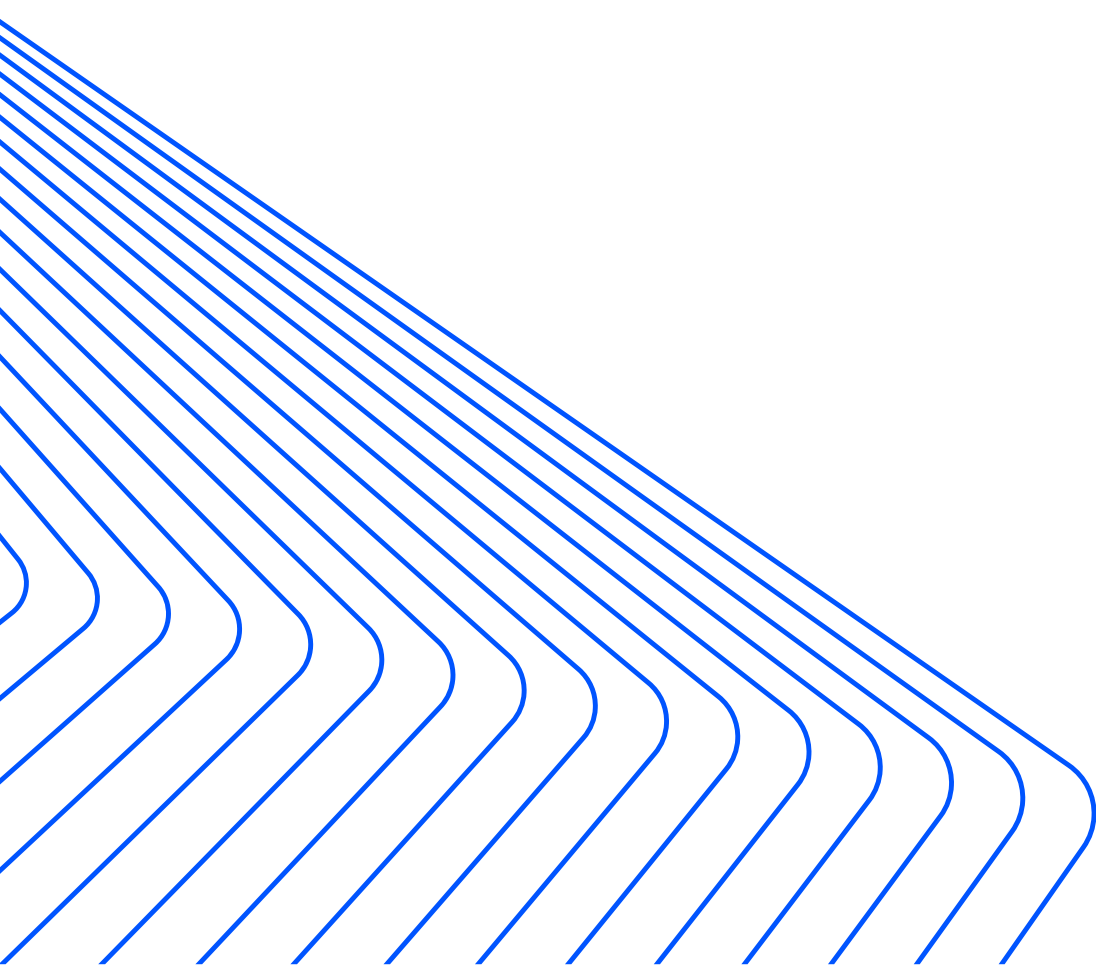# Accelerating Privilege Management Transformation

# Introduction

The world of Enterprise IT & technology infrastructure is changing at a fast pace. Enterprises are gradually re-engineering applications for the cloud. This transformation shift will be as significant as mechanization in prior generations of bare metal & virtual infrastructure. Primary business drivers of moving infrastructure & applications to the cloud remain the need for growth & speed of service delivery.

Fueling this change, the need for new-age technological skills, security, software-defined networking will rise even as others' demands, including physical and manual skills, will fall. Enterprises are continually rethinking how to re-organize in the cloud-first world. Embracing this change for enterprises means engaging with the new generation of service providers, onboarding new teams, building new departments like DevOps, cloud transformation combined with design & implementation of new security design processes.

Enterprises must embed zero trust principles and focus on data security & identity management while developing specific security strategies for securing endpoints, applications, and infrastructure. This whitepaper discusses how different sets of enterprises adapt to change and presents solutions for designing privilege management strategies.

## Understanding complexity of modern privilege management practices

Cloud services such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud are a compelling proposition for many enterprises because of self-service, skill-driven, pay-as-you-go approach, and need-based scalability. Cloud advantage allows enterprises with much needed faster time to market and improved service quality than on-premises infrastructure. Cloud adoption survey suggests four types of organization exist

- ones with 100% on-premises infrastructure,
- hybrid with mostly cloud
- hybrid with most on-premises and
- 100% cloud.

With significant investment trends in cloud strategy, more enterprises plan to move workloads to the cloud. The role of security teams in the cloud operating model is crucial because no one else can broker across multiple parties involved, including applications, infrastructure operations & governance. The security team's role in modern times is more to do with risk-taking rather than risk elimination.

For an organization making this shift, the fundamental challenge is to reskill individuals with new cloud capabilities and building design & operations capabilities to deliver required security assurance to business. Irrespective of legacy or modern infrastructure, enterprises must maintain skills by augmenting internal teams or via outsourcing.
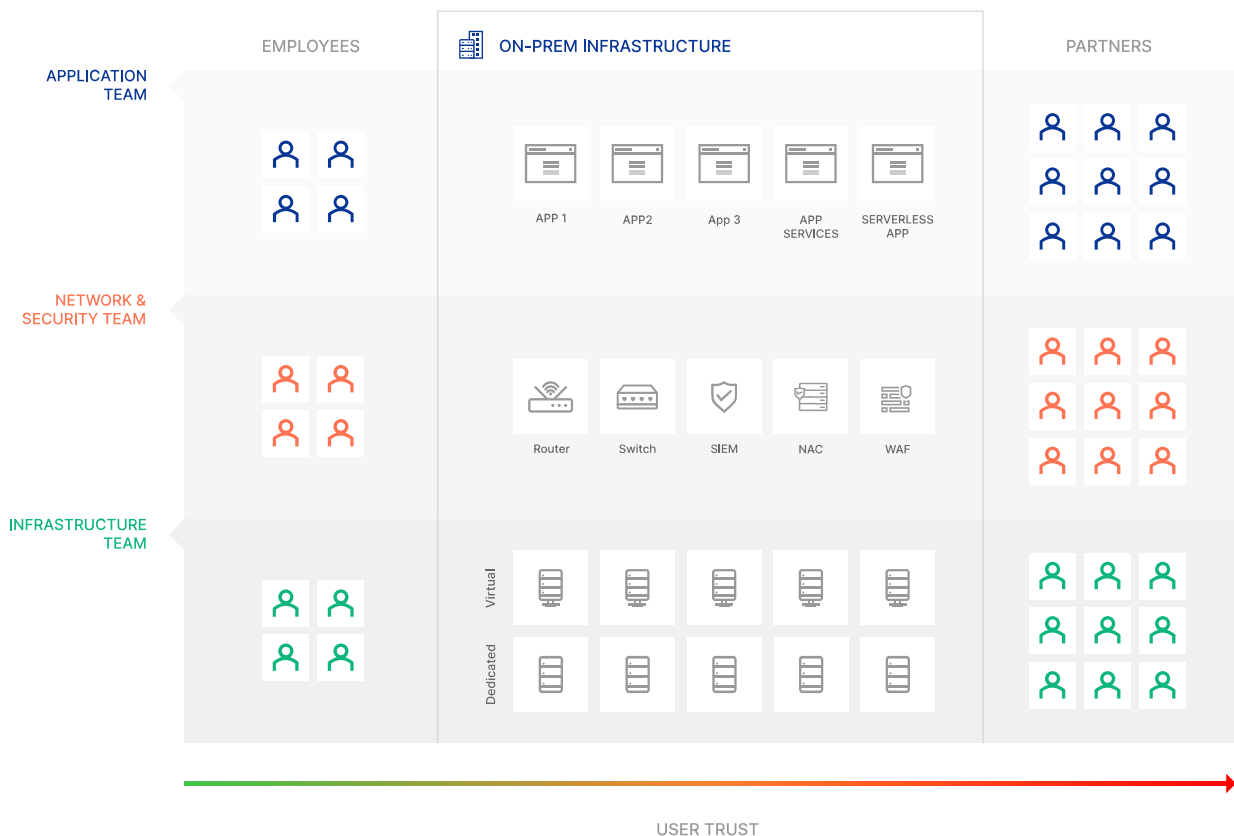
Looking back, in a typical on-premises model with a mix of bare-metal, virtual infrastructure, the "IT Security Playbook" starts with securing & managing passwords in a vault and monitoring privileged sessions over operating systems, databases, network elements.

Most of the leading organizations have solved initial deployment challenges of privileged access management by keeping in mind a perimeter-based approach. The challenge still exists for most enterprises to figure out how to solve issues of data leakage, lateral movements & encryption of sensitive traffic when users are accessing from multiple locations and unknown endpoints.

In the era of anywhere access, most enterprises' challenge is

- How to deliver seamless access to diverse teams comprising operations, managed service providers, applications service providers to securely access from anywhere with consistency and the least friction possible.

- Manage privileges at endpoints or implement zero-trust policies

- Secure increasing number of machine identities

- Consolidate privilege management with auditable records & centralize policy management for endpoints, application, and workloads



EMPLOYEES     ON-PREM INFRASTRUCTURE     PARTNERS

APPLICATION TEAM

APP 1   APP2   App 3   APP SERVICES   SERVERLESS APP

NETWORK & SECURITY TEAM

Router   Switch   SIEM   NAC   WAF

INFRASTRUCTURE TEAM

Virtual

Dedicated

USER TRUST

Enterprises embrace cloud strategy either with a single or multi-cloud to extend primary or secondary hosting facilities replicate the same playbook of securing privileged users. With cloud strategy, enterprises can scale compute & resource on-demand, move from securing physical perimeter to dynamic perimeter, move from virtualization management to cloud consoles, secure IP-based applications to layers of active services & application functions.

The complexity of managing hybrid IT, single cloud or multi-cloud, increases the complexity of privilege management by converging networks, authentication methods, and most importantly, users' addition.



USER TRUST
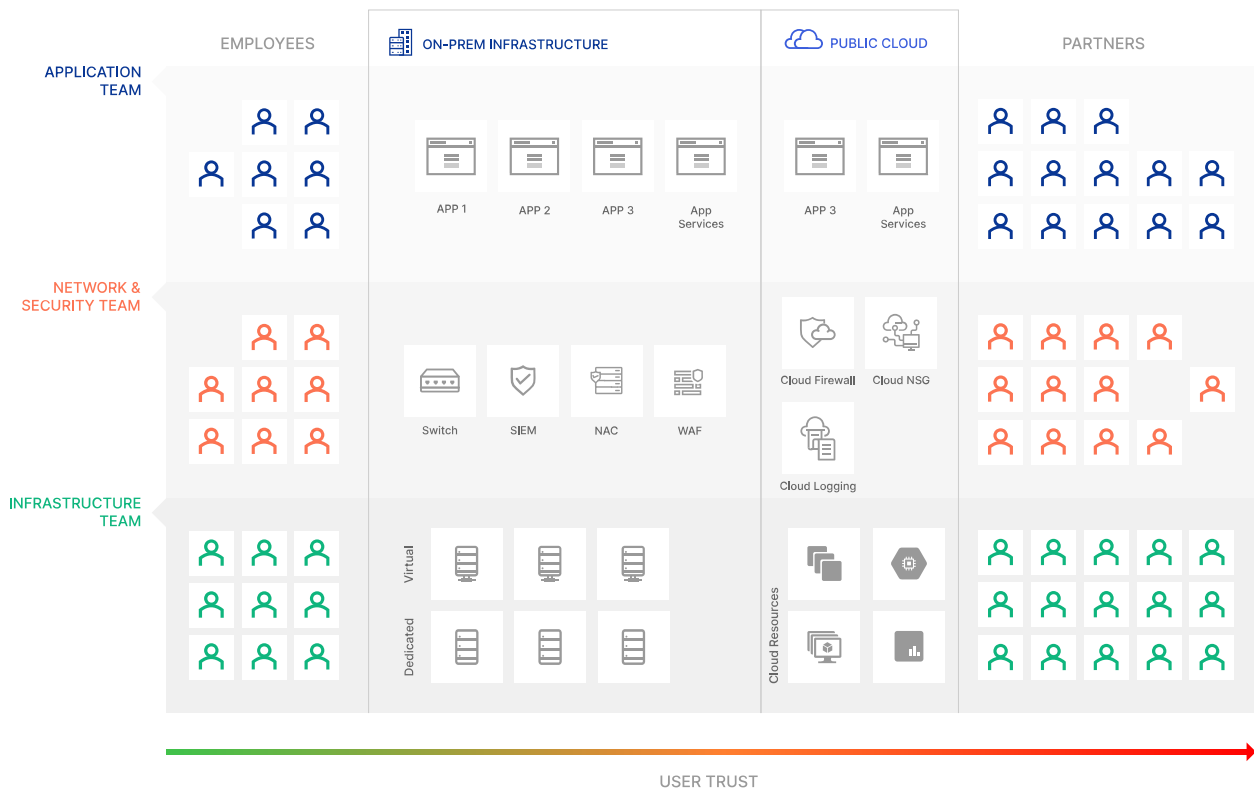
No matter of deployment types of privilege management solutions, enterprises express frustration with the process of integrating or extending legacy privileged access management technologies with new cloud environments or enabling anywhere access for monitoring & securing privileged sessions. The trouble spots include:
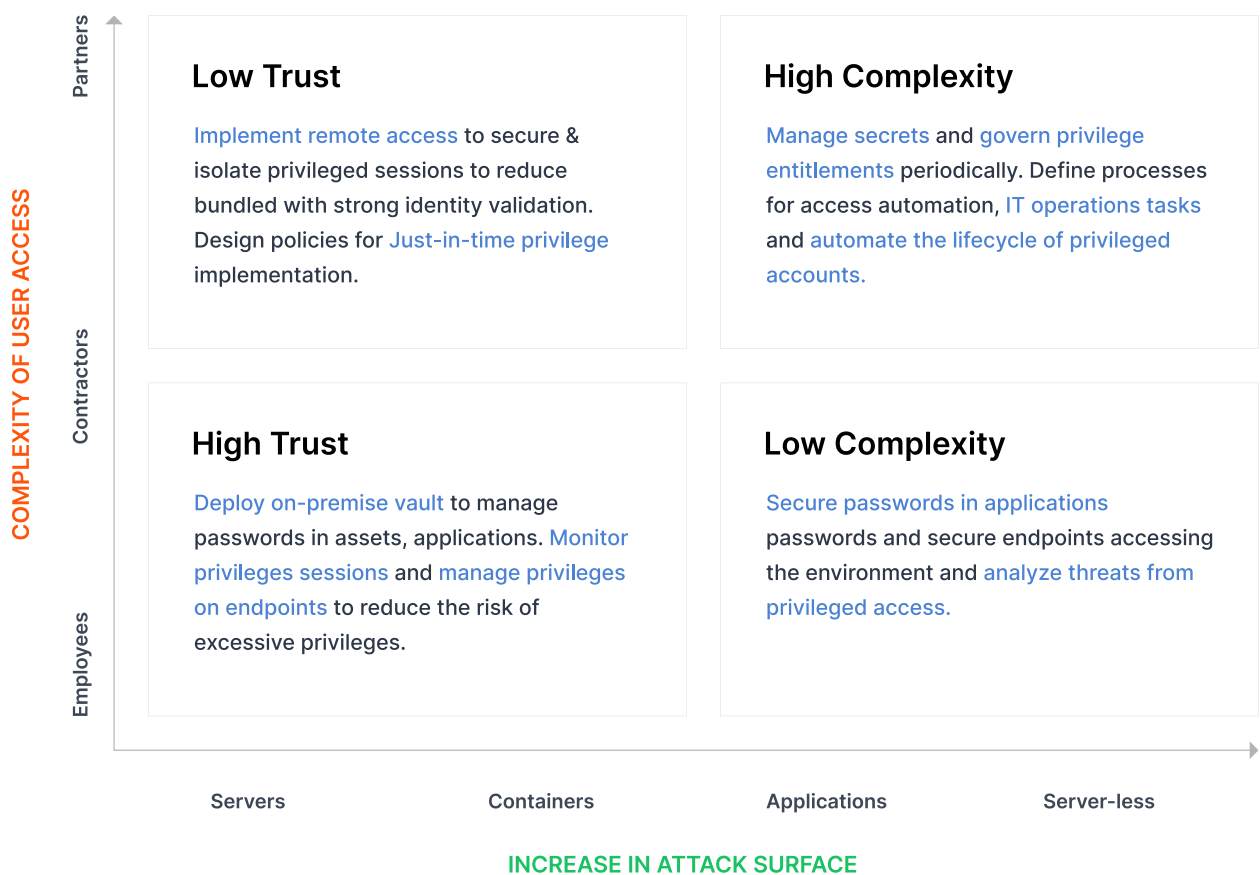
- Lack of support for supporting multi-sites or cloud environments, including high appliance costs on cloud environments.
- Lack of integration with native cloud provider services enabling discovery, SSO, authentication, infrastructure
- The high operational cost of managing system operations

## Adapting privilege management in complex environments

Making fundamental shifts from traditional privilege management solutions deployed already and quickly onboarding workforce with anywhere access can seem large and complex. Security leaders' urgent questions are how to go beyond extending on-premises deployed privilege management solutions to reimaging speed and scale.

Keeping in mind the drivers of digital transformation, privilege management solutions must align to business objectives. Two forces at play forcing security leaders to make fundamental shifts from legacy privileged management solutions are

1. Increasing attack surface with growing asset classes.
2. Controlling risk of anywhere privileged access

### Low Trust

Implement remote access to secure & isolate privileged sessions to reduce bundled with strong identity validation. Design policies for Just-in-time privilege implementation.

### High Complexity

Manage secrets and govern privilege entitlements periodically. Define processes for access automation, IT operations tasks and automate the lifecycle of privileged accounts.

### High Trust

Deploy on-premise vault to manage passwords in assets, applications. Monitor privileges sessions and manage privileges on endpoints to reduce the risk of excessive privileges.

### Low Complexity

Secure passwords in applications passwords and secure endpoints accessing the environment and analyze threats from privileged access.

**COMPLEXITY OF USER ACCESS** (Partners, Contractors, Employees)

Servers    Containers    Applications    Server-less
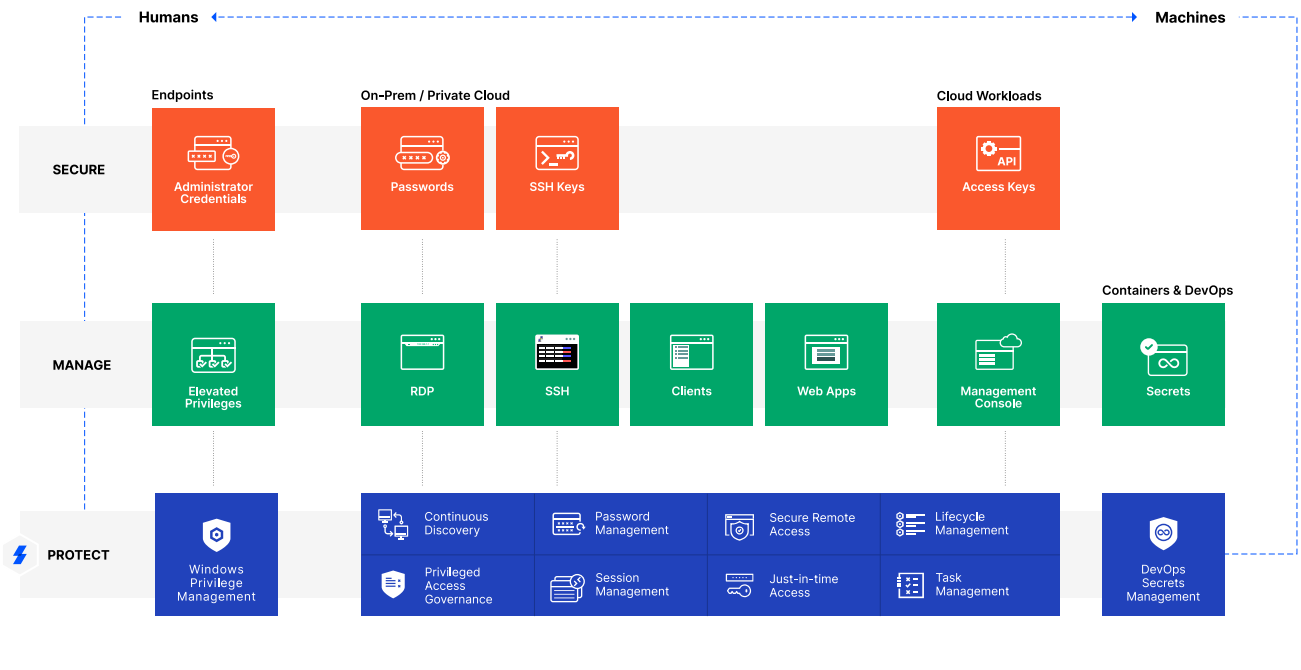
**INCREASE IN ATTACK SURFACE**

Enterprises can only make gradual & sustainable improvements to their privilege management approach by balancing risk and understanding what to do next.

# Implementing Privilege Management capabilities at scale

Many different products provide more straightforward options for integration at the start. Still, they often add to complexity with specialized services, complementing license costs that restrict enterprises from unlocking the desired services' potential in due time. Simultaneously, technologies not integrated or purpose-built for the cloud-first world may add costs, much more complexity, and weight.

Typically, enterprises find it challenging to adopt privilege management technologies due to the long build cycle and dynamic team structures. While enterprises tend to have a solid understanding of the threats in an on-premises environment combined with VPN-led moderate remote work – their knowledge of how to mitigate against cyber risk from the cloud & anywhere access is often spottier.



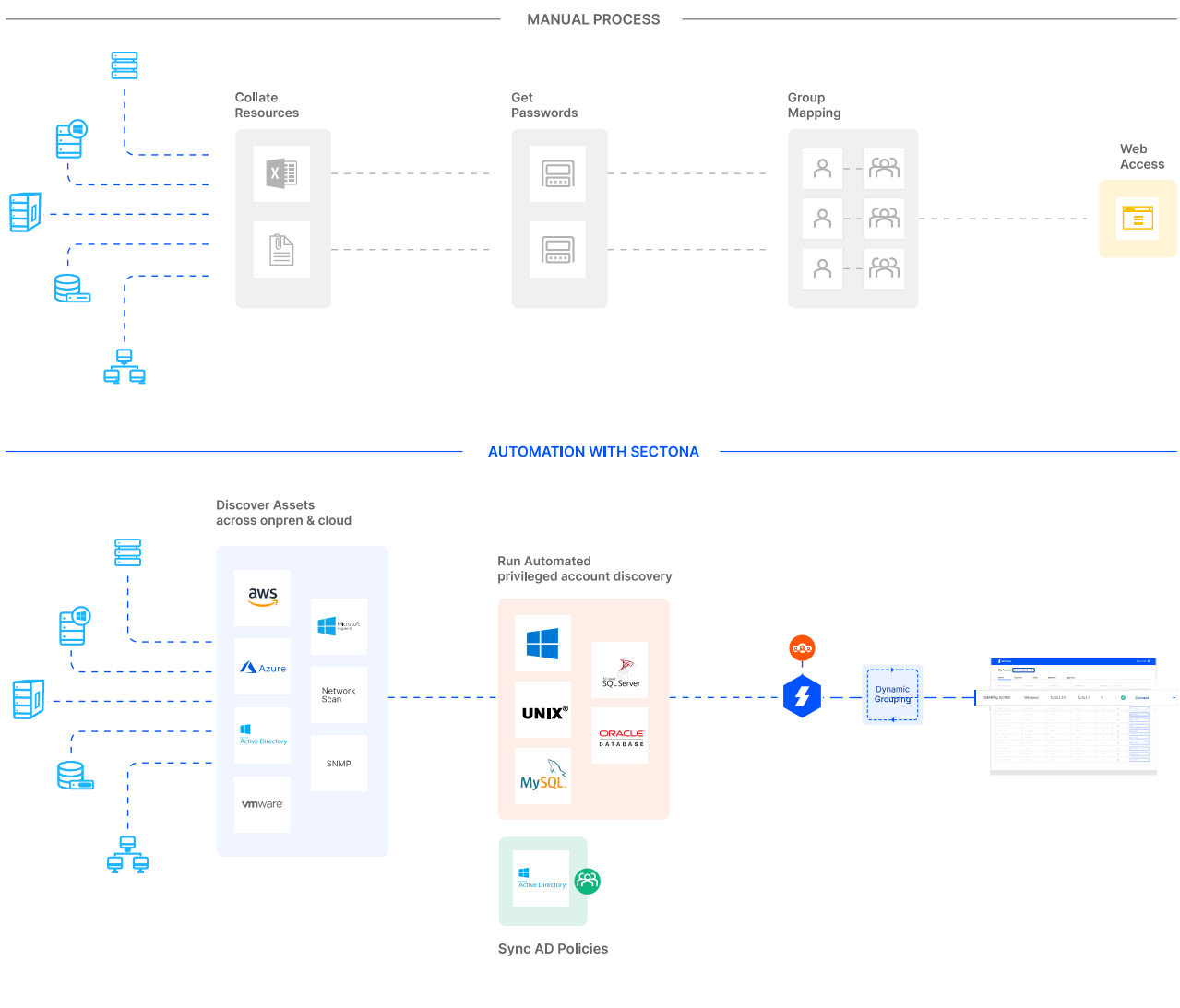| | Humans | | | | | | Machines |
|---|---|---|---|---|---|---|---|
| | Endpoints | On-Prem / Private Cloud | | | | Cloud Workloads | |
| **SECURE** | Administrator Credentials | Passwords | SSH Keys | | | Access Keys | |
| | | | | | | | Containers & DevOps |
| **MANAGE** | Elevated Privileges | RDP | SSH | Clients | Web Apps | Management Console | Secrets |
| **PROTECT** | Windows Privilege Management | Continuous Discovery / Privileged Access Governance | Password Management / Session Management | Secure Remote Access / Just-in-time Access | Lifecycle Management / Task Management | | DevOps Secrets Management |

Sectona Security Platform brings together elements to secure privileges on growing attack surfaces for organizations. The complete platform is developed from the ground up and integrated by default for ease of use. In working with customers around

regions, we have found that leveraging an integrated privileged management solution focusing on automation, simplicity, light build, and bringing multiple teams into a single platform can help achieve the desired velocity.

## Automate Access Provisioning

Privilege Management projects typically start with the discovery phase of assets tracked in multiple CMDB systems, spreadsheets, and files. Traditional approaches in discovery remain either leveraging AD discovery and network scan. Often these are limited to one-time activities at the start of the project or limited to assets classes like Active Directory and not continuous in nature, leaving gaps in regular operations.

In this era of digital flows, enterprises must take all possible steps to automate security operations to reduce operational costs and avoid human errors. Users demand access to services granted as soon as creation, while operations teams spend more time coordinating and waiting for information than actually doing the job.

MANUAL PROCESS

Collate
Resources

Get
Passwords

Group
Mapping

Web
Access

AUTOMATION WITH SECTONA

Discover Assets
across onpren & cloud

Run Automated
privileged account discovery

Network
Scan

SNMP

Dynamic
Grouping

Sync AD Policies

Sectona Continuous Discovery capability is a starting point to provide dynamic access to end-users without human intervention.
Sectona Continuous Discovery leverages deep integration with major cloud providers, including AWS & Azure,

VMWare vSphere and Hyper-V for private cloud, SNMP for network devices, and network scan. This integration with common asset data provides a single master database of assets in your environments.

With major enterprise deployments running Windows Active Directory, discovery tightly integrates with native policies reducing time to group, categorize and grant access to Windows infrastructure without replicating trust built-in Active Directory Domain.

The second part of the discovery process provides high visibility of privileged accounts integrated with the vault or outside the vault. Discovery capabilities are supported across server infrastructure of major Windows & Unix flavors, Microsoft SQL, Oracle Database & Oracle MySQL, and Windows Workstations.

Once set in motion, discovery can automatically execute jobs to find new resources across multi-cloud, multi-site environments along with associated privileged accounts & combining strong dynamic rules-based groups to provide user access eventually.

## Simplify anywhere privileged access

Providing endpoints loaded with security tools to every user accessing or using VPNs or jump hosts are not scalable options for every enterprise considering the time to implement servers & operational resource requirements. In the world of anywhere access, Understanding & verifying the identity of the remote workforce is another challenging task that acts as a gatekeeper to who gets access to what.

Privilege users accessing from any location requires the combined capability of identity verification and session isolation to reduce risks of data leakage & to isolate untrusted endpoints from connecting to the network. Solution with heavy use of Microsoft Terminal Servers is burdensome for IT, while technologies using endpoint agents are susceptible to password hijacking issues.

Sectona Security Platform integrates with multiple trusted identity providers such as cloud identity and access management (IAM) platforms, SAML-based systems, Cloud MFA providers for authentication to verify users' identity accessing from any location & provide secure access over browsers with or without VPN.

Sectona Security Platform provides secure remote access technology to access assets spreads across multi-site or multi-cloud environments using any browser. The web browser is one of the most common applications in use today. Browsers provide a standard approach to any user to access any compatible application.

Sectona provides browser-first session initiation & monitoring approach enabling RDP, SSH, Application, FTP, SFTP access over a browser with the privileged single sign-on & session management.

Automating credential injection using Sectona Vault & implementing Zero Standing Privileges (ZSP) for remote users with dynamic provisioning & elevation capabilities reduces the risk of credential theft or privilege abuse.
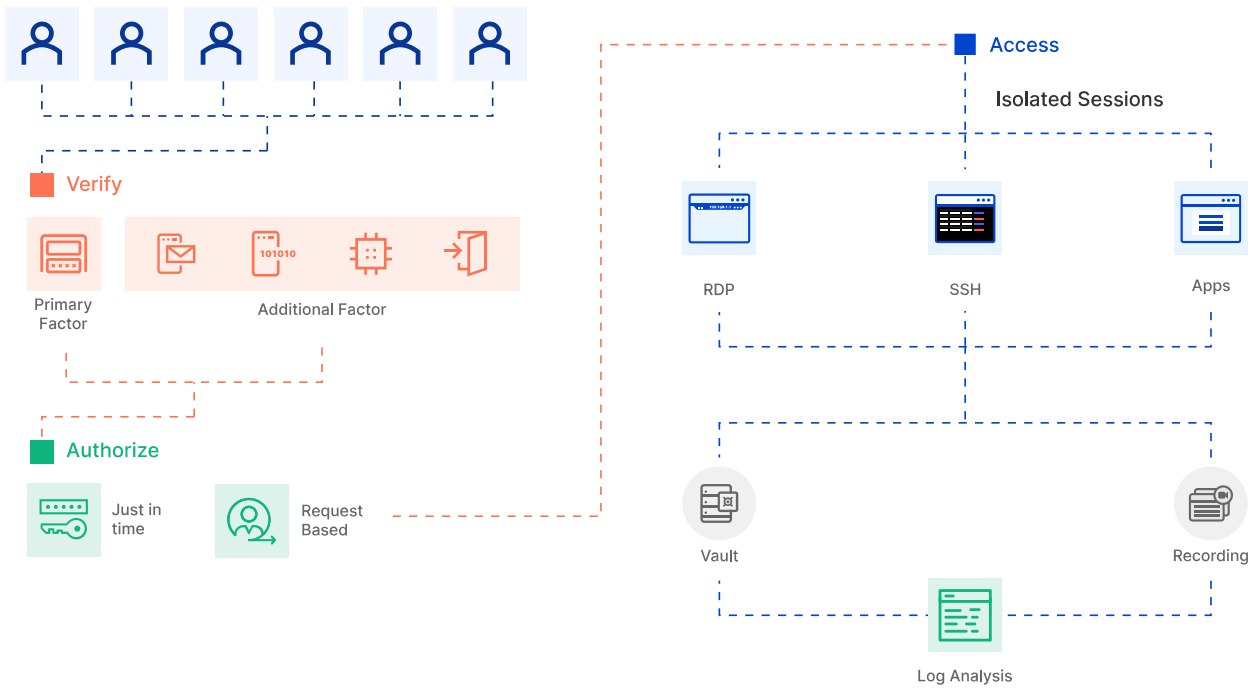
## Build & Design challenges

Modern enterprises looking to set up extended sites in the cloud or move to cloud environments require easy-to-extend solutions without the heavy lifting of virtual images or physical appliances.

Sectona Security Platform delivers a highly modular and customizable privilege management experience for your employees, contractors, and partners. Every component of the platform is designed to be modular & scalable, from deploying various secure session proxies for routing sessions across multiple sites to replicating vaults across sites.

The modularity of components allows building scalable architecture to save on resources as you scale as and when required. Sectona platform is built upon a secure & reliable vaulting technology, self-managed and hardened based on industry best practices.



Central Management
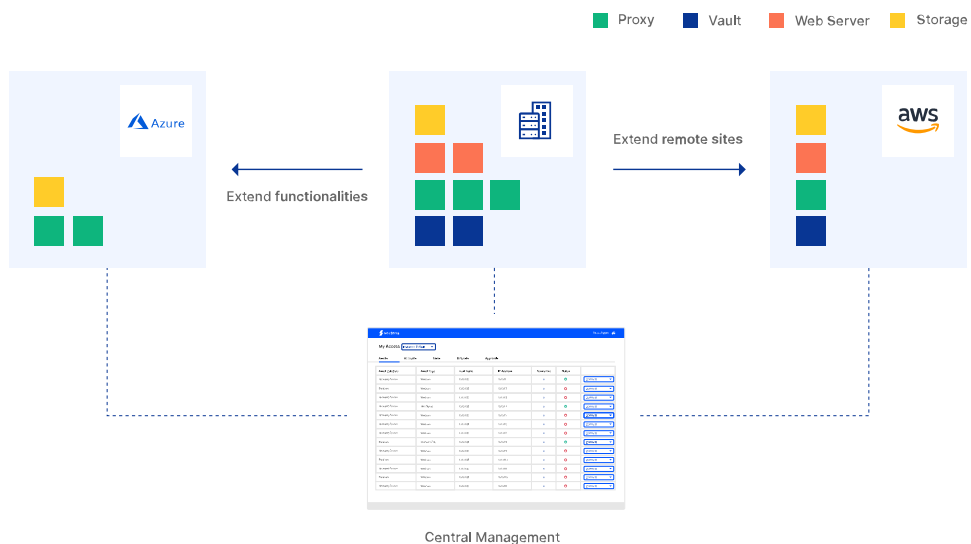
# Unlock governance paradigm

Technology infrastructure & operations environments are complex. External vendor relationships add more complexity. Most of the users hold more access than they require at any given time. Adding 100s of privileged users in a normal outsourcing arrangement of infrastructure managed services leads to complex access entitlements of users who may not require the desired privileged access.

PAM entitlements are built over the hierarchy of group-level entitlement, and often all privileges to be vaulted in password vaults is a long process. Over a period of time, users can be granted access to named, built-in, or shared accounts by ad-hoc techniques and can be difficult to manage with manual processes. Security teams demand coverage or continuous

governance of privileged accounts running in the infrastructure.

Without an integrated platform to continually govern access to users granted over a period effectively can lead to catastrophic issues related to excessive privilege. Sectona uses robust privileged account discovery techniques and reconciles accounts within and outside the vault. This discovery data is passed into privileged access governance for certification and attestation.

Integrated PAM and PAG capability with Sectona provides the ability to govern accounts, including service accounts, application accounts, and set review cycle.
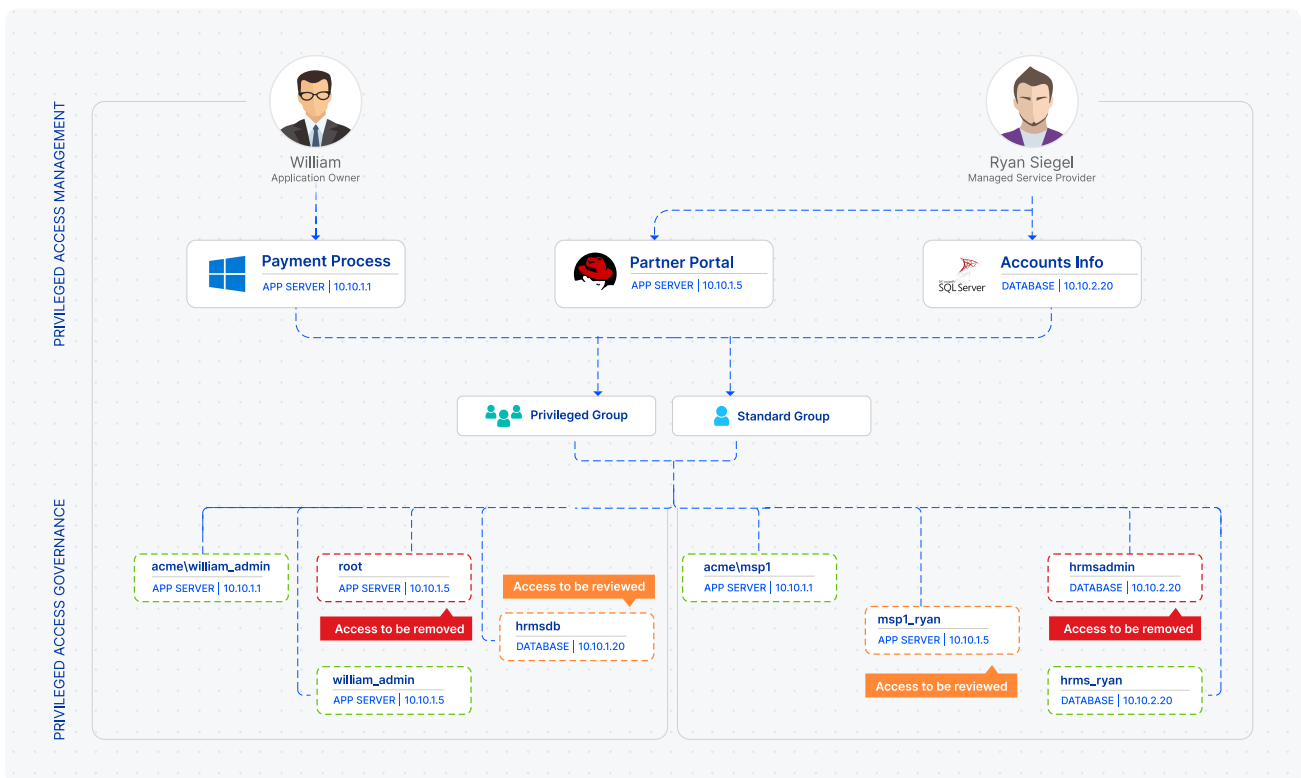
## Protecting against risky endpoints

Endpoints remain vulnerable and susceptible to attacks like lateral movement & excessive privilege abuse. Endpoints, such as workstations and servers, remain ideal targets to infiltrate a network successfully. Vulnerability levels increase as endpoints move outside the network, which is new normal than endpoints remaining within a network.

Sectona Security Platform provides an integrated endpoint Privilege

Management system to eliminate excessive privileges for users on endpoints, remove all local admin accounts, & enforce least-privilege policy via discovery, learning, and securing.

On-demand scalability of privilege management over endpoints, allows enterprises to secure critical business users from executing malicious applications.
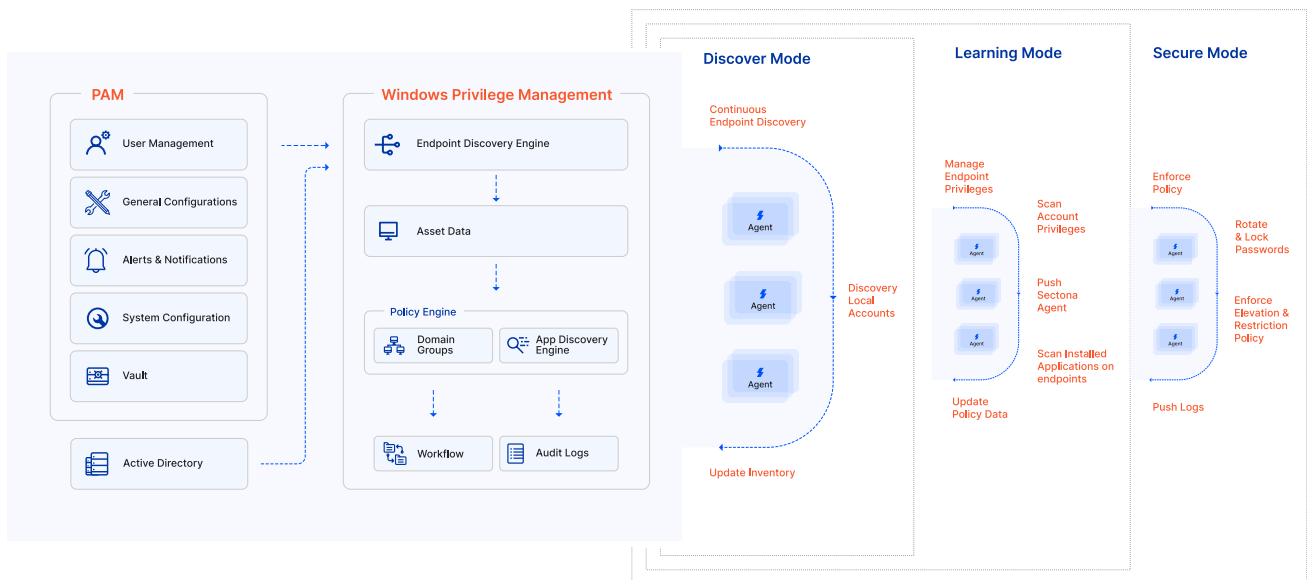


## Solve security issues with unstoppable rise of apps

Sectona Security Platform is designed to securely store & manage secrets in a specialized vault designed to handle tokens, certificates, encryption keys.

DevOps Secrets Management (DSM) is built on a common framework provided by Sectona Security Platform. DSM is an integrated component of Sectona Security Platform built on a common shared, scalable framework. Leveraging a strong foundation of shared platform provides flexibility for building scalable & fault-tolerant deployment to enterprise development.

With extensive auditable capabilities, be in control who access secrets and complete detailed activities of machine identities. DSM also supports rest based APIs, CLIs to integrate natively with public & private cloud infrastructure including SSH interfaces.

# Conclusion: Improve time to value

Privilege Management challenges across growing attack surfaces have become prevalent over the years and costing companies millions due to delayed project lifecycle & fragmented expectations from privilege management technologies.

Organizations on the path of initiating privilege Management programs may plan with a new integrated, scalable, resource-effective privilege management approach. In contrast, an organization with a mature privilege management program remains watchful of growing costs in resources, licensing, and usability can plan to migrate to a new integrated approach gradually.

## sectona

Sectona is a Privileged Access Management company that helps enterprises mitigate risk of targeted attacks to privileged accounts spread across data centers and cloud. Sectona delivers integrated privilege management components for securing dynamic remote workforce access across on-premises or cloud work-loads, endpoints and machine to machine communication.

For more information, visit www.sectona.com and follow @sectona1 on Twitter or @Sectona on linkedin