



# Alliances

 **Digital Alliances**

continue collaboration

CISO Alliances Nairobi

Feb 10<sup>th</sup> 2021

In Partnership with





In partnership with **BeyondTrust**

**CISO Alliances**  
**Digital Alliances**  
continue collaboration

"Six Myths of PAM Busted"  
**Nairobi**

Wed 10th of February 15.00-16.30 (EAF)  
To register: [phil@alliances.global](mailto:phil@alliances.global)  
[www.alliances.global](http://www.alliances.global)

Session Leader:  
Morey Haber, CTO & CISO  
BeyondTrust

Session Leader:  
Brandon Haberfeld, Global Head of  
Operating System - Investec

During the session Morey Haber, CTO & CISO - BeyondTrust in addition to Brandon Haberfeld, Global Head of Operating System - Investec led an in-depth analysis of the six myths / common misconceptions of PAM and first-hand experience of the PAM Journey.

- The Ever-Increasing Threat
- Attack Vectors & Weakest Links
- Today's IT Environment
- The Six PAM Myths

### Six Myths of PAM?

- Myth #1 The Zero Trust Model is achievable
- Myth # 2 To enable PAM you must move to shared accounts
- Myth # 3 PAM is only managing privileged accounts
- Myth # 4 PAM only helps you manage & control Active -Directory accounts
- Myth # 5 Vendor access can be secured using VPN
- Myth # 6 The cost of PAM, including financial and businesses changes, is not worth the risk

**MYTHS**  
**BUSTED**

## FOOD FOR THOUGHT /TOPICS DISCUSSED



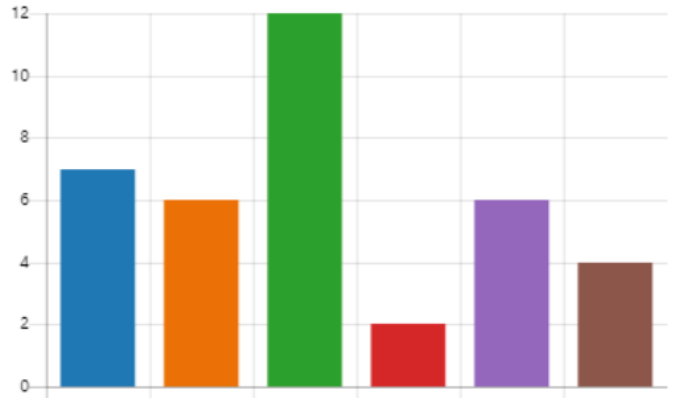
### Community Poll 1

Prior to today session which of the 6 myths of PAM have crossed your mind?

[More Details](#)



- Myth #1 The Zero Trust Model... 7
- Myth # 2 To enable PAM you ... 6
- Myth # 3 PAM is only managi... 12
- Myth # 4 PAM only helps you ... 2
- Myth # 5 Vendor access can b... 6
- Myth # 6 The cost of PAM, incl... 4



### Community Poll 2

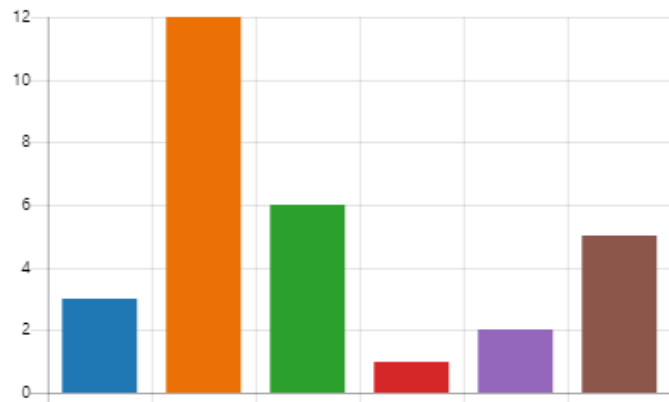


. Where did you hear the myths?

[More Details](#)



- Media 3
- Industry 12
- Peers 6
- Analyst organisations 1
- Security Agency 2
- From Personal experience 5



# Digital Alliances

continue collaboration

## Myth #1



### **Myth #1: The Zero Trust Model is achievable**

- 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



©BeyondTrust 2021 | 8

## Myth #2



### **Myth #2: To enable PAM you must move to shared accounts**

- There are several issues with using shared accounts:
  - Harder to audit
  - Even harder to change behaviors
  - Scope of risk if account is compromised
  - Need for attestation of events who



©BeyondTrust 2021 | 13

## Myth #3



### **Myth #3: PAM is only managing privileged accounts**

- 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.



©BeyondTrust 2021 | 16



## Myth #4



### **Myth #4: PAM only helps you manage & control Active Directory accounts**

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



©BeyondTrust 2021 | 20

## Myth #5



### **Myth #5: Vendor access can be secured using VPN**

- 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



©BeyondTrust 2021 | 23

## Myth #6



### **Myth #6**

The cost of PAM, including financial and businesses changes, is not worth the risk



©BeyondTrust 2021 | 24

## FOOD FOR THOUGHT /TOPICS DISCUSSED



### PAM Journey Recommendations/Experiences:



- Educate senior executives to understand and acknowledge zero trust is unachievable
- Organisations who do not security technology in build stage will face trouble and consequences



- Importance of a clean architecture - Do not consider as a product
- Legacy software is not the only problem
- Tools themselves have interesting problem due to need of functional accounts



- Segregation to allow accounts to do what is needed
- Challenges in shared accounts - Primarily in infrastructure part of IT, Databases etc.



- Use of tiering in place for certain functions
- Ability to mitigate worst case scenario is linked to maturity of PAM
- VPN just moves parameter for security - Risk of VPN is unacceptable
- BYOD bring problems and risk to the business i.e. illegal to scan, poor anti-virus, use of unwired connections



- Condition Access - Shut down avenues as solves PAM journey as well as data management
- Cost when protecting assets - choice has to be made with right product set



- Half effort to PAM will cause challenges down the line

### How to start PAM Journey?



### Common angle is to initially protect those highly sensitive:

- Try to get to every account possible
- Identify what is interactive vs. automated - separate human accounts without specific focus
- Have ability to rotate all accounts at once
- Single identity is the most important aspect in PAM journey - requires up front work for identity hygiene



### Supportive Links



- <https://www.beyondtrust.com/blog/entry/avoid-common-privileged-access-pitfalls>
- <https://www.beyondtrust.com/resources/videos/beyondtrust-privileged-access-management-platform-overview>
- <https://www.beyondtrust.com/blog/entry/cloud-pam-5-keys-to-a-successful-foundation>

## FOOD FOR THOUGHT /TOPICS DISCUSSED



Questions posed by audience:



- Educate senior executives to understand and acknowledge zero trust is unachievable
- How would you manage various services attached to a 'functional account' - some real life experiences?
- Brandon - how did you manage system/application accounts - did you have some DevOps on the application side? it's easier on the PAM side but what about the application/database side



- How do you manage PAM with Active Directory RedForest?
- What are the major non-functional capabilities that one needs to look for in a PAM Vendor?



- Is PAM hosted on the cloud?
- Does it also support Multi-cloud platform?

Additional audience comments.....



"Am thinking Zero-trust works better for all users instead of PAM, because PAM is for Privileged Access only."



"I like the centralization into AD!"



"If you can remove the need for VPN access for vendors, then that's worth it. Vendors only require specific system access"

