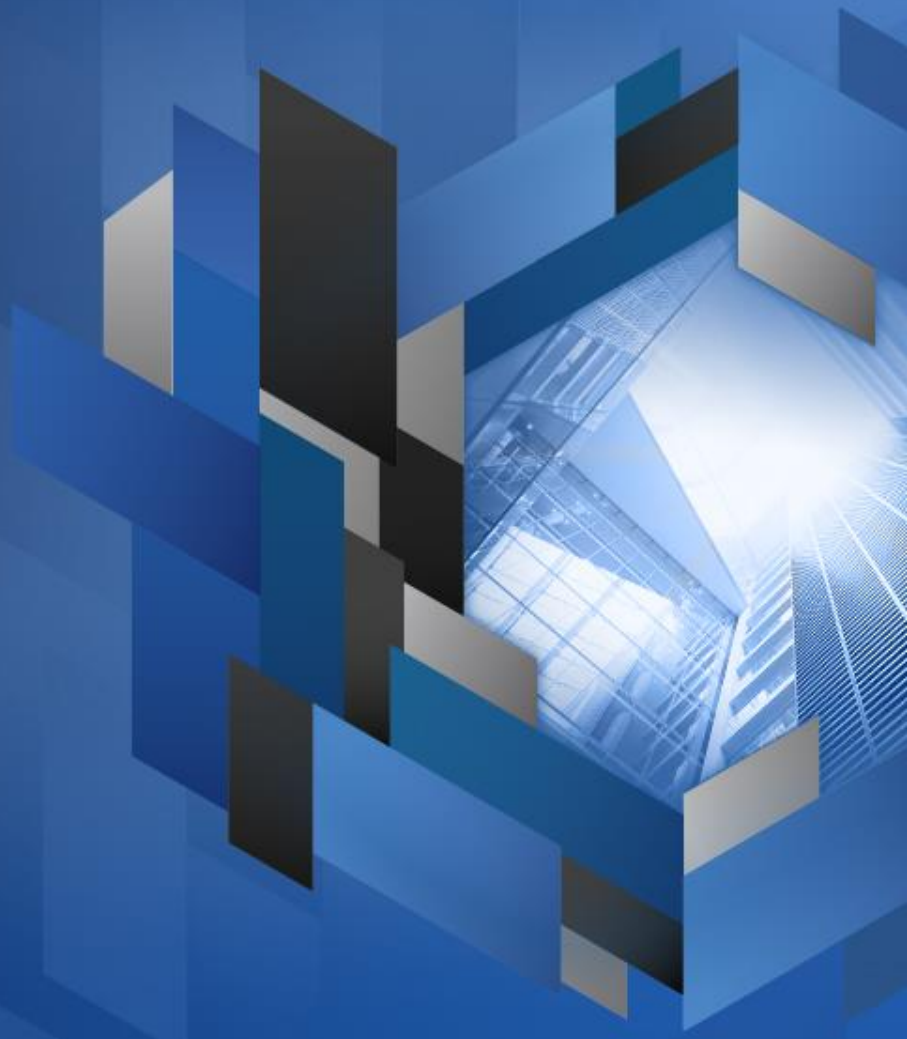


Making Privilege a Priority

Troy Brueckner, CISSP
District Manager, Midwest

NEbraskaCERT CSF
August 16, 2017

The Real Cyber Battleground: Inside the Network

Over 90% of organizations have been breached

- In the past: “I can stop *everything* at the perimeter”
- Today: “I can’t stop *anything* at the perimeter”

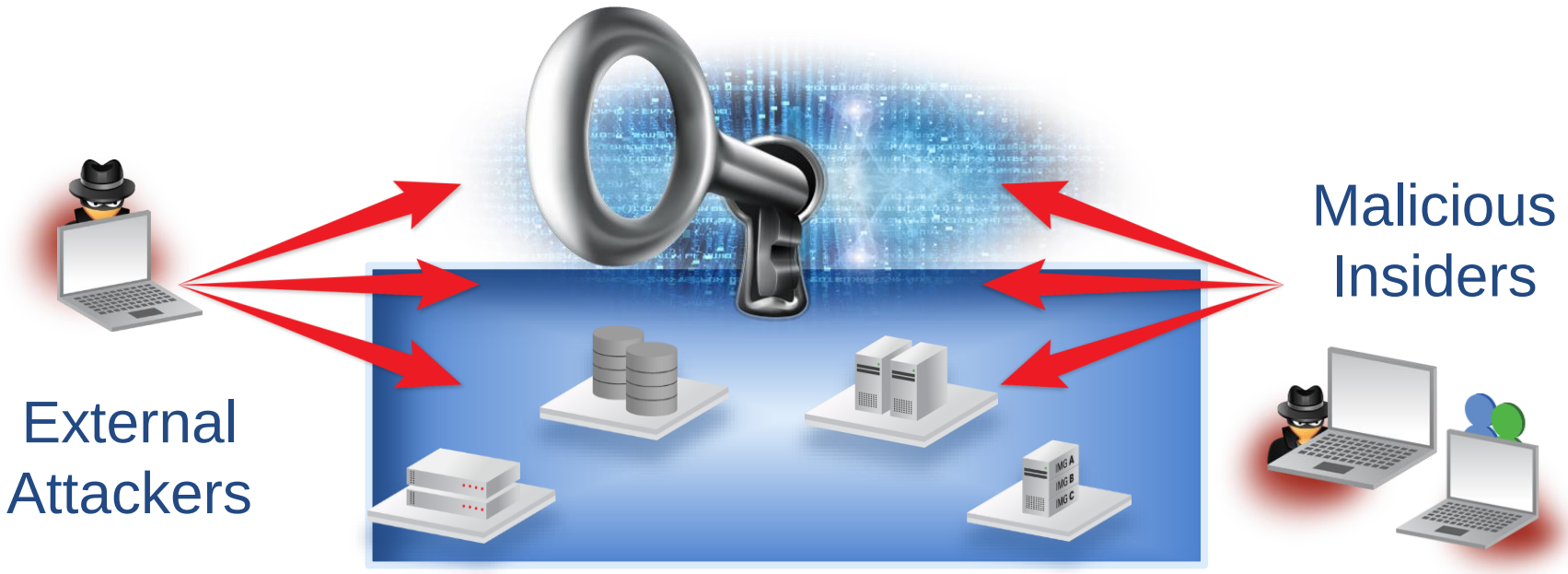
Information security focus shifts to inside the network

- Over 35% of breaches are internal – driven by malicious and unintentional insiders
- Compromised credentials empower any attacker to act as an insider

Compliance and audit requirements focus on privileged accounts

- Privileged accounts provide access to the most sensitive and valuable assets
- Information exposure damages brand reputation and customer confidence

Privileged Accounts - “Keys to the IT Kingdom”



Privileged Account Security Provides
Proactive Protection and Detection

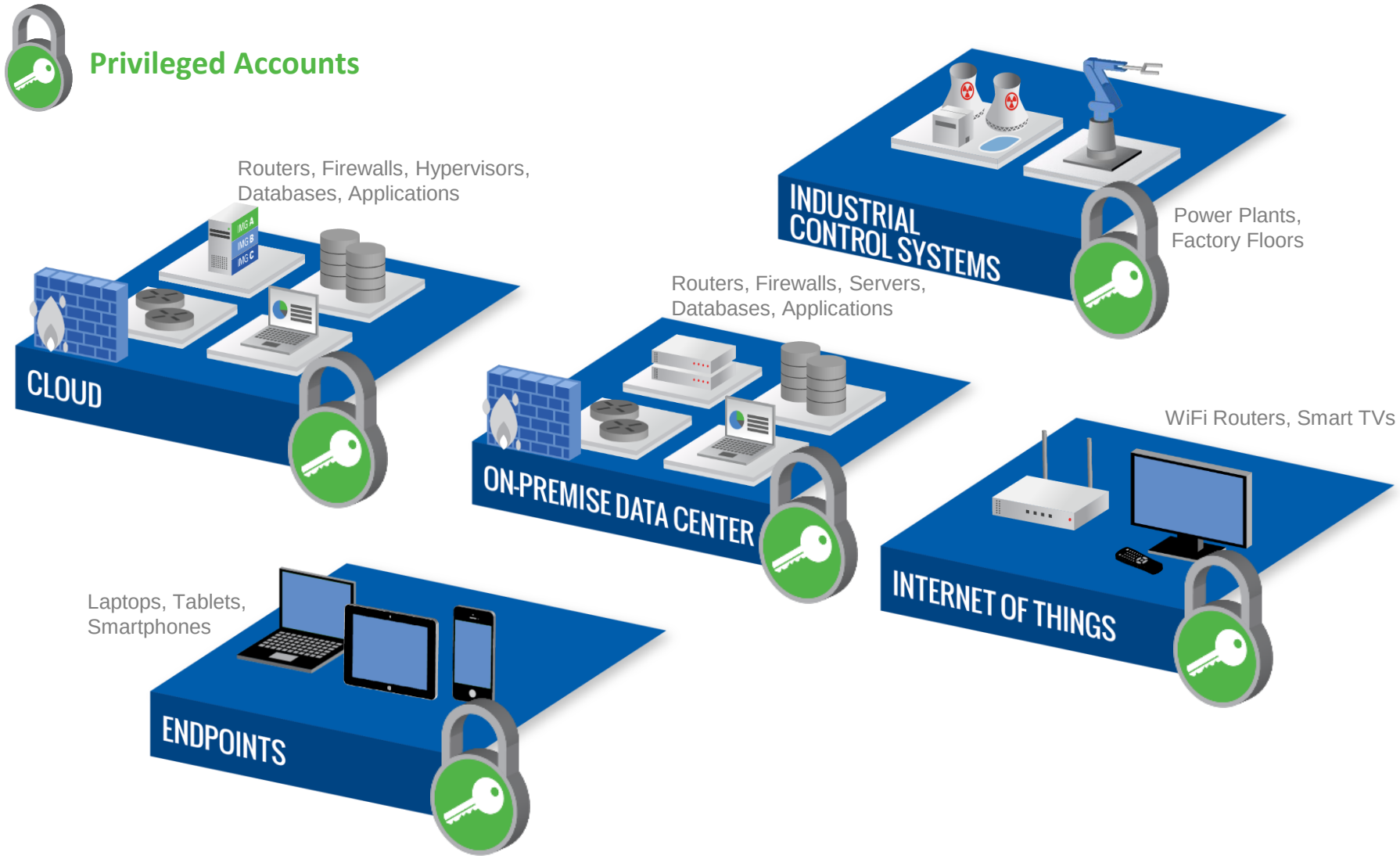
An Attacker Must Obtain Insider Credentials

"…100% of breaches involved stolen credentials."

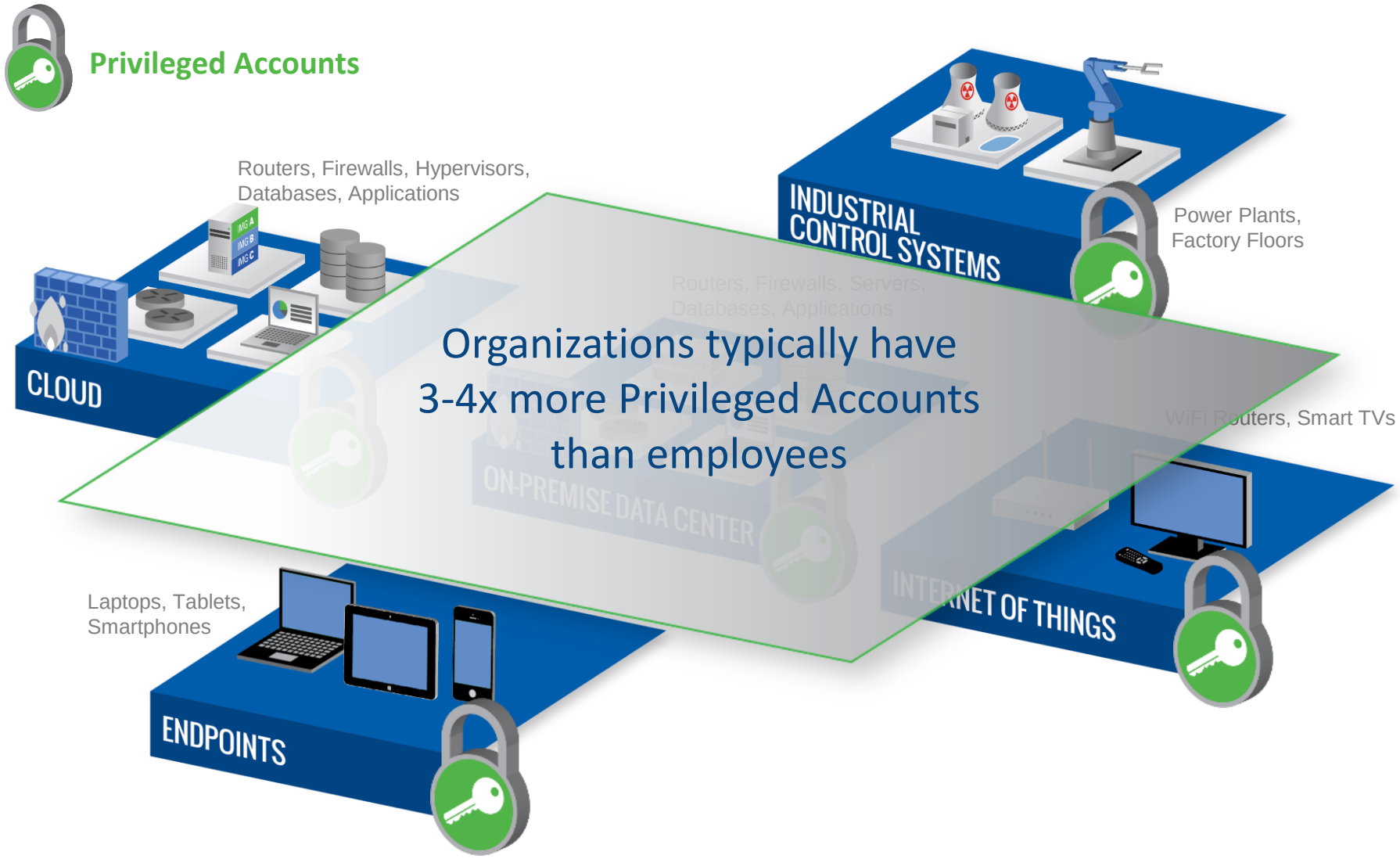
"APT intruders…prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts."

Mandiant, M-Trends and APT1 Report

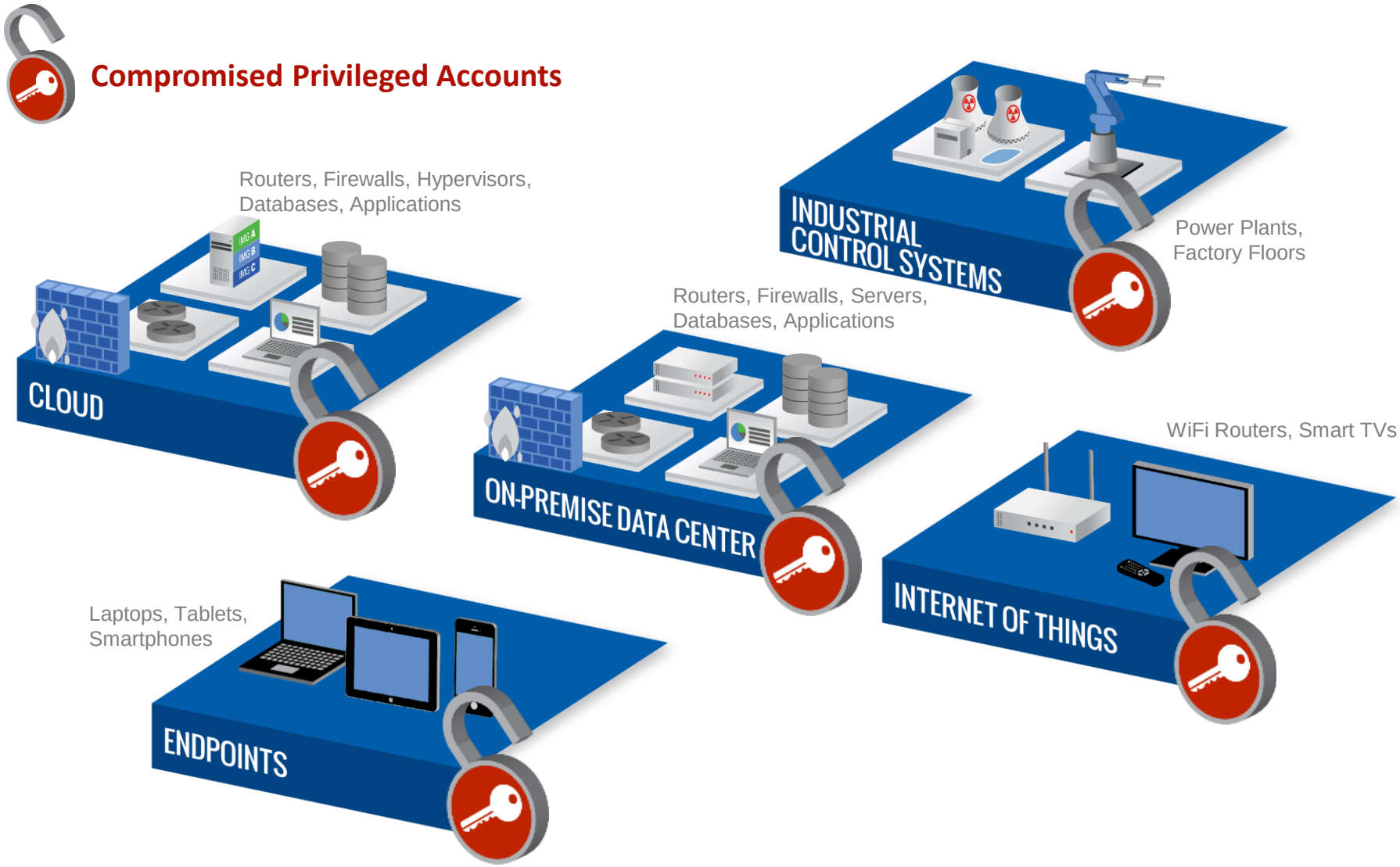
Privileged Credentials are Everywhere



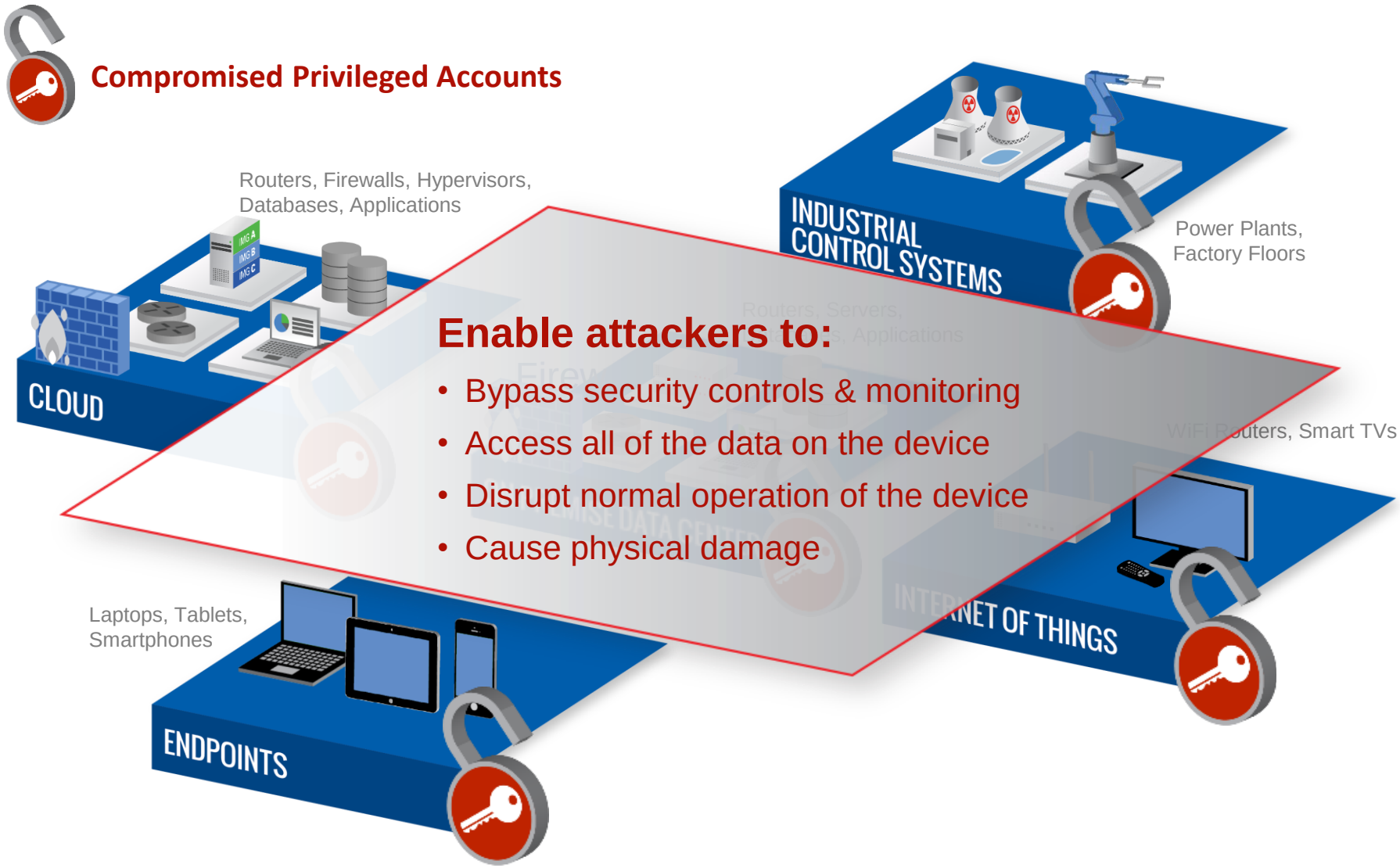
Privileged Credentials are Everywhere



Hijacked Credentials Put the Attacker in Control

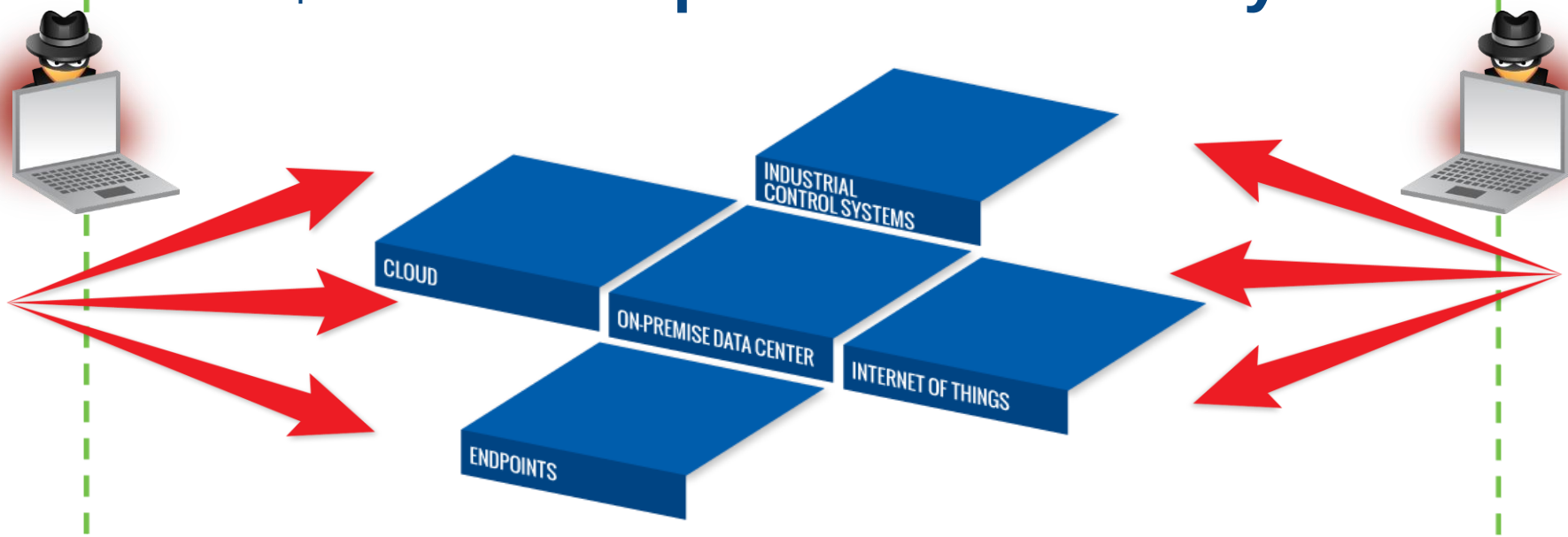


Hijacked Credentials Put the Attacker in Control



Perimeter Defenses Are Consistently Breached

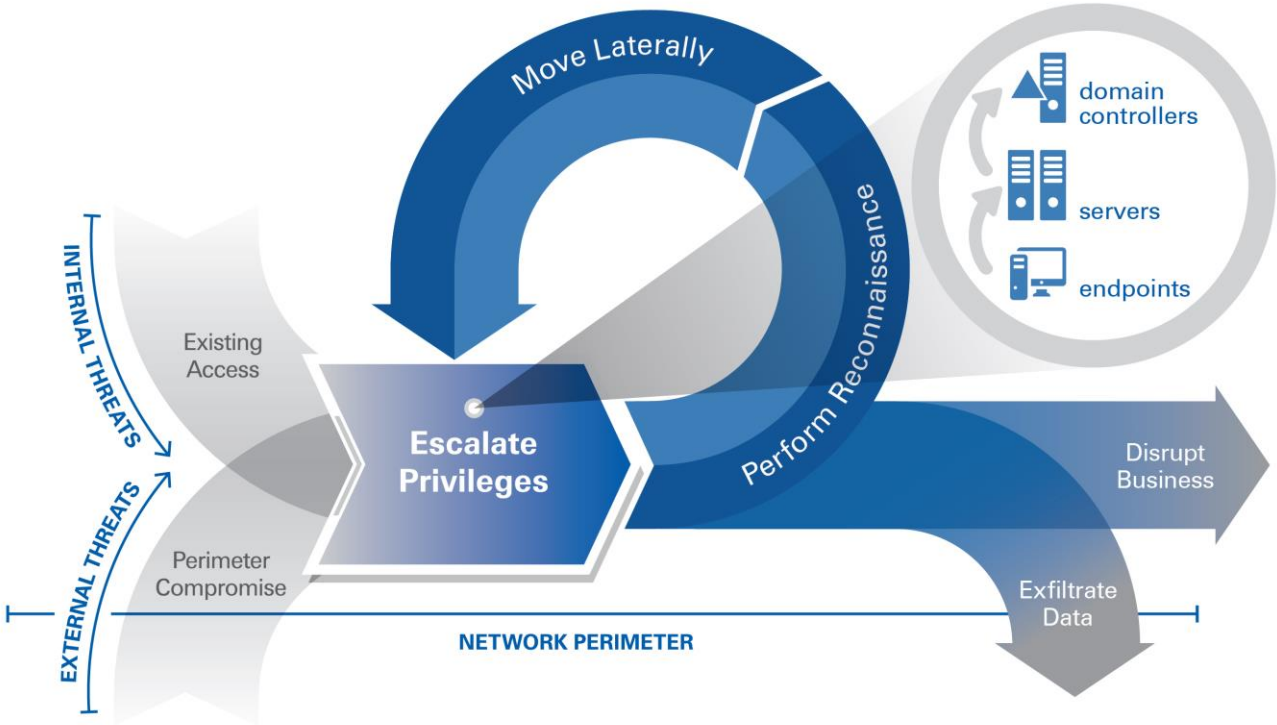
$28 billion spent on IT security!



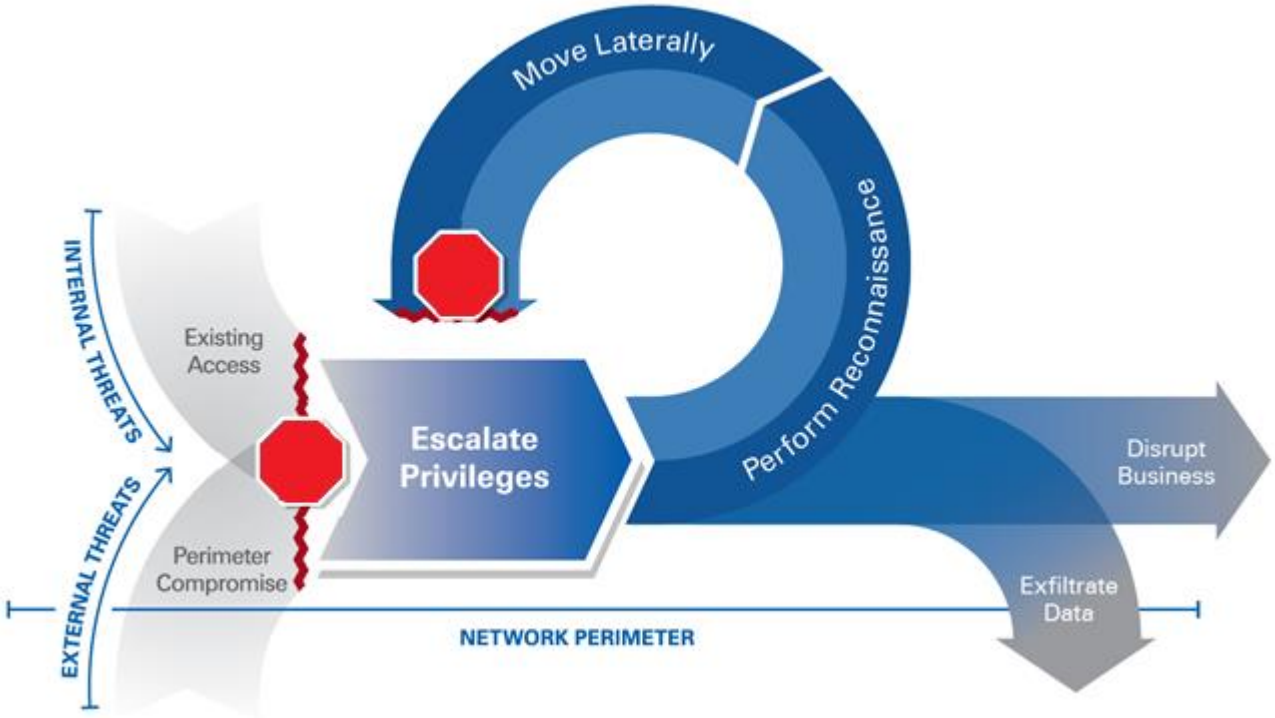
Over 90% of organizations **breached!**

Sources: IDC and Ponemon Institute

Privilege Escalation Enables Asset Escalation



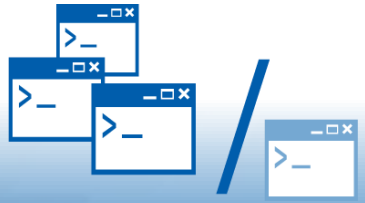
Breaking the Attack Chain



Comprehensive Controls on Privileged Activity

Lock Down Credentials

Protect privileged passwords and SSH keys



Isolate & Control Sessions

Prevent malware attacks and control privileged access

Continuously Monitor

Implement continuous monitoring across all privileged accounts

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

TOP FIVE:
What Everyone Should Be Doing

1. Restrict Privileged Access to Critical Systems

Restrict privileged access to tier-0 and high value systems, most commonly domain/enterprise admin's access to Domain Controllers.

This should be done in conjunction with Multifactor authentication, Identity Management and proper network segmentation and tiering.

Once the access is established, monitor behavior to the systems and stop known bad process such as Mimikatz.

- Impersonation of a privileged user leads to the ability to perform a total network takeover such as an advanced Kerberos attack or Golden Ticket.
- Access to critical assets is often part of some user's day to day activities, making it hard to separate an outsider impersonation or rogue insider.
- Many times the same account used to access the high value systems is also the account used for all production support, making the operational impact of account management very high.

1. Restrict Privileged Access to Critical Systems

Benefits:

Multiple layers of security and control are keys to mitigating the key risks of credential theft, impersonation and total network takeover. Creating credentials boundaries and decoupling the user from the account devalues the credential and requires the attacker to steal multiple things to get to multiple places. In the event an account is compromised, the attacker should not be able to connect directly to the high value asset. Assuming the attacker is able to impersonate and gain access to the asset, the behavior of the user will change and good blacklisting techniques can be applied. The recommendation addresses both rogue insiders as well as outsiders impersonating insiders.

2. Remove Local Admin Rights and Apply Greylisting to High Value User Systems

Remove local Admin rights and apply greylisting to high value user systems such as financial, Developer, Domain Admins or HR laptops/workstations.

- Each organization will identify its own subset of high value end-points. Attackers will target these systems with phishing attacks or similar ways to “land”.
- An organization’s high value end points are valuable to attackers as a way to either impersonate the user to critical systems, plant malware, or gain a higher level of permission for lateral movement.
- Many times organizations struggle to apply proper whitelisting or remove local admin rights for complex or external high value users such as developers and vendors due to perceived operational risk and perceived impact to the business
- Attackers have many vectors to gain control of the network, so even if they don’t land on the critical users end point, they would be looking to move laterally to that system after mapping the network.
- Removing local admin rights from high value users can be difficult, and companies fail to apply the best practice due to operational risk and perceived impact to the business.

2. Remove Local Admin Rights and Apply Greylisting to High Value User Systems

Benefits:

Apply greylisting to prevent fraudulent process from running as the user to access data or install malicious code can also be an effective control against threats like ransomware which can run as non-privileged users.

The same greylisting is also a precursor to a good whitelisting program by silently collecting approved privileged escalations of the users without any impact to operations or current access.

Removing local admin rights of users is a common best practice and has proven to limit malware infections which many times require the need for local admin rights.

Guarding against credential theft is also a critical benefit, since it's common for high value user to have higher level hashes and ability for the attacker to escalate permissions.

3. Randomize Built-In Admin Passwords

Randomize built-in Admin passwords on top technologies. Common examples are local admin on windows, root on Unix/Linux and SA/SYS and SYSTEM on databases

- Attackers rely on the ability to move laterally in technologies with large footprints such as servers, desktops, and databases.
- Organizations struggle to change passwords frequently. Even if a password is changed to a complex and random password, it's frequently the same on multiple end points.
- Privileged access can be represented, stolen, and misused in many forms including passwords, tokens and keys
- Disabling and renaming accounts is a good best practice, but the accounts almost always still exist and still represent risk.

3. Randomize Built-In Admin Passwords

Benefits:

Unique and complex credentials create boundaries between systems blocks an attacker from stealing one set of credentials and using them in many places.

Backdoor accounts are seldom used on a day-day basis and represent a minimal user and business impact.

Frequent rotation of built-in accounts to a strong randomly generated password is a common part of most audit and compliance requirements.

4. Protect High-Value Service Accounts

Protect high-value service accounts used for automation, discovery and vulnerability management by removing the persistency on the systems and devices. Critical accounts and keys should be consumed dynamically and changed frequently. Common examples are:

Vulnerability Management (Qualys, Rapid7, Tenable, etc.)

Automation (Chef, Puppet, Ansible, Jenkins, Docker, EC2, etc.)

Discovery (ServiceNow Discovery, ForeScout, etc.)

- Sensitive service accounts are not only at risk when unchanged and hard coded, but also when exposed to end users and during the import/update process.
- Due to the elastic nature of dev ops and infrastructure as a service, lateral movement and lack of credentials boundaries are exponentially greater with these very permissioned accounts.
- Many systems run off hours to limit the network impact at the time of scan or discovery, thus making it nearly impossible to manually change and rotate credentials.
- Attackers use these accounts with high levels of access to nearly every system in the environment as an easy gateway for lateral movement and additional credential theft.

4. Protect High-Value Service Accounts

Benefits:

Enterprises can immediately protect high-value accounts that are frequently targeted in penetration tests *and* live attacks by attackers or red teams.

Even though the systems live for a short amount of time, the accounts used in templates and to create the systems are no longer static.

5. Protect Private and Public Cloud Access

Protect new high-impact levels of access to the modern data center such as virtual consoles and keys for public and provide cloud. Sensitive service accounts are not only at risk when unchanged and hard coded, but also when exposed to end users and during the import/update process.

- Most public cloud options such as AWS provide a customer specific set of keys with very high levels of access and no way to rotate or protect them. Stealing these keys provides an attacker the ability to comprise the environment in multiple ways.
- Virtual console access buys an attacker time by allowing copies of systems to be created and compromised offline. This level of access also is the heart of the cloud operations and can easily shut down or disrupt a business from a single pane of glass.

5. Protect Private and Public Cloud Access

Benefits:

Storing, isolating and rotating the credentials used for critical access decouples the privileged access from the individual allowing an organization to have much more control over what people do and when.

Recording these sessions also provides information to complement a big data program and recover from an unintentional or malicious change and downtime. .

Questions?

Troy.Brueckner@CyberArk.com

https://www.linkedin.com/in/TroyBrueckner/

https://www.cyberark.com/