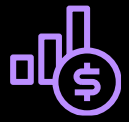
Privileged accounts: The weakest link in the ransomware attack chain?

Patrick Ancipink
Product Marketing Mgr, IBM Security Verify
patrick.ancipink@ibm.com

Dinesh Jain
Product Manager, IBM Security Verify
dineshjain@in.ibm.com

Brian Carmen
Senior Sales Engineer, Delinea
brian.carmen@delinea.com

Cyberattacks are the top cause of business disruption, with ransomware leading the way



$1.59M

portion of data breach costs attributable to lost business, including business disruption, system downtime, lost customers and reputation losses.[1]

21%

of all security attacks in 2021 were the result of ransomware, continues to be top attack type.[2]

20%

Share of breaches initially caused by compromised credentials, the most common initial attack vector.[1]

Ransomware is an organized cybercrime activity that is on the rise and continuing to evolve

Double Extortion:

Occurs about 60 percent of the time attackers couple ransomware with stealing data

Ransomware pays:

We estimate Sodinokibi / Revil alone earned $120m, trending to a billion-dollar business

Shift to Ransomware-as-a-Service:

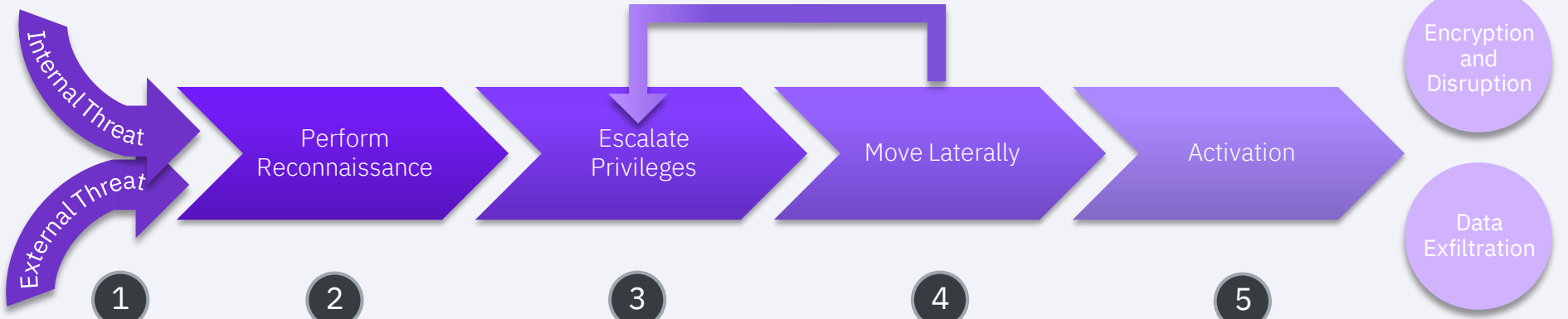
Affiliate or franchise operations, enables multiple infection vectors using the same ransomware

Incidents are taking longer to remediate:

Trending to 400+ hours in 2021

[1] IBM Security Cost of a Data Breach Report 2021
[2] IBM Security X-Force Threat Intelligence Index 2022

Ransomware, insider threats, and other persistent attacks are highly sophisticated and can go undetected for weeks or months



1

Phishing / spear phishing

Malware downloaded

2

Scan networks

Infiltrate on-prem & cloud

Resist detection & removal

Link command & control

3

Access privileged accounts

Leverage admin rights

4

Identify additional targets

Self propagation

5

Encrypt files & databases

Locate & encrypt backups

Exfiltrate high-value data

Example Targets

Crown Jewels

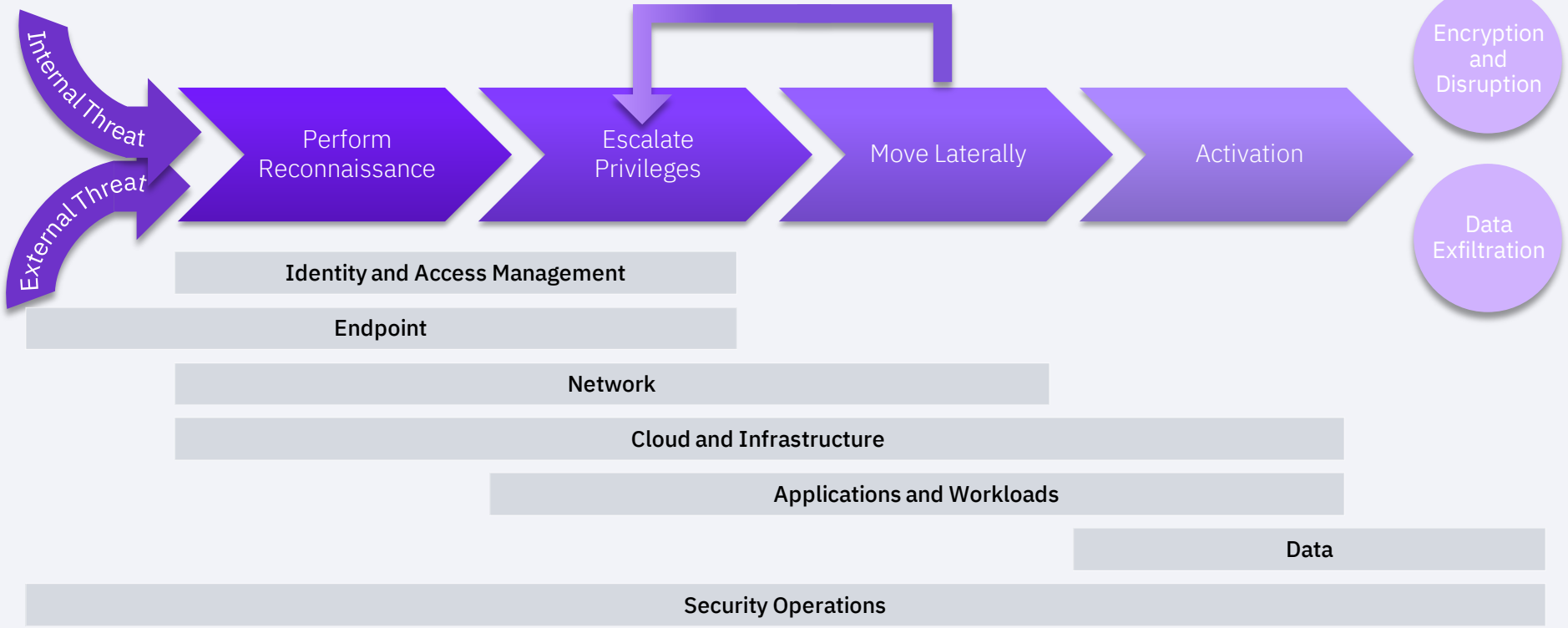
Intellectual Property

PII

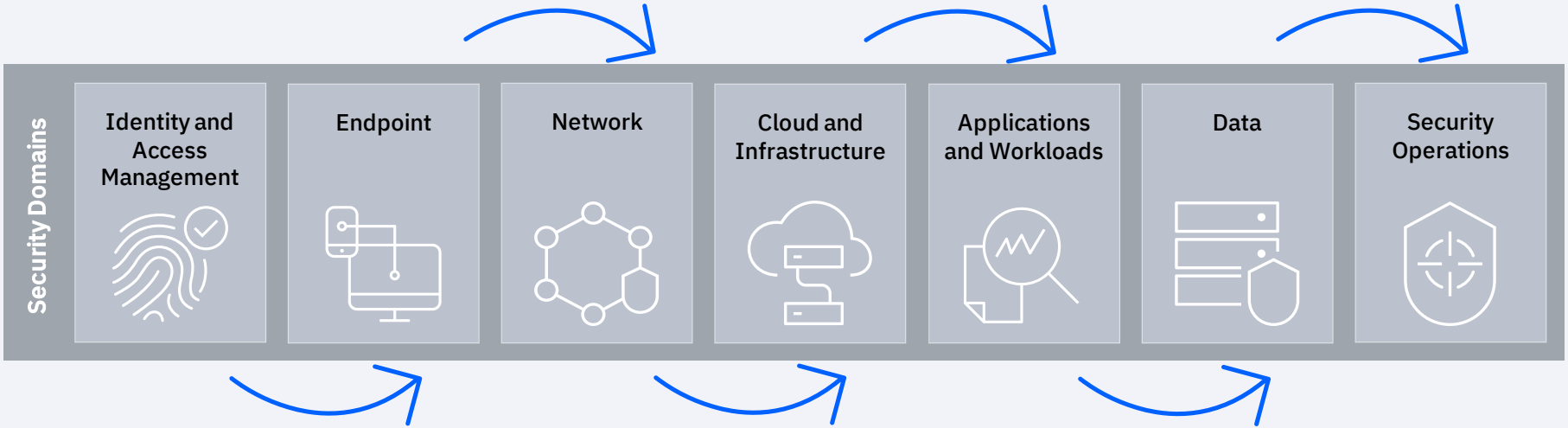
POS and OT

Understanding the attack chain is critical for preparation, protection, and prevention

There are many individual controls that can be applied to enable protection and improve detection…



...However, no single tool can holistically solve the challenge of business disruption due to cyber attacks.



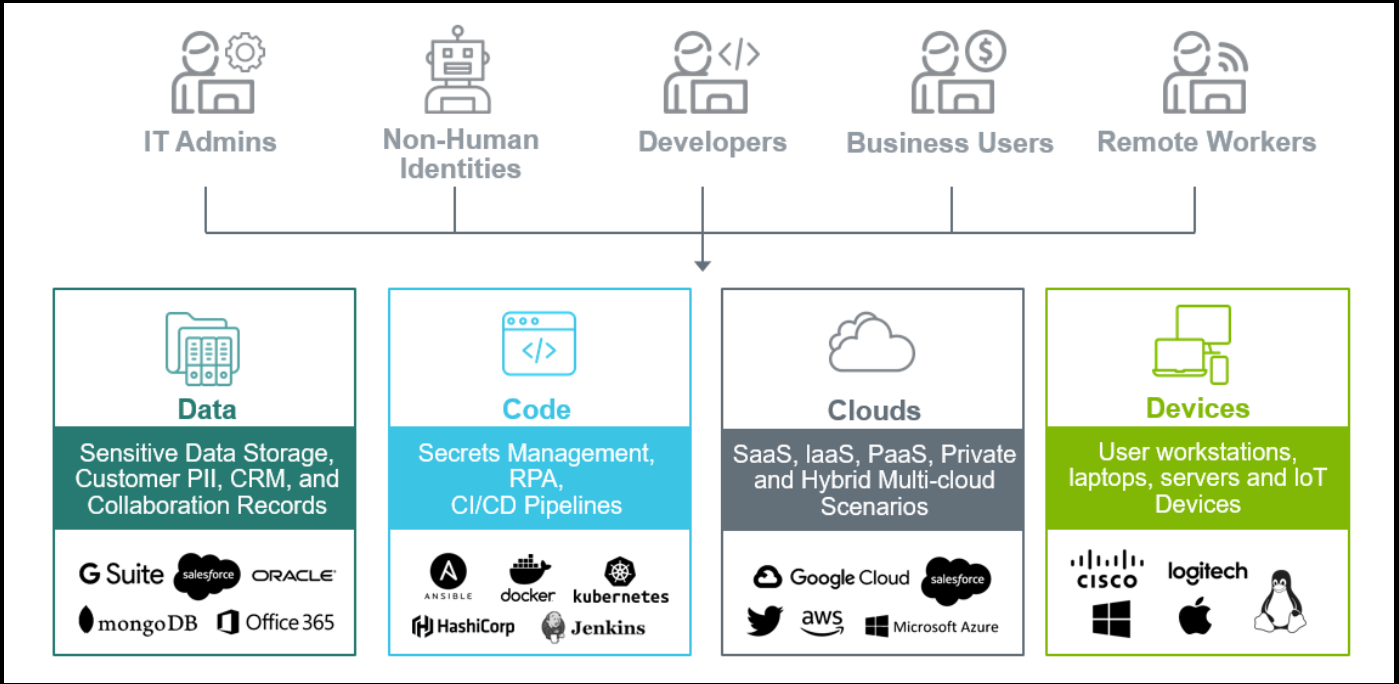
It demands open integration across security and IT domains.

Apply a zero trust approach and focus on the specific outcomes and capabilities that will have the greatest impact for each use case

	Ransomware: Preparation and protection	Ransomware: Detection, response, and recovery	Compromised credentials and account takeover	Data exfiltration from malicious insiders
Get Insights				
Cyber Risk Management	●	○	●	●
Data Discovery & Classification	●	○	○	●
Unified Endpoint Management	○	●	●	●
Vulnerability Management	●	●	○	○
Enforce Protection				
Activity Monitoring	●	○	●	●
Adaptive Access	●	●	●	●
Endpoint Privilege Management	●	○	○	○
Identity & Data Governance	●	○	●	●
Multi-Factor Authentication	●	○	●	○
Micro-segmentation	●	●	○	○
Privileged Access Management	●	○	○	●
Detect & Respond				
Data Resilience	●	●	○	○
Endpoint Detection and Response	●	●	●	○
Network Detection	○	●	●	●
Security Information and Event Management	○	●	●	●
Security Orchestration Automation and Response	○	●	●	●
Threat Intelligence	○	●	○	○
User and Entity Behavior Analytics	○	●	●	●

To put zero trust into action to reduce the risk of business disruption you'll want to consider each of the critical capabilities (rows) indicated (●) for the specific use cases you want to address (columns).

Across the IAM landscape, privileged users are at the biggest risks with any cyber attack, including ransomwares



Zero Trust mandates a “never trust, always verify, enforce least privilege”

Privileged Access Management (PAM) is a well-established security best practice, but several organizations have a false sense of confidence against ransomware because they have weak or incomplete protection of privileged users, workstations and servers.

Common privilege access gaps

Just applying vault to secure passwords is not enough !!!

Over-entitlements, inconsistent access policies often exposes higher risks when gets compromised

Weak authentication makes it easier for threat actors to comprise privileged credentials

Lack of end-point protection for workstations and servers makes it easy for threat actors

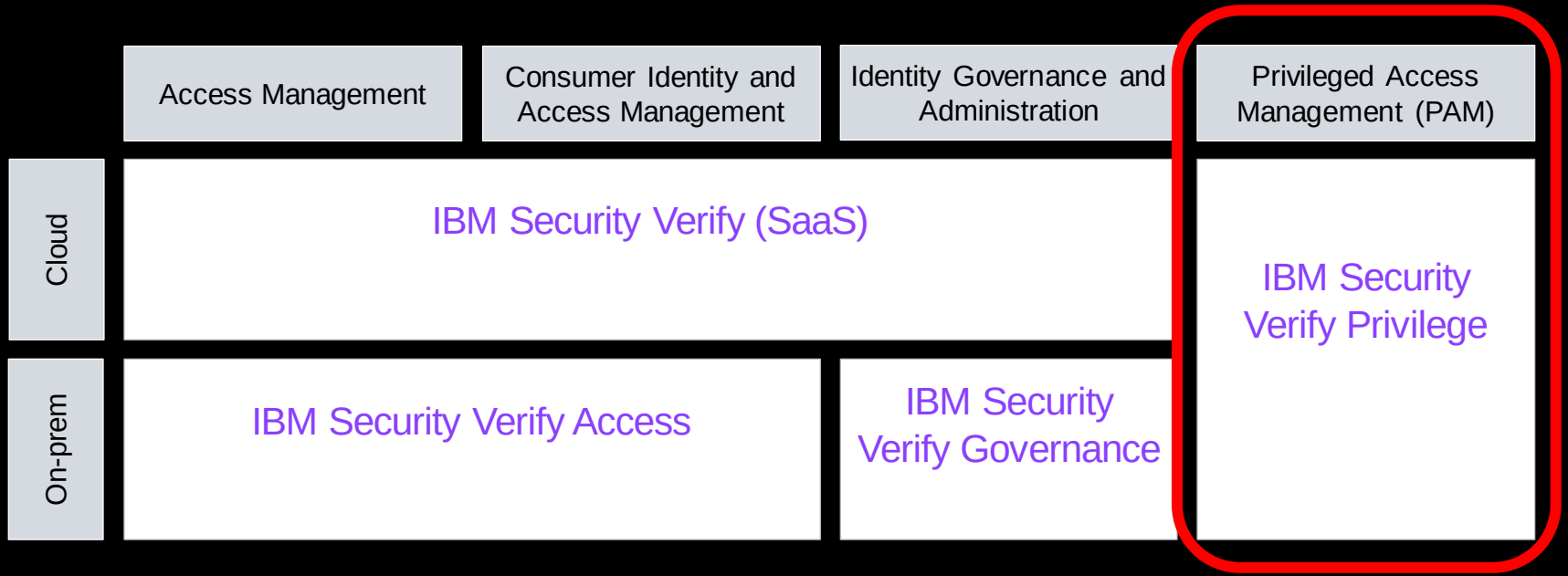
Missing a broader Zero Trust approach limits the value of a PAM solution from protecting privileged users and access to critical data

Ryuk Case study: An exemplar double extorsion ransomware targeting financial organizations

Initial Access & Foothold		Expand	Impact
Campaign & Infection	Staging & Recon	Privilege access	Exfiltration & Encryption

• MS Word documents inside of a password protected archives via phishing emails (reply chain attack)
• Macro downloads a DLL from a URL which is loaded by regsvr32.exen
• Once DLL is loaded (default.tmp) it drops and executes a JavaScript file to download the payload
	• Keep Malware (Valak) up-to-date
	• Install NetSupport Manager to gain interactive access
	• PowerShell ADRecon Tool is executed
		• Power Shell Remoting Session is initiated
		• PowerShell downloads additional tools
		• Domain Admin creds are acquired
		• Scheduled Task executing script from SystemApps
		• Attacker moves laterally to another system via PowerShell (likely Cobalt SMB Beacon)
		• Performs heavy recon of the environment using network scanners, Nagios, and Vcenter
		• Pivots from PowerShell access to a tunnelled RDP connection
			• Exfiltrate data to Mega.nz via MEGASync
			• Attacker uses AtExec to create a scheduled task to perform a “gpudpate /force” to disable Windows Firewall, disable Windows Defender, and enable WinRM to accept connections for any host.
			• Wide spreading ransomware (Ryuk) via CrackMapExec
			  • Use well known file name to disguise itself
			  • Terminate services to block detection
			  • Encrypt files with AES-256. The header "HERMES" is added to the beginning of each file
			  • All encrypted files are saved with a ".ryk" extension.
			  • A ransom note named "RyukReadMe.html" is created

Introducing PAM with IBM Security Verify Portfolio



Powerful PAM made easy with IBM Security Verify Privilege

Privilege Vault

Discover, manage, protect, and audit privileged accounts across your organization.

End User Served
IT & Security Admins

Use Cases
Vaulting, Auditing & Privileged Access Control

On-Premises
Cloud

Add-ons
Vault Analytics
Vault Remote
Account Lifecycle Manager

Privilege DevOps Vault

Manage credentials for applications, databases, CI/CD tools, and services without causing friction in the development process.

End User Served
DevOps / Engineers

Use Cases
High-Velocity Secrets Management

Cloud

Privilege Manager

Enforce least privilege security, and control application rights on endpoints / workstations.

End User Served
Desktop / Helpdesk

Use Cases
Application Control & Least Privilege

On-Premises
Cloud

Privilege Server Suite

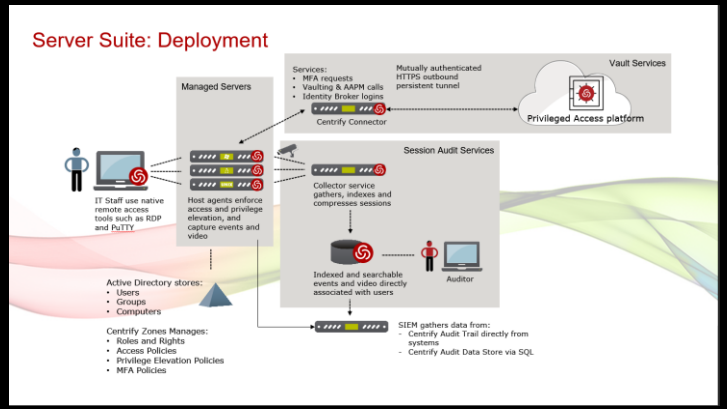
Minimize the attack surface and control privileged access to hybrid enterprise servers with just-in-time and just enough privileges

End User Served
IT & Security Admins

Use Cases
Unify Identity Services
Just-in-time
Least privileges

On-Premises

Verify Privilege Server Suite – Protect your enterprise servers from Cyber Attacks



Server Suite

Limit Access for Just Enough, Just-in-Time Privilege

Minimize the attack surface and control privileged access to the hybrid enterprise with just-in-time and just enough privilege, identity assurance and advanced monitoring and reporting.

MFA FOR PRIVILEGED ACCESS
Reinforce secure access to critical systems and privileged accounts.

PRIVILEGE ELEVATION
Grant just enough privilege across Windows, Linux and UNIX systems.

LOCAL ACCOUNT & GROUP MANAGEMENT
Reduce the risk of local privileged groups and service accounts.

AUTHENTICATION
Consolidate identities and leverage enterprise authentication services.

SESSION RECORDING & MONITORING
Monitor and record privileged sessions and changes to critical files.

AUDITING AND REPORTING
Enforce accountability for privileged activity and prove compliance.

Authentication Service

- Active Directory Bridging
- Local Account & Group Management
- Centrify Zone Technology
- Group Policy Management
- Machine Identity & Credential Management
- MFA at System Login

Active Directory Bridging

Extend the benefits and power of Active Directory to centrally manage and control access to your hybrid infrastructure

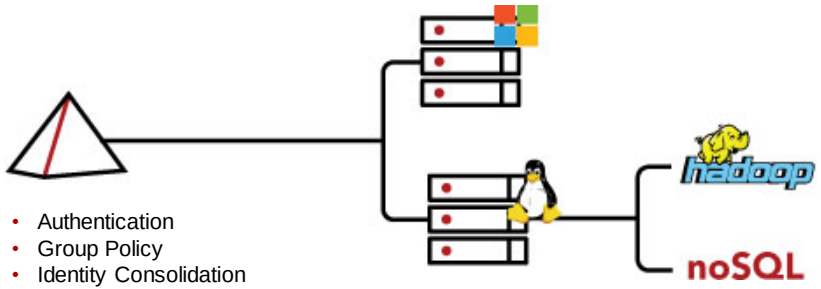
Reduce your attack surface by consolidating identities in Active Directory

Extend Active Directory to non-Windows systems for centralized management, governance, and delegation

Extend AD services such as Kerberos and Group Policy to non-Windows systems

Easily integrate PAM with even the most complex AD architectures

Make AD migration painless leveraging both Active Directory and Centrify tooling



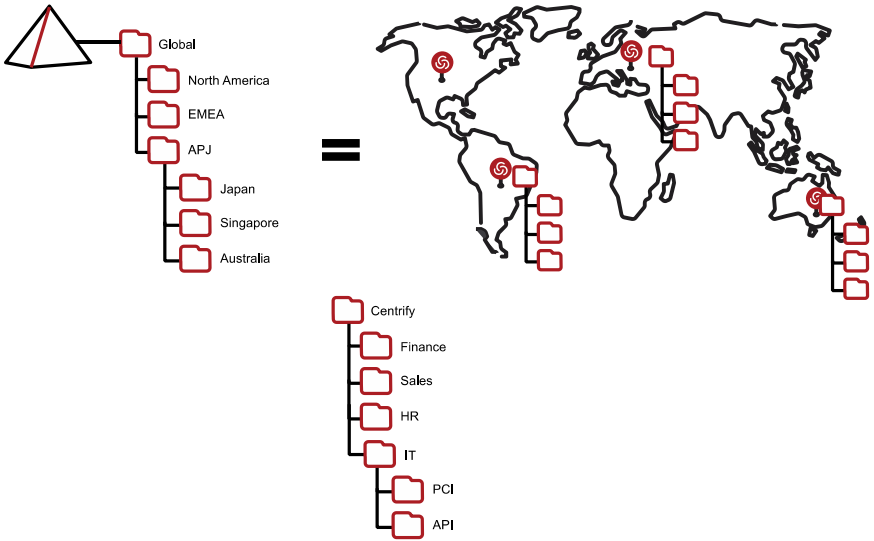
- Authentication
- Group Policy
- Identity Consolidation
- Fine-grained Authorization
- Kerberos-based SSO
- Complex AD Architectures
- Migration Tools

SERVER SUITE

Zone Technology

Active Directory is a powerful management tool. Centrify Zones take it to the next level

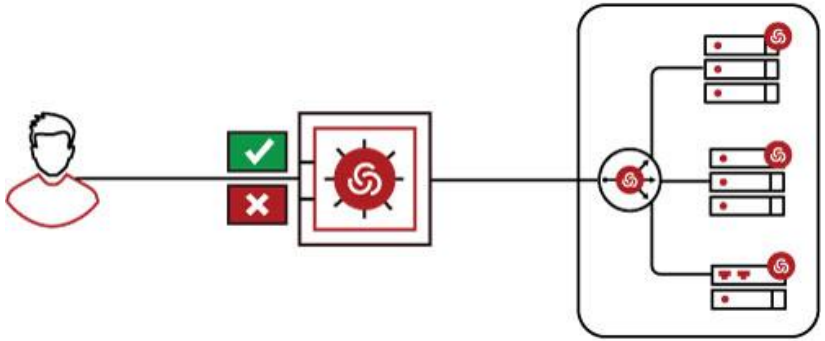
- Leverage Zones to centrally manage users, computers, and roles, cross-platform
- Create hierarchical parent-child zones that map to your preferred RBAC governance model, based on (e.g.) geography, department, or groups of regulated systems
- Consolidate identities reducing the attack surface by giving admins a single, unique ID for cross-platform login
- Import Linux/UNIX users without having to rationalize different namespaces, UIDs and GIDs in advance



MFA at System Login

Protect the primary attack interface to your critical infrastructure – system login

- Ensure only authorized humans are accessing your critical infrastructure
- Add an additional layer of identity assurance with MFA for Windows, Linux, and UNIX
- Stop malware and bots in their tracks
- Centrally manage MFA policies for system login — and all other critical access control points
- Leverage built-in 2nd factors (e.g., smartcard) or your existing authenticators (e.g., YubiKey or RADIUS)



Leverage MFA from Verify SaaS with Gateway for RADIUS

Privilege Elevation Service

- Privilege Elevation
- Delegated Privilege Role & Policy Management
- Time-Based Role Assignments
- MFA at Privilege Elevation

Delegated Privilege Role & Policy Management

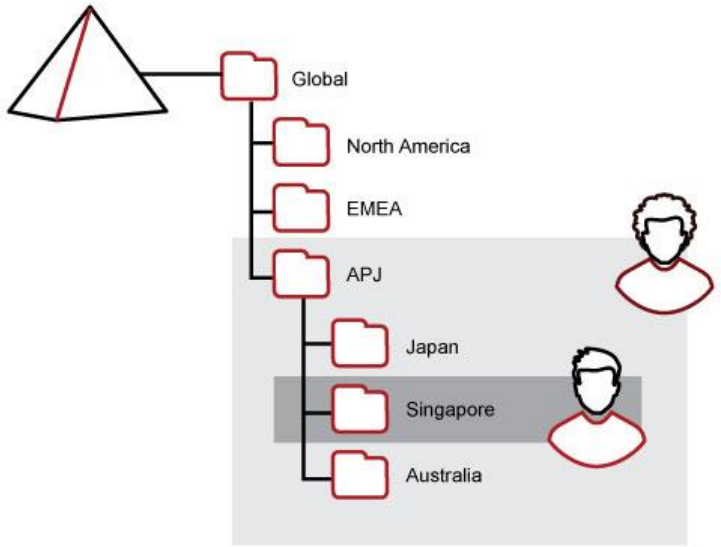
Hierarchical Zones enable more effective and efficient administrative delegation

Managing users, computers, roles, and rights can be hugely complex, operationally intensive, and painful for auditors

Simplify with centralized management and reporting from your existing Active Directory

Leverage Centrify's hierarchical Zone Technology to simplify:

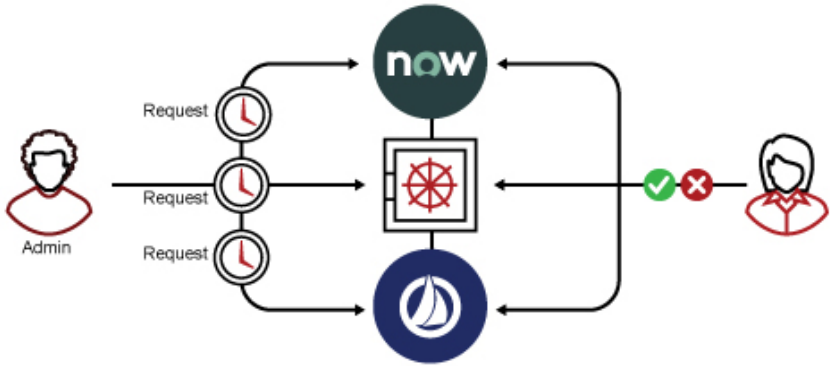
- Creation and maintenance of an access control governance model;
- Delegated administration and separation of duties; and
- Role management with common roles inherited top-down across all Zones.



Time-Based Role Assignments

Maintain a consistently low risk posture by granting additional rights on a temporary basis

- Temporary role assignments allow us to better control risk, maintain a small attack surface, and limit lateral movement
- Core to this principle is time-boxing; approve requested roles for a limited time period
- Once the limit is reached, automatically revoke the roles to re-establish the original lower-risk state
- Chose your workflow: Centrify built-in or 3rd-party workflows from ServiceNow and SailPoint



IBM Security Verify Privilege helps you to protect enterprise servers from Ransomware attacks

IBM Security Verify Privilege Server Suite

Limit Access for Just Enough, Just-in-Time Privilege

Minimize the attack surface and control privileged access to the hybrid enterprise with just-in-time and just enough privilege, identity assurance and advanced monitoring and reporting.

MFA FOR PRIVILEGED ACCESS
Reinforce secure access to critical systems and privileged accounts.

PRIVILEGE ELEVATION
Grant just enough privilege across Windows, Linux and UNIX systems.

LOCAL ACCOUNT & GROUP MANAGEMENT
Reduce the risk of local privileged groups and service accounts.

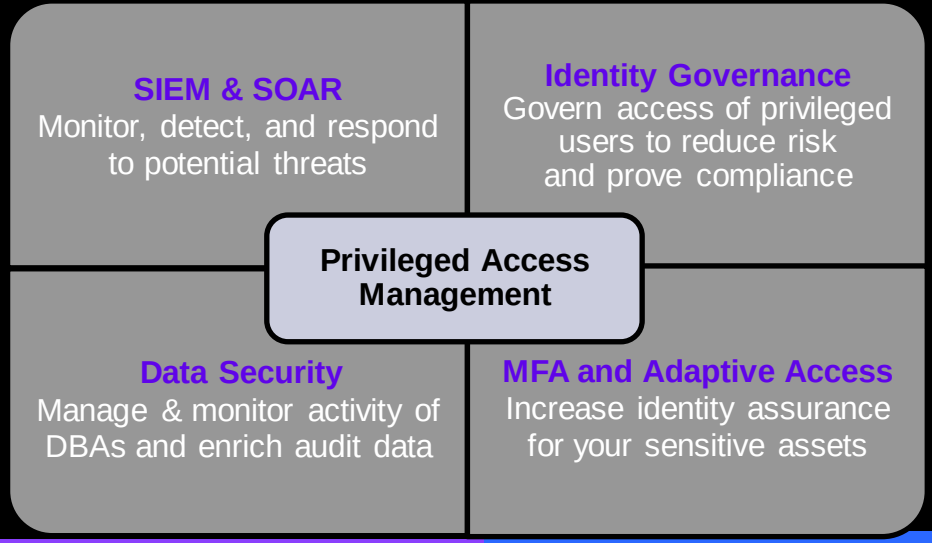
AUTHENTICATION
Consolidate identities and leverage enterprise authentication services.

SESSION RECORDING & MONITORING
Monitor and record privileged sessions and changes to critical files.

AUDITING AND REPORTING
Enforce accountability for privileged activity and prove compliance.

Integrate with the IBM Security ecosystem - Zero Trust

Zero Trust mandates a “never trust, always verify, enforce least privilege”



QRadar / CP4S

Notify security administrator if a user shows unusual or risky behavior in Privilege Vault

Verify Governance

Ensure governance policies are enforced, simplifies managing of business and admin users

Guardium

Manage privileged accounts, track privileged access usage, and enrich audits with identity context

Verify SaaS

The privileged user authenticates with MFA for security, and is continually authenticated using transparent risk assessment

Next Steps

Request for Demo

Engage with IBM expert in your region to request for a comprehensive demo of IBM Security Verify Privilege Server Suite

Solution Brief

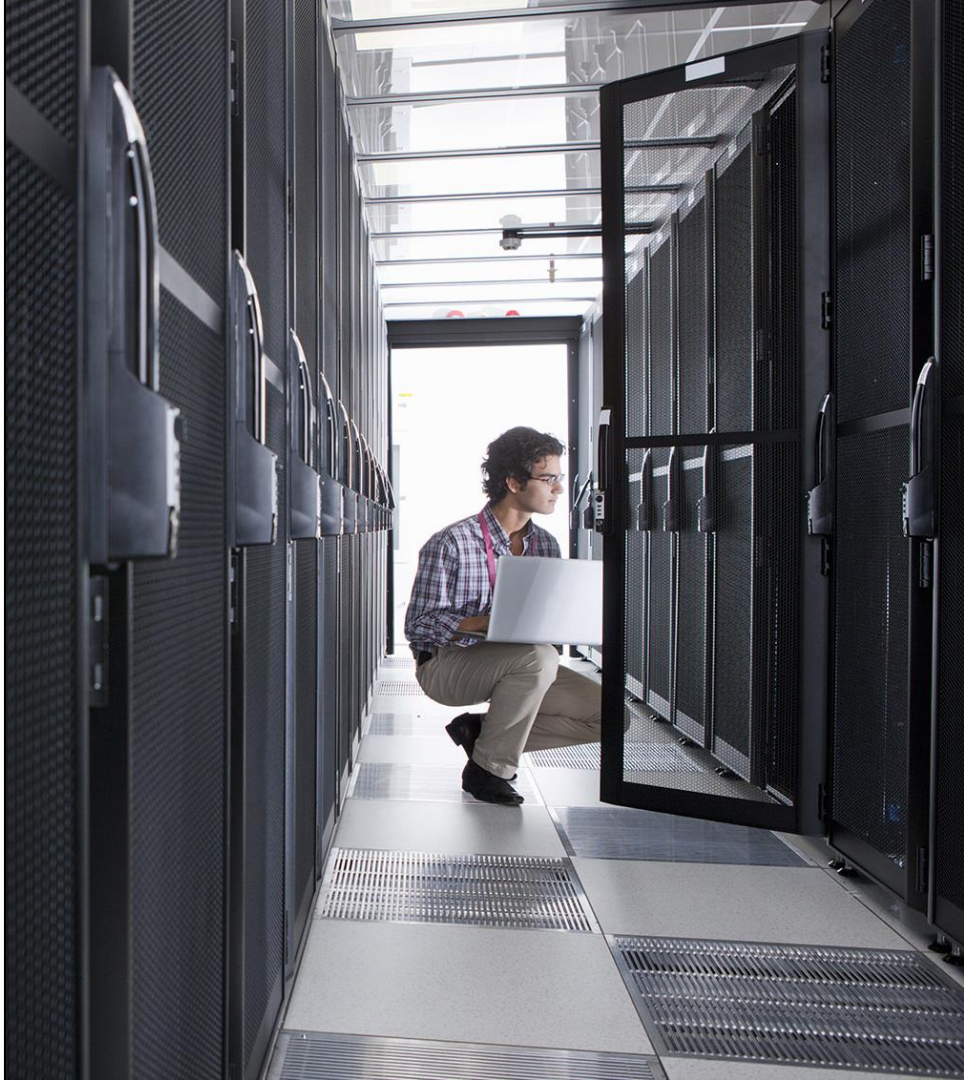
Go through Server Suite Data Sheet to understand its value proposition and use cases it can address: https://www.ibm.com/downloads/cas/A5WE5WP7

Learn more about Verify Privilege

Learn more about IBM's comprehensive PAM offering – IBM Security Verify Privilege - https://www.ibm.com/security/privileged-access-management

2022 Master Skills University (MSU)

Register for Server Suite Deep-dive session at 2022 MSU on April 7th - https://www.ibm.com/events/event/pages/ibm/vofowomb/1581037797007001pjad.html



Thank you

Patrick Ancipink
Product Marketing Manager, IBM Security Verify
patrick.ancipink@ibm.com

Dinesh Jain
Product Manager, IBM Security Verify
dineshjain@in.ibm.com

Brian Carmen
Senior Sales Engineer, Delinea
brian.carmen@delinea.com