The History and Evolution of Privileged Access Management

Jeff Zupan

Jeff.Zupan@OneIdentity.com

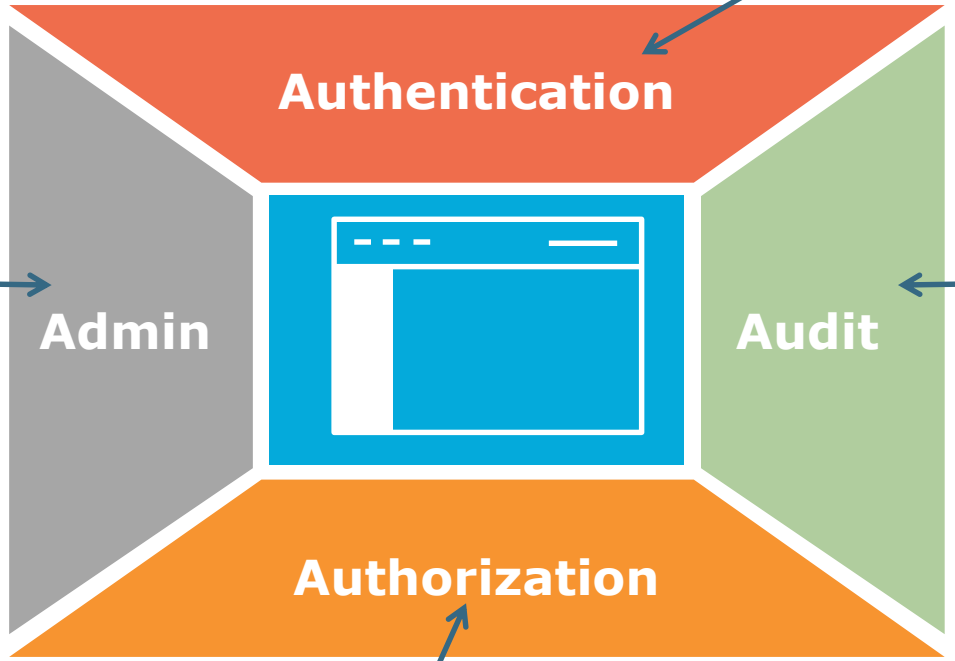
ONE IDENTITY

What is Privileged Access Management?

- Privileged Access Management consists of the tools and techniques an organization can use to safeguard data by protecting the users and accounts that have elevated rights(privilege) to systems containing valuable or sensitive data. It is required to:
  - Secure and control access to privileged accounts
  - Assign individual accountability to administrator access and activities
  - Provide an indelible audit trail of activities performed with elevated privileges
  - Ensure compliance with regulations

Privileged accounts are special…

One password, shared across lots of people (anonymous)



You need admin access to do any of this stuff

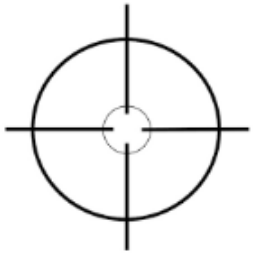
Don't know what's done with admin rights … or who did it

Rights are all or nothing – SUPERusers

Managing Privileged Access

Since privileged access is a necessary evil, we must control what we can…

- Scope
  - Horizontal – how many and which devices can the privileged user access
  - Vertical – how much privilege do they require on the device to perform the task



- Time
  - When do they need privilege
  - How long do they need it

History – the early years

- Physical Access
  - Attached Terminals
  - Very limited networking

- Privileged Password Management up until the early 2000's
  - Manually managed, i.e. "envelopes in a safe"
  - Homegrown scripts or applications
  - Stored in a file
  - Unmanaged due to resources required versus perceived risk

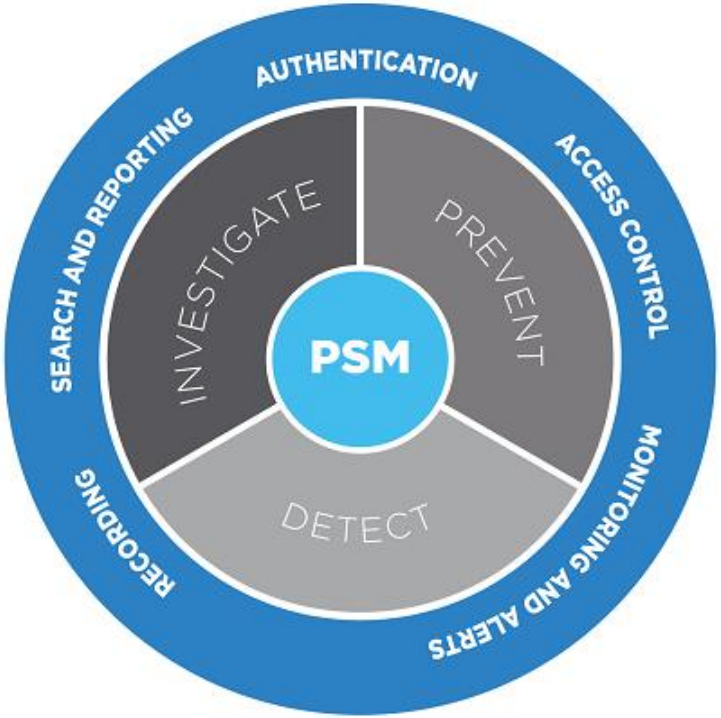
History – solutions emerge

Privileged Password Management

- Full-lifecycle password management
  - Scheduled checks and resets
  - Post-Use reset
- Embedded workflow
- Individual accountability
- Segregation of duties
- Very strong security

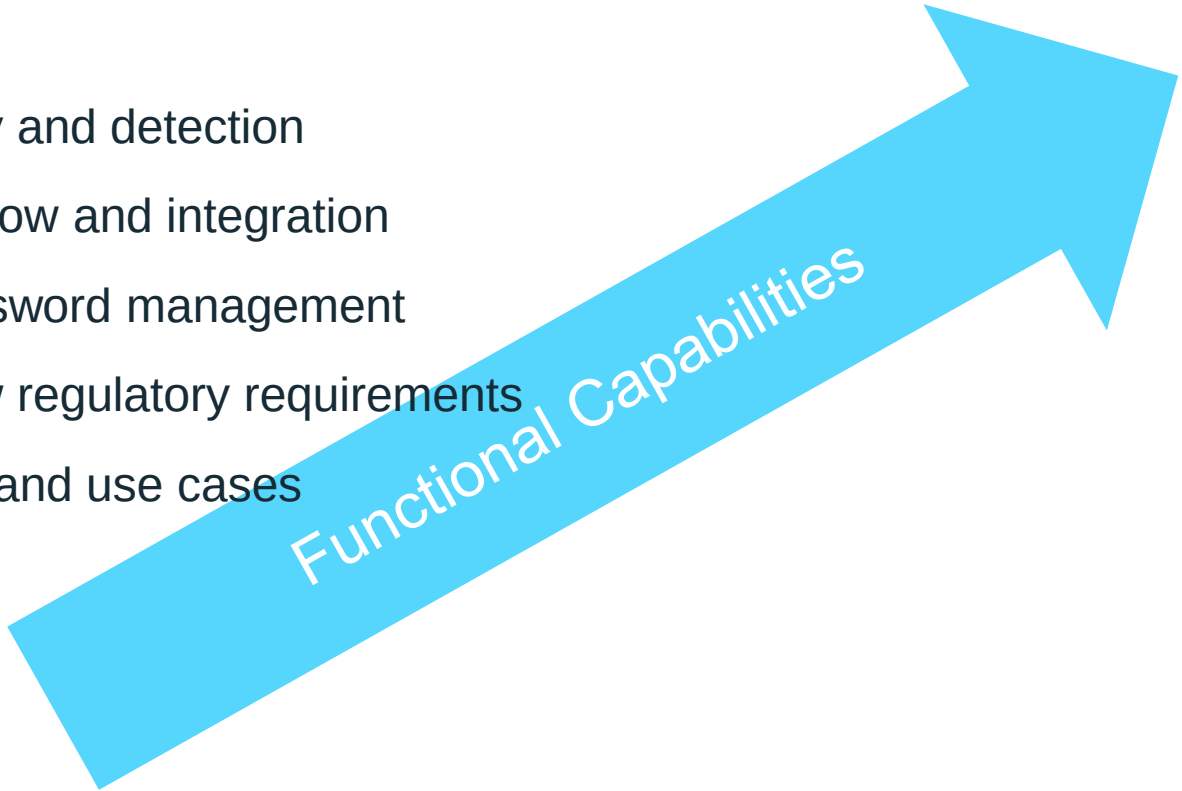
History – solutions emerge, continued

- Privileged Session Management
  - Eliminated the need-to-know the credential
  - Complete recording for auditing and forensics
  - Real-time monitoring
  - Command blacklisting and whitelisting
  - Network segregation
  - Access from anywhere



The solutions evolve

- Better discovery and detection
- Improved workflow and integration
- Application password management
- Adapting to new regulatory requirements
- More platforms and use cases
- Resiliency



But, the challenges continue to evolve as well

- Bad actors constantly exploit weaknesses
- Careless or malicious insiders
- Everything and everyone connected
- Users, resources and entitlements everywhere
- Security teams are increasingly reactive

A few statistics…

39 seconds

54%

87+105

$2T

What are the next steps?

Managing the password is not enough

- Better integration with Identity Governance
- Risk-based Approach to privileged access
- Behavioral Analytics and machine learning
- Identity Analytics
- Convergence of PAM and PEDM
- Hybrid PAM

Managing Risk - Like two sides of a coin

Eliminate Risk “At Rest”

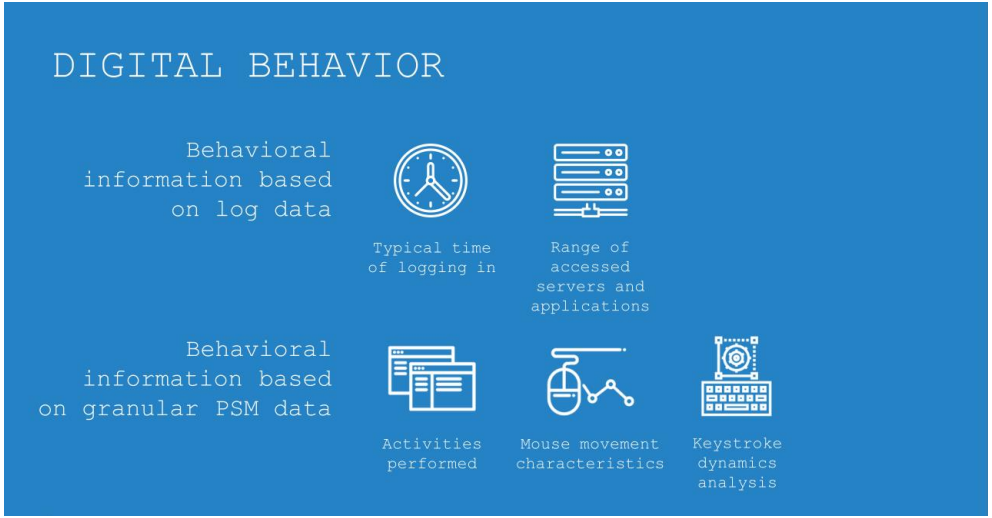
- Remove entitlement grants before someone can abuse or exploit them
- Reduce risk before bad behavior occurs and impacts the business

Eliminate Risk “In Motion”

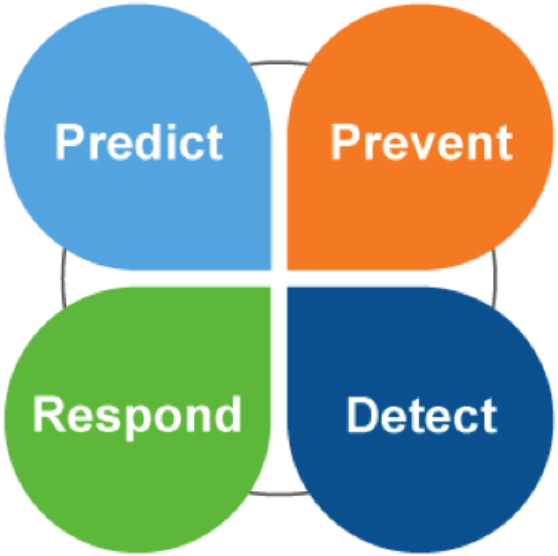
- Detects user behavior deviations
- Determines which anomalous behavior trends could result in a real threat

Frictionless analytics using Machine Learning

- Gather users' digital footprints
- Hardware & device fingerprinting
- Define what is normal, build user baselines
  - Leverage machine learning; peer-group analysis
- Identify unusual and risky events in real-time
  - Behavioral biometric inputs (keyboard, mouse)
  - Historical command usage & norms
  - Temporal usage & norms
- Evaluate risk in <u>real-time</u> and <u>proactively</u> request confirmation of activity from end-user or manager



Protect yourself against cyber attacks




ONE IDENTITY™