



CYBERARK

Learn From the Experts: CyberArk Privileged Account Security

Łukasz Kajdan, Sales Manager Baltic Region
Veracomp SA

Stallion Shooting Event 20.06.2014



Privileged Accounts are Targeted in All Advanced Attacks

“Anything that involves serious intellectual property will be contained in highly secure systems and privileged accounts are the only way hackers can get in.”

Avivah Litan, Vice President and Distinguished Analyst at Gartner

Privileged Accounts are Targeted in All Advanced Attacks

“...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

Analyst review

**Best Advanced Persistent Threat (APT)
Protection
Winner**

CyberArk Privileged Account Security solution (v8),
CyberArk,

Highly Commended

Lumension Endpoint Management and Security
Suite, Lumension Security

Zscaler for APTs, Zscaler

Finalist

FireEye Security Platform, FireEye,

Lancope StealthWatch® System- Best APT Solution, Lancope,

Trend Micro Deep Discovery, Trend Micro,

WebSense TRITON Enterprise, WebSense,



2014 SC Awards Europe Winners

Analyst review



Privilege Management

Leaders in innovation, product features, and market reach for Privilege Management.
Your compass for setting the right course in the market.



By Peter Cummings
pc@kuppingercole.com
January 2014



CYBERARK®

Analyst review

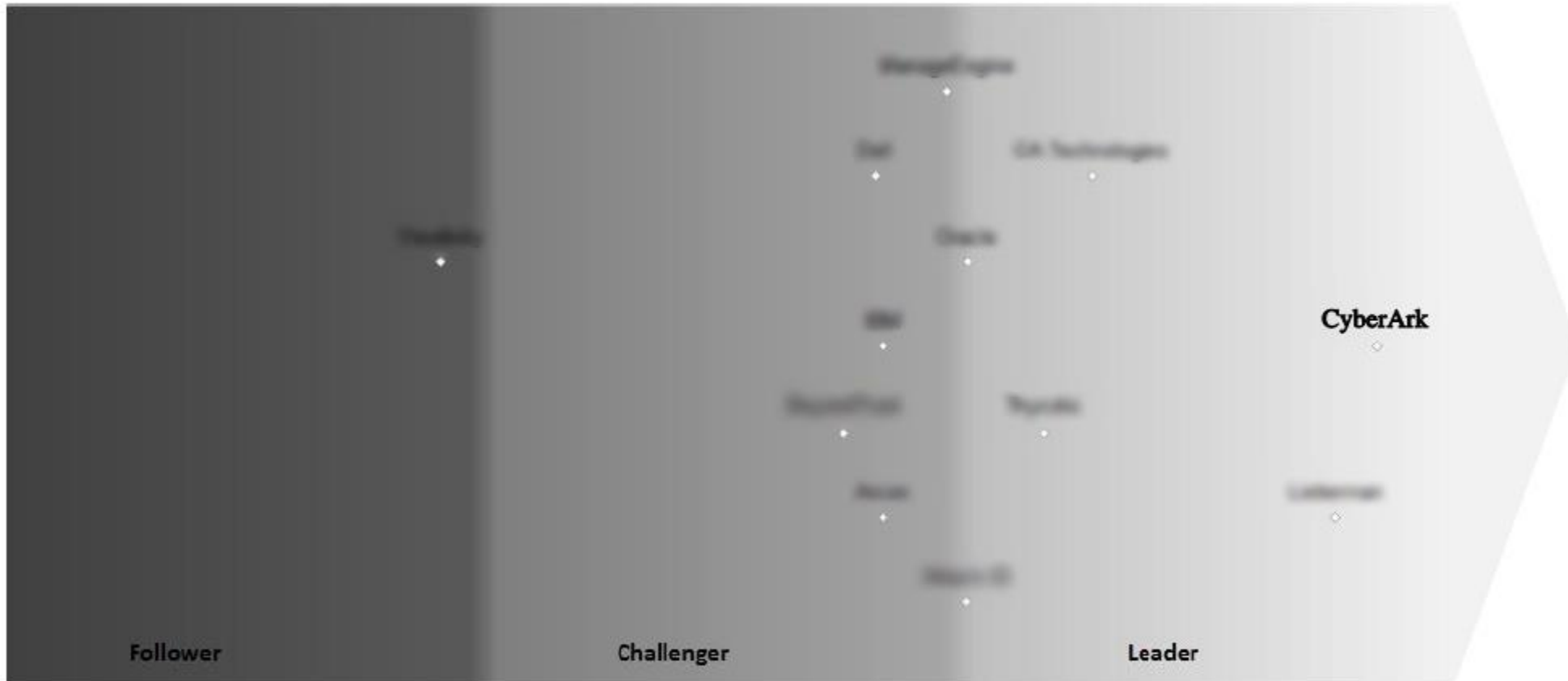


Fig. 1: The Overall Leadership rating for the Privilege Management market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.]

In this Leadership Compass CyberArk takes the Overall Leadership in Privilege Management.

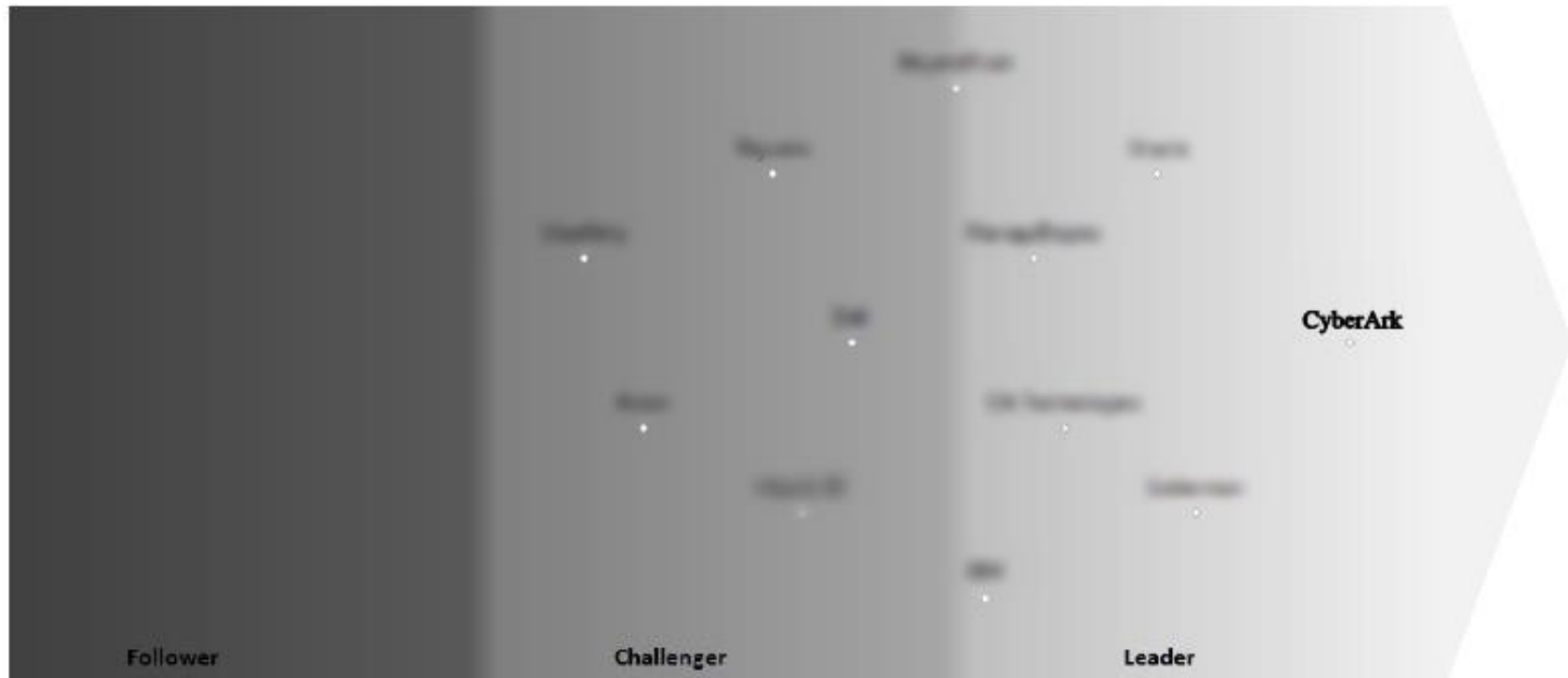


Fig. 2: Market Leaders in the Privilege Management market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.]

Market Leadership is not only about number of clients. When we look at this category we also consider the partner network based on geographical regions, numbers and spread. We also take into account the geographical dispersion of customers and financial stability of the company. If the company's clients are based in one region or a company only has one partner in each region, the company cannot be classified as a Leader in this segment.



Regulations



A.11.2. Managing user access

- Users registration
- Managing the privildges
- Managing user passwords
- Preview of access

D Recomendation



- Predefined rulles for access control
- Control over third party access (App service)
- Password lenght requiremnts
- Rulles about encryption and storing the keys

Sarbanes-Oxley
Financial and Accounting Disclosure Information



And others

CyberArk Customers

Communications and media



belgacom



Financial Sector



ING GROUP



Deutsche Bank



citibank



MIZUHO



Comerica

FINANSBANK



BNP PARIBAS

BARCLAYS

Medical sector



AstraZeneca



NOVARTIS

serono
biotech & beyond



McKESSON

Energy and mining



PEOPLES ENERGY



Progress Energy

Direct Energy

SUNCOR ENERGY

ENBRIDGE

Industry



DURACELL

VOCALINK



TARGET

BRAUN

Mohegan Sun
a world at play



Mercedes Benz

ConAgra Foods

AVIS Budget

linea directa



MOTOROLA

CyberArk Overview



Trusted experts in privileged account security

- Over 1,500 *privileged account security* customers – it's all we do!

- Founded in 1999
- HQ – Boston MA



Approach privileged accounts as a security challenge

- Designed and built from the ground up for security



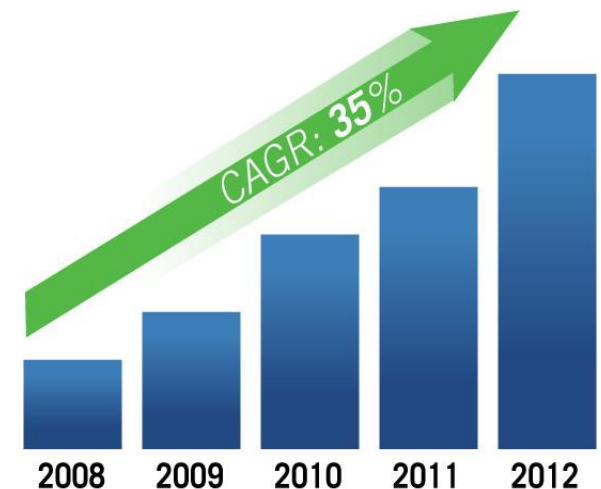
Focus on solving business problems

- Privileged account security goes well beyond audit



Only comprehensive privileged account security solution

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

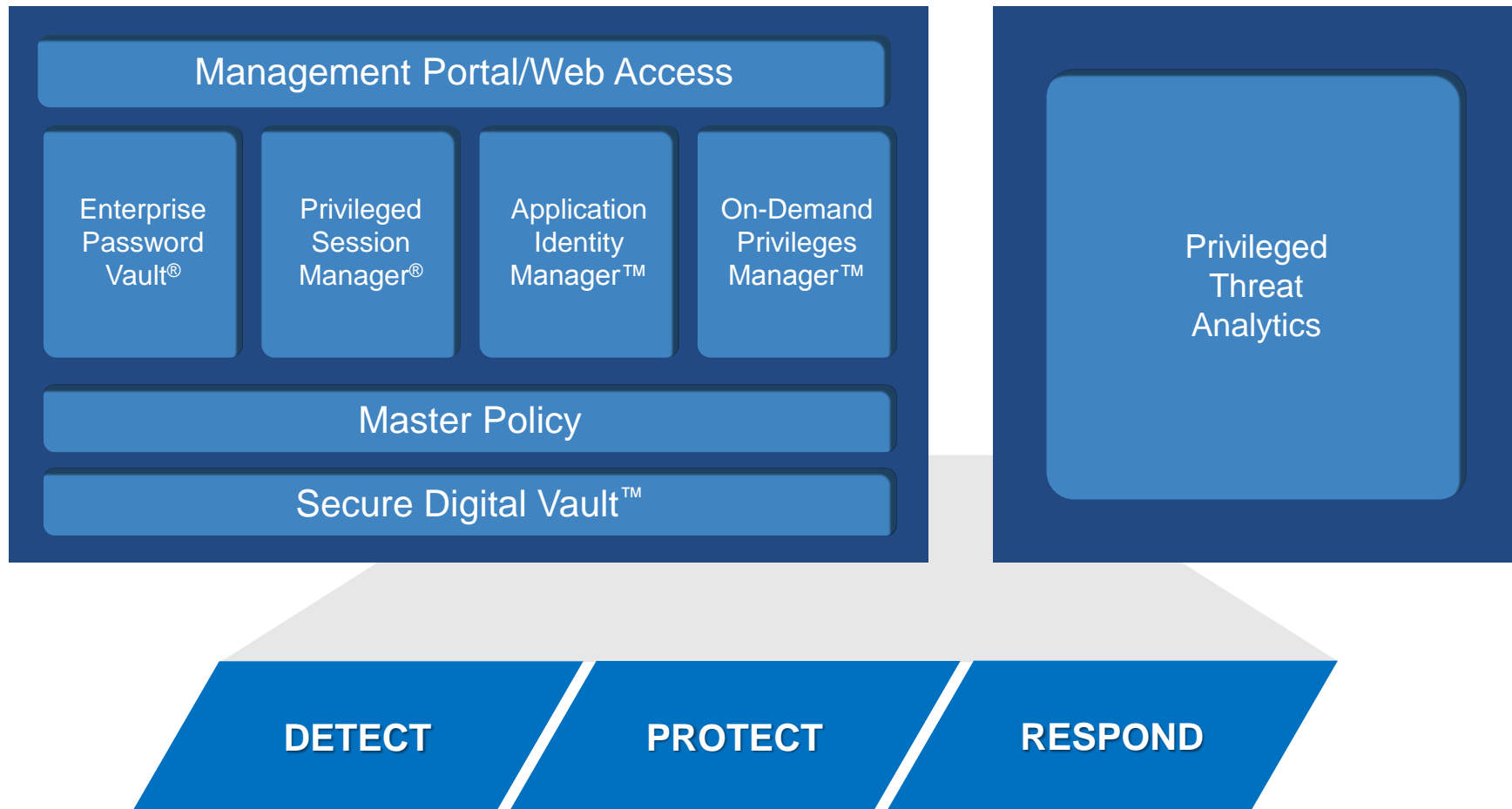


CYBERARK®

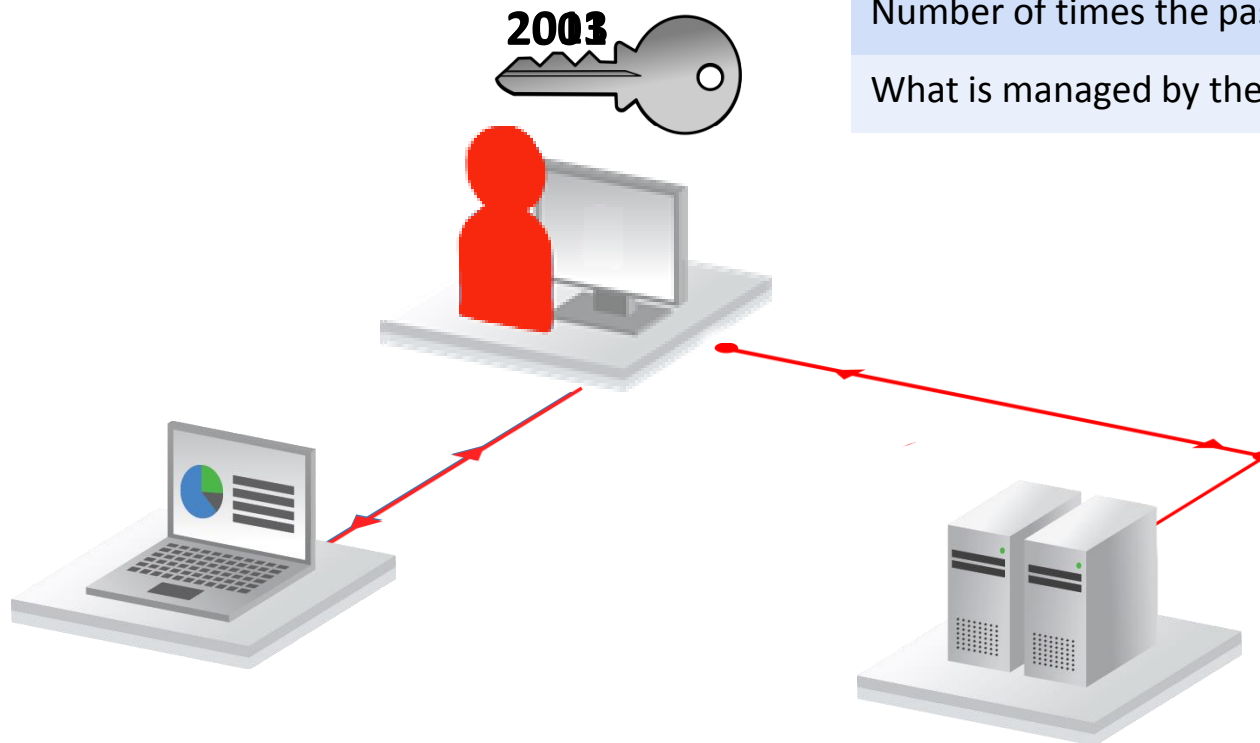
Stopping the Attack That's Inside Your Network



CyberArk Solutions



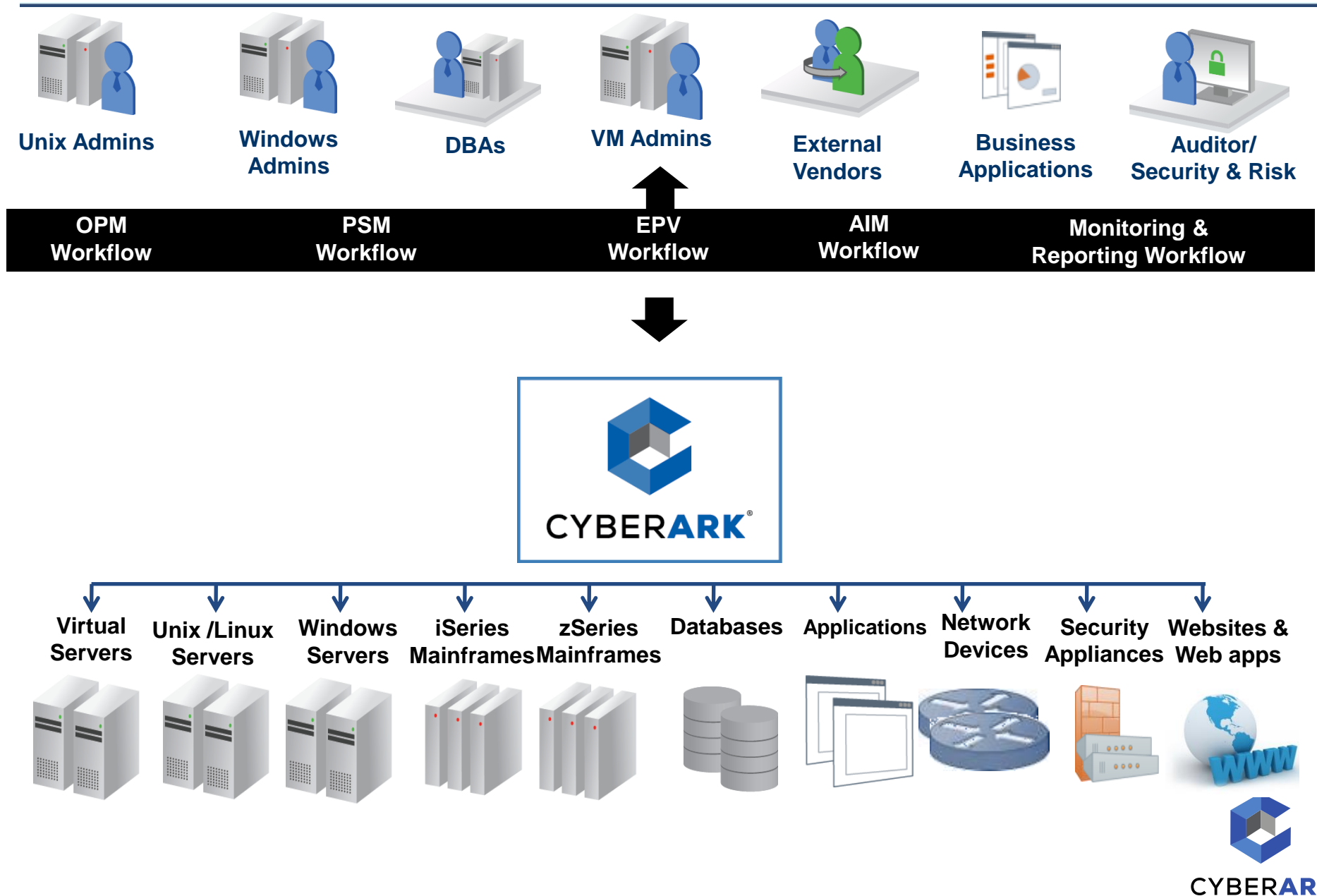
Risk Assessment Case



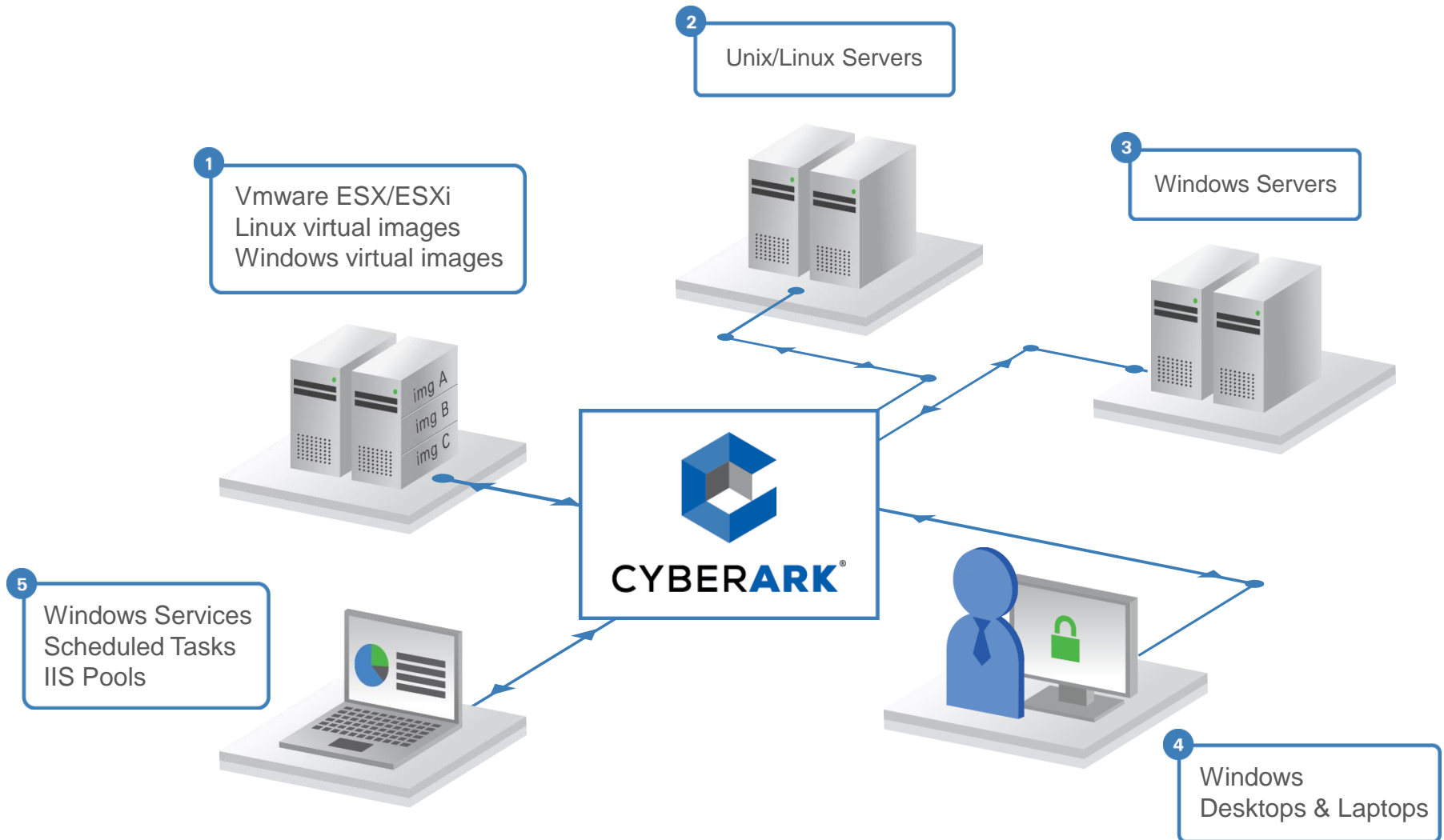
Number of employees that knew the password and have left the company	40+
Number of times the password was used	100,000+
What is managed by the account	unknown



Unified Workflows

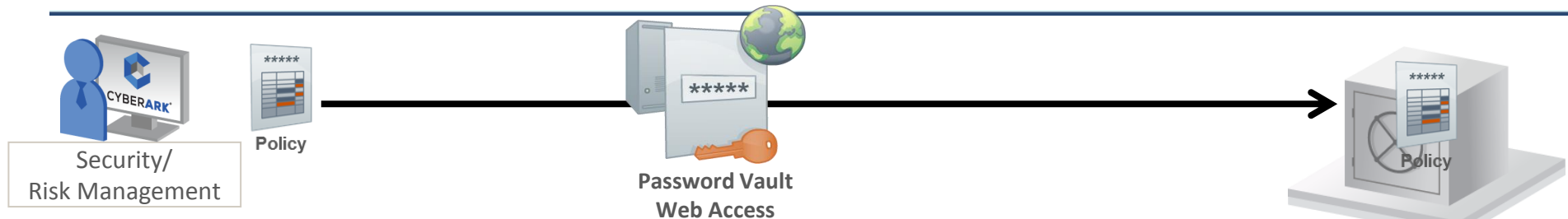


Automatically Discover Privileged Accounts Across the Datacenter



Where do all the privileged and superuser accounts exist?

Central and Integrated Policy Definition



WinDomainAccount

Search... Go

- Configuration
 - General
 - Privileged Account Management
 - CPM Plug-in
 - Password Change**
 - Password Verification
 - Password Reconciliation
 - Notifications
 - Generate Password

Properties

Name	Value
AllowManualChange	Yes
PerformPeriodicChange	No
OneTimePassword	No
ExpirationPeriod	90
HeadStartInterval	5
FromHour	-1
ToHour	-1
ChangeNotificationPeriod	-1
DaysNotifyPriorExpiration	7
ExecutionDays	
EnforcePasswordPolicyOnManualChange	Yes
EnforcePasswordVersionsHistory	7



Central Policy Manager

System	User	Pass
Unix	root	tops3cr3t
Oracle	SYS	tops3cr3t
Windows	Administrator	tops3cr3t
z/OS	DB2ADMIN	tops3cr3t
Cisco	enable	tops3cr3t



CYBERARK

Discovery & Audit DNA

Discovery

Setup

Results

Select discovery sources

☒ **Active Directory**

Connect to the Active Directory that contains the assets to be scanned

☒ **Scan from file**

Import a file that specifies the machines to be scanned

Next

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



Open reports folder

? About DNA

Discovery

Setup

Results

1 > 2 | Active Directory Discovery

Which user to use for scanning?

? What's this?

Enter domain administrator credentials

User

Password

Domain

What to scan?

? What's this?

Select Active Directory Organizational Unit (OU)

No OU selected

Browse

Note: Scanning will be performed on this OU and its sub-OUs

☐ Scan Windows

Workstations

Servers

Both

☐ Scan Unix

(Include both Workstations and Servers)

Back

Next

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



Open reports folder

? About DNA

Discovery

Setup

Results

1 > 2 | Active Directory Discovery**Which user to use for scanning?**

? What's this?

Enter domain administrator credentials

User

Password

Domain

What to scan?

? What's this?

Select Active Directory Organizational Unit (OU)

No OU selected

Browse

Note: Scanning will be performed on this OU and its sub-OUs

☐ Scan Windows

Workstations

Servers

Both

☐ Scan Unix

(Include both Workstations and Servers)

Back

Next

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



Open reports folder

About DNA

Discovery

Setup

Results

1 > 2 | Active Directory Discovery

Which user to use for scanning?

What's this?

Enter domain administrator credentials

User

Password

Domain

What to scan?

What's this?

Select Active Directory Organizational Unit (OU)

No OU selected

Browse

Note: Scanning will be performed on this OU and its sub-OU's

☐ Scan Windows

Workstations

Servers

Both

☐ Scan Unix

(Include both Workstations and Servers)

Back

Next

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



📁 Open reports folder

? About DNA

Discovery

Setup

Results

1 > 2 | Active Directory Discovery**Which user to use for scanning?**

? What's this?

Enter domain administrator credentials

User

Password

Domain

What to scan?

? What's this?

Select Active Directory Organizational Unit (OU)

dna

Browse

Note: Scanning will be performed on this OU and its sub-OUs

☒ Scan WindowsWorkstations
(2)Servers
(0)Both
(2)☐ Scan Unix (0)

(Include both Workstations and Servers)

Back

Next

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



Open reports folder

About DNA

Discovery

Setup

Results

① > ② | Setup scanning from a file

Import Machines

Select the file that specifies the machines

D:\CyberArk DNA\C ... achines_list6.csv

Browse

Imported machines: 2

[Click to download CSV template](#)

Back

Start Scanning

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



[Open reports folder](#)[About DNA](#)

Discovery

Setup

Results

OS detection in progress...

Your license limits scanning to 100 Windows and 30 Unix computers.

Total Computers Scanned

0 of 3



Stop

Windows Scan Results

Computers

Found

3

Scanned successfully

0

0%

0% failed partially, 0% failed. [What's this?](#)

Accounts

Found

0

Non-compliant

0

0%

[What's this?](#)

Unix/Linux Scan Results

Computers

Found

0

Scanned successfully

0

0%

0% failed partially, 0% failed. [What's this?](#)

Accounts

Found

0

Non-compliant

0

0%

[What's this?](#)

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



Open reports folder

About DNA

Discovery

Setup

Results

Scanning in progress...

Your license limits scanning to 100 Windows and 30 Unix computers.

Total Computers Scanned

3 of 4

69%

Stop

Windows Scan Results

Computers

Found	Scanned successfully
3	2 67%

33% failed partially, 0% failed. [What's this?](#)

Accounts

Found	Non-compliant
20	1 5%

[What's this?](#)

Unix/Linux Scan Results

Computers

Found	Scanned successfully
1	0 0%

0% failed partially, 0% failed. [What's this?](#)

Accounts

Found	Non-compliant
0	0 0%

[What's this?](#)

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



Discovery

Setup

Results

Scanning in progress...

Your license limits scanning to 100 Windows and 30 Unix computers.

Total Computers Scanned

3 of 4

69%

Stop

Windows Scan Results

Computers

Found	Scanned successfully
3	2 67%

33% failed partially, 0% failed. [What's this?](#)

Accounts

Found	Non-compliant
20	1 5%

? [What's this?](#)

Unix/Linux Scan Results

Computers

Found	Scanned successfully
1	0 0%

0% failed partially, 0% failed. [What's this?](#)

Accounts

Found	Non-compliant
0	0 0%

? [What's this?](#)

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



Discovery

Setup

Results

Scanning complete

Your license limits scanning to 100 Windows and 30 Unix computers.

Total Computers Scanned

4 of 4

100%

Stop

Windows Scan Results

Computers

Found

3

Scanned successfully

2

67%

33% failed partially, 0% failed. [What's this?](#)

Accounts

Found

20

Non-compliant

1

5%

[? What's this?](#)

Unix/Linux Scan Results

Computers

Found

1

Scanned successfully

1

100%

0% failed partially, 0% failed. [What's this?](#)

Accounts

Found

11

Non-compliant

0

0%

[? What's this?](#)

Your audit report is ready

[? What's in the report?](#)

Open Report

New Scan

About DNA

Version 4.1.0.54

CyberArk DNA™ is an innovative, agentless discovery and audit tool that scans an organization's network for data related to privileged accounts; typically a complex, manual process.

The easy-to-use scanner discovers and analyzes each account, then generates a report that allows auditors and decision makers to evaluate the status of privileged accounts management in the organization. This simple, three-step process leads to better and more efficient risk management of privileged accounts.

CyberArk's award-winning Privileged Identity Management and Privileged Session Management suites protect, manage and monitor privileged access and sessions. This enables organizations to meet compliance requirements, improve productivity and protect against insider and APTs.



CyberArk DNA™ | Discovery and Audit Report

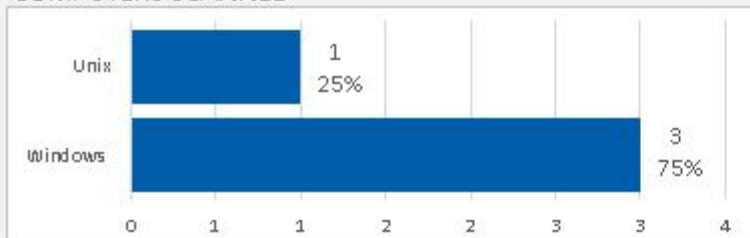


EXECUTIVE SUMMARY

ABOUT THE SCAN

Scan date	18 czerwca 2014 10:45:25
Licensee name	CyberArk - Evaluation
Created by	KR-SMAZURCZYK\Sebatian.Mazurczyk
Password policy	Passwords of compliant accounts are changed every 90 days
Windows computer types	Servers and workstations
Windows object types	Accounts, Service Accounts
Unix computer types	Servers and workstations
Unix object types	Accounts
LDAP path	DC=dna,DC=local

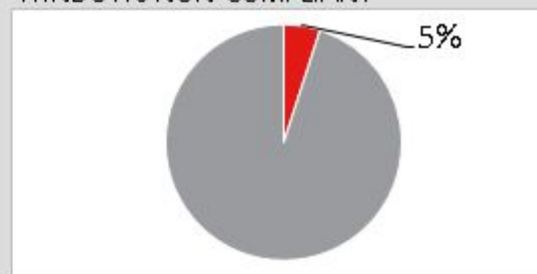
COMPUTERS SCANNED



O/S	#
Windows	3
Unix	1
Total computers scanned	4

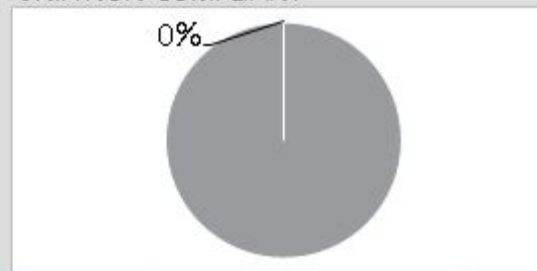
COMPLIANCE STATUS

WINDOWS NON-COMPLIANT



Non-compliant accounts	1
Compliant accounts	19
Total Windows accounts	20

UNIX NON-COMPLIANT



Non-compliant accounts	0
Compliant accounts	11
Total Unix accounts	11





CYBERARK

Privileged Threat Analytics

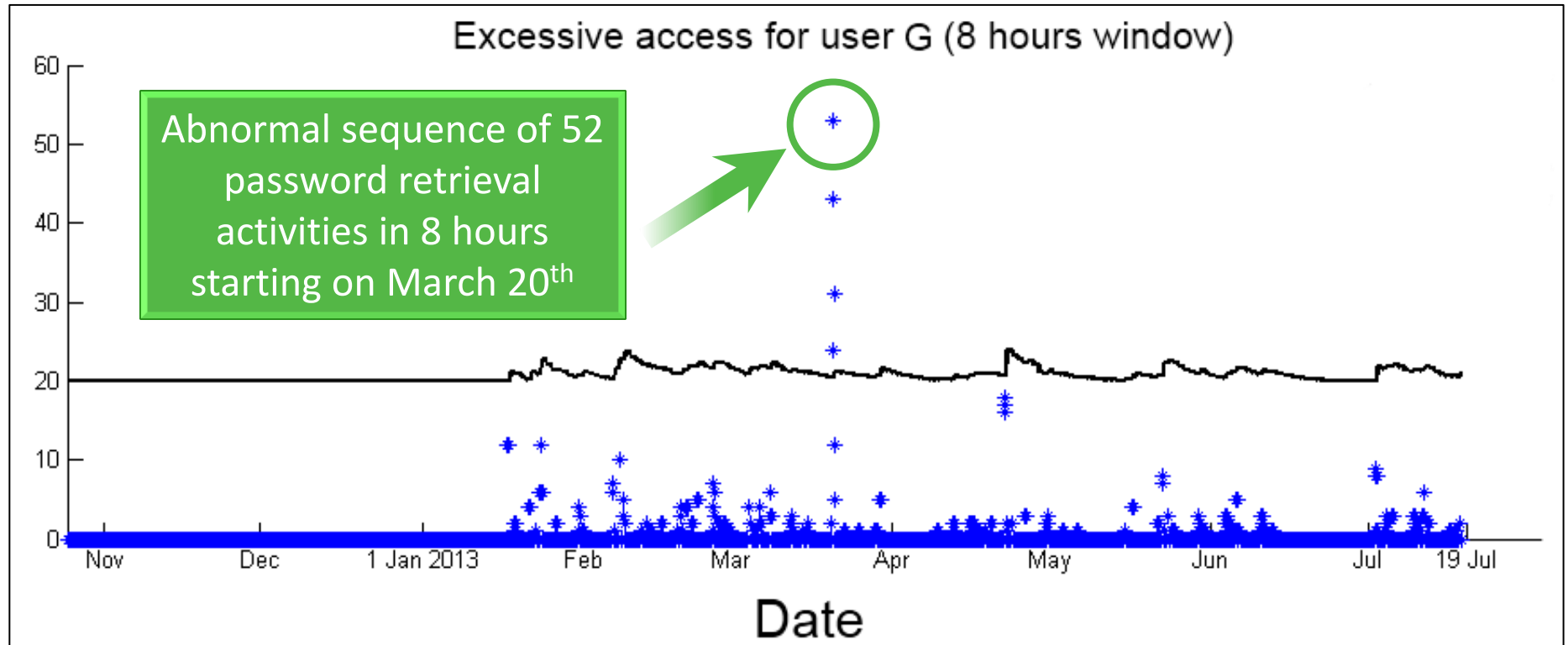
Introducing Privileged Threat Analytics

CyberArk's Privileged Threat Analytics detects malicious privileged account behavior.

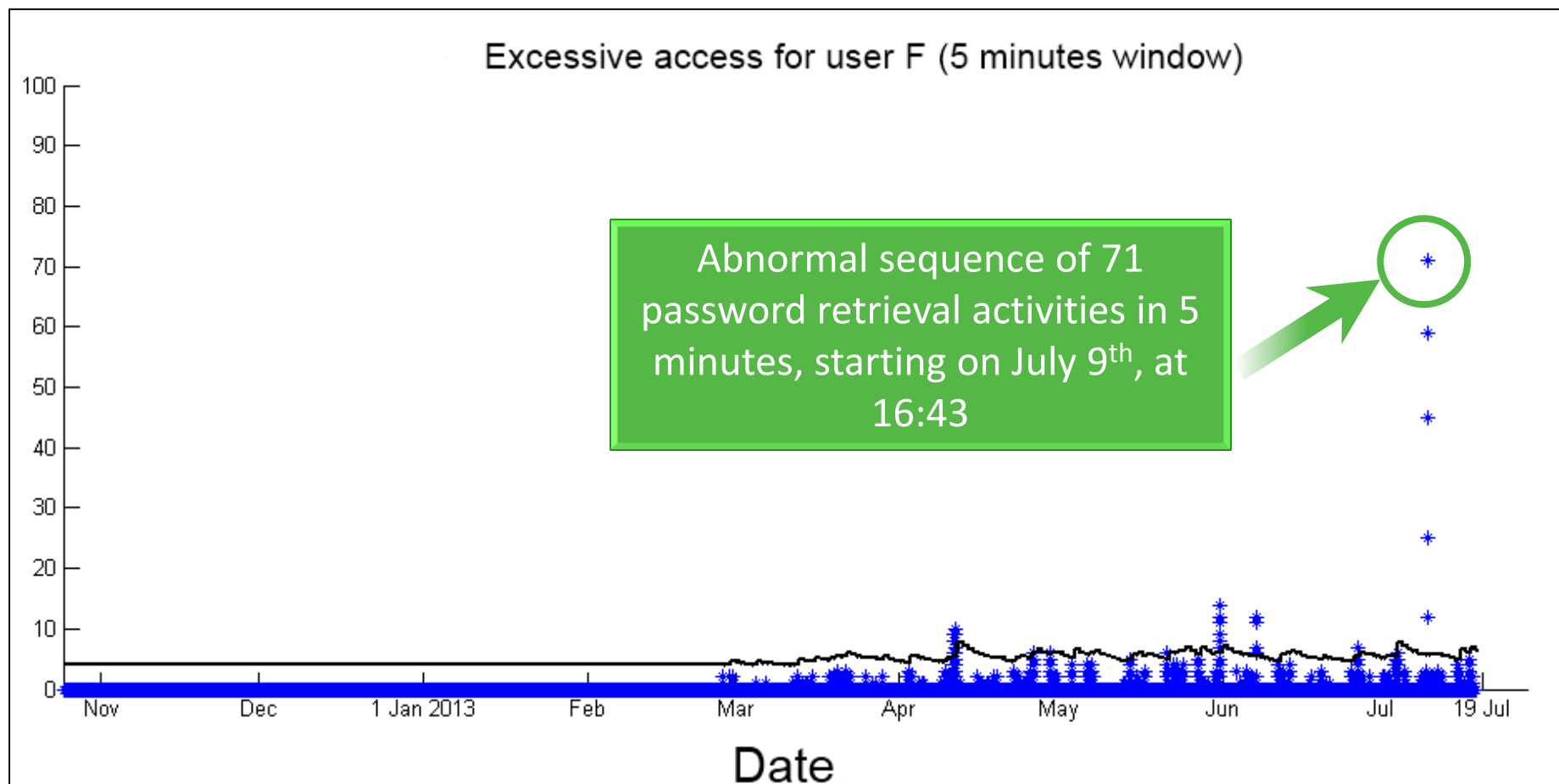
By comparing current privileged activity in real-time to historical activity, CyberArk can detect and identify anomalies as they happen, allowing the incident response team to respond, disrupting the attack before serious damage is done.



Excessive Access to Privileged Accounts



Excessive Access to Privileged Accounts



Source: Data of CyberArk customer analyzed in the CyberArk labs



CYBERARK

Questions?



CYBERARK

Thank you.