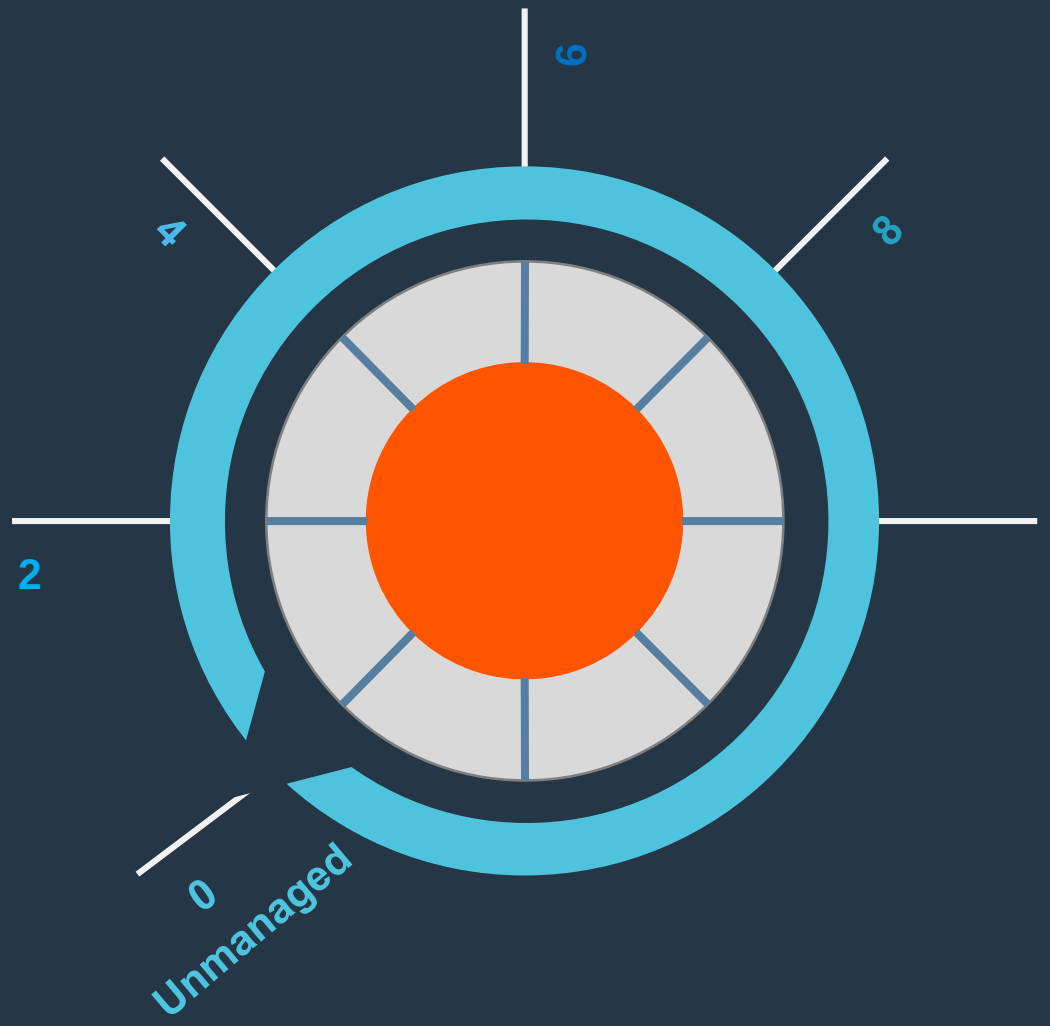
MYTH BUSTED

There are several issues with using shared accounts:

- Harder to audit
- Even harder to change behaviours
- Scope of risk if account is compromised
- Need for attestation of events who



The Security Dial Goes to 11



MYTH #3

PAM Is Only Managing Privileged Accounts

Myth #3: PAM Is Only Managing Privileged Accounts

MYTH BUSTED

- Managing privileged accounts is the tip of the proverbial PAM iceberg.
- It's just **one of the many pillars** needed to support an effective security strategy.
- PAM includes securing remote access, vulnerability management, auditing, password and session management and more elements.
- Securing privileged accounts should be part of a more thorough approach **to optimal security.**

MITRE ATT&CK Framework

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

ATT&CK™

Remote Access

KNOWN MALICIOUS USE OF REMOTE ACCESS TOOLS FOR LATERAL MOVEMENT

- APT1, APT3, APT39
- WannaCry
- OilRig
- TA505
- ….and more!

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

PAM: The #1 Security Project for 2019

Project 1: Privileged access management (PAM)

Privileged accounts (or administrative or highly empowered accounts) are attractive targets for attackers. A PAM project will highlight necessary controls to apply to protect these accounts, which should be prioritized via a risk-based approach. PAM projects should cover human and nonhuman system accounts and support a combination of on-premises, cloud and hybrid environments, as well as APIs for automation.

MYTH #4

PAM Only Helps You Manage & Control Active Directory Accounts

Myth #4: PAM Only Helps You Manage & Control Active Directory Accounts

MYTH BUSTED

- Todays IT environments are **multi-platform**
- **Growth of Mac/Linux** presenting a different attack surface
- **DevOps is growing**
- BYOD challenges
- More diverse networks

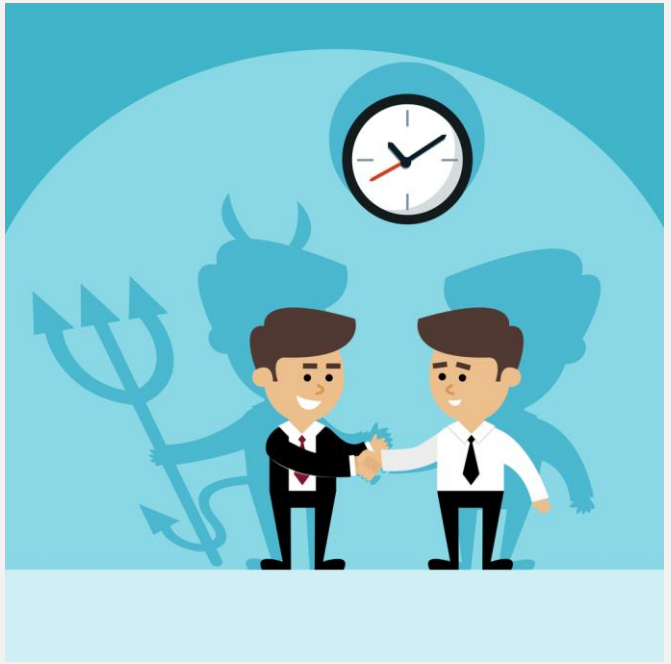
MYTH #5

Vendor Access Can Be Secured Using VPN

Myth #5: Vendor Access Can Be Secured Using VPN

MYTH BUSTED

- Should you treat vendors the same as employees?
- Just-In-Time capabilities
- 4 eyes: Chaperoning of vendors
- A true secure remote access solution is required – with the right architecture and full audit trail capabilities



MYTH #6

PAM Requires a Big IT Team/Effort To Implement & Manage

Myth #6: PAM Requires a Big IT Team/Effort To Implement & Manage

MYTH BUSTED

- **Automation** can deliver significant savings (*JIT, automated discovery, onboarding*)
- Work with **partners**
- PAM is not just passwords – PAM is a journey and you can **achieve quick wins**
- Focus on **ROI/efficient time-to-value**

Quick Wins

- Ensure tool **covers ALL platforms**
- Manage Existing Dedicated Accounts
- Auto/continuous discovery
- Vendor access with **zero footprint**
- Session management – **reduce attack surface massively**
- Reduce number of administrative rights in the network
- Quick Start Policies

The BeyondTrust Advantage

Market Leader

Ranked as PAM leader in Gartner MQ & Forrester Wave

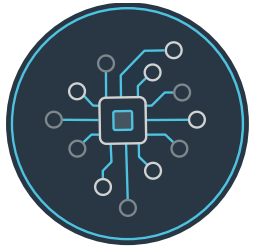
Proven Experience

20,000 customers in 80+ countries

Global Presence

800 employees in 20+ countries and an extensive partner networks

Broadest Portfolio



Integrated PAM Platform with best in class products

Innovative Platform

Expansive roadmap and wide range of integrations

Customer Driven

90% renewal rates and exceptional customer support

Key Takeaways

FOUR CONSIDERATIONS CISO's SHOULD BE ASKING

1	Do you feel you've done everything you can to secure your organization?	Or are you worried about a cybersecurity compromise
2	Are you getting the most out of your PAM solution?	Or are you only using a small percentage of it
3	Do you know about all of your organizations privileged accounts?	Or do you feel there is still some work to be done to discover them
4	Do I know what is Fact vs Fiction when it comes to PAM ?	Or have you been led to believe someone else's truth

Q&A

THANK YOU

Central Region Rep

Ted Remble

TRemble@BeyondTrust.com

BeyondTrust