MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

MAKING LIFE EASIER FOR IT:

CREDENTIAL MANAGEMENT ON CONNECTED AND DISCONNECTED SYSTEMS

Richard A. Weeks

Vice President of Channels and Alliances / Bomgar

@ricweeks / @bomgar

AGENDA

Today’s Cybersecurity Landscape

Identity Management Challenges – Think Differently

The Unique Challenge of Offline Security Management

2017 – RECORD BREAKING YEAR FOR DATA BREACHES

- 2017 set record for **most data breaches and most data compromised** in a single year (according to Risk Based Security)
- **5,207 total breaches** recorded, with more than **7.8 billion records exposed**
- Despite **$90 billion spent on information security** in 2017 (according to Gartner)

CURRENT CYBERSECURITY LANDSCAPE

Headwinds: Culture of Availability & Convenience

Technology architecture:

- IT Systems designed for ***convenience*** of IT and users
- ***No*** "***stop loss***" in most designs (Uber, Equifax, others)
- Limited control over allowing access to ***everything,*** any time, from anywhere

People and processes:

- **No Prioritization of Resiliency or Loss Minimization**
- Little to ***no formal security oversight*** of operations and processes
- No ***regular*** security health checks (drift, intrusions, open doors)

RESULT: IT PROBLEMS AND ISSUES

- Good security configurations drift off target
- Bad designs never get cleaned up after deployments
- Existing practices/processes generate unintended consequences of excessive capabilities
- Little thought to limiting lateral motion in compromises
- Machines rarely get rebooted and credentials live in memory forever

TIMELINE OF AN ATTACK

Start of Attack

Hackers Target Employees with Phishing Email

20 Minutes Later

Hackers Login to Employee Webmail Using Stolen Credentials

30 Minutes Later

Hackers Send Second Round of Phishing Email from Internal Addresses

4 Hours Later

Hackers Get Privileged IDs Needed to Access All Private Data

4.5 Hours Later

Hackers Finish Extracting Payment Card and Other Private Data

Attackers are targeting your privileged credentials to get the access they need

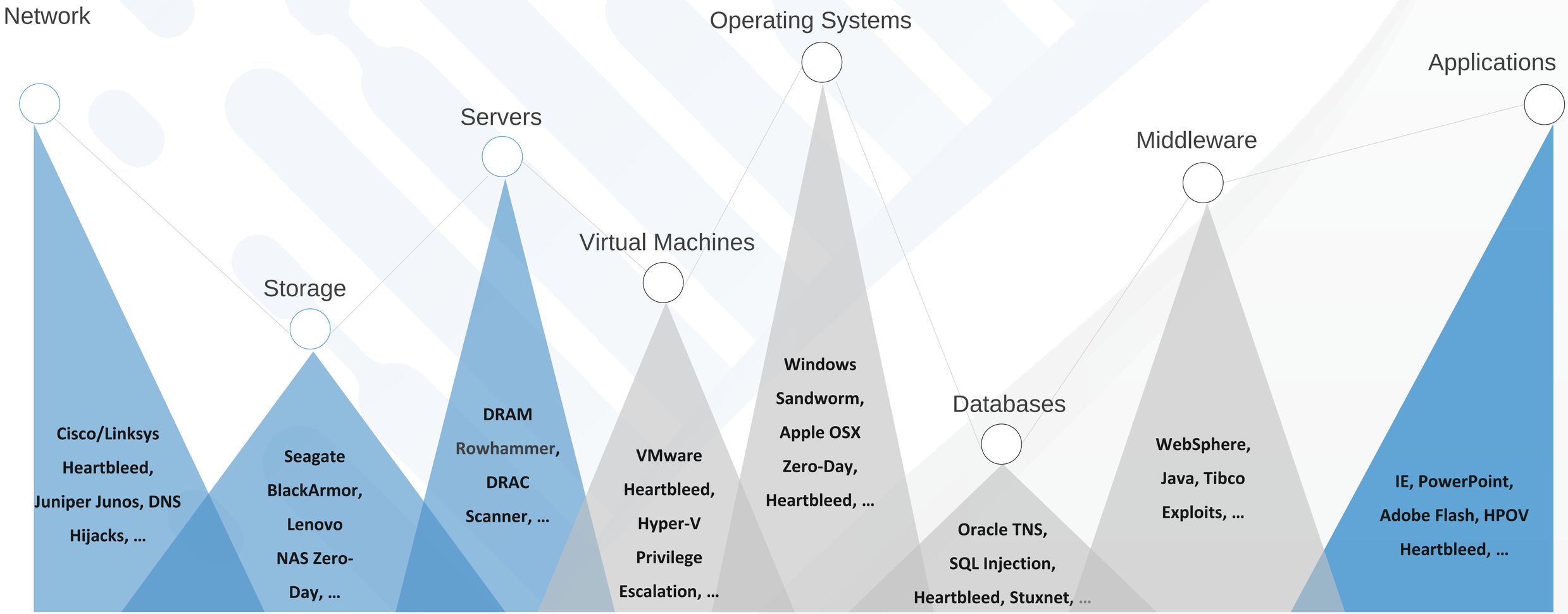
INTRUSION SUCCESS RATES

- Nearly 100% Success Rates with:
  - Pass-the-hash, Golden Ticket, Clear Text Passwords
- WCE
  - http://www.ampliasecurity.com/research/wcefaq.html
- Mimikatz
  - https://github.com/gentilkiwi/mimikatz

…and these are just the FREE tools

Identity Management Challenges

CREDENTIALS THROUGHOUT THE STACK



CREDENTIAL MANAGEMENT COMPLEXITY

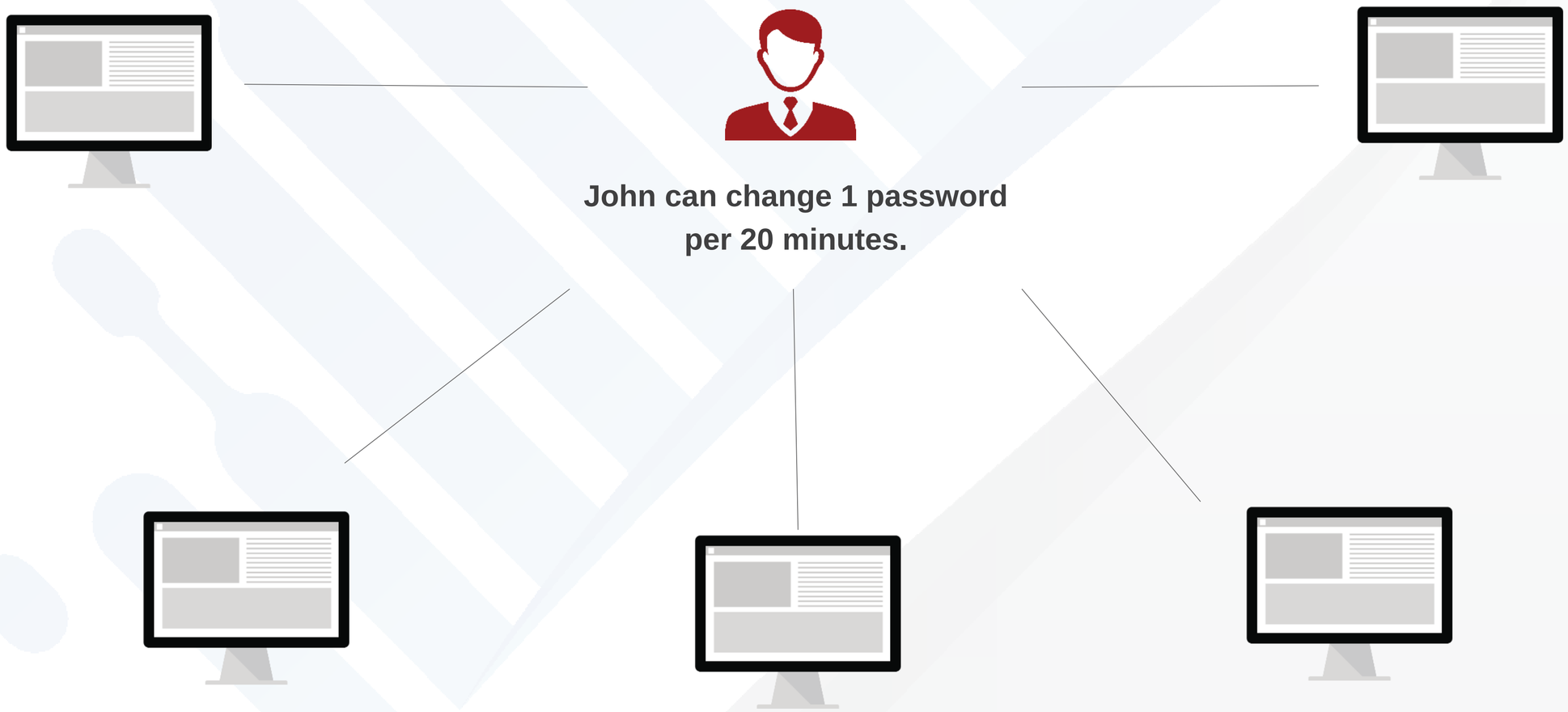
Local Admins
Domain Admins
Windows Service Accounts
Windows Scheduler Task RunAs Identities
Windows Scheduler At Service Accounts
COM+ Application Identities
DCOM Object RunAs Identities
IIS6 Metabase Account Info
IIS7 Account Info
SCOM RunAs Accounts

- Accounts in .NET Config
- Credentials in SQL Server
- String Replacements
- SharePoint
- Logon Cache
- Auto Logon Account
- Local Cache JAVA Client
- SQL Reporting Services
- IBM, Oracle, SAP, others…

… and this is only <u>Windows</u>

MANUAL PASSWORD MANAGEMENT USELESS

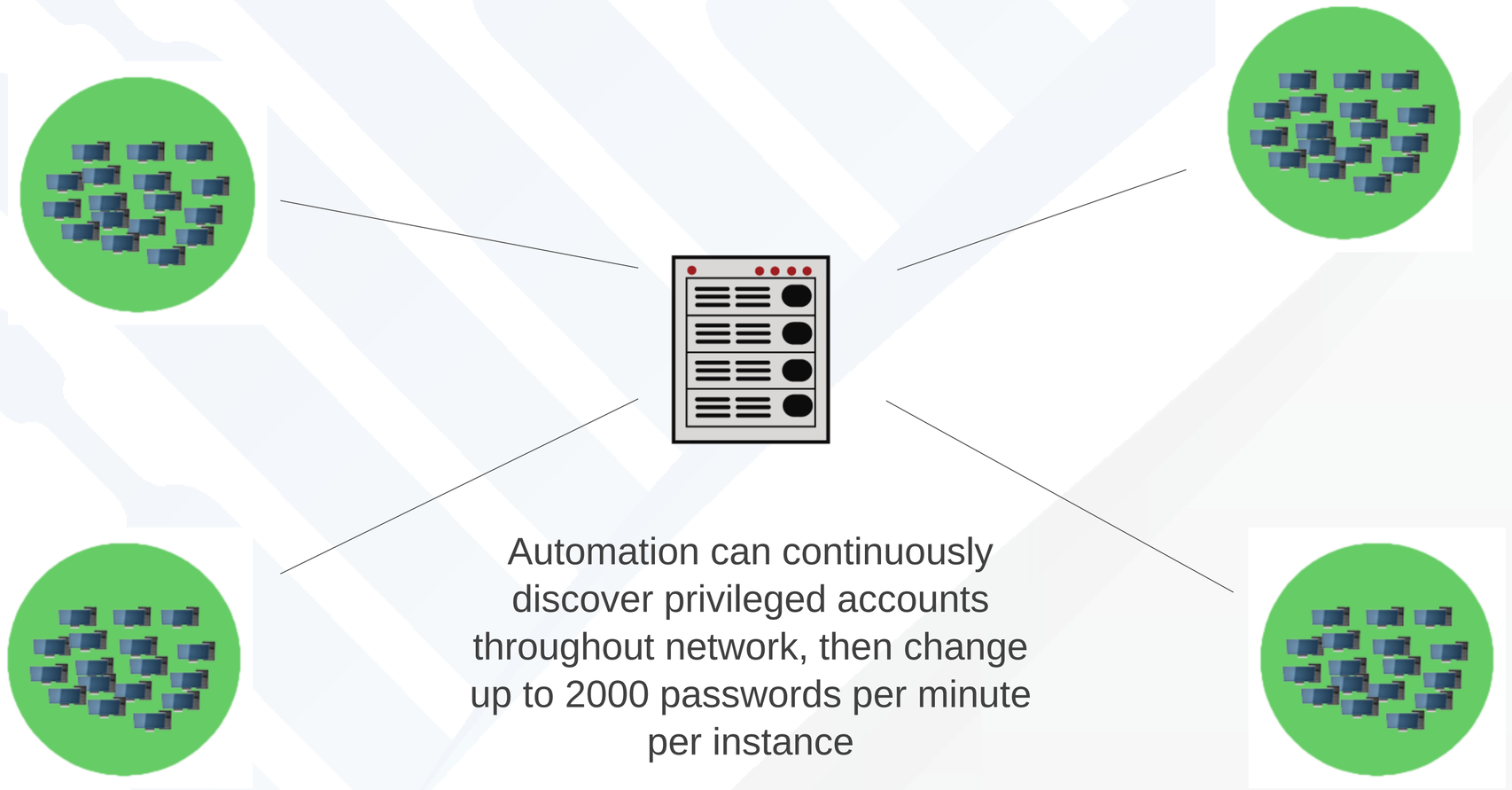
Change Passwords Manually



John can change 1 password per 20 minutes.

AUTOMATED CREDENTIAL MANAGEMENT

Change Passwords/SSH Keys Programmatically



Automation can continuously discover privileged accounts throughout network, then change up to 2000 passwords per minute per instance

RETHINK CREDENTIAL AGES

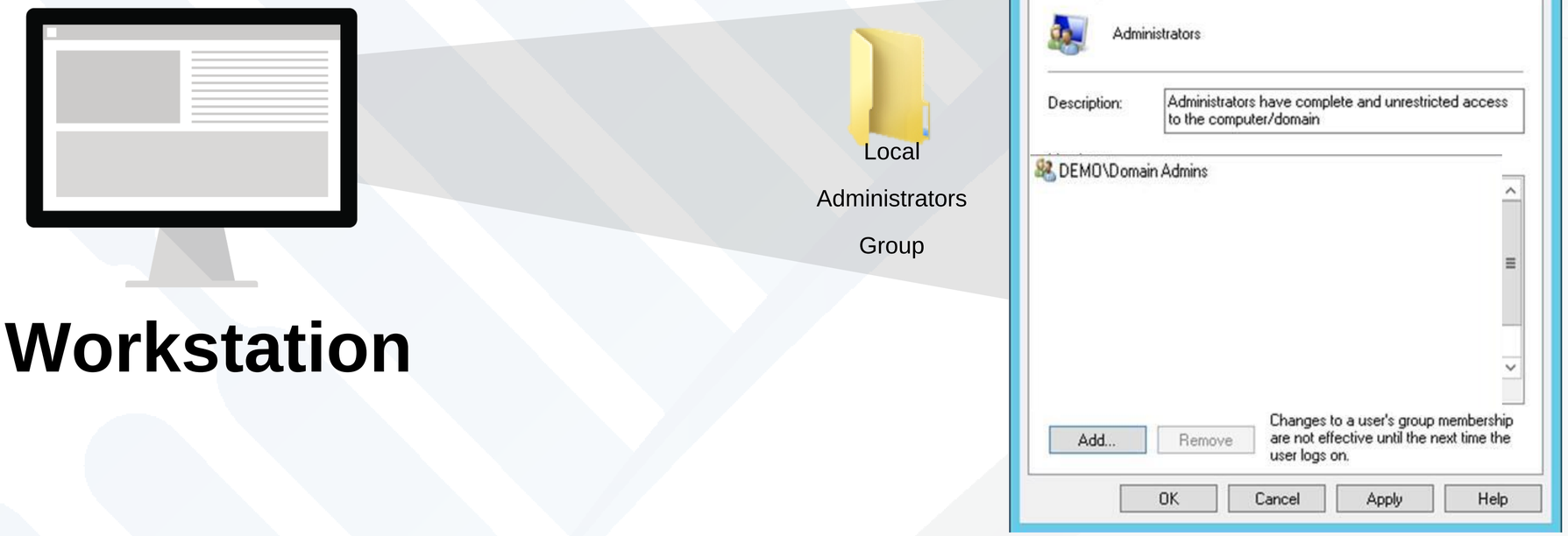
- Change privileged credentials **every 2-24 hours**
- Implement continuous auto discovery + remediation in closed loop
- Stop lateral motion via common credentials (same password on each system--randomize instead)
- Forcibly expire all Kerberos tickets via double password changes on ticket granter service at 24 hours or less

RETHINK LOCAL ADMINS

- Existing users are local admins on their machines
- Allows extraction of password hashes by attackers
- Use time limited local account escalation (Just in Time Admin) – temporarily change local group memberships

PURGE LOCAL ADMINISTRATORS MEMBERSHIPS

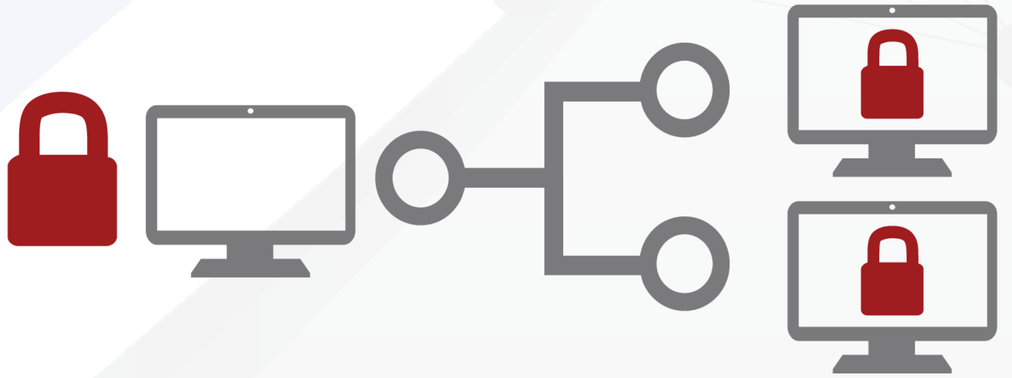
Remove Members of the Local Administrators Group



Workstation

RETHINK DOMAIN ADMINS

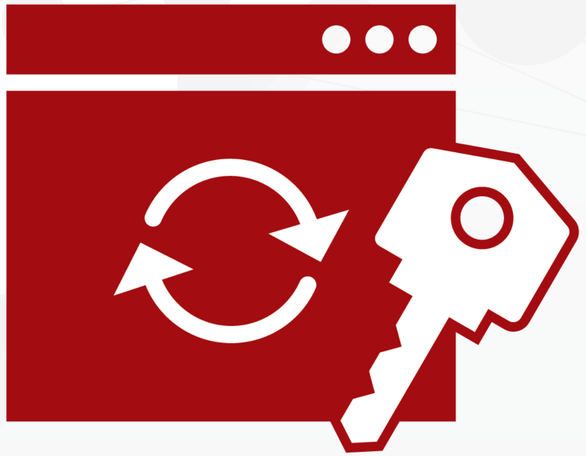
- Every time a domain admin account connects to a machine, credentials can be extracted and used by attacker
- Escalate user-level domain accounts locally or…
- Use short lifetime one-time use administrator accounts



A NEW LEVEL OF CONTROL & AUTOMATION

Limit Credential Lifetimes and **Control Credential Disclosure**

- Measure key and password lifetimes in minutes
- Automate fully: No human configuration or management
- Change 1000’s of keys and passwords/minute with modern non-vault solutions
- Assume continuous breach and act accordingly
- Mitigate losses



Must be managed on all systems on the network – connected, as well as disconnected, systems

Disconnected Systems Pose Unique Challenges

THE DISCONNECTED REALITY

Systems may never be in contact with corporate IT management systems once deployed.

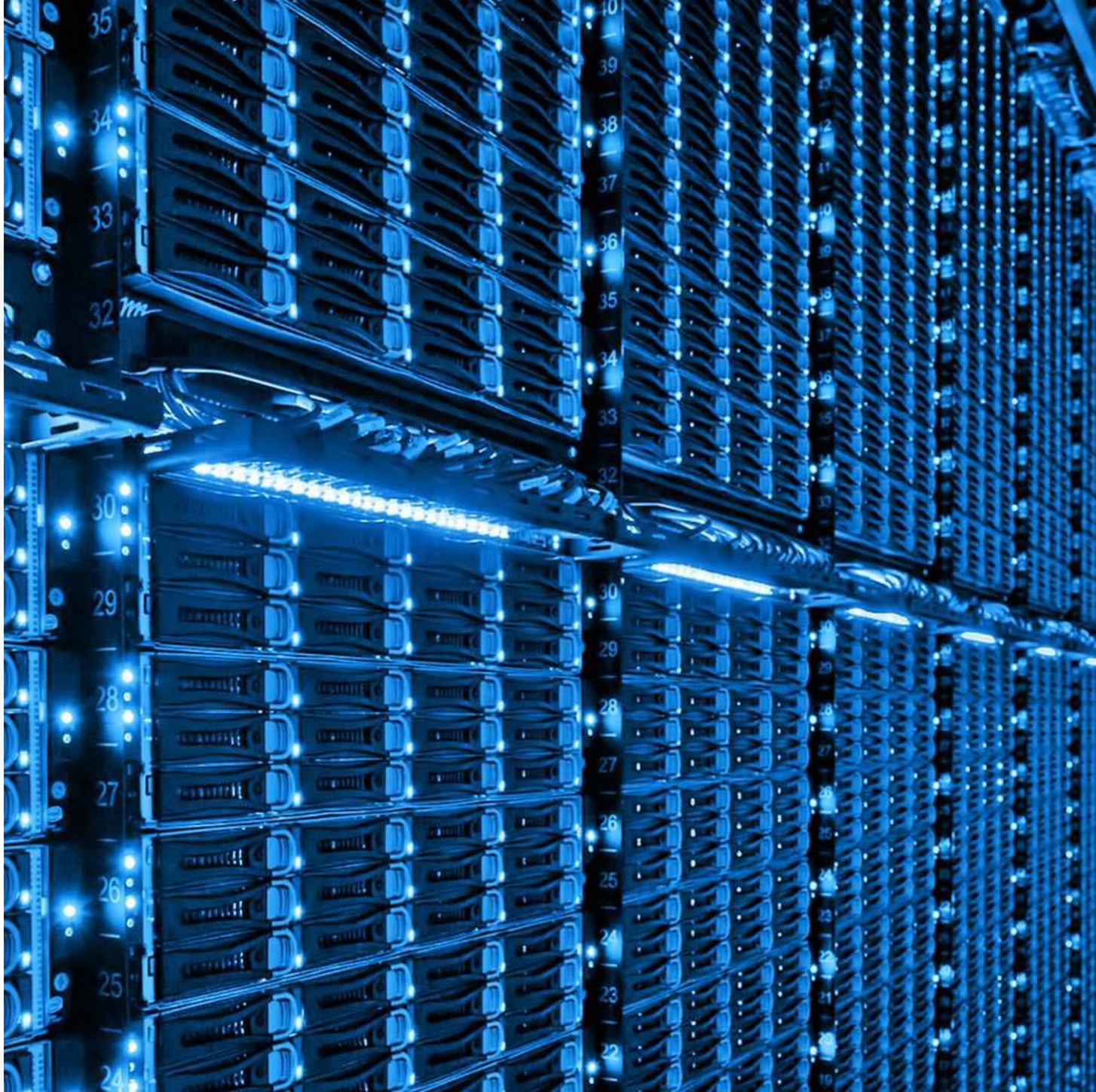
In today’s mobile-first and cloud-first world, most organizations operate with many disconnected systems.

HOW CAN YOU MANAGE WHAT YOU CANNOT CONNECT TO?

- Field workers
- “Cloud-first” users
- Air-gapped networks
- Software Defined Networks

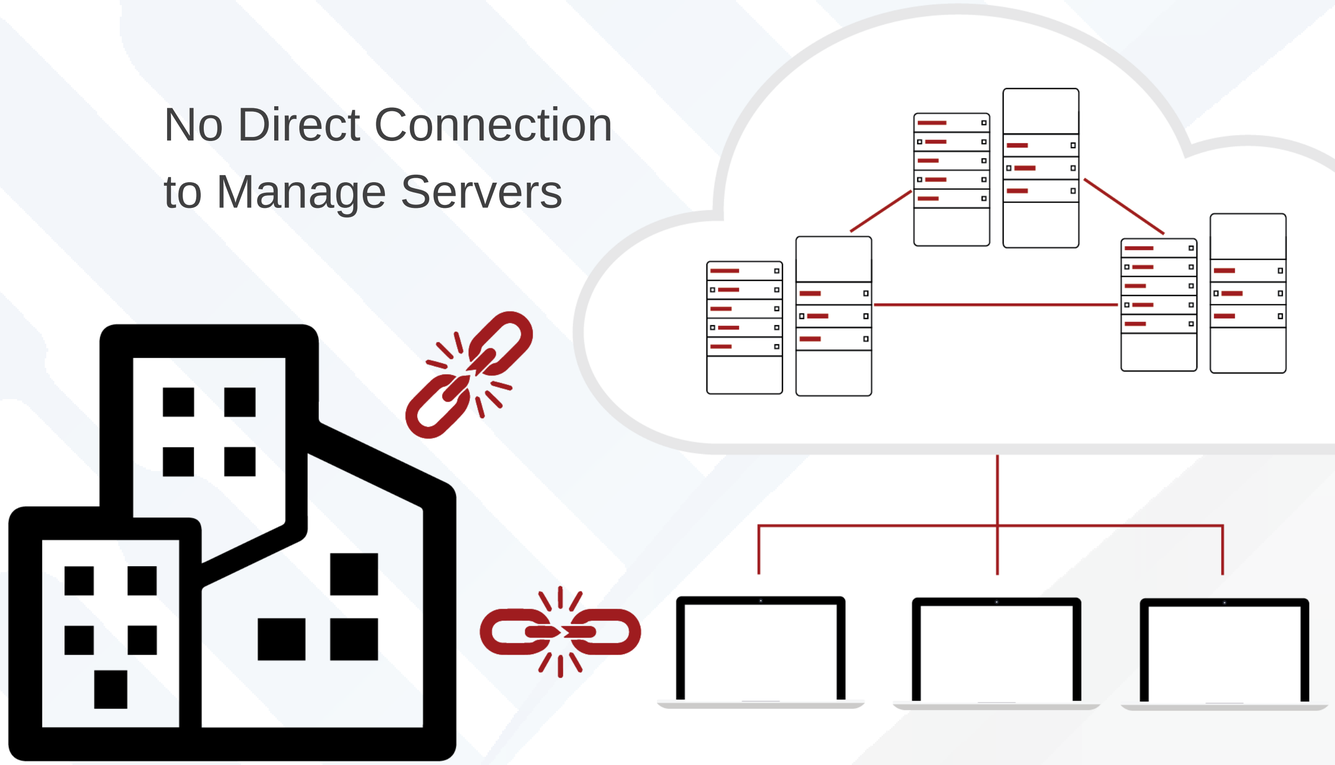
Even when disconnected, systems still need automatic and regular changes to credentials.

TODAY’S REALITY: SERVERS, WORKSTATIONS, DMZS, AIR GAPPED NETWORKS



TODAY'S REALITY: CORPORATE ASSETS ARE NOT ALWAYS CONNECTED

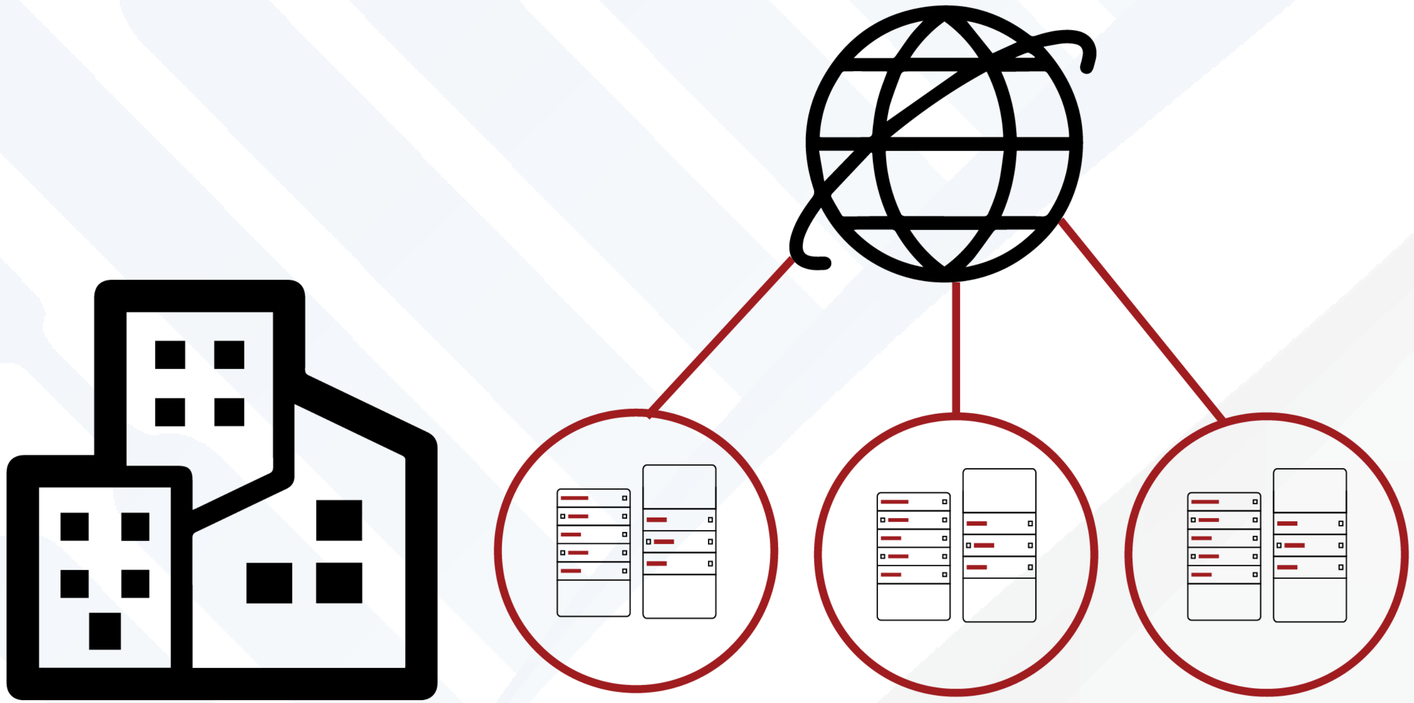
No Direct Connection
to Manage Servers



Corporate HQ

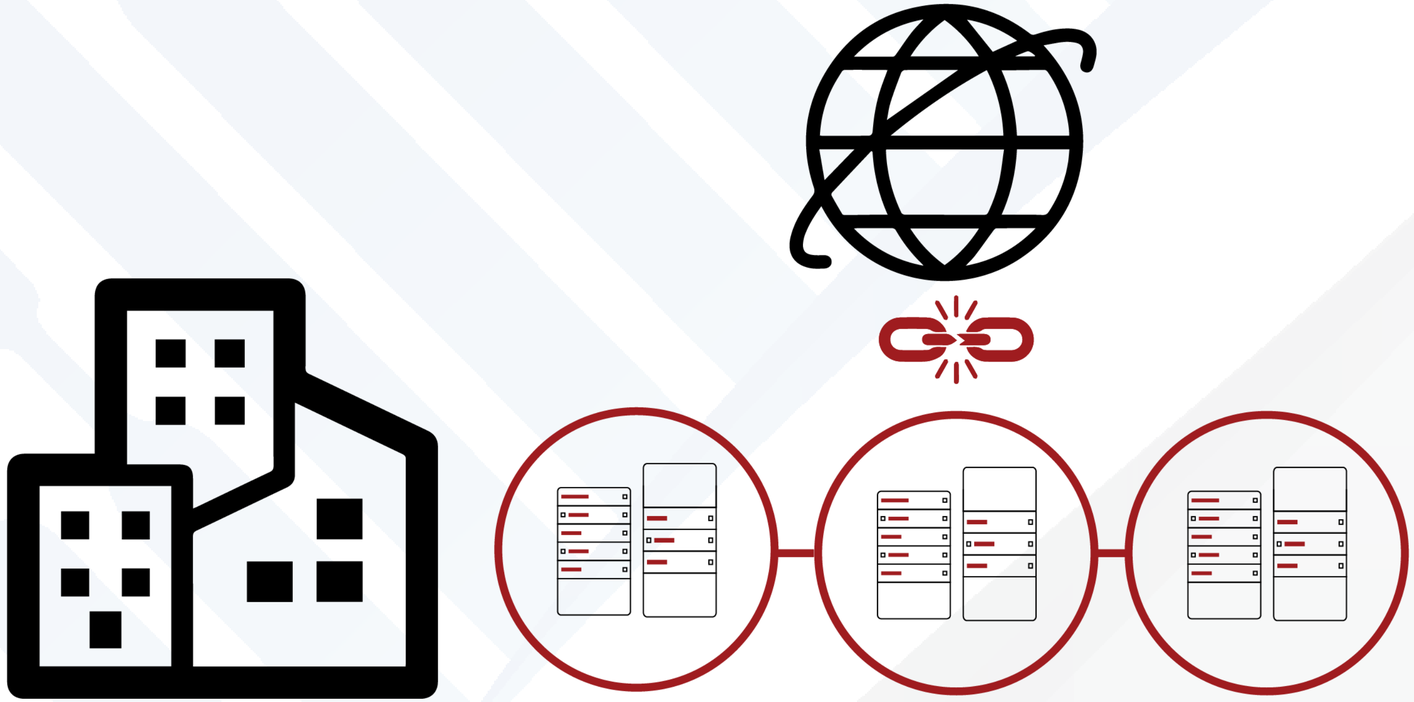
No Connection to Laptops

TODAY'S REALITY: BUSINESS UNIT ASSETS ARE NOT AVAILABLE TO IT FOR MANAGEMENT



Corporate HQ

TODAY'S REALITY: AIR-GAPPED NETWORKS NEED TO BE SECURED FROM INSIDER THREATS



Corporate HQ

ONLINE VS OFFLINE SYSTEMS

Online: Managed directly from a central management system.
Disconnected machines marked for auto-retry.

Offline: Rarely if ever connect to corporate management systems.

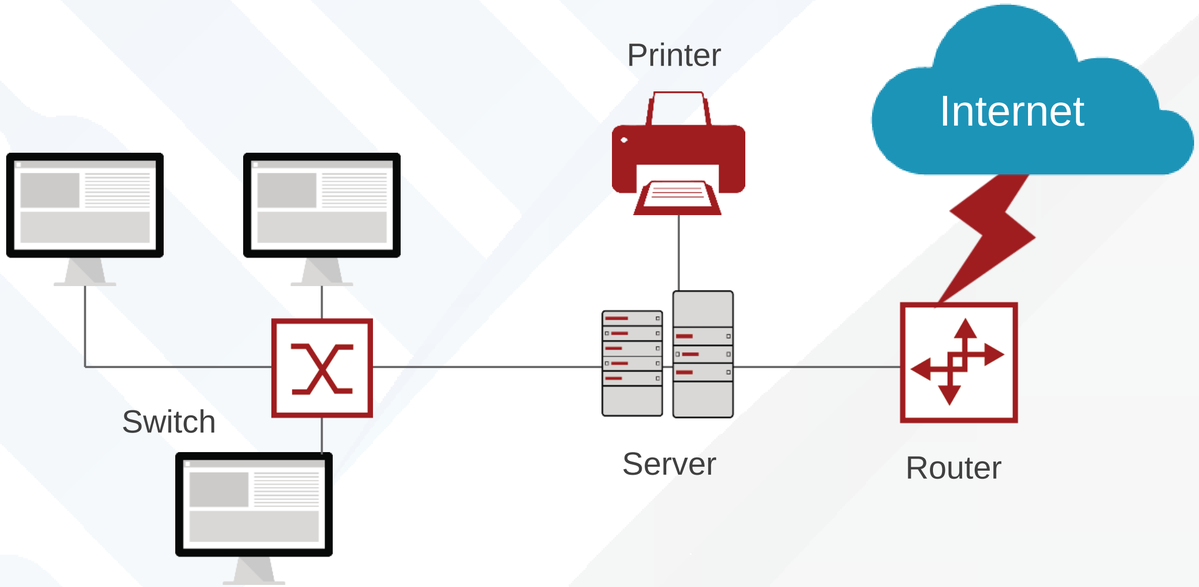
Both:

- Need to be secured with controlled and audited access
- May contain high value information
- Can cause serious consequences from compromise

ONLINE IDENTITY MANAGEMENT

Legacy On-Premises

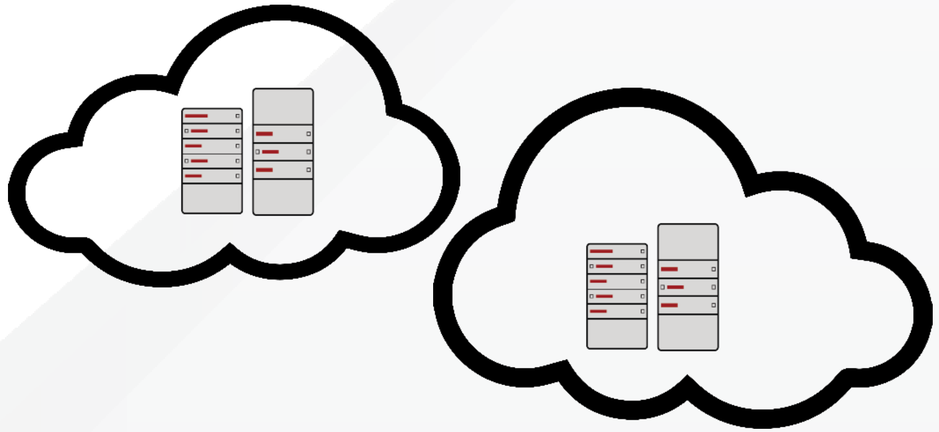
- Everything connected all the time and manageable from central core at any time
- Agents installed on systems lacking management surface
- Retry offline systems
- Built before cloud, mobile users, laptops, enclaves, and sophisticated attacks



OFFLINE IDENTITY MANAGEMENT

Cloud, Mobile Workers, Enclaves

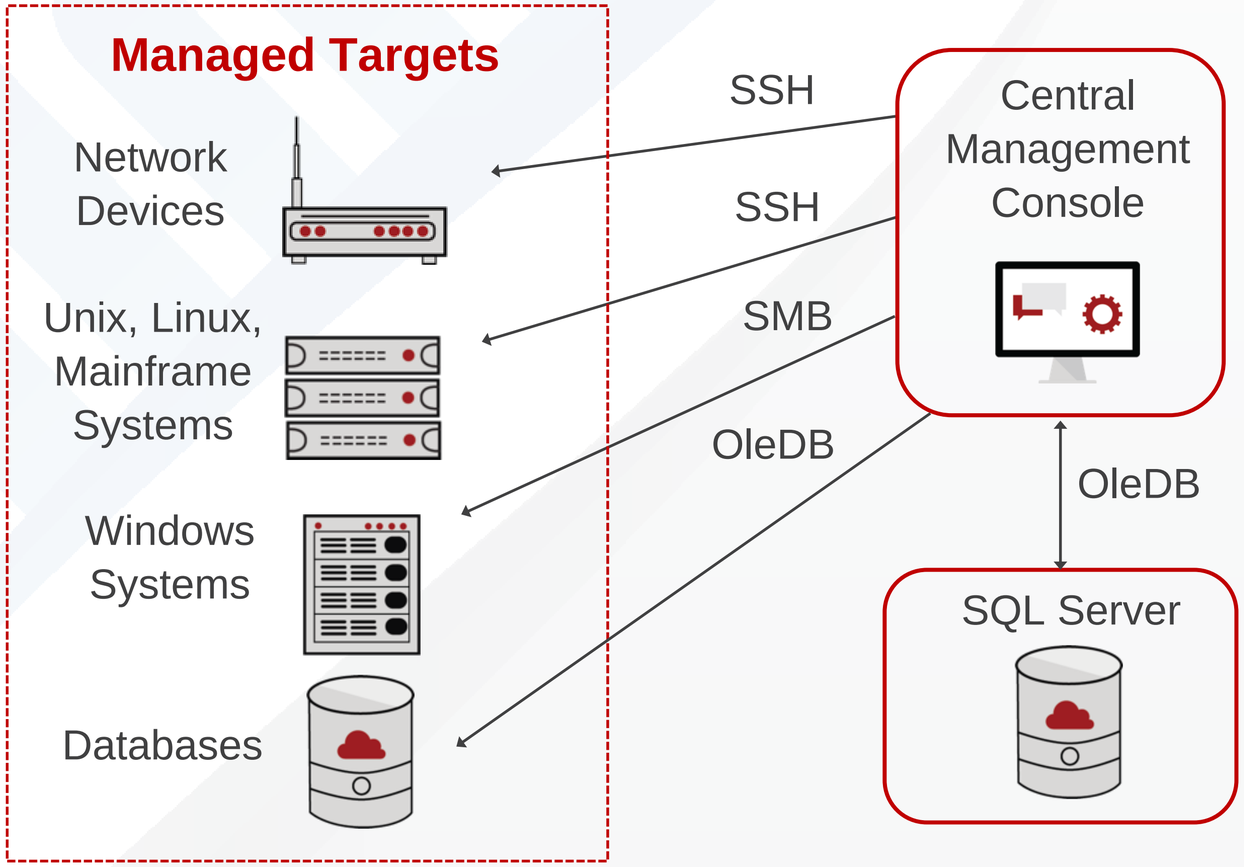
- Systems may be temporarily or permanently disconnected from corporate network
- May be no connectivity from DMZs and enclaves to corporate network
- Mobile worker with laptops need identity management but without agents



PUSH/PULL MODELS

ONLINE SYSTEMS: CENTRAL DISCOVERY & PUSH MODEL

- Find, connect, and manage remote systems from a central or distributed core
- Always on, always connected
- Retry for offline systems
- Assumptions of security, identity, and existing surface area



OFFLINE SYSTEMS: DISTRIBUTED PULL MODEL

- Applications installed on remote systems perform autonomous activity
- Try to connect to an Internet connected gateway to pull new settings
- Use shared secrets or independently verifiable challenges to obtain local elevation
- No assumption of connectivity, identity, or permissions

Shopfloor Automation

Working from Home

AGENTS VS. APPLICATIONS

AGENTS VS. APPLICATIONS

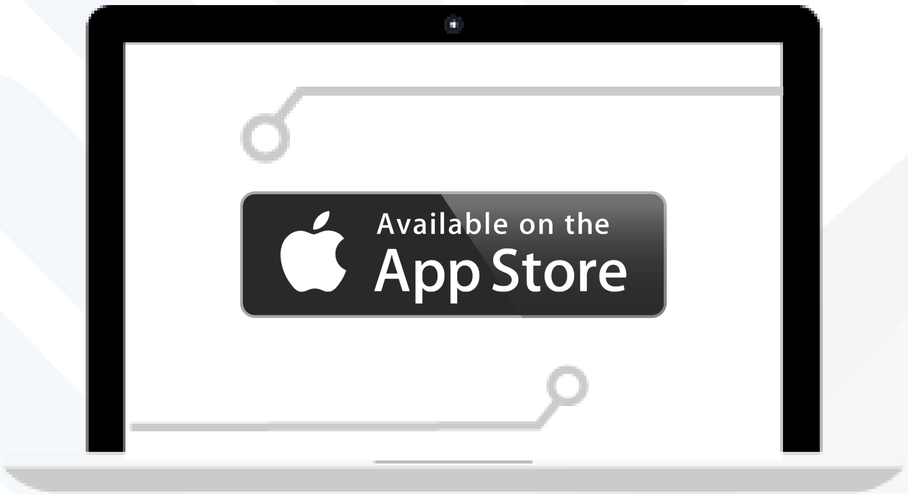
CONNECTED ENVIRONMENTS HAVE “DIRECT CONNECTIONS”

- Agents are generally not required for connected corporate environments
- Agents can be installed on machines or networks to proxy connections to core
- Agents can create a surface area on a machine where native RPCs don’t exist

AGENTS VS. APPLICATIONS

DISCONNECTED SYSTEMS USE “MANAGEMENT APPLICATIONS”

- Operate autonomously (secure machine environment)
- Reach out over Internet in trusted/untrusted manner to get updates
- Cryptography and open standard communications used (REST/JSON)



THE MICROSOFT LAPS OPTION

Many organizations still rely on Microsoft LAPS, which is a good solution in some situations. However, LAPS:

- Is Windows-only and works for systems that are connected to AD
- Uses a random number generator to create a local password that is stored in clear text
- Password updates occur on remote machines only if they are domain connected
- There is no management interface

THE FUTURE

- We started in a Microsoft Windows world with Linux and UNIX as part of the connected environment
- Today's world is open-source, no central core, and operating in a hostile environment without customers paying for infrastructure or software licenses
- Hybrid on-premises, cloud-based SAAS, managed security services (MSS) is the future of security management

SUMMARY

- Minimize damage caused by intrusions
- Assume automated attacks and mitigate continuously
- Don’t allow insecure machines with weak credentials and unmanaged accounts on the network
- Require changes in domains, admin account usage, credential lifetimes
- Secure offline systems to ensure protection of entire network

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Richard A. Weeks

Vice President of Channels and Alliances / Bomgar

@ricweeks / @bomgar