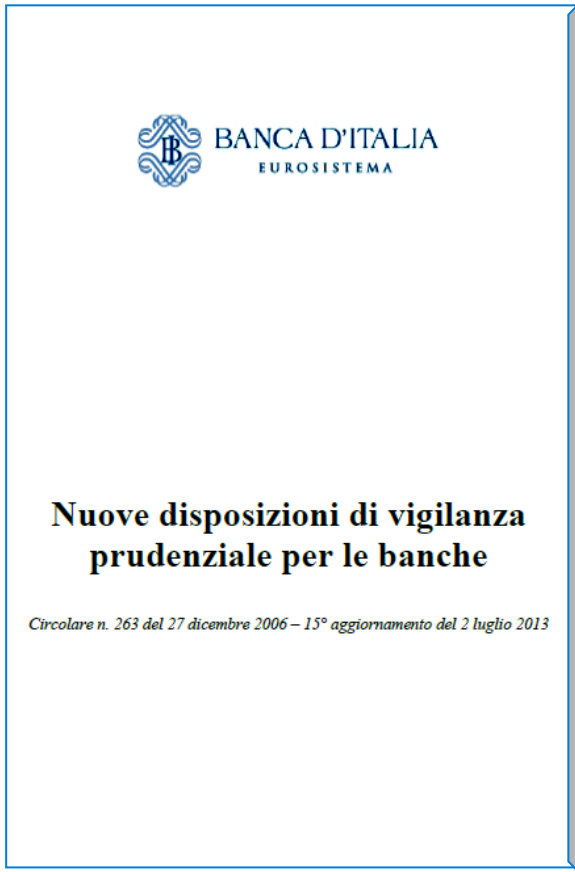
CyberArk e la Circolare n°263: risposte tecnologiche

Marco Di Martino
Sales Engineering and Professional Services Manager
SEMEA Region

La Circolare 263 –

Titolo V - Capitolo 8 - IL SISTEMA INFORMATIVO



SEZIONE IV - LA GESTIONE DELLA SICUREZZA INFORMATICA

3. La sicurezza delle informazioni e delle risorse ICT

"Tali misure sono distribuite su diversi strati, <<… >> comprendendo:

- la procedura di **autenticazione per l'accesso alle applicazioni e ai sistemi;** in particolare sono garantiti **l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione, l'osservanza degli standard definiti all'interno nonché delle normative applicabili,** ad es. in materia di composizione e gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche;

- le procedure per lo svolgimento delle operazioni critiche, garantendo il **rispetto dei principi del minimo privilegio e della segregazione dei compiti** (ad es., specifiche procedure di abilitazione e di autenticazione, **controlli di tipo four eyes, o di verifica giornaliera ex post**);

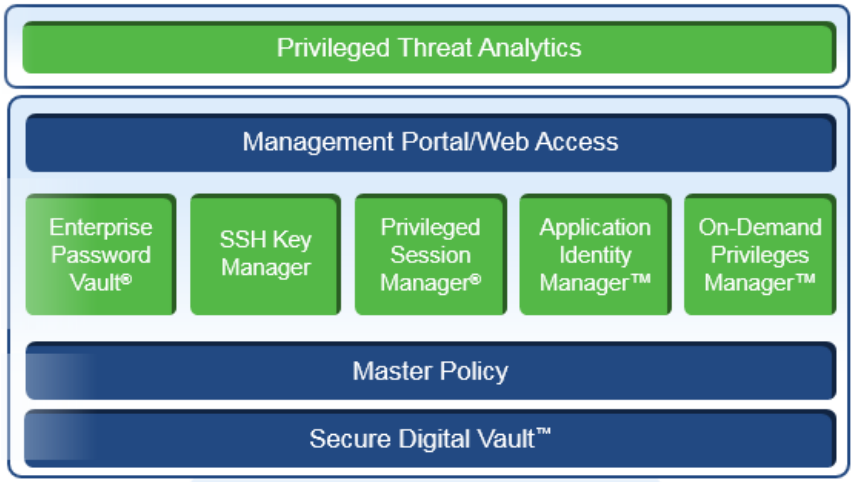
- **il monitoraggio, anche attraverso l'analisi di log e tracce di audit, di accessi, operazioni e altri eventi** al fine di prevenire e gestire gli incidenti di sicurezza informatica; **le attività degli amministratori di sistema e altri utenti privilegiati delle componenti critiche sono sottoposte a stretto controllo;**

- le regole di **tracciabilità delle azioni svolte**, finalizzate a consentire la verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora, contesto operativo e altre caratteristiche salienti della transazione. **Le tracce elettroniche sono conservate per un periodo non inferiore a 24 mesi in archivi non modificabili** o le cui modifiche sono puntualmente registrate."

CYBERARK

La Circolare 263 - CyberArk

- CyberArk è l'**unica soluzione sul mercato** che, **in un unico prodotto** , permette la **completa gestione delle utenze privilegiate e del loro utilizzo.** I diversi moduli permettono di **rispondere ai requisiti derivanti dalla Circolare 263** gestendo le utenze privilegiate presenti su applicazioni e sistemi **senza effettuare cambiamenti invasivi** sugli stessi.



La suite PAS (Privileged Account Security) di CyberArk è composta dai seguenti moduli:

Enterprise Password Vault®

Soluzione che permette di **proteggere, gestire e tracciare** tutti gli **account privilegiati impersonali**

Privileged Session Manager™

Isola, controlla e monitora le attività amministrative svolte in sessioni con account privilegiati in modo da proteggere database, ambienti virtuali, dispositivi di rete e server da attacchi interni ed esterni e **fornire evidenze di audit relativamente alle attività svolte.**

Application Identity Manager™

Permette di **eliminare** le **credenziali contenute in script e applicazioni garantendone la riservatezza e la sicurezza**

On-Demand Privileges Manager™

Soluzione per la **gestione e il monitoraggio delle utenze privilegiate e "superuser"**.
L'utilizzo di utenze impersonali (come "root“) da parte degli utenti viene controllato mediante una **politica di autorizzazione all'utilizzo granulare, registrando poi i comandi eseguiti e gli output ottenuti.**

SSH Key Manager

Soluzione per la **gestione dell'intero ciclo di vita della chiavi di autenticazione SSH**.
Permette la **discovery, provisioning e la rotazione delle chiave sui target server**

CYBERARK

CyberArk Overview

Trusted experts in privileged account security

- 1,800 *privileged account security* customers
- 40% of Fortune 100

Approach privileged accounts as a security challenge

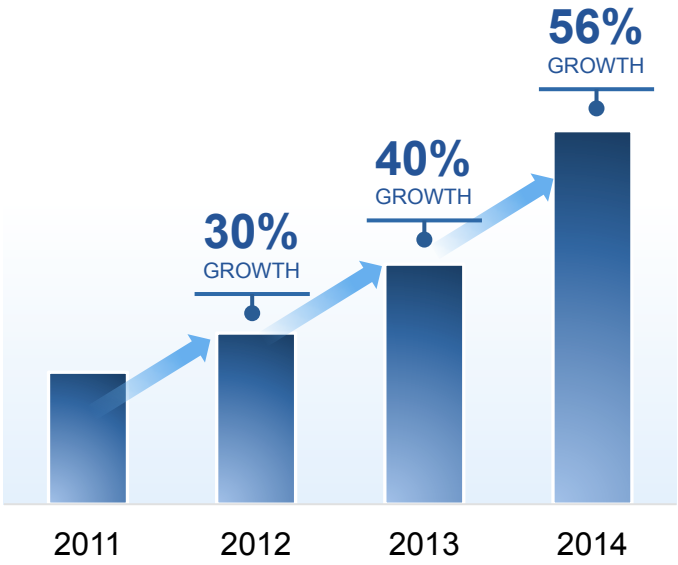
- Designed and built from the ground up for security

Twelve years of innovation in privileged account controls, monitoring and analytics

- First with vault, first with monitoring, first with analytics
- Over 100 software engineers, multiple patents

Only comprehensive privileged account security solution

- One solution, focused exclusively on privileged accounts
- Enterprise-proven



CYBERARK®

IDC Names CyberArk the PAM Market Leader

IDC MarketScape: Worldwide Privileged Access Management

"CyberArk is the PAM pure-play "big gorilla" with the most revenue and largest customer base."

Source: IDC 2014

SOURCE: "IDC MarketScape: Worldwide Privileged Access Management 2014 Vendor Assessment", by Pete Lindstrom , December 2014, IDC Document #253303

CYBERARK®

Privileged Accounts: Pathway to Cyber Attacks

BlackPOS Attacks Retailers

At the end of 2013 and continuing into 2014, several large retail organizations were attacked using BlackPOS, a type of malware targeting point of sale systems. The malware was transferred into at least one of the organizations using **privileged** network credentials assigned to a remote vendor

Attackers use email spam to infect point-of-sale terminals with new malware

MORE LIKE THIS

- New malware program Punkey targets point-of-sale systems
- New malware program PoSeidon targets point-of-sale systems
- Cybercriminals borrow from APT playbook in attack against PoS vendors

on IDG Answers

How to convert Google Docs to Word format?

Credit card terminals have used same password since 1990s, claim researchers

MORE LIKE THIS

- 166816 (Z66816): A post-RSA Conference recap
- CSO50 winners announced
- White Lodging Services confirms second payment card breach

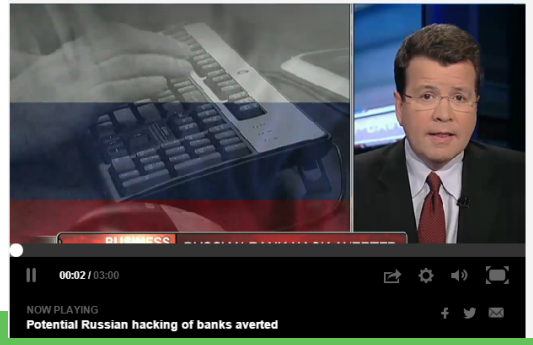
on IDG Answers

How to retrieve data lost from Outlook address book after creating a shortcut?

New Russian Hacks Target US Banks

By Elizabeth MacDonald · Published May 14, 2015 · FOXBusiness

153 405 7



More from Fox Business

"…once they have privileged credentials, they are pretty much home free."

Deloitte, 2014

CYBERARK

An Attacker Must Obtain Insider Credentials

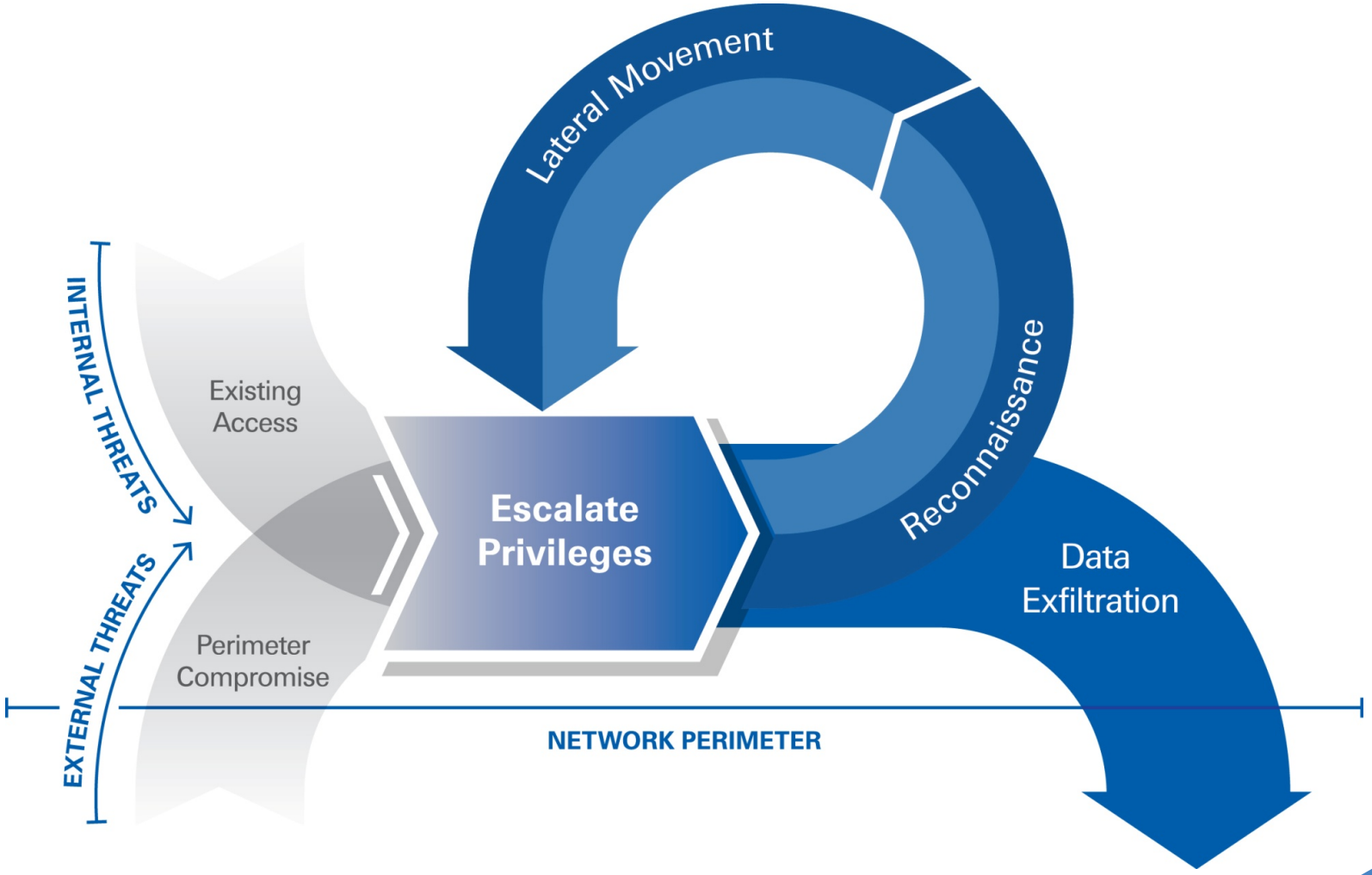
"…100% of breaches involved stolen credentials."

"APT intruders…prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts."

Mandiant, M-Trends and APT1 Report

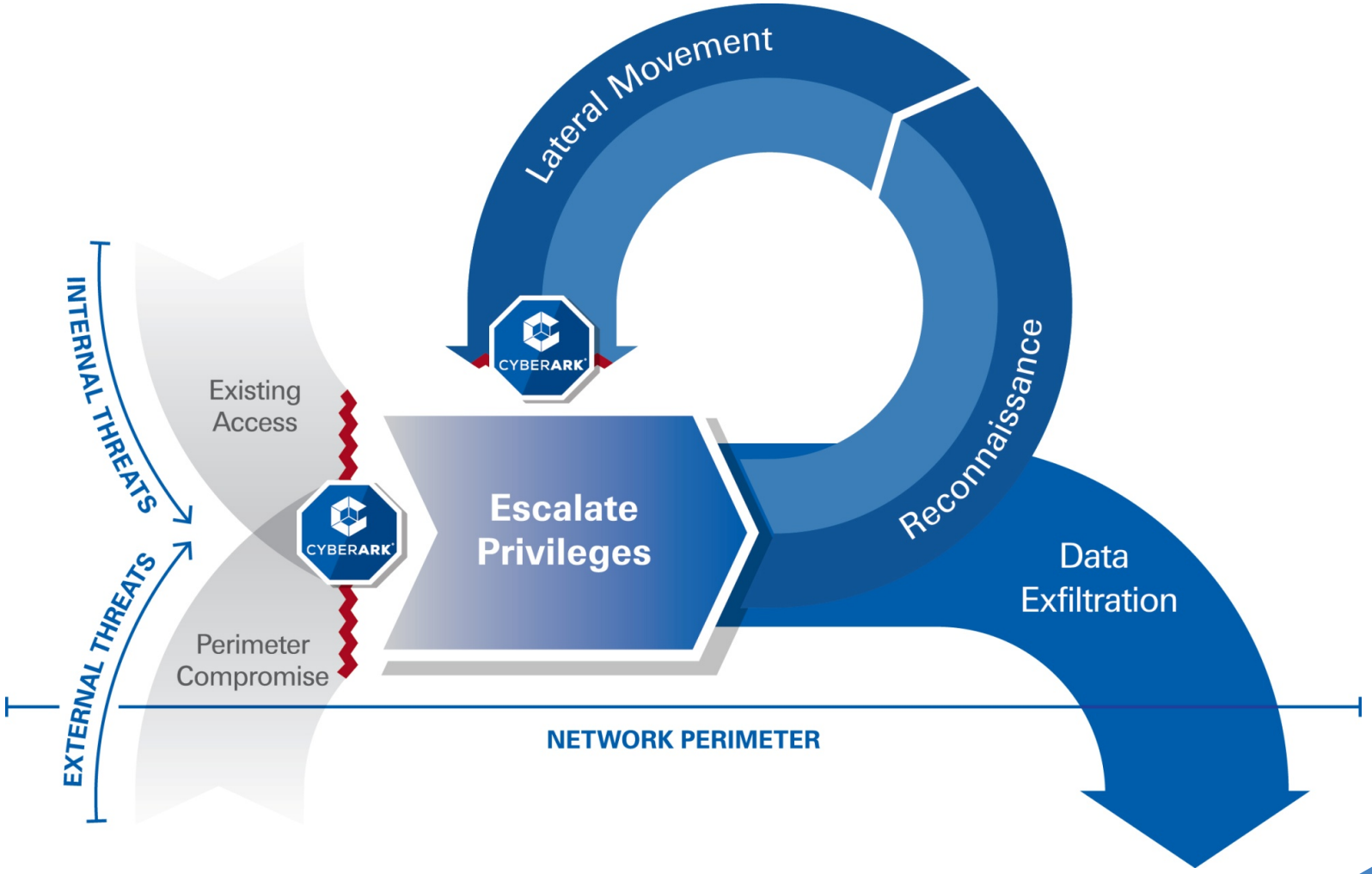
CYBERARK

Privilege is At The Center of the Attack Lifecycle



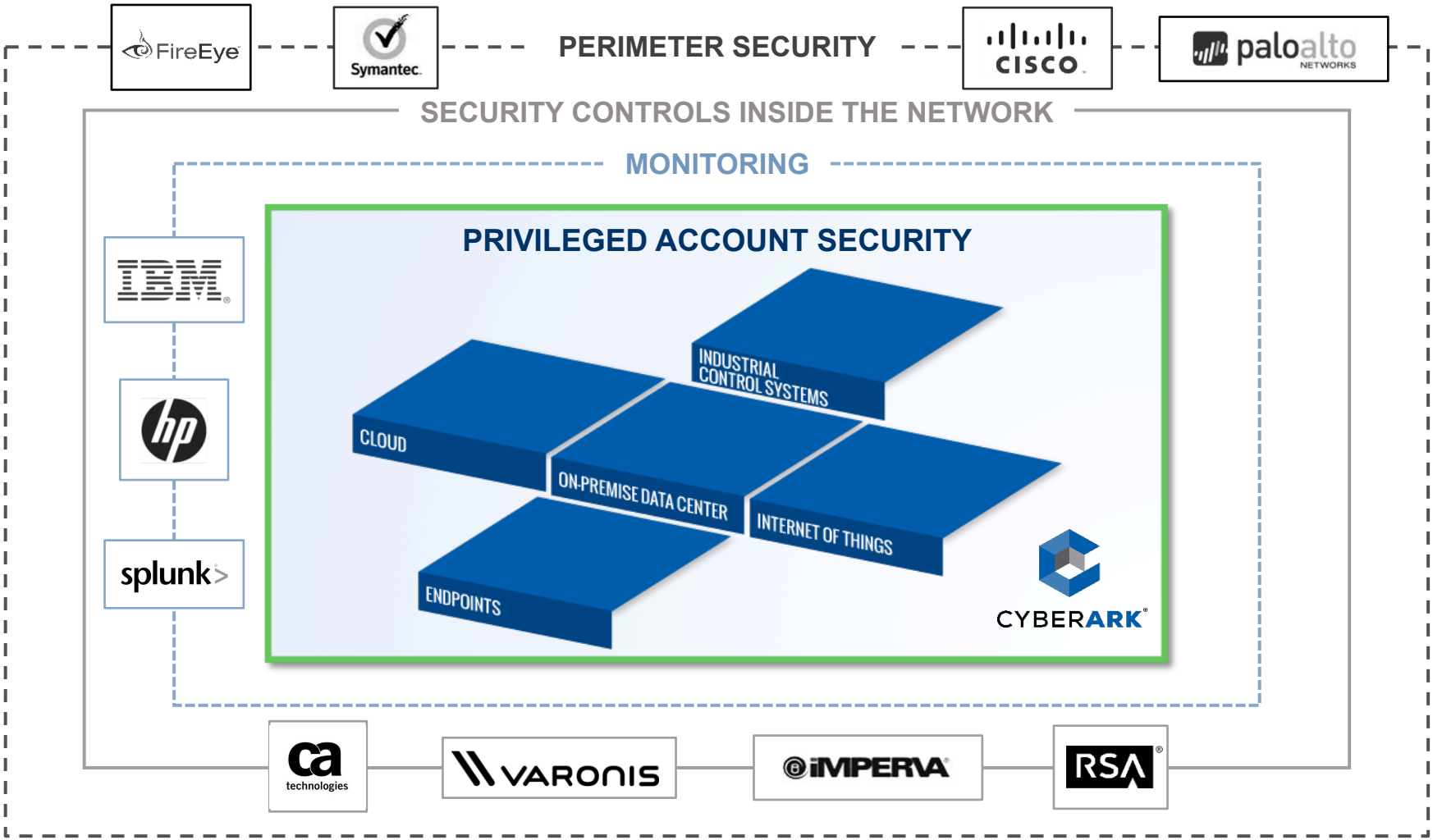
CYBERARK

CyberArk Breaks the Attack Chain



CYBERARK

CyberArk Delivers a New Critical Security Layer



CYBERARK

CyberArk's Integration Across the Enterprise

Databases

- Oracle
- MSSQL
- DB2
- Informix
- Sybase
- MySQL
- Any ODBC

Operating Systems

- Windows
- Unix/Linux
- AS400
- OS390
- HPUX
- Tru64
- NonStop
- ESX
- OVMS
- Mac

Applications

- SAP
- WebSphere
- WebLogic
- Windows:
  - Services
  - Scheduled Tasks
  - IIS App Pools
  - IIS Anonymous
  - COM+
- Oracle Application ERP
- System Center Configuration Manager

Generic Interface

- SSH/Telnet
- ODBC
- Windows Registry
- Web Interfaces
- Web Sites

Network Devices

- Cisco
- Juniper
- Nortel
- Alcatel
- Quntum
- F5

Security Appliances

- FW1, SPLAT
- IPSO
- PIX
- Netscreen
- FortiGate
- ProxySG

Directories and Credential Storage

- AD
- SunOne
- Novel
- UNIX Kerberos
- UNIX NIS

Remote Control and Monitoring

- HMC
- HPiLO
- ALOM
- Digi CM
- DRAC

Expand to include more add category Universal Connector and platform support or other Controlled Availability (CA) Plug-ins. Sample

CYBERARK

CyberArk's Privileged Account Security Solution

Behavioral Analytics

- Privileged Threat Analytics

Proactive Controls, Monitoring & Management

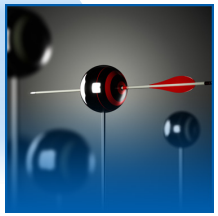
- Management Portal/Web Access
- Enterprise Password Vault®
- SSH Key Manager
- Privileged Session Manager®
- Application Identity Manager™
- On-Demand Privileges Manager™

Shared Technology Platform

- Master Policy
- Secure Digital Vault™

Protect

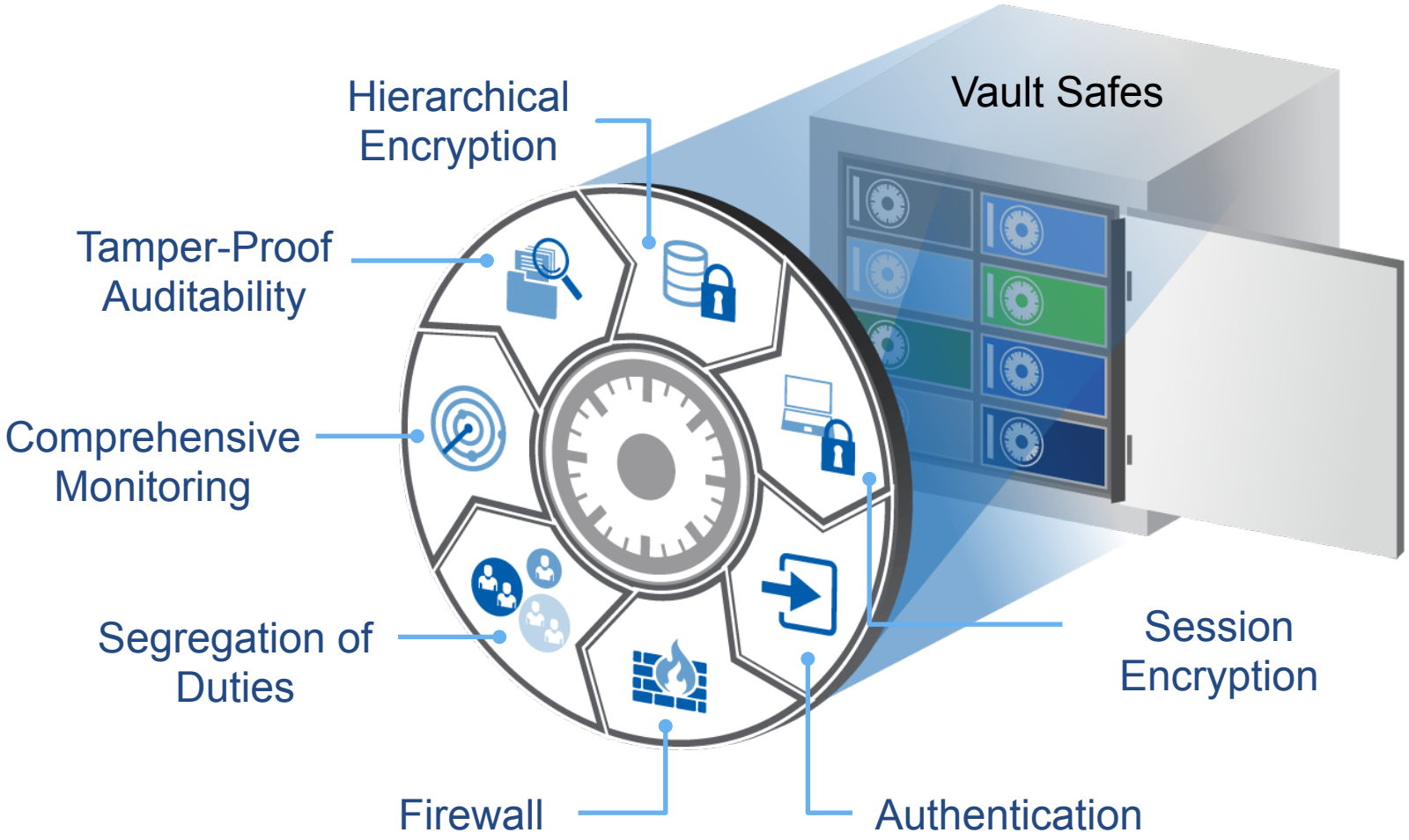
Detect



Respond

CYBERARK®

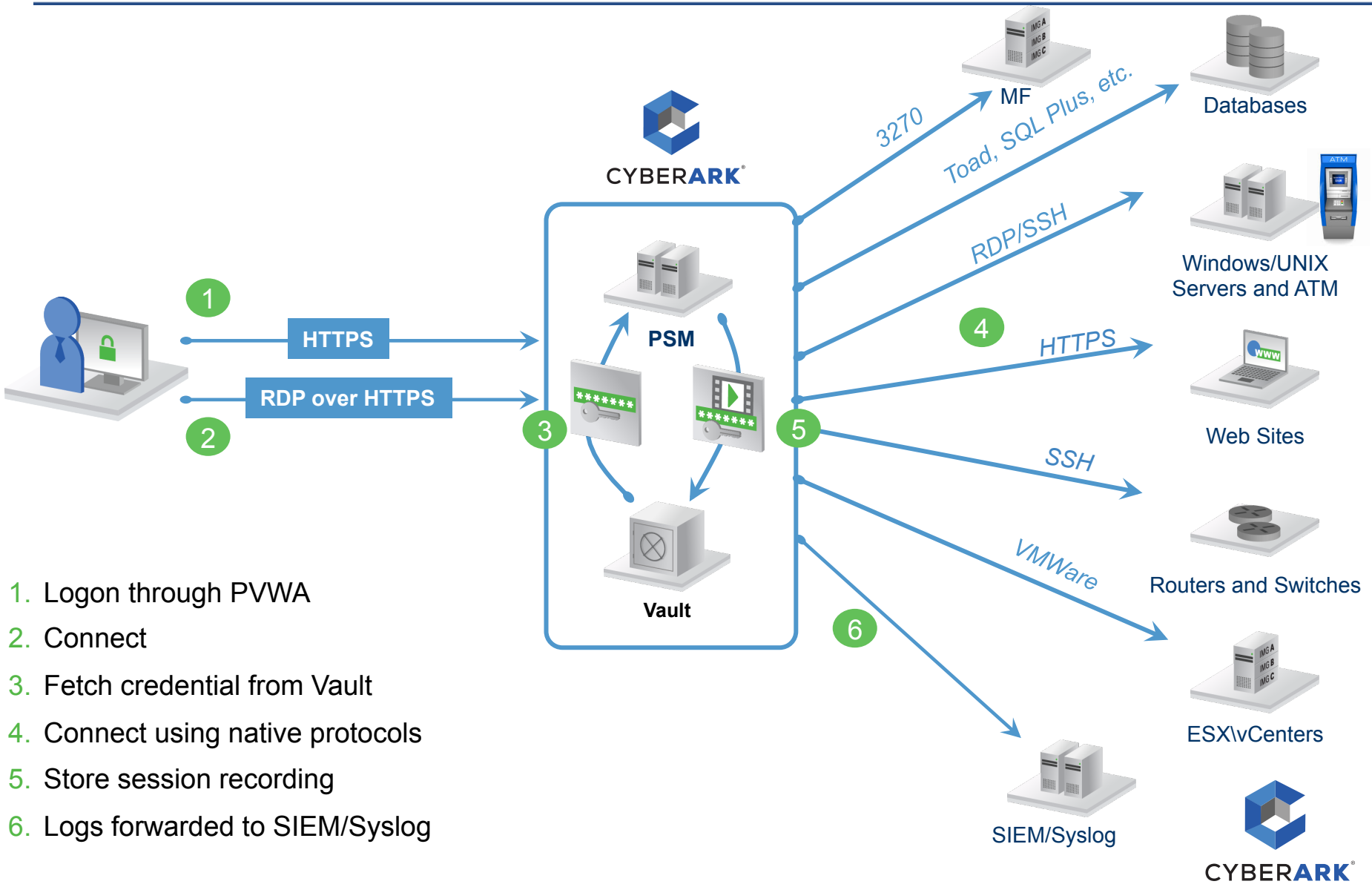
Layers of Security in the Digital Vault



CYBERARK

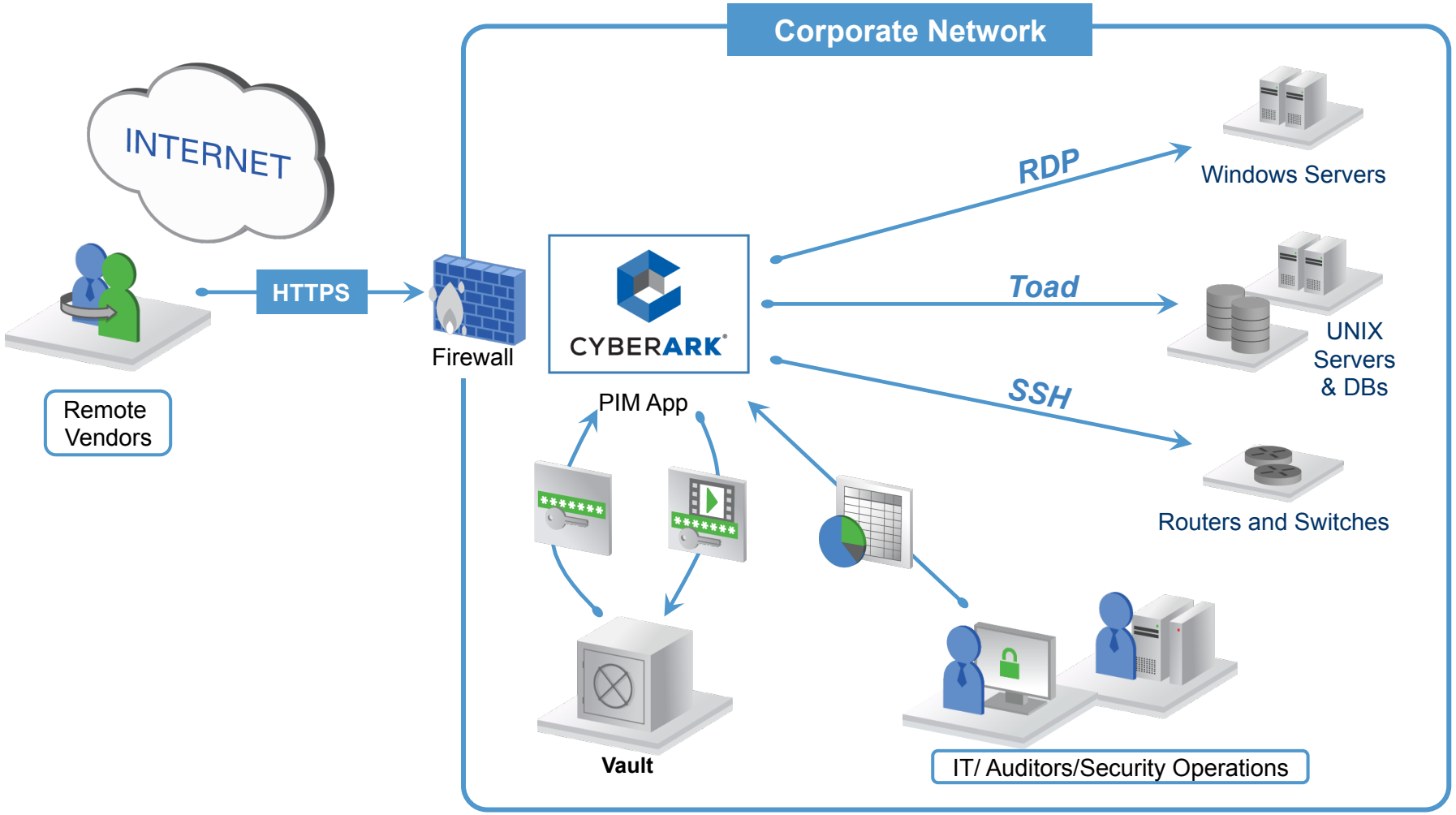
Privileged Session Management

CyberArk Privileged Session Manager



1. Logon through PVWA
2. Connect
3. Fetch credential from Vault
4. Connect using native protocols
5. Store session recording
6. Logs forwarded to SIEM/Syslog

Privileged Account Security for Remote Vendors

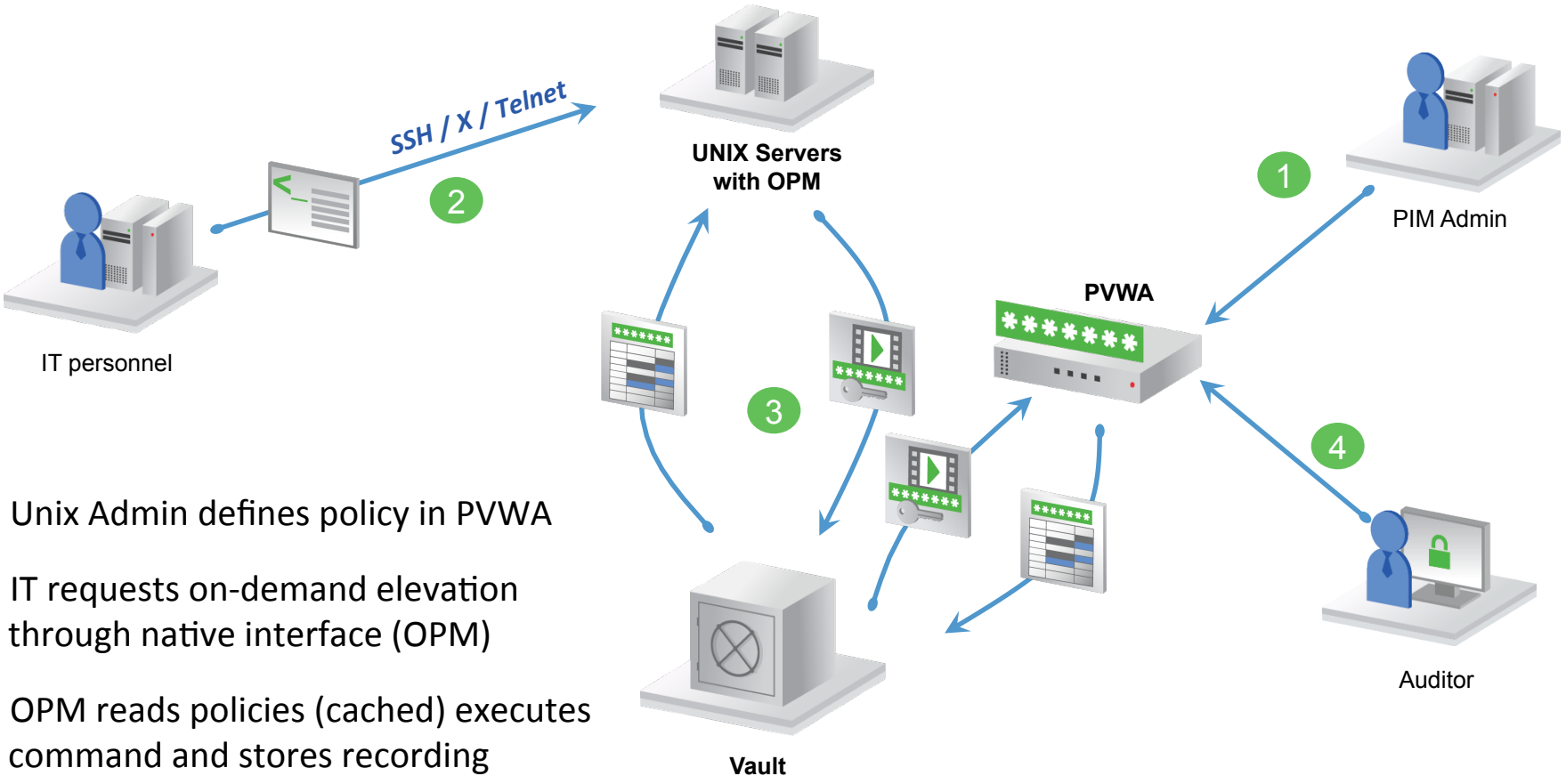


CYBERARK

CYBERARK

On-Demand Privilege Manager

CyberArk On-Demand Privileges Manager



1. Unix Admin defines policy in PVWA
2. IT requests on-demand elevation through native interface (OPM)
3. OPM reads policies (cached) executes command and stores recording
4. Auditor reviews commands recordings / audit reports

CYBERARK

Application Identity Manager

Eliminating Hard Coded Passwords

Configuration Files & Databases

- Web Config files
- INI/text files
- Application Databases

```
<Resource name="jdbc/db1"
  auth="Container"
  type="oracle.jdbc.pool.OracleDataSource"
  driverClassName="oracle.jdbc.driver.OracleDriver"
  factory="oracle.jdbc.pool.OracleDataSourceFactory"
  url="jdbc:oracle:thin:@oracle.microdeveloper.com:1521:db1"
  user="scott"
  password="tiger"
  maxActive="20"
  maxIdle="10"
  maxWait="-1" />
```

Application Servers

Also in registry, FTP credentials and more

Service Accounts

- Windows service
- Scheduled tasks
- IIS application pool
- IIS Directory Security
- COM+
- Registry

Hard-Coded, Embedded Credentials

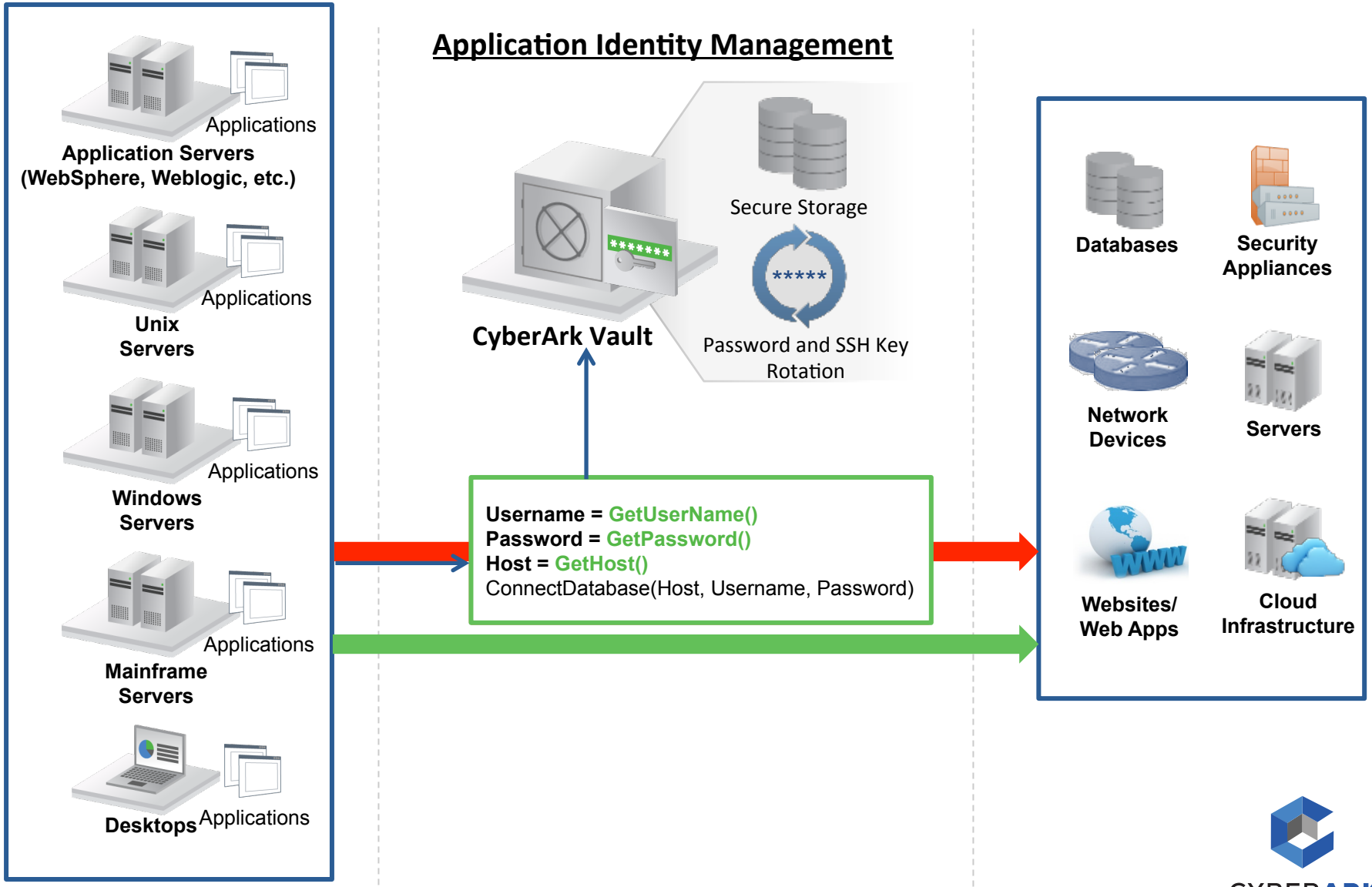
```
Password = "y7qer$1"
Host = "10.10.3.56"
```

Third Party Applications

ORACLE QUALYS McAfee

CYBERARK

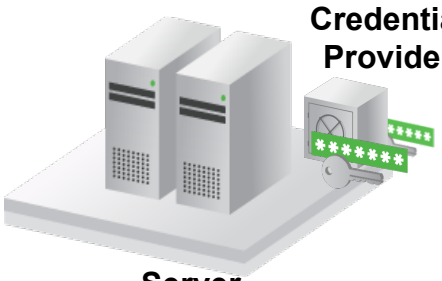
Application Identity Manager: A high level perspective



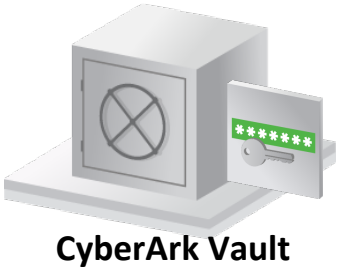
CYBERARK

Completely eliminate hard-coded and stored credentials

- Application Identity Manager enables the complete elimination of hard-coded credentials from code as well as SSH keys stored on servers



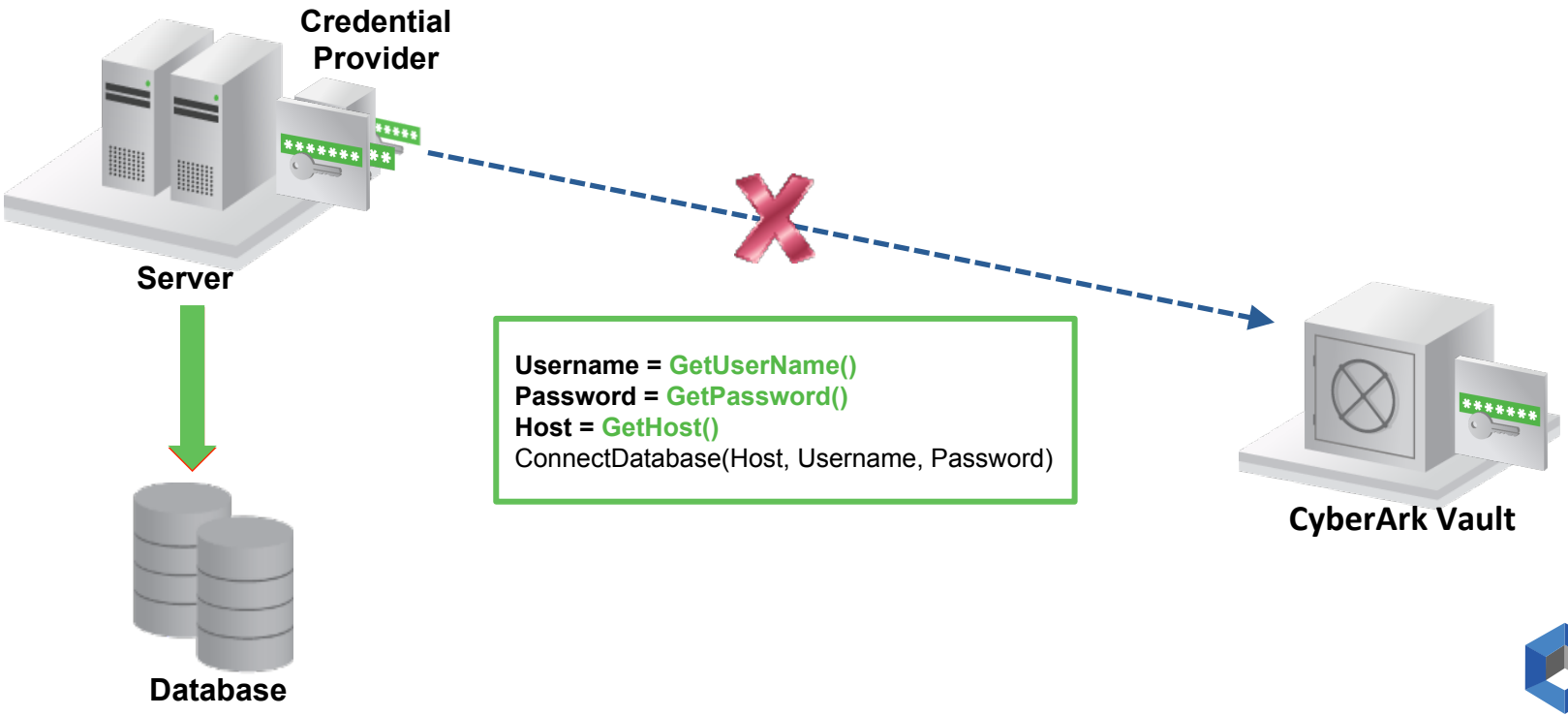

```
Username = GetUserName()
Password = GetPassword()
Host = GetHost()
ConnectDatabase(Host, Username, Password)
```



CYBERARK

High performance and availability

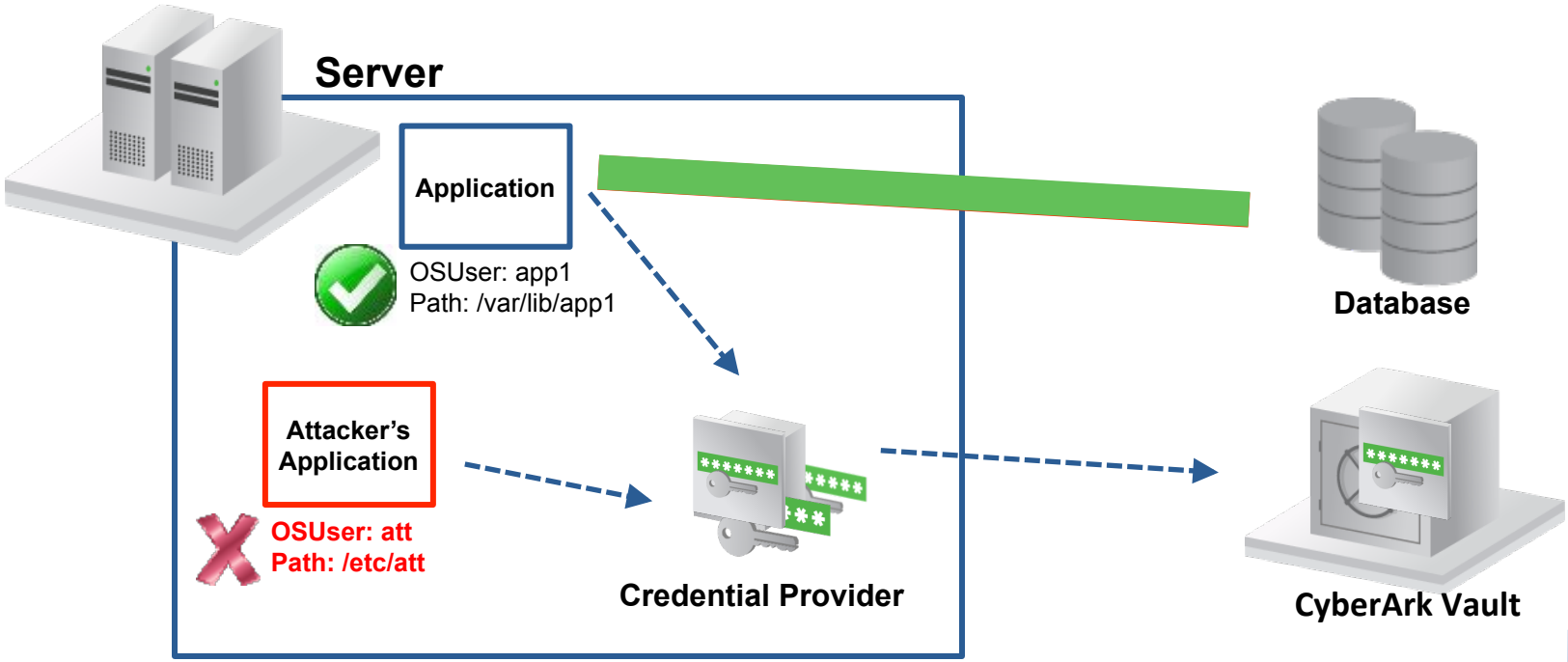
- Application Identity Manager's secure local cache stores retrieved credentials for high performance and availability
- The secure local cache enables quick retrieval of credentials
- In case a network outage should occur, credentials will always be available from the secure local cache



CYBERARK

Strong authentication of applications requesting credential

- To achieve the highest level of security, it is critical to verify the origin of credential requests and prevent attackers from:
  - Impersonating applications
  - Tampering with application code
- Applications can be verified as trusted based on their a run-time characteristics such as: IP/hostname, OS User, path and hash



CYBERARK

CYBERARK

SSH Key Manager

Privileged Credentials are the Keys to the IT Kingdom

"…100% of breaches involved stolen credentials"

- Mandiant

While many organizations proactively manage privileged passwords, few manage the SSH keys that **provide the same level of access**.

CYBERARK

End-to-End UNIX Privileged Account Security Solution

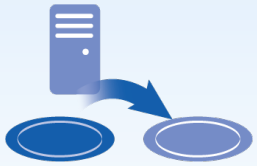
Discover UNIX accounts and **SSH keys**

NEW

Protect and manage root passwords and **SSH keys**

NEW

Secure jump server and session monitoring



Leverage AD Bridge Features for centralized user management and authentication

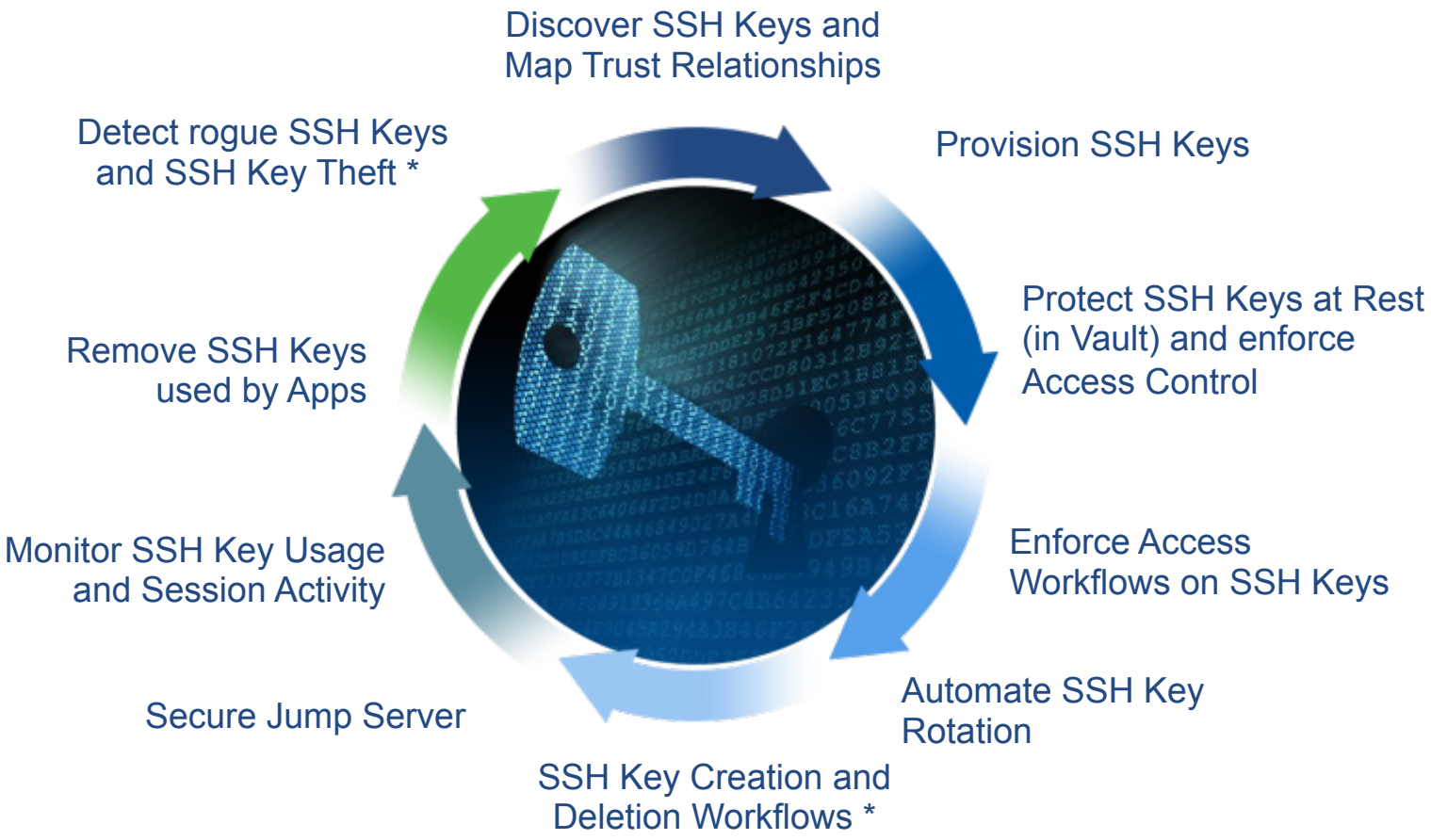
NEW

Enforce least privileged principle

Remove hard coded passwords and **SSH keys** from scripts

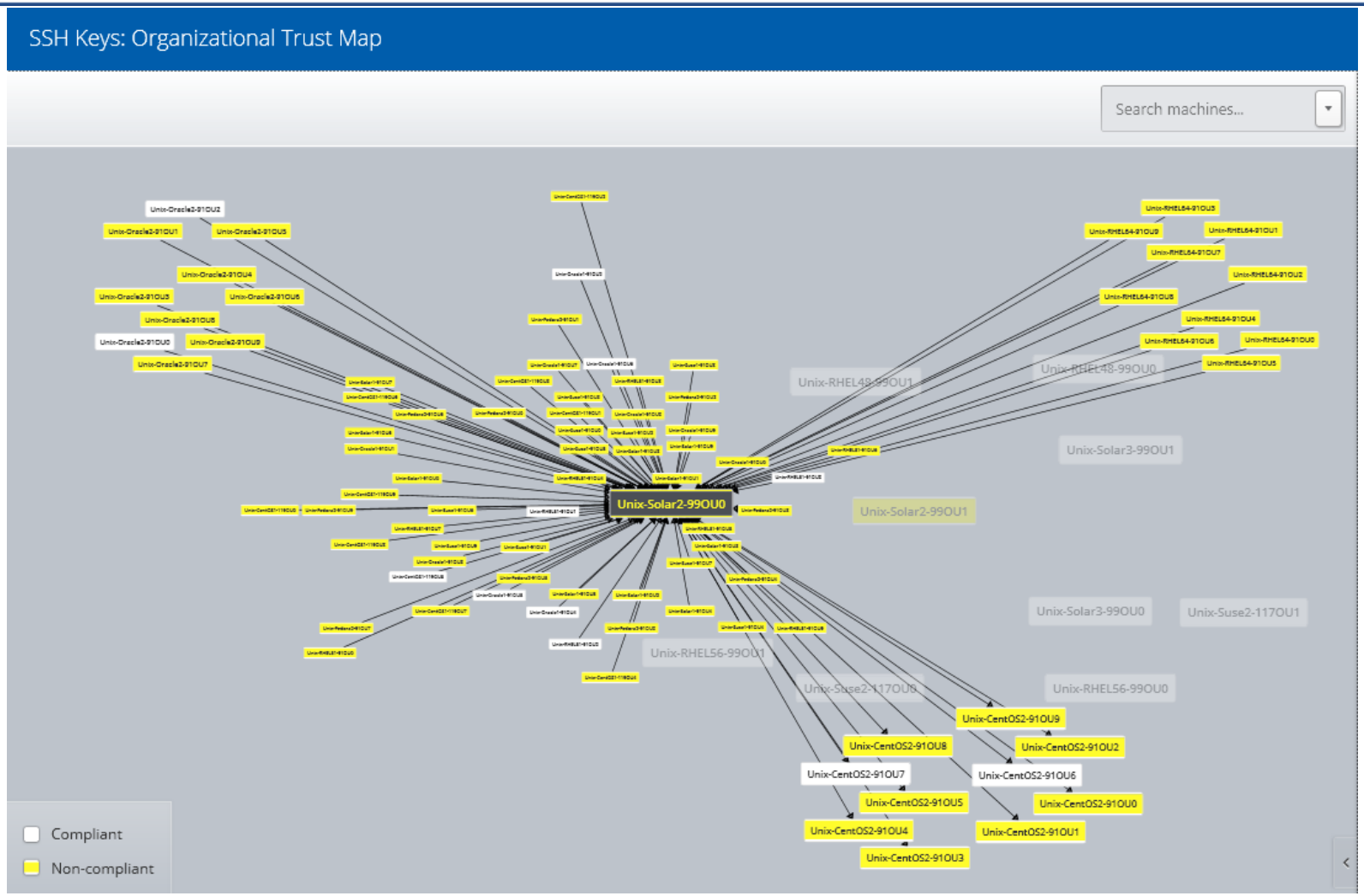
CYBERARK®

SSH Key Lifecycle Management



Provide **end-to-end SSH key and password lifecycle management** capabilities from a single platform

What company probably have



CYBERARK

Privileged Threat Analytics

Four Critical Steps to Stopping Advanced Threats

Discover all of your privileged accounts

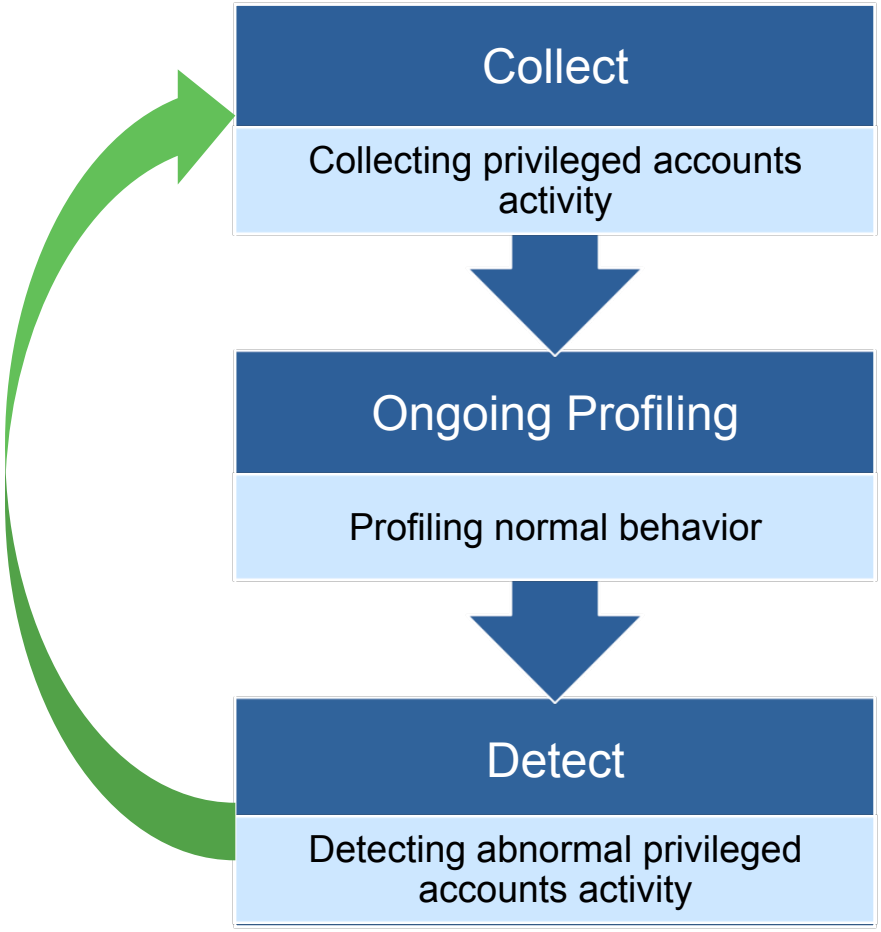
Protect and manage privileged account credentials

Control, isolate and monitor privileged access to servers and databases

Use real-time privileged account intelligence to detect and respond to in-progress attacks

CYBERARK®

What Privileged Threat Analytics does



CYBERARK

How Privileged Threat Analytics works

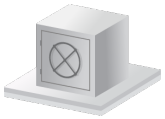
PRIVILEGED ACCOUNT ACTIVITY

Privileged User

Critical System Access

ORACLE

CyberArk Vault



SIEM Solution

ArcSight CERTIFIED CEF COMPLIANT

splunk>

RSA

McAfee COMPATIBLE

IBM

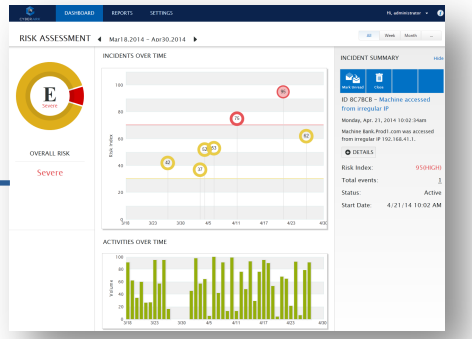
Behavioral Analysis: Self-learning statistical model based on a combination of patented algorithms, Vault access data, and target system data gathered from inbound SIEM integrations.

Behavioral Analysis

Normal

Abnormal

ALERT: SIEM & CyberArk



CYBERARK

PTA in Action

- An attacker infects a desktop with malware
- Via lateral movement, he obtains credentials to a privileged account that has access to a file server
- The attacker successfully logs into the file server with the stolen credentials

Irregular IP Alert!

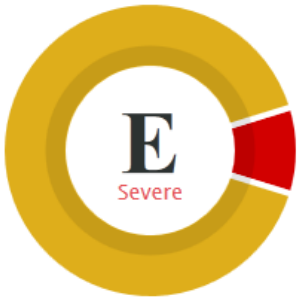
- Privileged Threat Analytics detects in real-time that the file server is being accessed by an unusual IP address

CYBERARK

RISK ASSESSMENT

Mar18.2014 – Apr30.2014

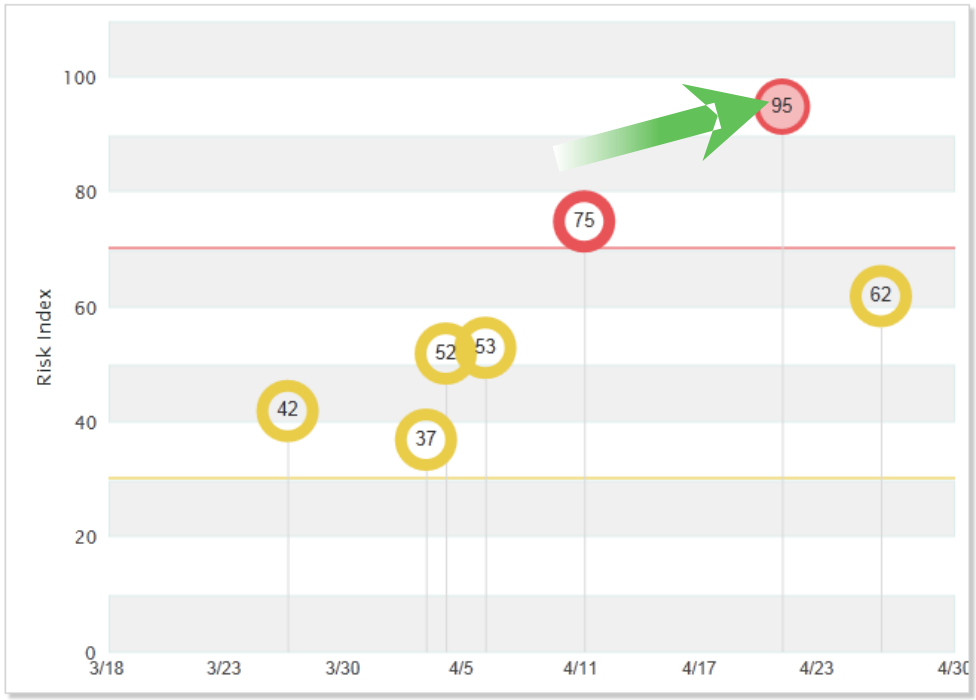
All | Week | Month | ...



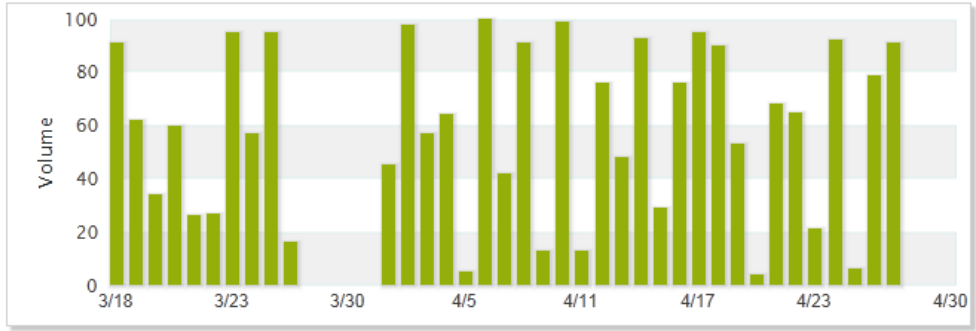
OVERALL RISK

Severe

INCIDENTS OVER TIME



ACTIVITIES OVER TIME



INCIDENT SUMMARY

Hide

Mark Unread | Close

ID 8C7BCB – Machine accessed from irregular IP

Monday, Apr. 21, 2014 10:02:34am

Machine Bank.Prod1.com was accessed from irregular IP 192.168.41.1.

DETAILS

Risk Index:	95(HIGH)
Total events:	1
Status:	Active
Start Date:	4/21/14 10:02 AM

Privileged Threat Analytics Key Benefits

The right data vs. all the data

Focus on critical privileged user and account activity to reduce "noise"

Privileged users vs. privileged accounts

Analyze fine-grained information on individual user activity

Patented analytic algorithms

Built-in algorithms automatically look for anomalous behavior

Real-time alerting

Disrupt in-progress attacks and minimize business impact

Integration with SIEM solutions

Simplify deployment and enhance information provided by a SIEM

CYBERARK®

Thank you!