Privilege Access Management

Who is the most privileged user in an enterprise?

a – Security administrator

b – CFO

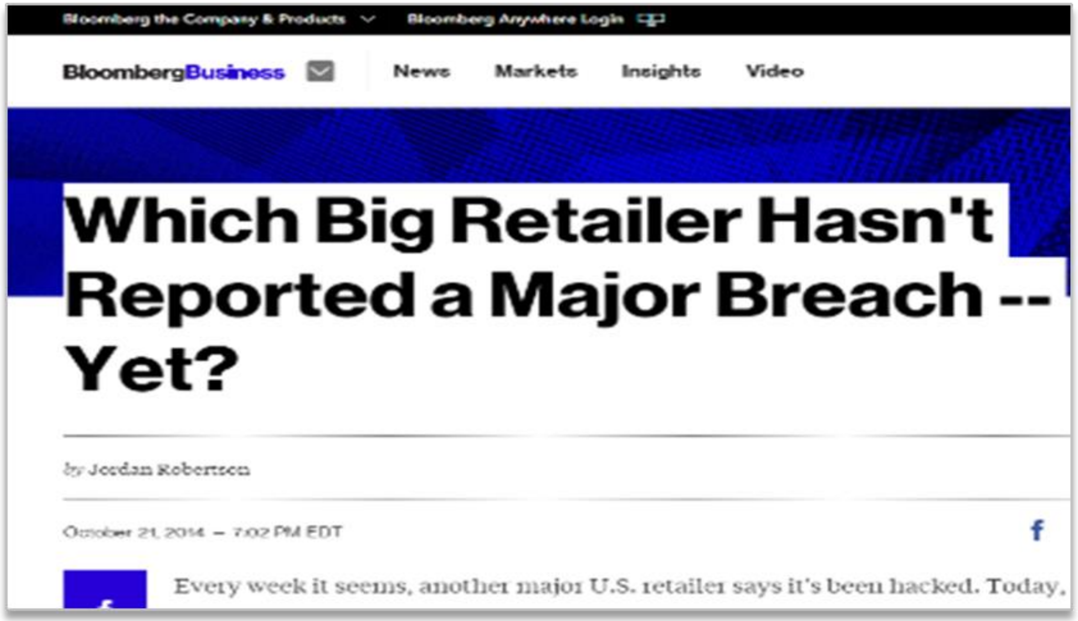
c – The summer intern who is now working for your competitor

Large US Retailer: March 2014 Attack Summary

COMPANY OVERVIEW	
Industry	Retail
Employees	27,000
Headquarters	USA

WHAT HAPPENED?

- Early 2014: 260,000 credit cards stolen from a large US retailer went up for sale
- Early 2015: The same retailer announced a second intrusion to POS systems



Bloomberg the Company & Products   Bloomberg Anywhere Login

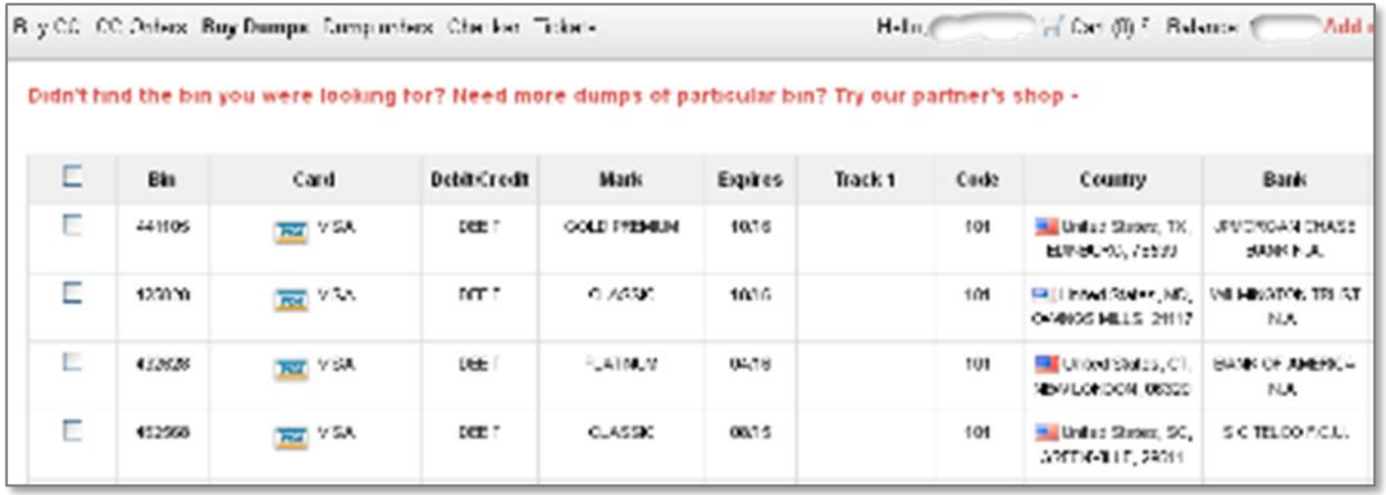
BloombergBusiness   News   Markets   Insights   Video

Which Big Retailer Hasn't Reported a Major Breach -- Yet?

by Jordan Robertson

October 21, 2014 – 7:02 PM EDT

Every week it seems, another major U.S. retailer says it's been hacked. Today,



Buy CC   CC Orders   Buy Dumps   Dumps orders   Checker   Tickets   Hello, [redacted]   Cart (0)   Balance [redacted]   Add

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop -

□	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank
□	441105	VISA	DEBIT	GOLD PREMIUM	10/16		101	United States, TX, [illegible]	JPMORGAN CHASE BANK N.A.
□	[illegible]	VISA	DEBIT	CLASSIC	10/16		101	United States, MD, OWINGS MILLS, 21117	WILMINGTON TRUST N.A.
□	432628	VISA	DEBIT	PLATINUM	04/18		101	United States, CT, NEW LONDON, 06320	BANK OF AMERICA N.A.
□	[illegible]	VISA	DEBIT	CLASSIC	08/15		101	United States, SC, [illegible]	S C TELCO F.C.U.

Information from public domain

Requirements for Privileged Accounts Management Solution

- Exceptionally secure solution for the keys of the kingdom

- Supreme performance, availability and disaster recovery due to its mission-critical nature

- Flexible distributed architecture to fit the enterprise complex network topology

- Single standard solution for a multi-facet problem

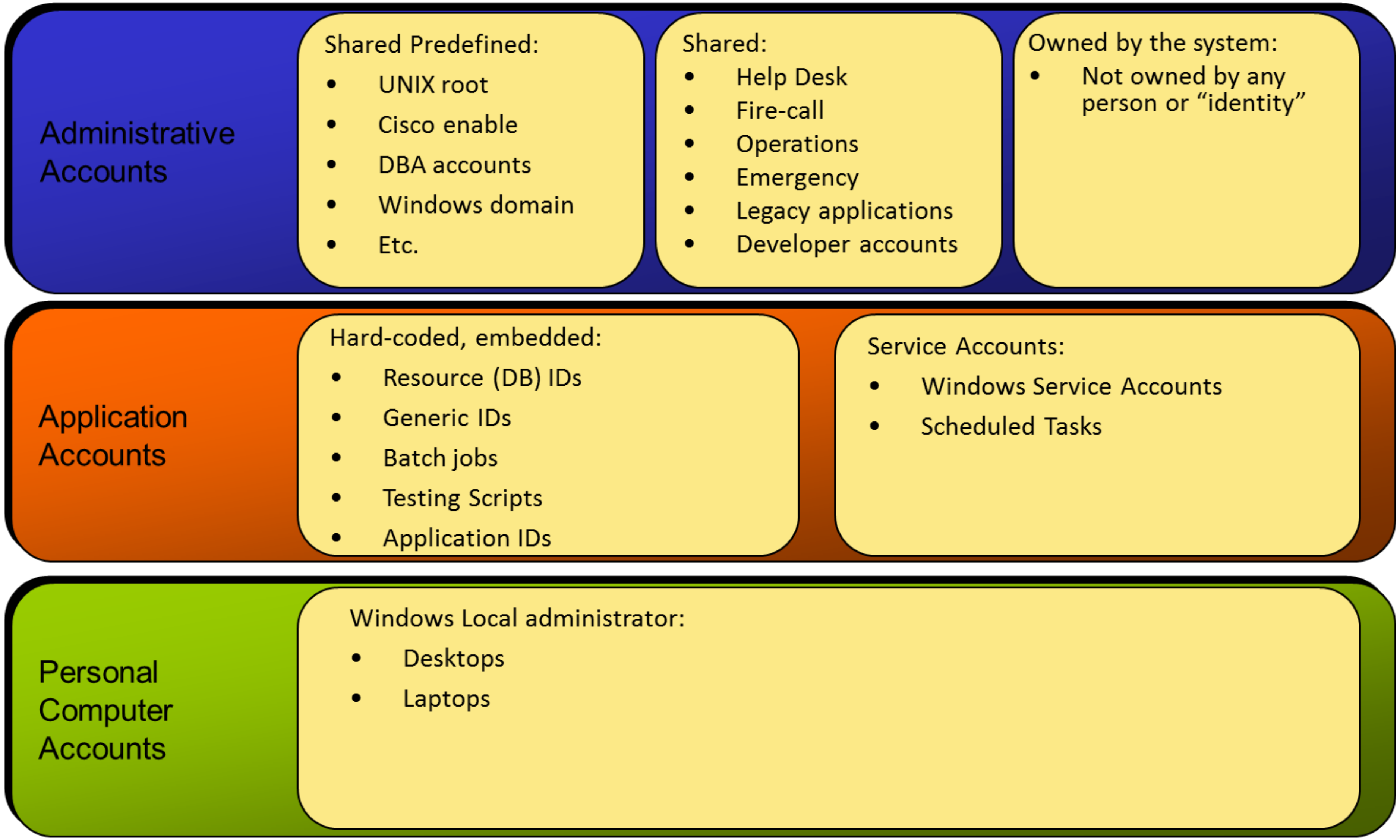
- Intuitive and robust interfaces

Who are Privileged Access Users

Users who have access to do the following activities are considered to have privileged access:

- Provision users
- Reboot servers
- System level administration access
- System administrator level access within an application security module that allows individuals to override the controls of the application
- IDs provided as part of third party software solutions used to complete installation of the software.
- IDs that are used to run applications.
- Administrators with the ability to grant access or elevate privileges on an in scope device

What are Privileged Accounts



Administrative Accounts

Shared Predefined:

- UNIX root
- Cisco enable
- DBA accounts
- Windows domain
- Etc.

Shared:

- Help Desk
- Fire-call
- Operations
- Emergency
- Legacy applications
- Developer accounts

Owned by the system:

- Not owned by any person or “identity”

Application Accounts

Hard-coded, embedded:

- Resource (DB) IDs
- Generic IDs
- Batch jobs
- Testing Scripts
- Application IDs

Service Accounts:

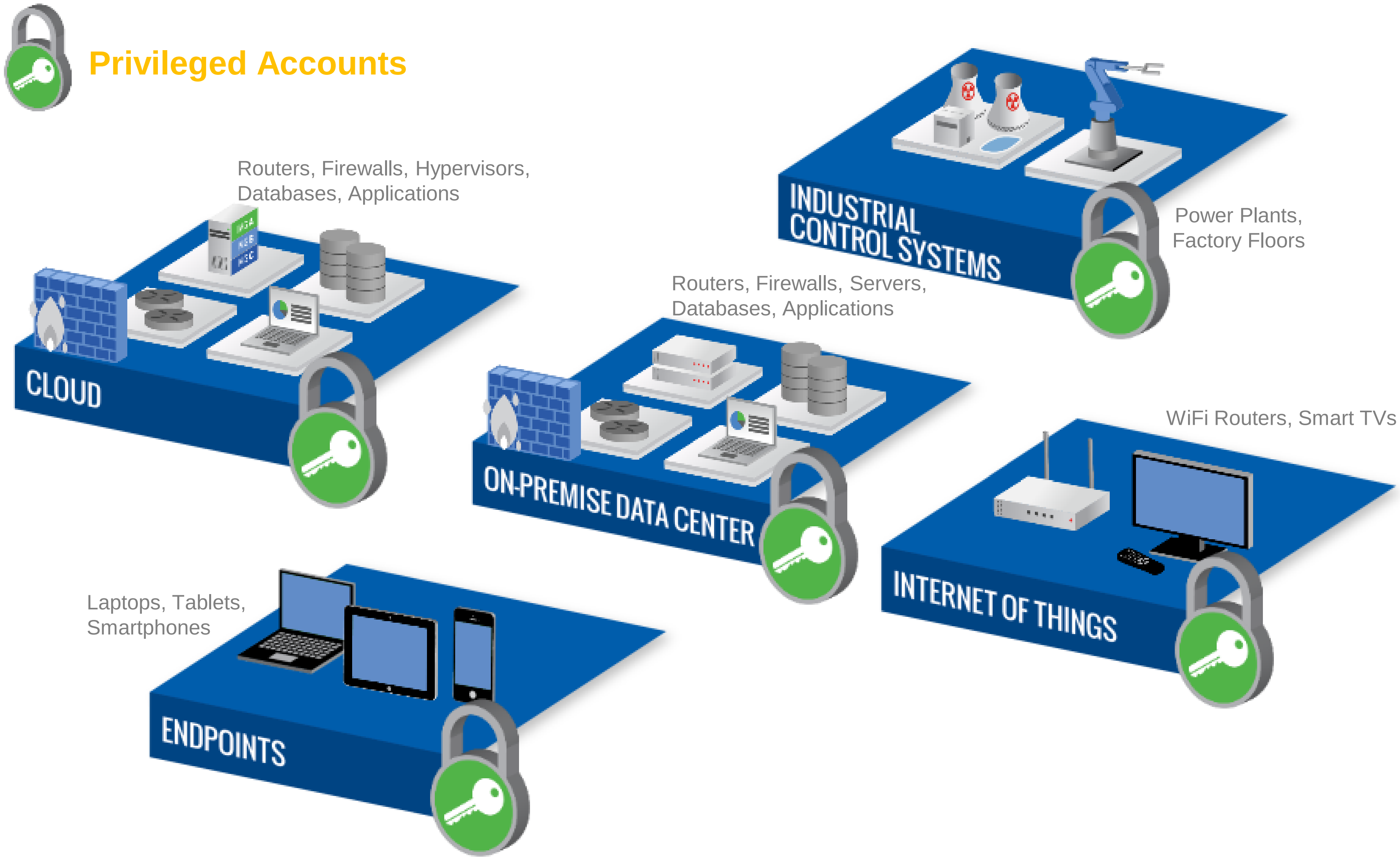
- Windows Service Accounts
- Scheduled Tasks

Personal Computer Accounts

Windows Local administrator:

- Desktops
- Laptops

Privileged Credentials are Everywhere



Privileged Accounts

Routers, Firewalls, Hypervisors, Databases, Applications

Power Plants, Factory Floors

Routers, Firewalls, Servers, Databases, Applications

WiFi Routers, Smart TVs

Laptops, Tablets, Smartphones

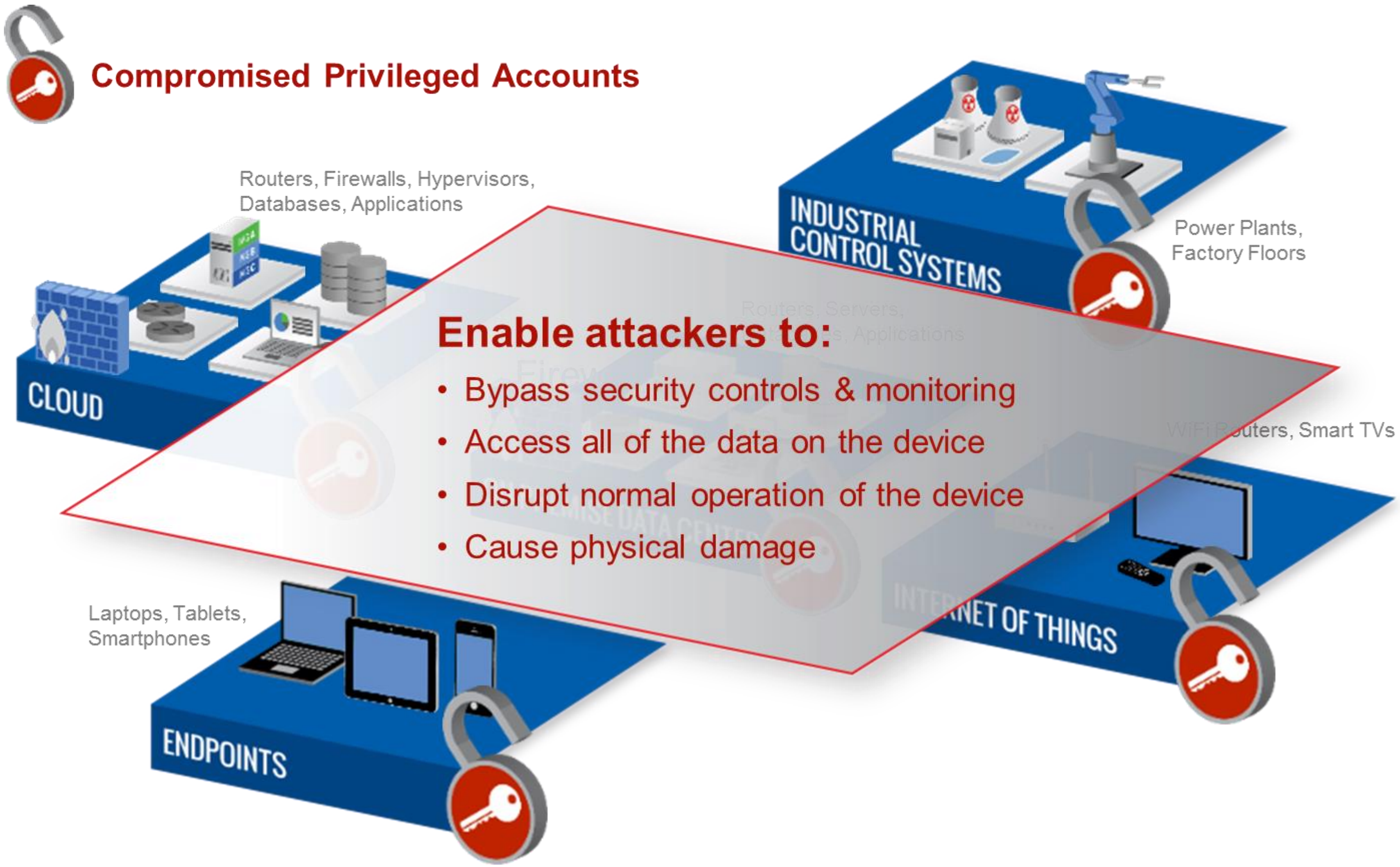
Privileged Accounts - Standards

- Common practices:
  - **Storage:** Excel spreadsheets, physical safes, sticky notes, locked drawers, memorizing, hard coded in applications and services
  - **Resets:** Handled by a designated IT members, call centers, mostly manual
  - **Known to:** IT staff, network operations, help desk, desktop support, developers
- Common problems:
  - Widely known, no accountability
  - Unchanged passwords
  - Lost passwords
  - Same password across multiple systems
  - Simplistic passwords – easy to remember
  - Passwords not available when needed

The Problem: Users with admin rights can…

- Install kernel-mode root kits
- Install system-level level key loggers
- Install Malicious ActiveX controls, including IE and Explorer extensions
- Install spyware and adware
- Install malware; “Pass-the-Hash” exploits
- Install and start services
- Stop existing services (such as the firewall)
- Access data belonging to other users
- Cause code to run whenever anybody else logs on to that system
- Replace OS and other program files with Trojan horses
- Disable/uninstall anti-virus
- Create and modify user accounts
- Reset local passwords
- Render the machine unbootable
- And more…

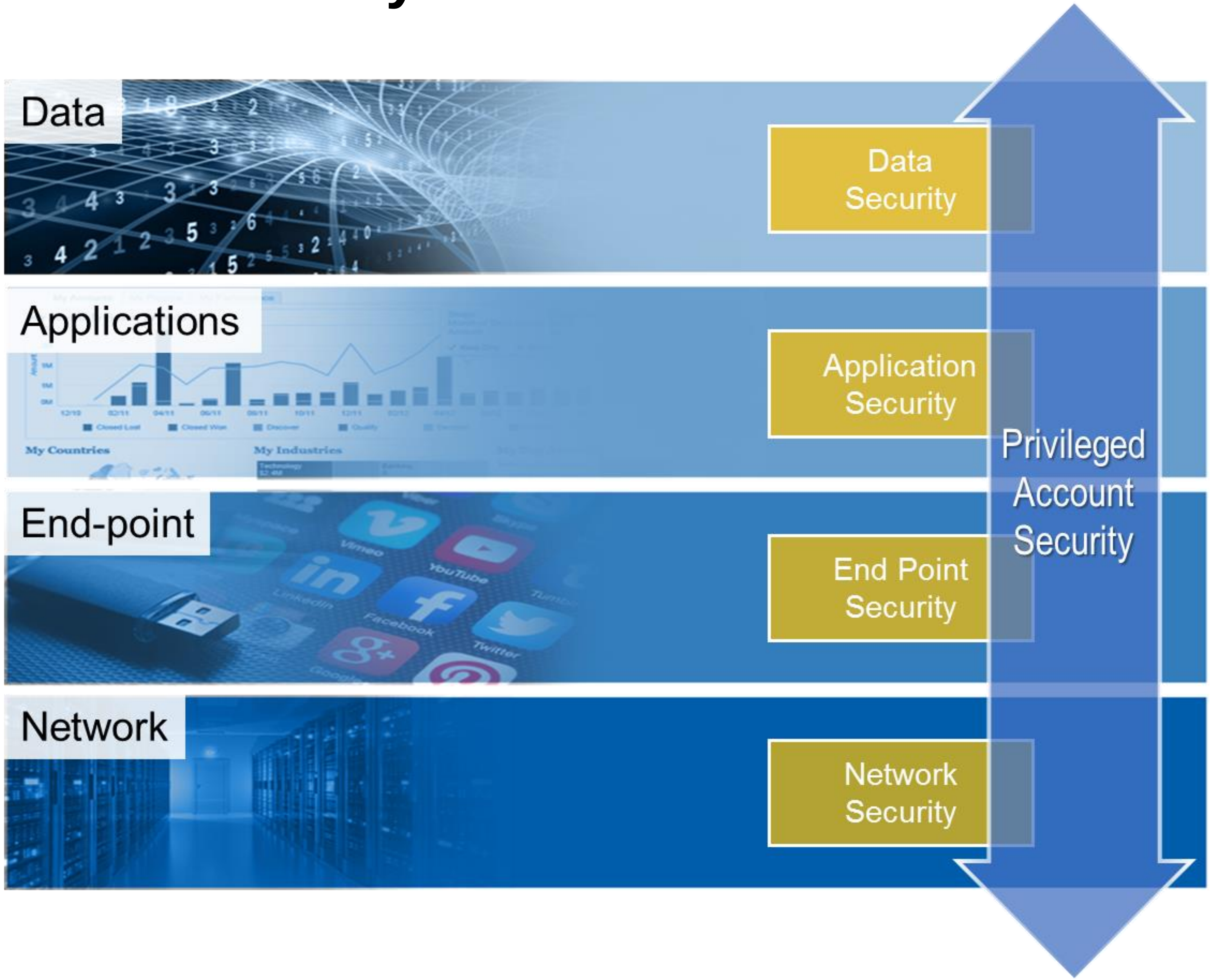
Hijacked Credentials Put the Attacker in Control


Compromised Privileged Accounts
Routers, Firewalls, Hypervisors, Databases, Applications
CLOUD
INDUSTRIAL CONTROL SYSTEMS
Power Plants, Factory Floors
Routers, Servers, ...s, Applications
WiFi Routers, Smart TVs
INTERNET OF THINGS
Laptops, Tablets, Smartphones
ENDPOINTS

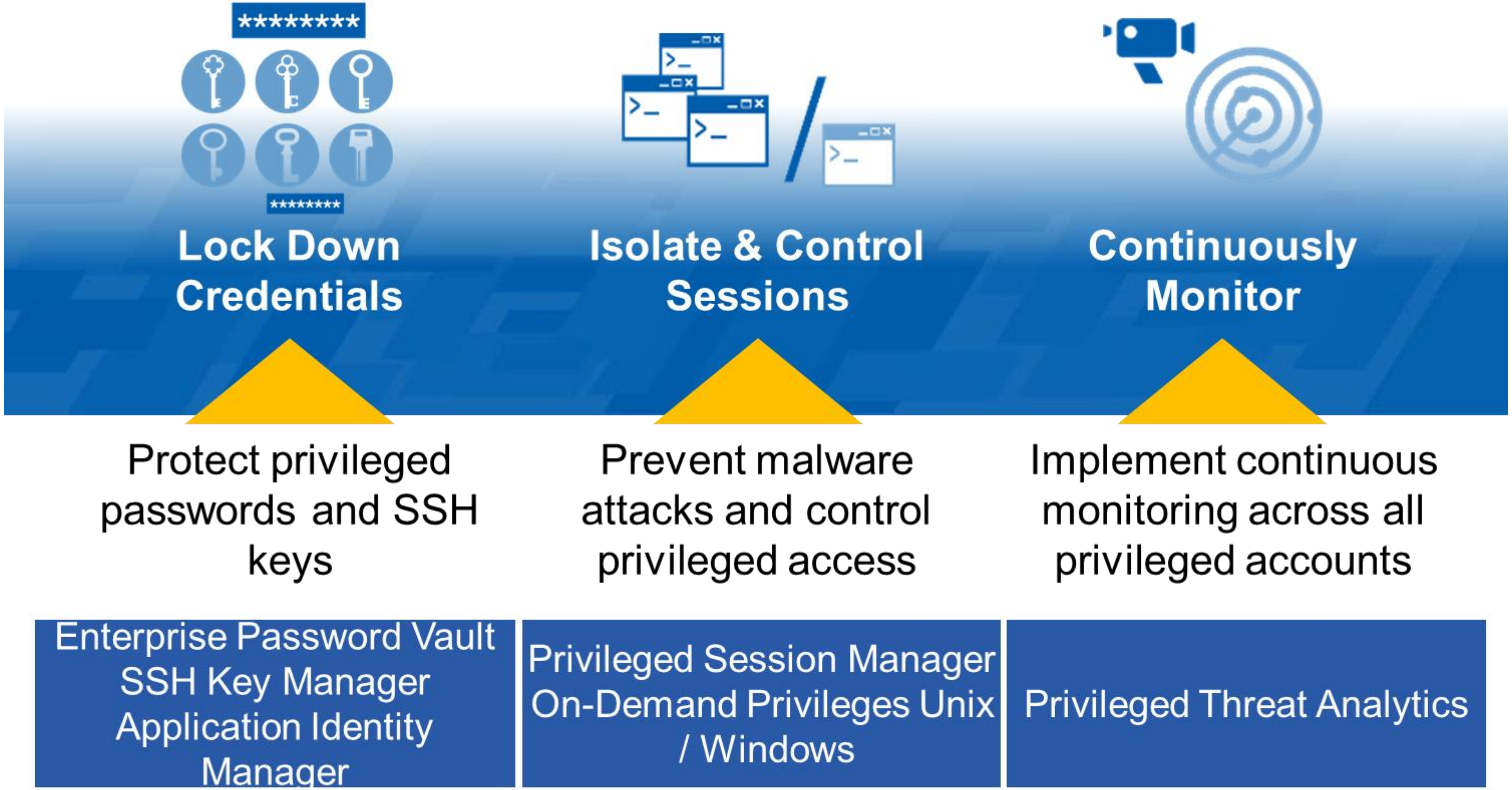
Enable attackers to:

- Bypass security controls & monitoring
- Access all of the data on the device
- Disrupt normal operation of the device
- Cause physical damage

Privilege Account Security Across the Stack



Comprehensive Controls on Privileged Activity



Lock Down Credentials

Protect privileged passwords and SSH keys

Enterprise Password Vault
SSH Key Manager
Application Identity Manager

Isolate & Control Sessions

Prevent malware attacks and control privileged access

Privileged Session Manager
On-Demand Privileges Unix / Windows

Continuously Monitor

Implement continuous monitoring across all privileged accounts

Privileged Threat Analytics

Thank You