PRIVILEGED IDENTITY MANAGEMENT IN THE CLOUD

ADAM BOSNIAN
CYBER-ARK SOFTWARE
Adam Bosnian is EVP Americas and Corporate Development at Cyber-Ark Software. He has more than 20 years of experience in defining and implementing successful security strategies for customers who need to better manage insider threats and meet goals associated with compliance and reliability. Bosnian specializes in the area of privileged identity management, focusing on the risks associated with powerful users or accounts with high-level and often anonymous access to sensitive applications, networks and systems. He also has extensive experience in technology, retail and financial services industries.
Privileged Accounts Defined

The problem posed by privileged accounts:

- Most powerful accounts in the organization
- Access sensitive information
- Rarely changed, known to many
- No individual user accountability

“Shared superuser accounts — typically system-defined in operating systems, databases, network devices and elsewhere — present significant risks when the passwords are routinely shared by multiple users.”

– Gartner, MarketScope for Shared-Account/Software-Account Password Management
Identity should not just be viewed as a reference for authenticating the entity but also gathers more information about the user for making access decisions.

Identity also includes the identities of the devices that applications run on, privileged users that manage that VM image, identities of other applications and services that application needs to interact with, identities of administrative users to manage the application and external identities outside of the enterprise that need access to the application....
Identity should not just be viewed as a reference for authenticating the entity but also **gathers more information** about the user for **making access decisions**.

Identity also includes the identities of the devices that applications run on, privileged users that manage that VM image, identities of other applications and services that application needs to interact with, identities of administrative users to manage the application and external identities outside of the enterprise that need access to the application….
Identity should not just be viewed as a reference for authenticating the entity but also gathers more information about the user for making access decisions.

Identity also includes the identities of the devices that applications run on, privileged users that manage that VM image, identities of other applications and services that application needs to interact with, identities of administrative users to manage the application and external identities outside of the enterprise that need access to the application....
Identity should not just be viewed as a reference for authenticating the entity but also gathers more information about the user for making access decisions.

Identity also includes the identities of the devices that applications run on, privileged users that manage that VM image, identities of other applications and services that application needs to interact with, identities of administrative users to manage the application and external identities outside of the enterprise that need access to the application….
Identity should not just be viewed as a reference for authenticating the entity but also gathers more information about the user for making access decisions.

Identity also includes the identities of the devices that applications run on, privileged users that manage that VM image, identities of other applications and services that application needs to interact with, identities of administrative users to manage the application and external identities outside of the enterprise that need access to the application....
Identity should not just be viewed as a reference for authenticating the entity but also gathers more information about the user for making access decisions.

Identity also includes the identities of the devices that applications run on, privileged users that manage that VM image, identities of other applications and services that application needs to interact with, identities of administrative users to manage the application and external identities outside of the enterprise that need access to the application….
Privileged Accounts Give System-Wide Access

“48% of data breaches were caused by privileged misuse”
Proactively manage privileged access to prevent such attacks

Who has access to privileged accounts?
- Administrators
- Contractors; Cloud Service Providers
- DBAs
- Terminated Employees
- Applications

Why are these breaches happening?
- Shared account usage
- Excessive privilege
- “Hidden/Sleeping” accounts
- No revocation of access
- Non-existent/unenforced access controls
- Infrequent replacement of credentials

* Verizon, Data Breach Investigations Report
Key Drivers for Privileged Account and Session Management

Insider Threats

Risk and Compliance

Moving to the Cloud

Targeted Cyber Attacks

“Access is not privileged enough: 52% can access restricted, confidential information beyond the requirements of their position”

Ponemon Institute, Global Privilege Study, Dec 2011
CONVICTED!!!

Jerome Kerviel, Societe Generale

Rajendrasinh Makwana, Fannie Mae

75% in Oracle DBA survey: Our organizations do not have a means to prevent privileged database users from reading or tampering with human resources, financial or other business application data in the databases.

Source: Independent Oracle Users Group
"Every defense company is constantly under attack. If anybody tells you they’re not, it just means they don’t know."

Northrop Grumman Chief Executive Wes Bush, Sep. 07, 2011
The Terminology Doesn’t Matter…

Cyber Attacks

Advanced Persistent Threat (APT)

Ongoing Targeted Attacks

Cyber Threat

Cyberwarfare
Targeted Attacks

- **Purposeful attacker** – not opportunistic
  - Organized, funded, directed
  - Criminal, government
  - Collects and acts on mission intelligence

- **Persistent** – will continue until target achieved
  - Continuously use various attack vectors

- **Covert** – prefer “low and slow” approach

Possible purposes:
- Collection of information
- Exploiting the network
- Sabotage
Sneak and Peek | How intruders broke into the Chamber of Commerce and stole data

Hackers in China break into the Chamber’s network, possibly through a ‘spearphishing’ attack that dupes an employee into clicking on a link or opening a document laced with spyware. This probably happened in Nov. 2009 or earlier.

Intruders obtain the passwords to obtain ‘administrator’ level access to the whole Chamber network. Intruders establish about a half dozen ‘back doors’ in the Chamber’s computer networks, so they can come and go as desired.

Intruders establish a network of roughly 300 Internet addresses, which give them outposts to issue directives to the spyware in the Chamber’s system. send new spyware to that system and offload stolen data.

Intruders in May 2010 are discovered by the FBI to be stealing data from the Chamber.

FBI alerts the Chamber.

The Chamber hires outside cybersleuths to investigate. The investigators find that the stolen data include the email of four employees who work on Asia policy issues. It isn’t possible to determine whether other information was stolen earlier.

The Chamber moves to shut down the spy operation and overhauls its network security. It continues to find suspicious activity such as a thermostat communicating with Chinese computers and a printer that spontaneously printed Chinese characters.
Increased Awareness with increased allocated budgets

“It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.”

President Obama, May 29, 2009

“I'm often asked what keeps me up at night? No. 1 is the cyber threat!”

Deputy Defense Secretary William J. Lynn III, February 13, 2010

“[...] the next Pearl Harbor that we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems”

Leon Panetta, before a Senate committee in a confirmation hearing for his appointment as Secretary of Defense, June 9, 2011
In today’s environment, any enterprise must work under the assumption that it is a potential target for attack.

Source: Mandiant derived from approximately 120 APT victims Mandiant had exposure to over the past 18 months.
"The Privileged Connection"

**Cyber-Attack on Canada**

"the attackers used “executive spear-phishing” to capture control of Canadian government officials’ individual machines [...] Once the attackers had access, they began to send emails from the officials’ computers, asking for passwords to various servers. [...] Many government officials gave up these passwords as the emails appeared to come from a trusted source. [...]"

Privileged accounts are a critical step in attacks to gain access to the enterprise’s core assets and cause damage. Privileged account passwords should never be shared among employees, or left static and unchanged…" - “Identity Week”, Sep 22, 2011
Realistic Approach to Neutralizing Advanced Targeted Threats

Minimize vulnerabilities and attack apertures, make sure the business can still operate — then focus on the threat.
Manage use and usage of shared accounts and passwords
Manage superuser privileges
Manage sessions for shared and other privileged accounts
Monitor usage of these accounts with "keystroke" granularity
The Complexities Of The Modern Datacenter

Line of Business A
- Business User
- Developer
- Infrastructure

Enterprise Central Datacenter
- IT Personnel
- Business Applications
- Operating Systems
- Infrastructure

Line of Business B
- Business User
- Developer
- Infrastructure

Public Cloud
- IT Personnel

Outsourced Datacenter
- IT Personnel

Outsourced IT Personnel

Cyber-Ark
Security That Empowers People™
Enterprise 1

**Business Application A**

**Business Application B**

**Operating Systems**

**Infrastructure**

**Enterprise IT Environment**

**Developer**

**Business User**

**Enterprise 2**

**Business User**

**IT Personnel**

**Characteristics:**
- Accessible anywhere, anytime
- No development & administrative costs
- Minimal waste – pay for what you use
PaaS

**Characteristics:**
- Minimal waste – pay for what you use
- No additional SW costs
- Agile development
- Shorter development lifecycles
IaaS

Enterprise 1
- Business Applications
- Operating Systems
- Infrastructure

IaaS

IT Personnel

Enterprise 2
- Business Applications
- Operating Systems
- Infrastructure

Ent. 1 Image

Ent. 2 Image
Hosted Datacenters

Hosted

Business Applications
Operating Systems
Infrastructure

IT Personnel

Enterprise IT Environment

Cyber-Ark
Security That Empowers People™
Managed Datacenters

Managed IT Personnel

Remote connection

Business Applications

Operating Systems

Infrastructure

Enterprise IT Environment
Risks When Moving To The Cloud

- Where is my data physically located?
- Is there strict tenant isolation?
- Who can access and view my data?
- Is there full HA & DR?
- What are the procedures of preventing data leakage?
- Is my data being backed up?
- Can I switch providers easily?
- What other risks are lurking out there?
Bottom Line

- **The right to audit**
  - Large enterprises want/need control of their data wherever it is

- **Periods of transition = uncertainty**
  - Security and PIM solutions required to protect sensitive data even in the cloud

- **Premium security services**
  - Allows vendors to offer the ‘Fort Knox’ security services customers are demanding

- **Become the ‘Trusted Advisor’**
  - If security for using the cloud is the customers key areas of concern, we need to be there with our knowledge and expertise
What to Do?

Privileged Activities are Everywhere!
What to Do? – 7 Steps to PIM/PAAM Best Practices

1) Include Privileged Identities within Security/IAM project(s) scope

2) Identify key systems, applications and databases
   - AND the underlying privileged account(s) that exist in each one

3) Identify Who **Should** have access to these accounts

4) Determine Who **Does** have access to these accounts

5) Define Policies for Privileged access to key systems
   - Dual-Control approval, time based access, password changes
   - Down to session and command level policies

6) Implement processes to automatically apply policy definitions
   - Manual or Automated

7) Monitor and report actual adherence to defined policies
   - Via SIEM tools, GRC tools, PIM reports et al
PRIVILEGED IDENTITY AND PRIVILEGED SESSION MANAGEMENT
Unified Workflows for Accessing Privileged Accounts

I need to check out the root password
I have this script that connects with “root” every night...

I just need “root” to patch the database
I need my service provider to connect remotely with “root”

Great, what are your “root” entitlements, who used it and why?
Privileged Identity Management Components

- **Portal/Web Access**
  - Password Vault and Policy/Log Management
  - Application Password Management
  - Privilege Escalation (sudo) Management

- **Policy Controller/Auto-discovery**

- **Secure Digital Vault**

- **External Vendors**
- **IT Personnel**
- **Auditors**
- **Developers & DBAs**

- **Any Device, Any Datacenter – On Premise, Managed, Hosted or In The Cloud**

**CyberArk**
Security That Empowers People™
Expanding from Managing Accounts to Managing Sessions

Portal/Web Access

Secure, manage and track privileged accounts

Isolate, control, and monitor privileged sessions

Policy Controller/Auto-discovery

Secure Digital Vault

Identity Management

Ticketing Systems

Monitoring & SIEM Applications

Enterprise Directory and more

Any Device, Any Datacenter – On Premise, Managed, Hosted or In The Cloud
PIM Minimizes Concerns In The Cloud

- **Policy-based access restriction** - full audit trail & accountability
- **Monitor activity**
  - Web interface to view activity and define policies & workflows
  - Session recording
- **Business continuity** - Password versioning if lost or broken
- **Integrate with my existing IT authentication systems** whether in the cloud or on-premise
- **Compliant-ready solution** – proven COTS solutions in thousands of organizations
- **Secure storage**
  - Tamper-proof vault for passwords & recordings
  - Password encryption when in transit & at rest
General PIM Capabilities for Cloud

- **Strict control over external administrators**
  - Session monitoring and recording
  - Privileged SSO to prevent divulging of credentials
  - Segregation of duties and granular admin access control
  - Detailed audit trails

- **PIM reporting**
  - Hosting provider can see full audit across the system while each customer can see their own sub-set of audit info, entitlements etc. (segregation of duties / multi-tenancy)
  - Policy level definition can be set per tenant (customer)

- **Protecting critical applications and databases**
  - Eliminating hard-coded passwords from scripts and applications
  - Protecting DBA and key application accounts
Cloud Provider With Multi-Tenant Infrastructure

- **Increase my selling value**
  - Offer premium security services; differentiate from competition

- **Protect my reputation & minimize financial losses**
  - Improve my security posture and reduce insider threat

- **Dispel security concerns**
  - Guarantee security best practices & prove to my customers that I am protecting their assets
  - **Strict tenant isolation** – built-in segregation of duties

- **Approach compliance with confidence**
  - e.g. SAS 70, PCI, SOX

- **Improve SLAs**
  - Automation & web-based system means better operational efficiency & quicker time to resolution

---

“We believe many organizations will pay a premium to cloud providers that are known to be secure.”

Cyber-Ark Privileged Identity & Session Management

Improving Your Security Posture With A Preventative Approach

- Minimize Insider Threats
- Approach Compliance with Confidence
- Protecting & Isolating Sensitive Assets
- Securing Critical Applications
- Advanced Protection from Persistent Threats
- Enable Secure Cloud Migration
- Continuous Activity Monitoring

Privileged Access Control
Cyber-Ark’s Solutions Suites:

- **Sensitive Information Management Suite**
  - Governed File Transfer Suite
  - Secure Email Manager
  - Sensitive Document Vault™

- **Privileged Identity Management Suite**
  - Enterprise Password Vault®
  - Application Identity Manager™
  - On-Demand Privileges Manager™

- **Privileged Session Management Suite**
  - PSM for Servers
  - PSM for Databases
  - PSM for Virtualization
Unified Workflows for Accessing Privileged Accounts

I need to check out the root password.

I have this script that connects with “root” every night...

Great, what are your “root” entitlements, who used it and why?

Virtual Servers

Unix/Linux Servers

Windows Servers

iSeries

zSeries

Mainframes

Mainframes

Databases

Applications

Network Devices

Security Appliances

Cyber-Ark

Security That Empowers People™
PIM for the Cloudy Enterprise – IaaS

My Enterprise

Privileged Session Manager

Vault

PVWA/CPM/PSM

Auditors

Security/Risk Management

Enterprise IT Environment
PIM for the Cloudy Enterprise – Managed Services
PIM for the Managed Service / IaaS / Hosting Providers

- Auditors
- IT
- Central Policy Manager
- IT Environment
- PVWA/CPM/PSM
- Vault (HA Cluster)
- Hosting Data Center
- Enterprise 1
- Enterprise 2
- Auditors
- Security/Risk Management
Key Takeaways

**Vendor Perspective**
- Increase selling value
- Protect reputation & minimize financial losses
- Dispel security concerns
- Strict tenant isolation
- Approach compliance with confidence
- Improve SLAs

**Customer Perspective**
- Policy-based access restriction
- Monitor activity
- Business continuity
- IT infrastructure integration
- Compliant-ready
- Secure storage
Summary: Privileged Identity & Session Management

- A comprehensive platform for isolating and preemptively protecting your datacenter – whether on premise or in the cloud
  - Discover all privileged accounts across datacenter
  - Manage and secure every credential
  - Enforce policies for usage
  - Record and monitor privileged activities
  - React and comply
USE CASES / DEMO
Who Dun it?

Auditing tools will only tell you what user was logged in not who it **REALLY** was!!

Cyber-Ark gives you the integration point to show WHO the user was.

Source: Independent Oracle Users Group
So What about multiple users??

In some organizations multiple users may need to use the same credential at the same time, how do you differentiate between the users?

Solution: Privileged Session Management:
Administrators may need to be restricted in what they can accomplish when using a privileged Identity.
Collaborate – Contribute – Connect

- [www.isaca.org/knowledge-center](http://www.isaca.org/knowledge-center)

- The Knowledge Center is a collection of resources and online communities that connect ISACA members – globally, across industries and by professional focus - under one umbrella. Add or reply to a discussion, post a document or link, connect with other ISACA members, or create a wiki by participating in a community today!