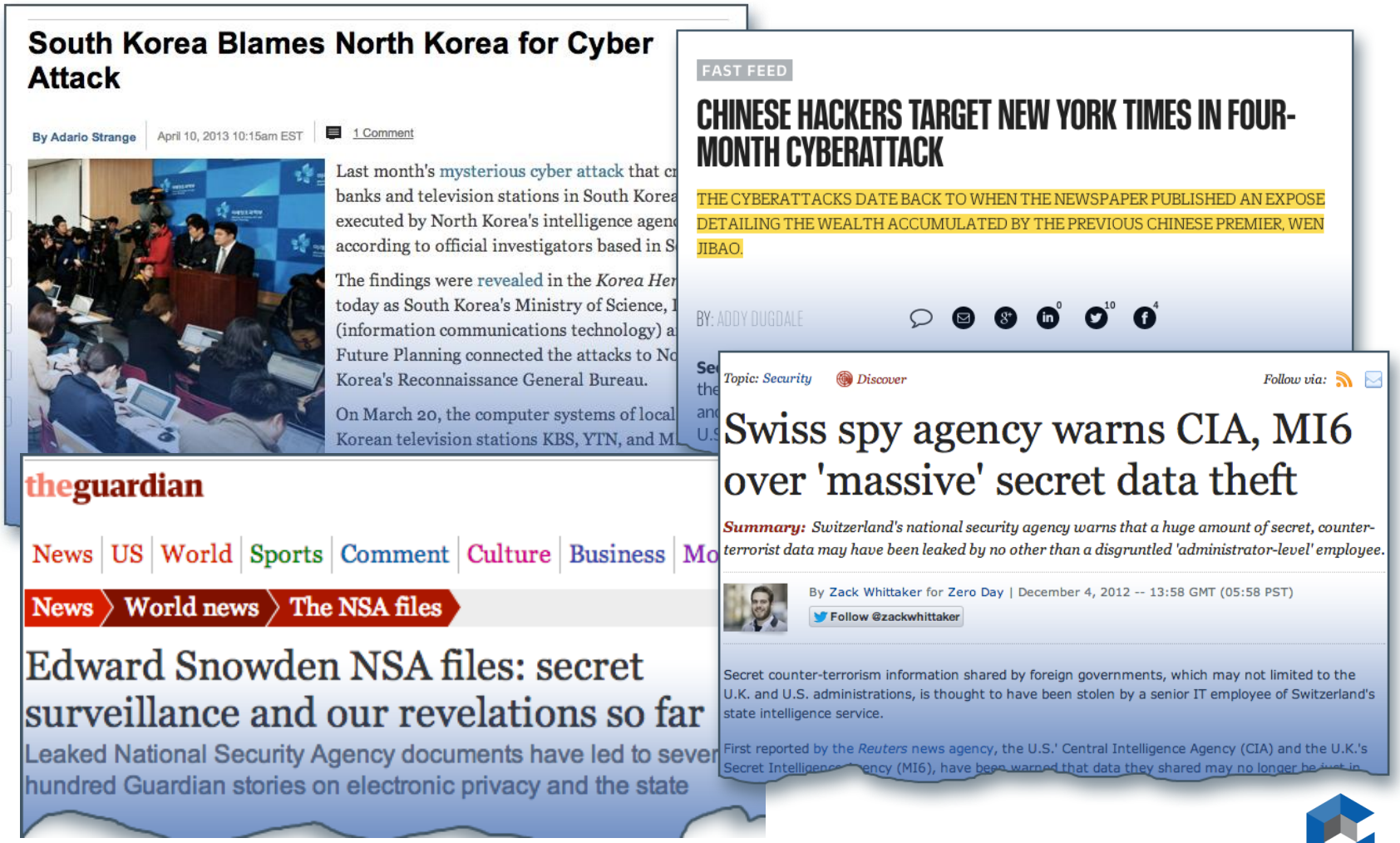
Targeted Attacks and the Privileged Pivot

Barak Feldman
National Director, CyberArk

Robert Jett
PNW Account Manager, CyberArk

Cyber Attacks: A Daily Event, Overwhelming Coverage



South Korea Blames North Korea for Cyber Attack

By Adario Strange | April 10, 2013 10:15am EST | 1 Comment

Last month's mysterious cyber attack that cr
banks and television stations in South Korea
executed by North Korea's intelligence agenc
according to official investigators based in S

The findings were revealed in the *Korea Her*
today as South Korea's Ministry of Science, I
(information communications technology) a
Future Planning connected the attacks to No
Korea's Reconnaissance General Bureau.

On March 20, the computer systems of local
Korean television stations KBS, YTN, and M

FAST FEED

CHINESE HACKERS TARGET NEW YORK TIMES IN FOUR-MONTH CYBERATTACK

THE CYBERATTACKS DATE BACK TO WHEN THE NEWSPAPER PUBLISHED AN EXPOSE DETAILING THE WEALTH ACCUMULATED BY THE PREVIOUS CHINESE PREMIER, WEN JIBAO.

BY: ADDY DUGDALE

theguardian

News | US | World | Sports | Comment | Culture | Business | Mo

News > World news > The NSA files

Edward Snowden NSA files: secret surveillance and our revelations so far

Leaked National Security Agency documents have led to sever
hundred Guardian stories on electronic privacy and the state

Topic: Security | Discover | Follow via:

Swiss spy agency warns CIA, MI6 over 'massive' secret data theft

Summary: *Switzerland's national security agency warns that a huge amount of secret, counter-terrorist data may have been leaked by no other than a disgruntled 'administrator-level' employee.*

By Zack Whittaker for Zero Day | December 4, 2012 -- 13:58 GMT (05:58 PST)

Follow @zackwhittaker

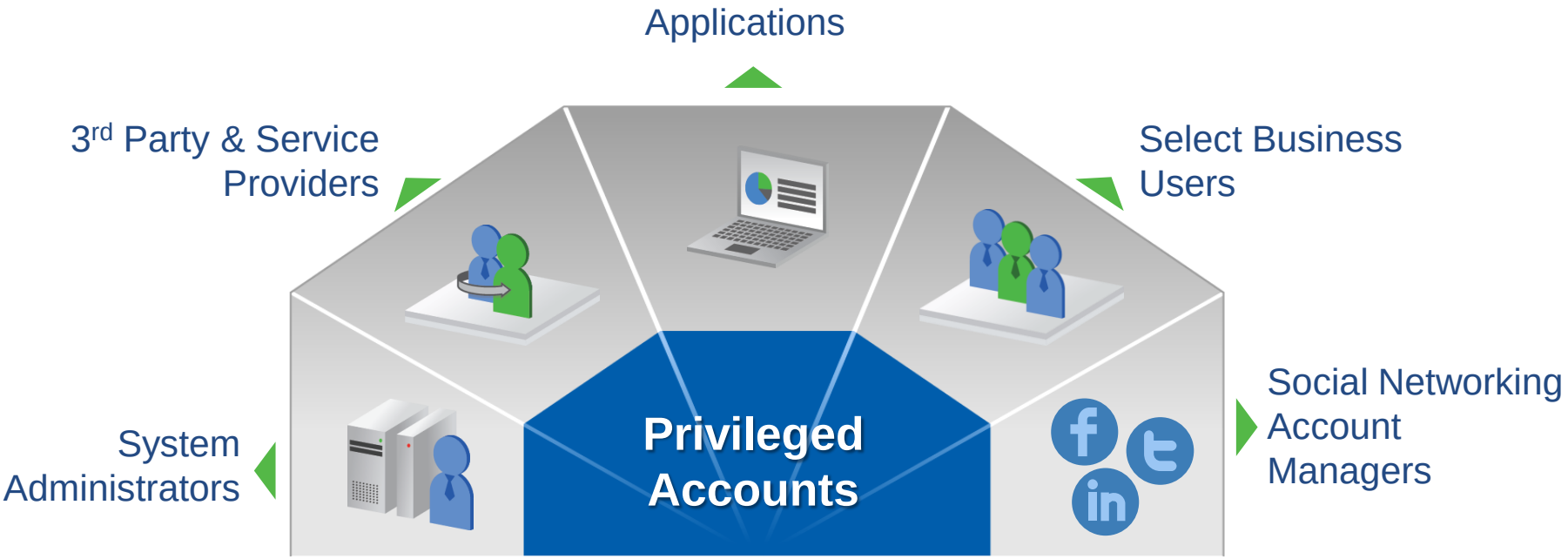
Secret counter-terrorism information shared by foreign governments, which may not limited to the U.K. and U.S. administrations, is thought to have been stolen by a senior IT employee of Switzerland's state intelligence service.

First reported by the *Reuters* news agency, the U.S.' Central Intelligence Agency (CIA) and the U.K.'s Secret Intelligence [illegible]ency (MI6), have been warned that data they shared may no longer be just in

CYBERARK

Regardless of where they started, they all became insiders!

Privileged Accounts Create a Huge Attack Surface

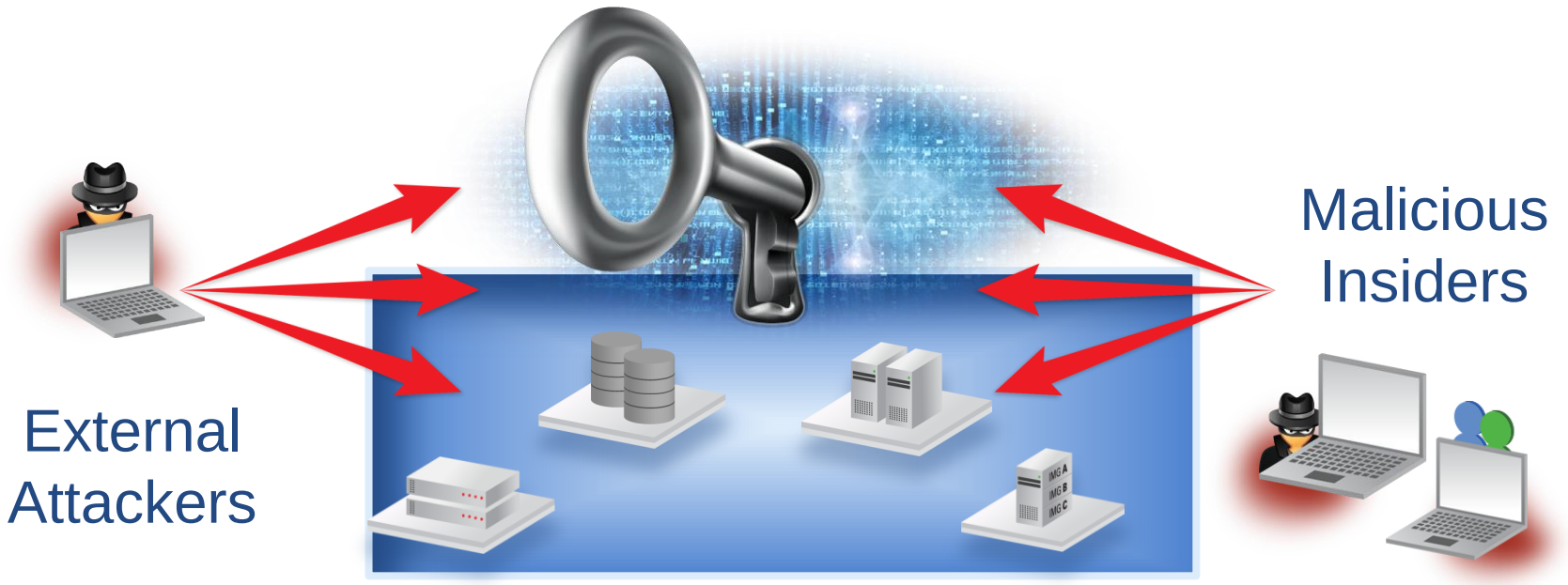


- Privileged accounts exist in every connected device, database, application, industrial controller and more!

- Typically a ~3X ratio of privileged accounts to employees

CYBERARK

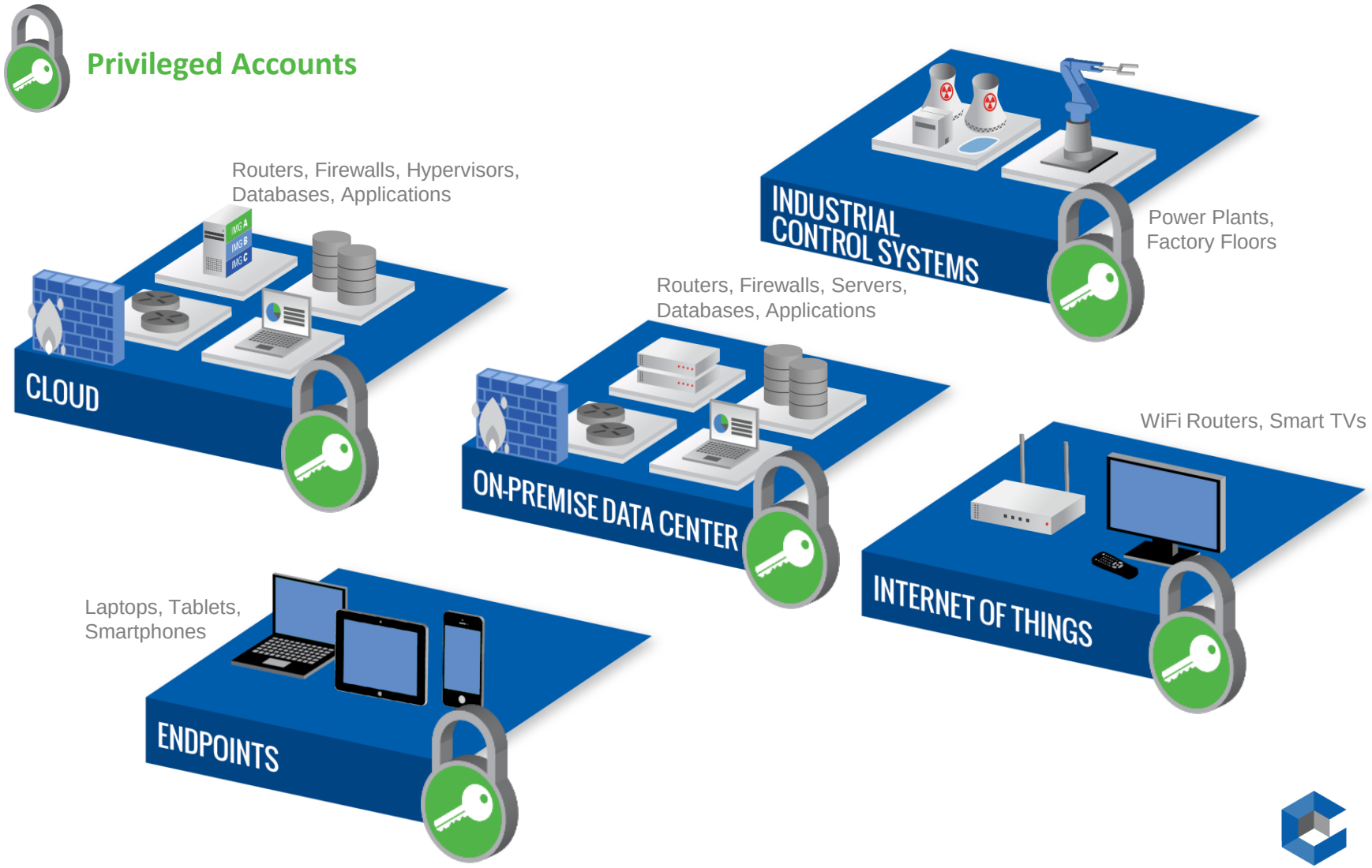
The One Thing Attackers Need to Succeed!



Privileged Accounts – “Keys to the IT Kingdom”

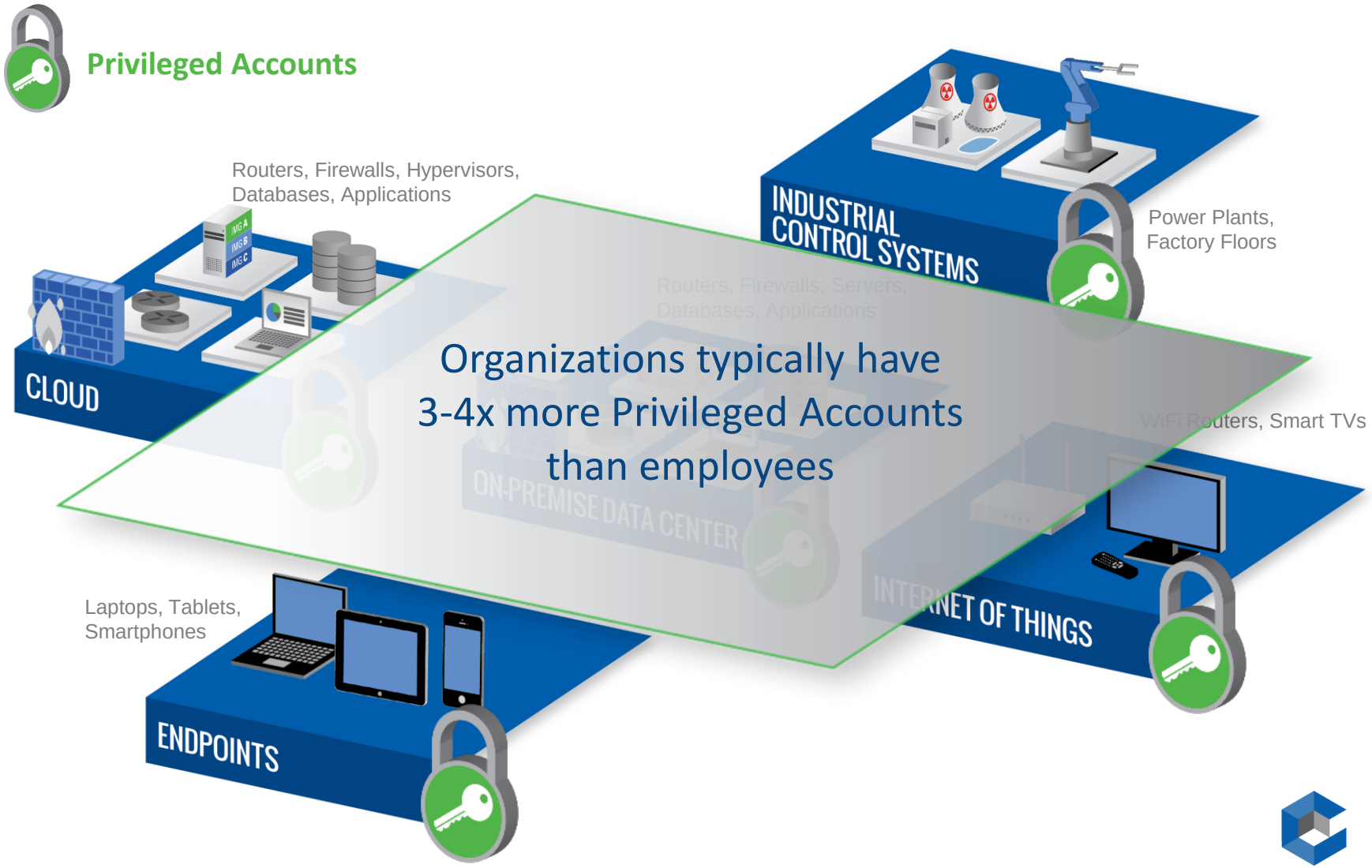
CYBERARK

Privileged Credentials are Everywhere



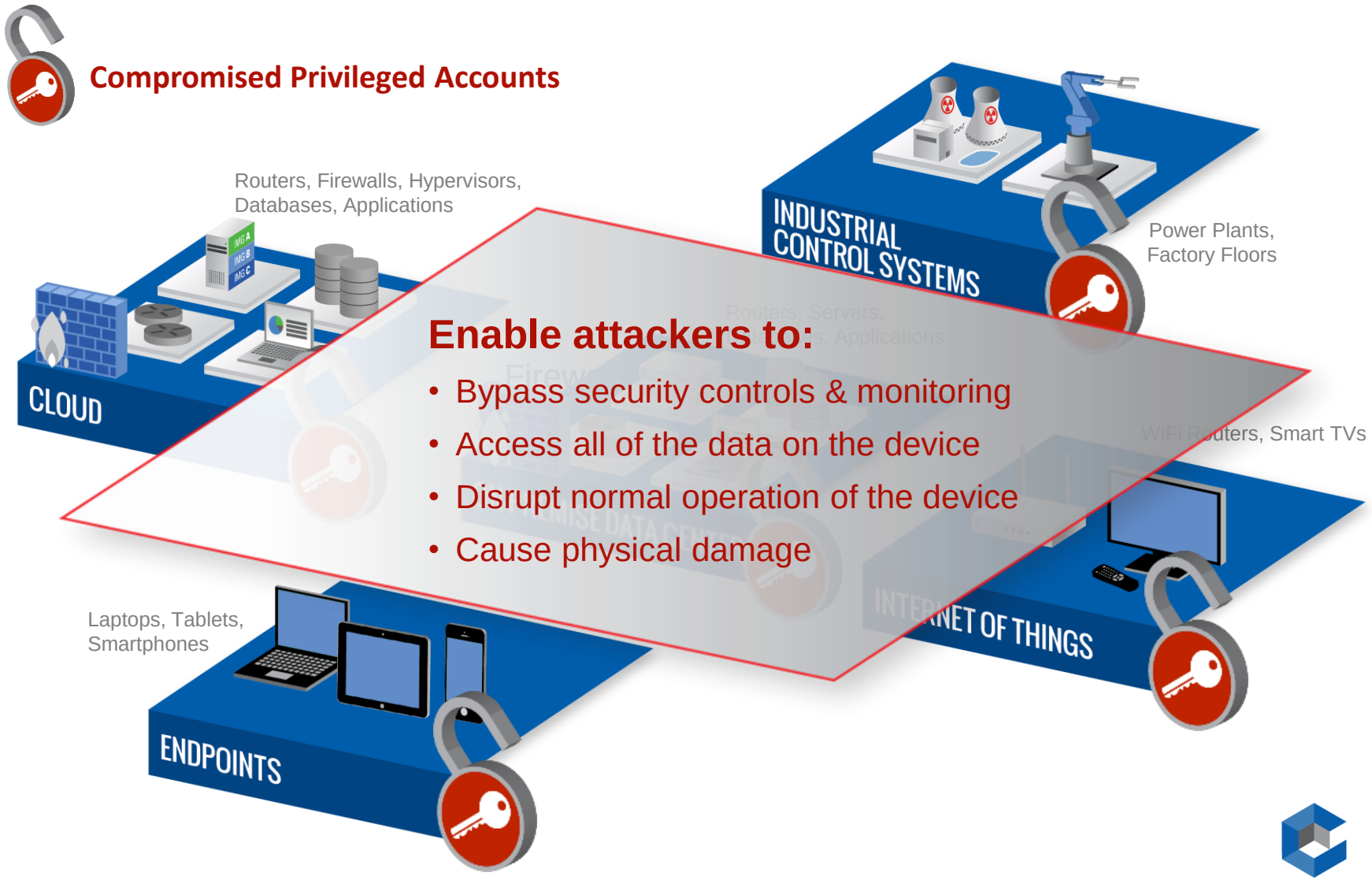
CYBERARK

Privileged Credentials are Everywhere



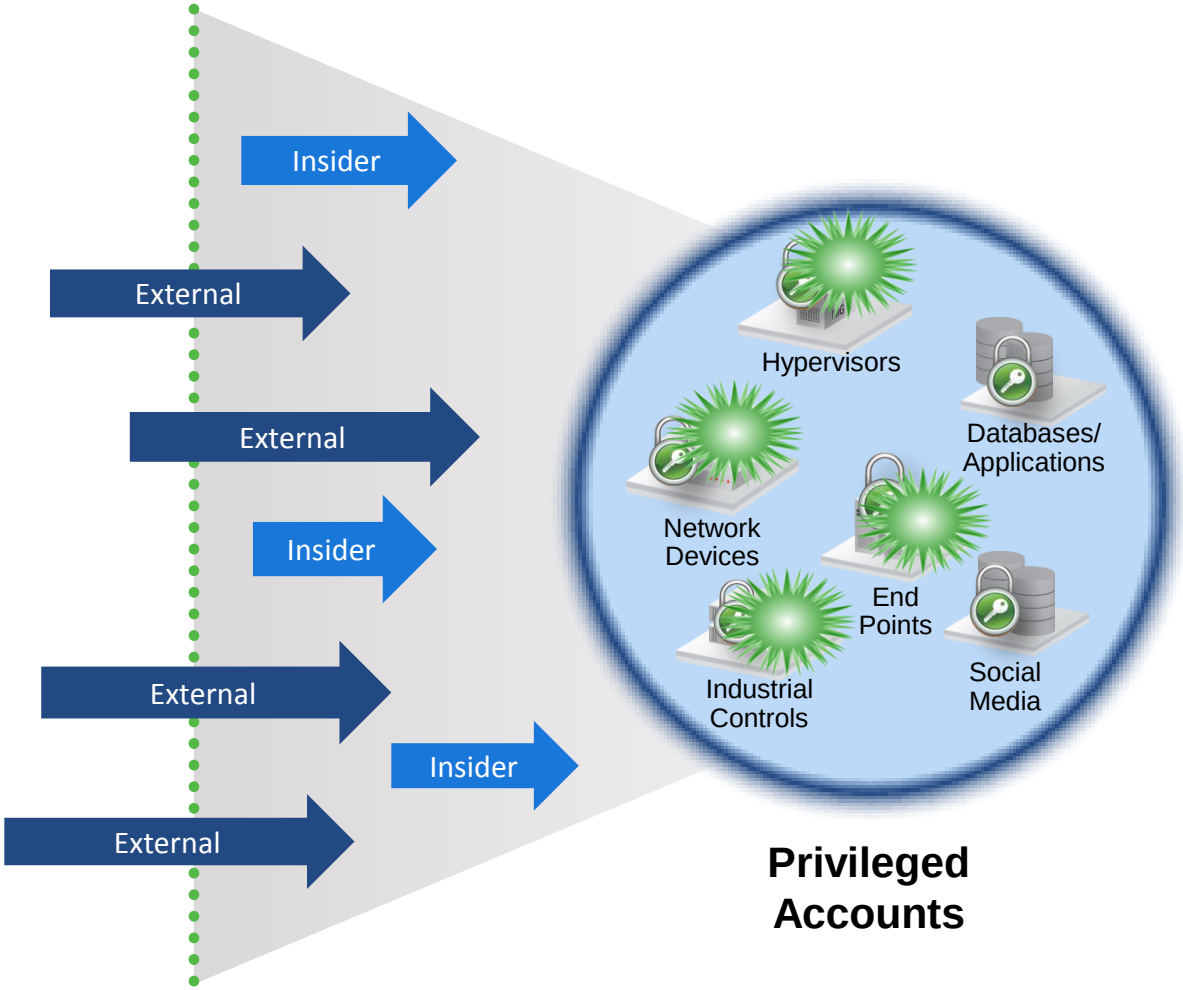
CYBERARK

Hijacked Credentials Put the Attacker in Control



CYBERARK

Proactive Protection, Detection & Response



Proactive protection

- Only authorized users
- Individual accountability
- Limit scope of privilege

Targeted detection

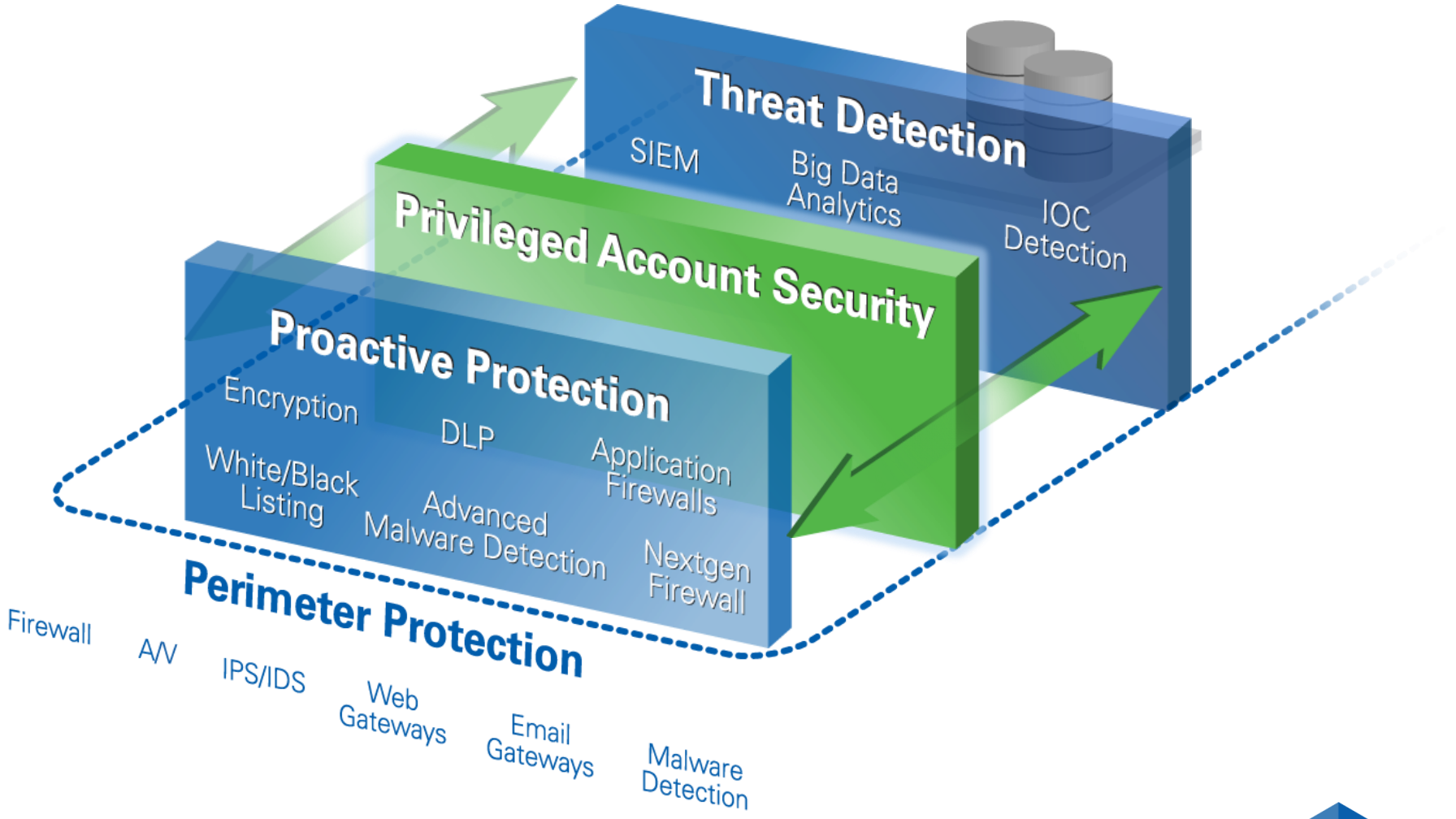
- Continuous monitoring
- Malicious behavior
- High risk behavior
- Alerting

Real-time response

- Session termination
- Full forensics record of activity

CYBERARK

Privileged Account Security – Now a Critical Security Layer



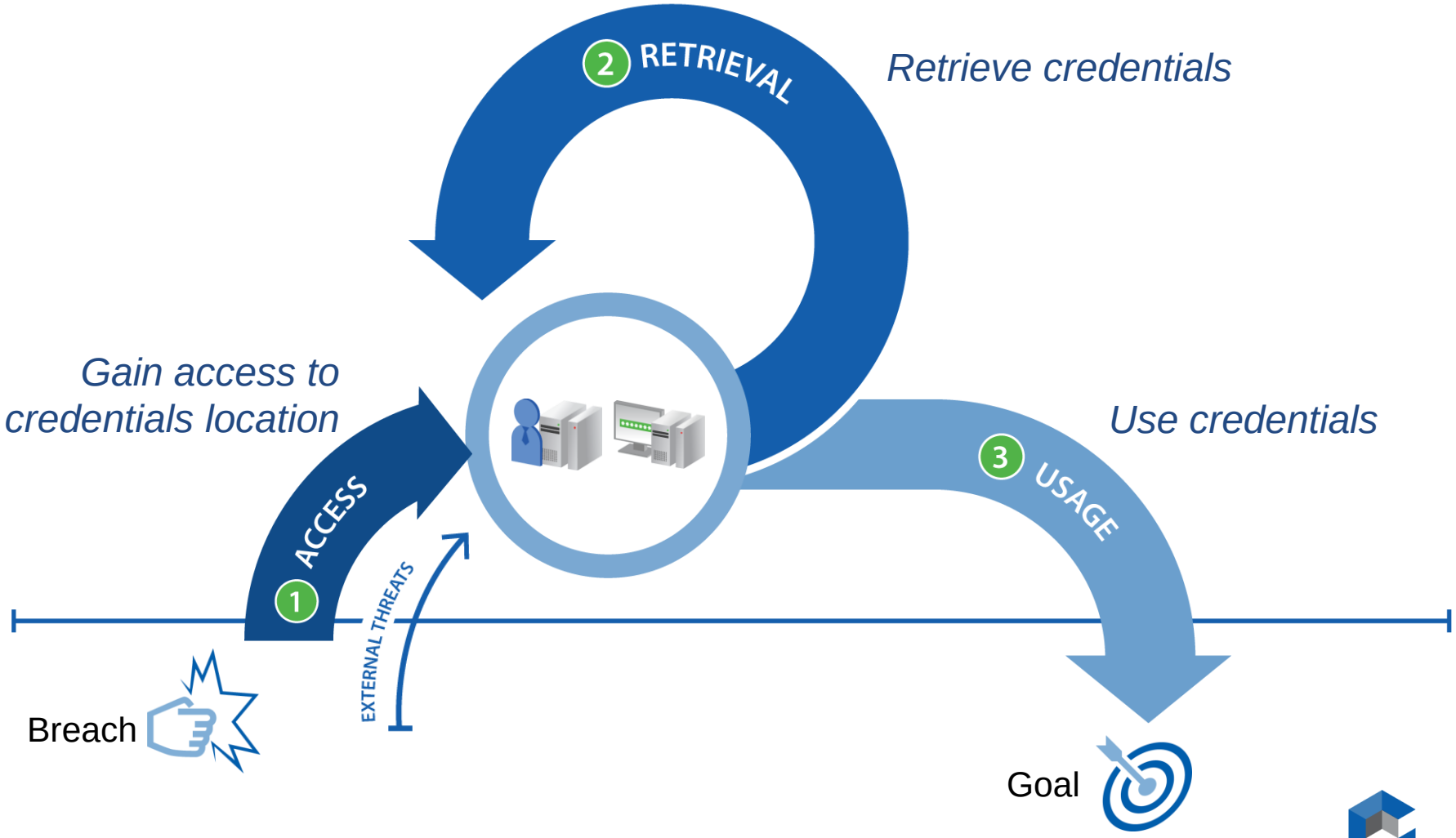
CYBERARK

Solving The Privileged Account Security Problem

Threats	▪ Advanced Threat ▪ Insider Threats ▪ Securing the Hybrid Cloud	▪ Securing Application Credentials ▪ Securing Shared Admin Accounts ▪ Sharing Sensitive Information
Audit & Compliance	▪ Control & Accountability for Privileged Users ▪ Monitor & Record Privileged Activity	▪ Compliance Reporting ▪ Remote User Access Control ▪ Auditing Secure File Transfer
Industrial Controls/SCADA	▪ Securing and Monitoring Shared Admin Accounts for ICS Systems ▪ Controlling and Monitoring Remote Vendors	▪ Smart Grid Security

CYBERARK

The Privilege Escalation Cycle



Primary Recommendations

Restrict Lateral Movement

- Assign a UNIQUE password on every endpoint for built-ins
- Establish Credential Boundaries on Domain; One-Time Passwords

Isolate High Value Assets

- Ensure users can not access sensitive assets directly from their endpoint
- Do not allow users or their machines to know a password (keyloggers, malware, etc.)

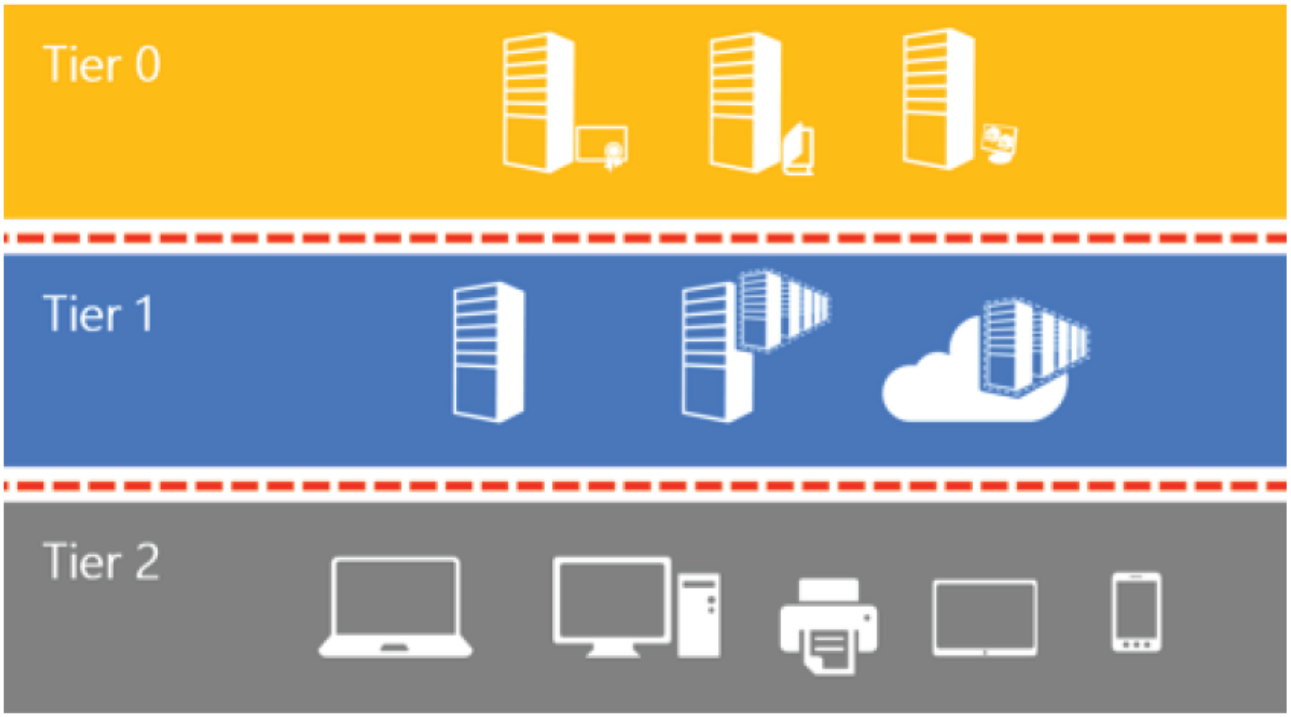
Monitor Behavior

- Look for changes in behavior for common privileged accounts and sensitive assets, especially indicators of credential theft
- Enable reactive countermeasures

CYBERARK®

Credential Boundaries

**See MSFT Whitepaper: Mitigating Pass the Hash Attacks and Other Credential Theft Version 2*



Tier 0 – Forest admins: Direct or indirect administrative control of the Active Directory forest, domains, or domain controllers

Tier 1 – Server admins: Direct or indirect administrative control over a single or multiple servers

Tier 2 – Workstation Admins: Direct or indirect administrative control over a single or multiple devices

CYBERARK

Strategic Best Practices Summary

Session Recording & Desktop Isolation

- Isolate High value assets and create a new layer of security using proxy server.
- Leverage Universal connectors and native access to enforce PIV cards and role based accounts.
- Record all privileged activity without the use of an agent

Password Management

- Change passwords to built-in accounts to a unique value per end point
- Frequently change passwords to minimize the risk of credential (hash) theft

Privileged Analytics and Anomalies

- Watch for anomalous behavior of privileged accounts and bypass of controls to limit and stop events in progress.

Least Privilege Access and App Controls

- Reduce a large number of privileged users from desktops and servers by using a least privileged escalation model in Windows desktops/Servers and Unix/Linux.

CYBERARK

What to do now – Getting Started

Identify

- Run free assessment tools to find out where privileged accounts exist and how they are being used/misused

Change

- Identify top 3-5 data center technologies and high Value assets and Isolate and change the built-in backdoor ids on each to a unique random password

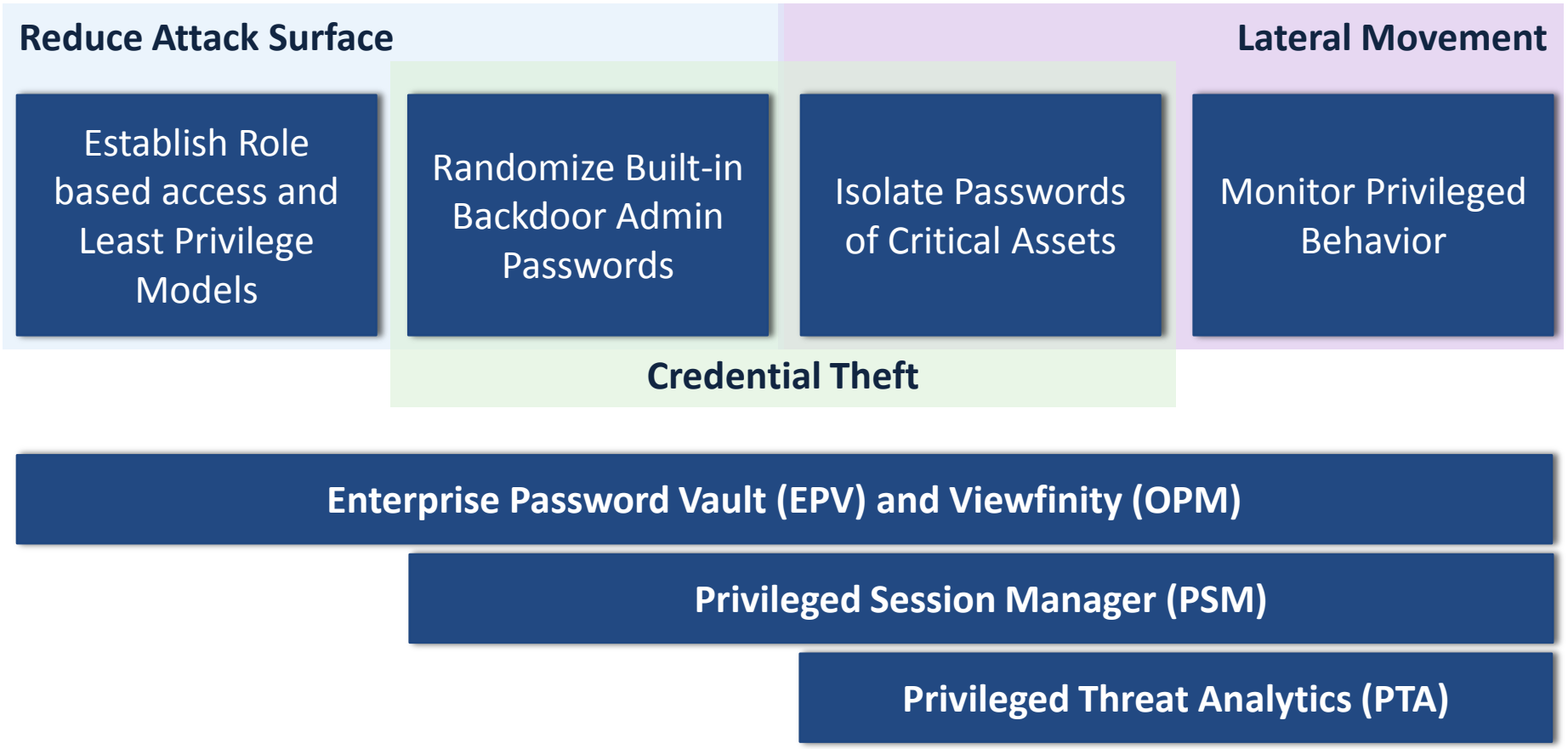
Isolate

- Identify what systems/information an ‘attacker’ would target and assign priority
- Prevent end users from accessing these devices directly moving forward and do not disclose passwords

CYBERARK®

CyberArk Maturity Model – Levels of Control

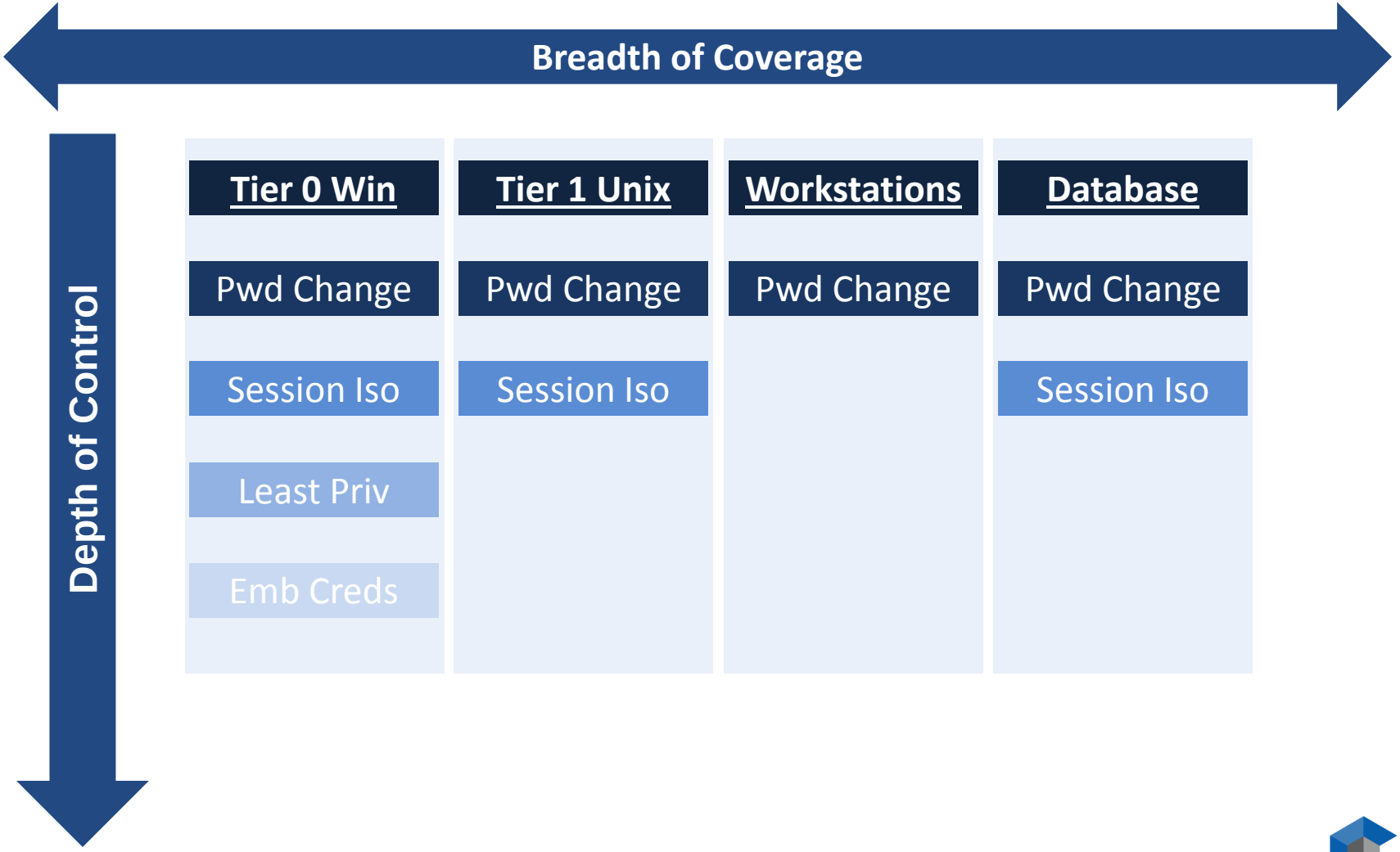
Primary Recommendations



CYBERARK

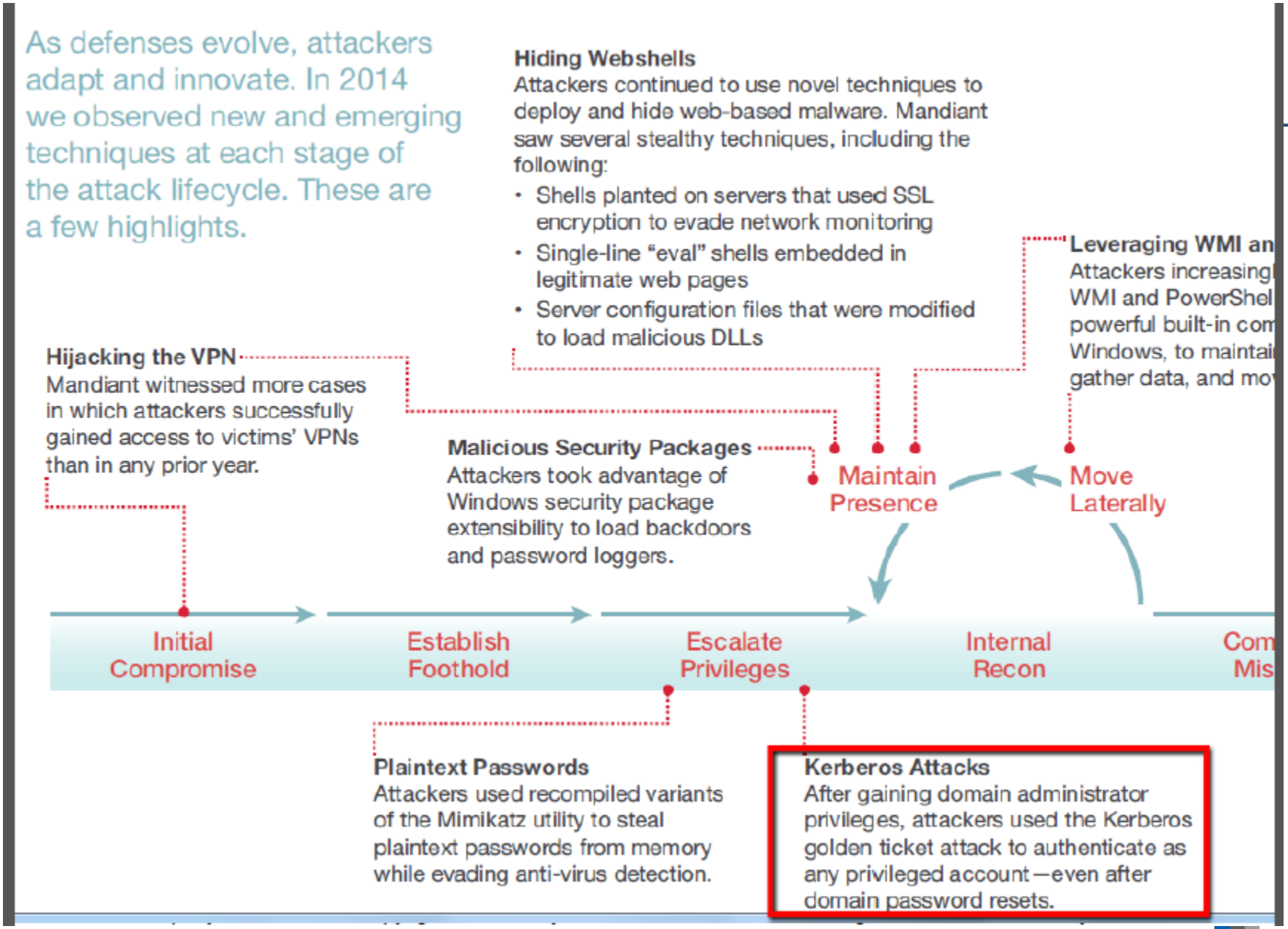
Extra Slides

How to Measure Success – Wide & Deep



CYBERARK

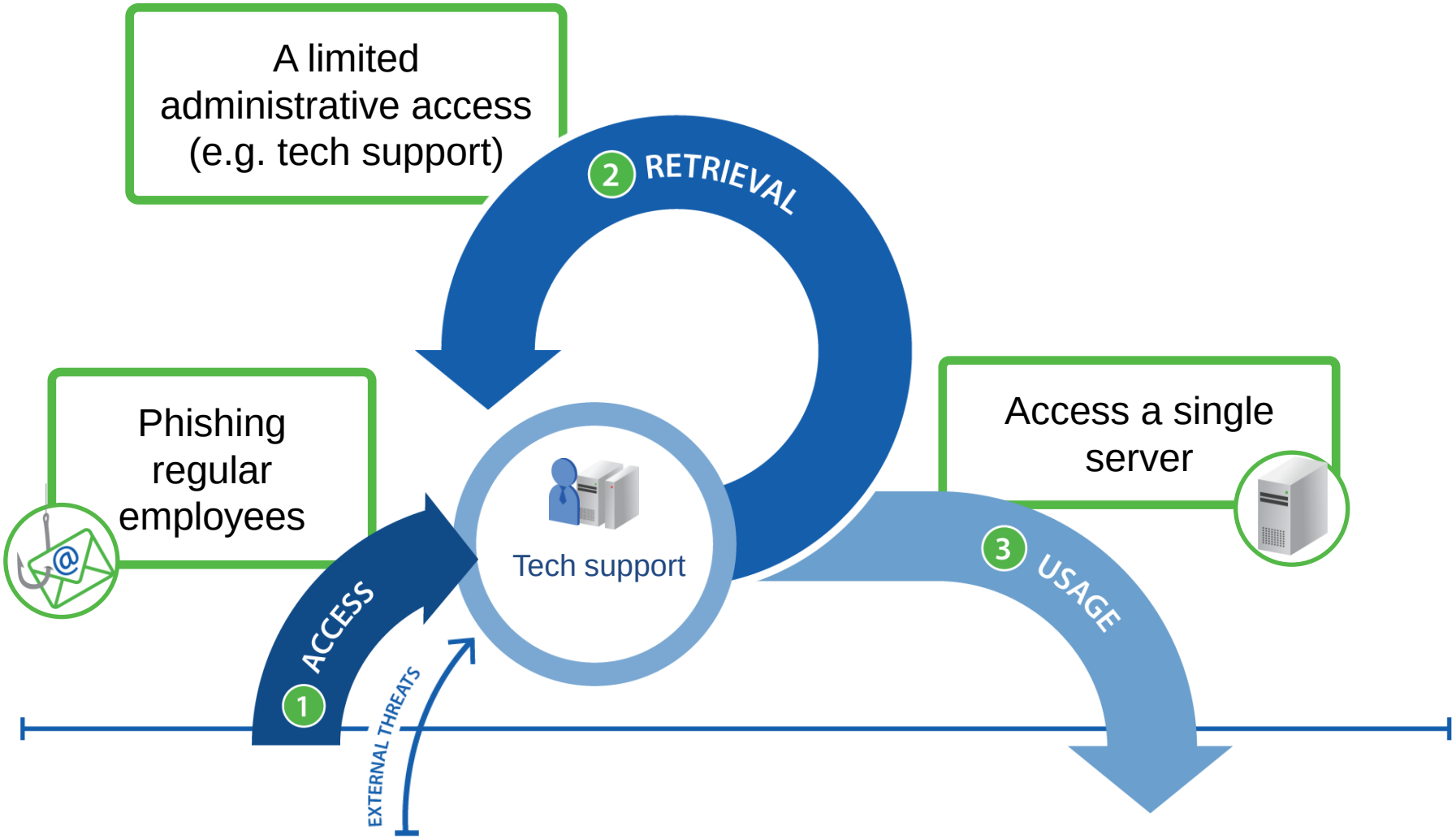
As defenses evolve, attackers adapt and innovate. In 2014 we observed new and emerging techniques at each stage of the attack lifecycle. These are a few highlights.



CYBERARK

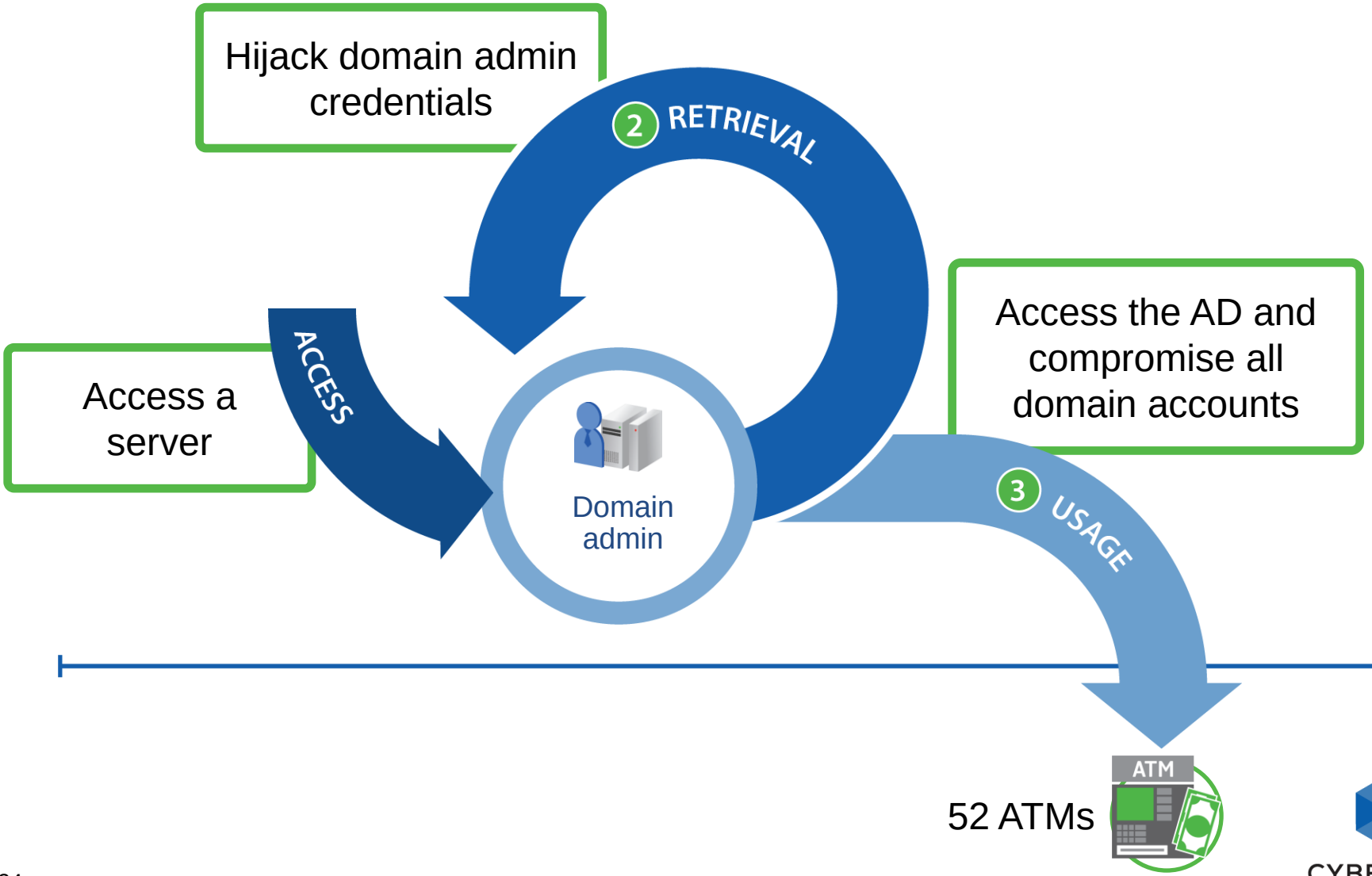
The Anunak/Carbanak Attacks

The Anunak/Carbanak Attacks

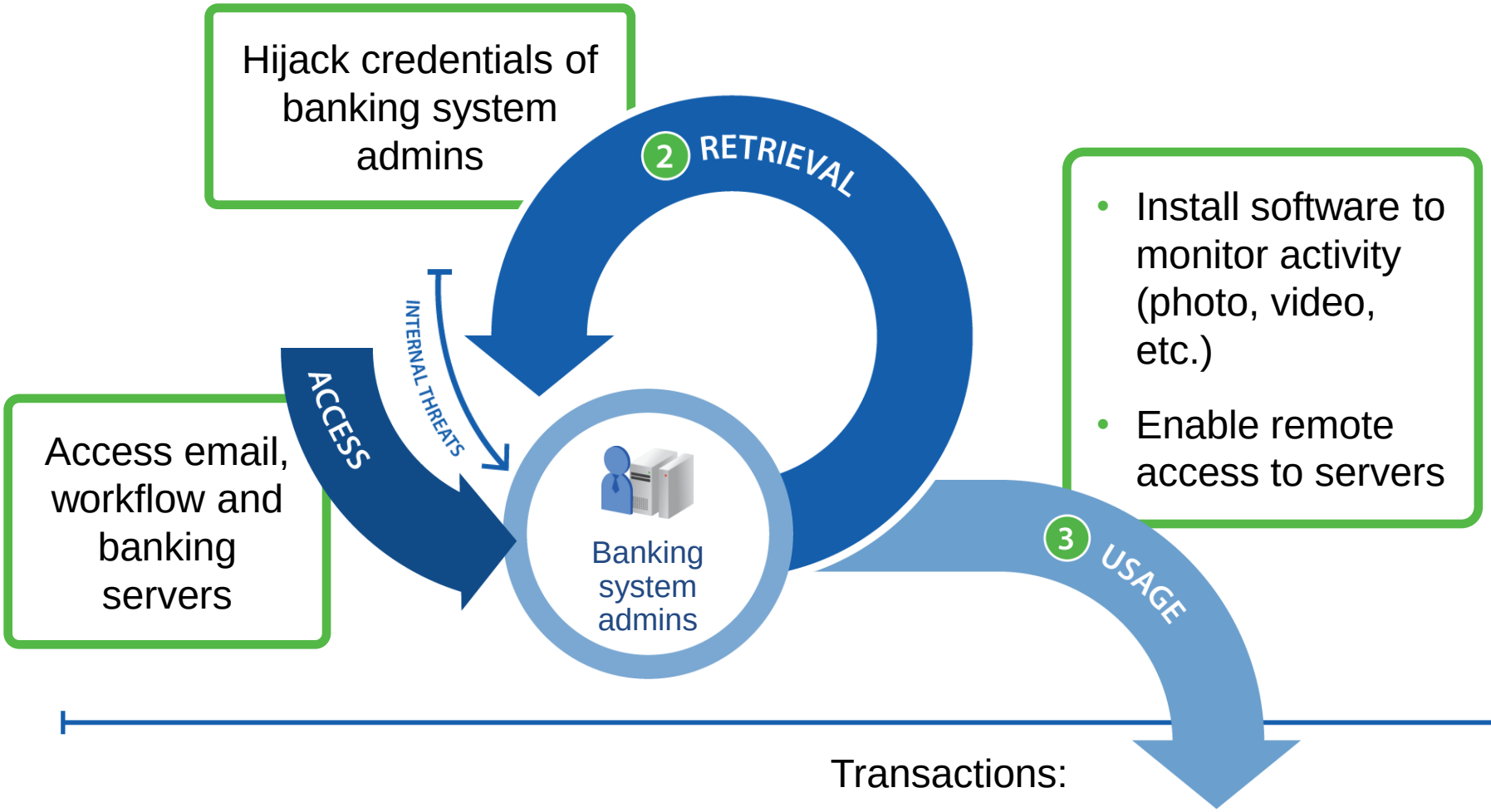


CYBERARK

The Anunak/Carbanak Attacks



The Anunak/Carbanak Attacks



Who are the attackers?

Does attribution help mitigation?

CYBERARK

CyberArk Contacts:

Rob Jett
Robert.jett@cyberark.com
(510) 717-9910

Barak Feldman
Barak.Feldman@cyberark.com