NTT DATA Digital Trusted Identity Services:

Identity Governance Administration, Identity as a Service, Single Sign-On, MFA and Privilege Access Management for Cloud, On-Premise and Hybrid environments

October 2020

Identity Challenges Faced by Today's Organization

- An increase in identity attacks

- Digital transformation shifts identity to serve as the control plane

- Many users and apps are outside of the corporate firewall

- Remote work creates new security needs, use cases and solutions

- Lost visibility and control of users

- New and ever-changing data privacy regulations

- Zero trust methodology requires a strengthened approach

Reimagine Security With Microsoft Azure Active Directory (AD)

HR apps

Windows Active Directory

AZURE AD

SaaS apps

Cloud-hosted apps

On-premises and web apps
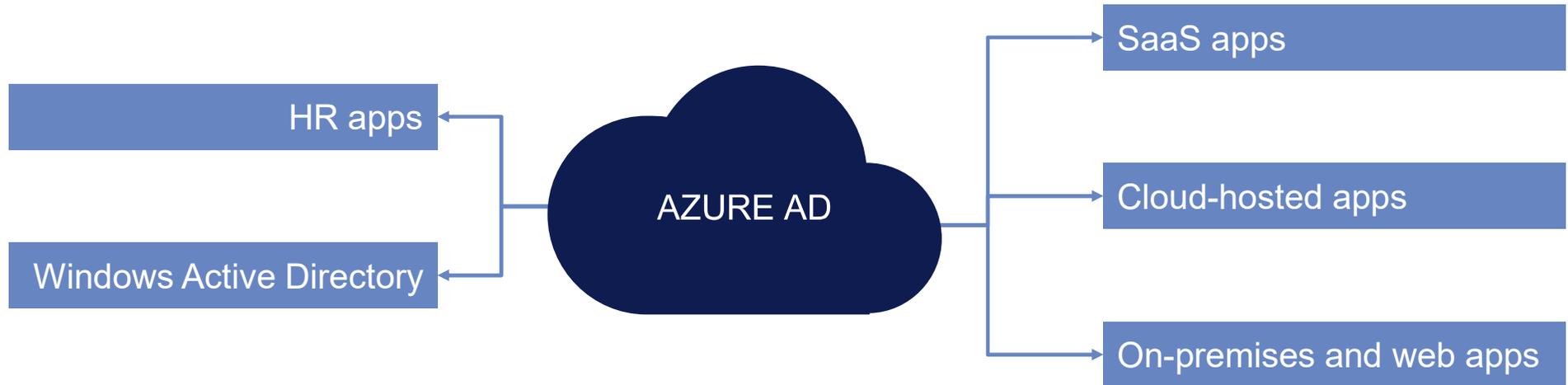
Visibility and control over blind spots

Connect to your existing solutions and gain a single consolidated view across your organization

Agile and efficient system

Natively integrate across the broader Cloud application ecosystem to deliver unique capabilities
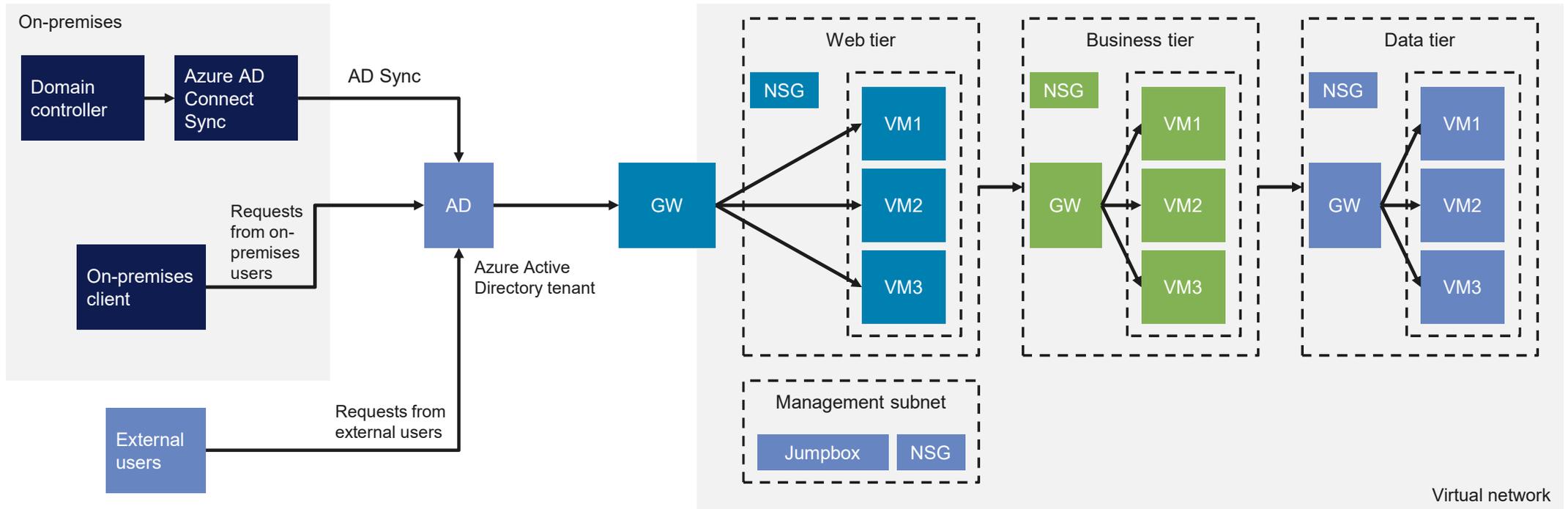
Zero trust protection against malicious attacks

Help drive zero trust objectives

Robust Ecosystem, Ready to Integrate With Your Existing Tools

Business Applications	zendesk cisco Webex SAP now ATLASSIAN Adobe
HR Management	successfactors An SAP Company workday. cornerstone
Secure Hybrid Access	CITRIX f5 zscaler Akamai
Password-less Authentication	yubico ensurity TECHNOLOGIES FEITIAN WE BUILD SECURITY IP IPification AUTHENTREND HID
Custom Authentication Factors	SECUREAUTH DUO Symantec VIP twilio PingIdentity. Entrust Datacard TRUSONA
Identity Governance	SAVIYNT Omada imprivata N8IDENTITY

Govern and Secure Your Users and Resources With Cloud Identity Services

On-premises

Domain controller

Azure AD Connect Sync

AD Sync

On-premises client

Requests from on-premises users

AD

Azure Active Directory tenant

GW

External users

Requests from external users

Web tier

NSG

VM1

VM2

VM3

Business tier

NSG

GW

VM1

VM2

VM3

Data tier

NSG

GW

VM1

VM2

VM3

Management subnet

Jumpbox   NSG

Virtual network

A pragmatic and phased deployment refines user experience, controls, governance and best practices in a mindful manner
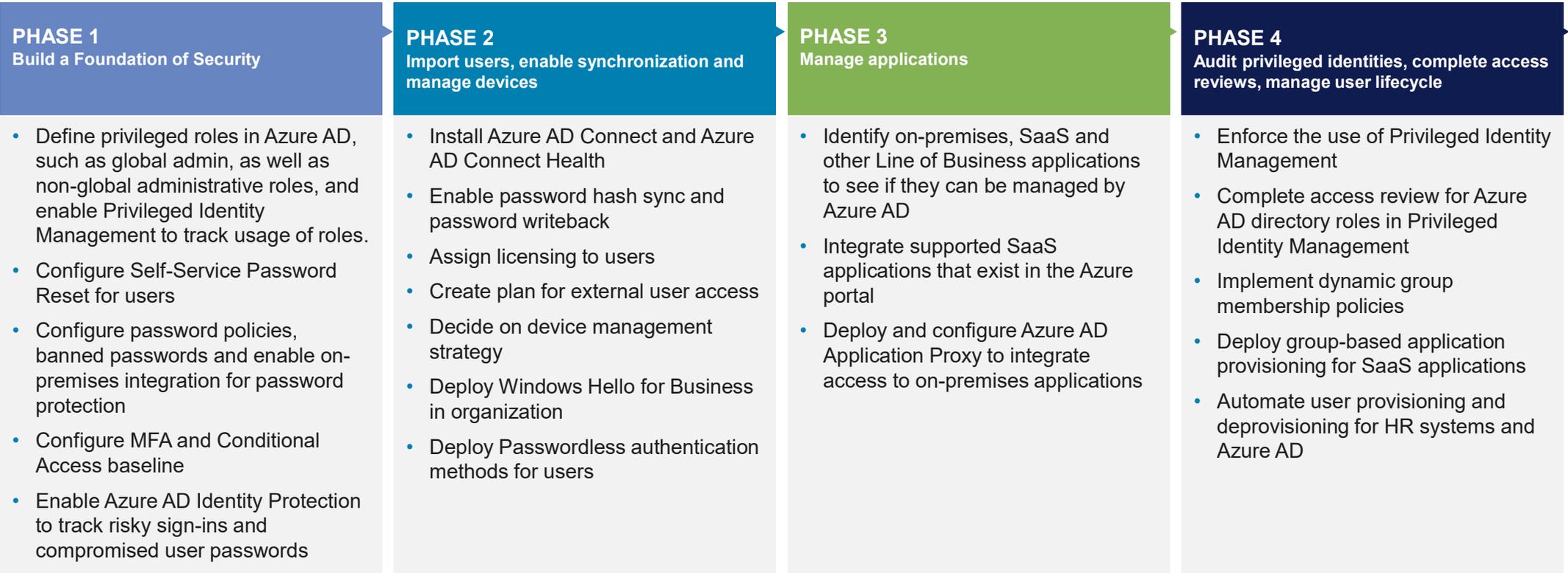
Azure AD Benefits

- Optimize costs
- Enable operational excellence
- Increase performance efficiency
- Improve reliability and user experience
- Enhance security and control

NTT DATA Digital Trusted Identity Services – Advisory Engagement Overview

Identity and Access Management Review

- Deliver an Identity workshop to identify elements of the existing Identity and Access Management (IAM) architecture.
- Discuss business concerns and requirements around identity.
- Output – IAM evaluation report and top-line objectives, concerns and requirements.

Intro to Azure Active Directory

- Review features and functionalities of Azure Active Directory (AD) and how these can be used to securely manage identities and assets
- Discuss how Azure AD capabilities can address your concerns and specific goals to accomplish
- Output - prioritized list of objectives

User Identity Provisioning

- Review current user provisioning process.
- Discuss options for provisioning and authenticating user identities in Azure AD, including Azure AD Connect, ADFS, and AD DS.
- Output - defined recommendations for managing identity provisioning and authentication options.

Deploy and Manage Devices

- Identify options and benefits of different device join scenarios, such as Azure AD Join and Hybrid Azure AD Join.
- Discuss Enterprise State Roaming and possible deployment options.
- Output - defined policies that meet your device management and data roaming requirements.

Driving Application Adoption

- Compare methods for delivering apps to end users via Azure AD.
- Discuss Single Sign On (SSO) and provisioning users into 3rd party apps.
- Review use of Azure AD authentication in building applications.
- Output – Identify key LOB apps that can leverage AAD SSO and implementation strategy.

Engage with External Users

- Determine use cases for external partners and customers requiring access to internal resources.
- Design options for B2B and B2C scenarios.
- Output - defined policies that meet customer data security and identity lifecycle manageability objectives.

Securing Identities

- Discuss use of self-service password reset, multifactor authentication, Conditional Access, Privileged Identity Management and Managed Identities in Azure AD to ensure security of user and admin accounts.
- Output - agree on a set of technical controls to design and implement for identity protection.

Design Guide

- Summarize the gathered intel, established parameters, configuration details and data.
- Output - a design guide, architectural diagram and an implementation plan combining your requirements and NTT DATA best practices.

Overview of the NTT DATA Digital Trusted Identity Services Implementation Phases

PHASE 1 Build a Foundation of Security	PHASE 2 Import users, enable synchronization and manage devices	PHASE 3 Manage applications	PHASE 4 Audit privileged identities, complete access reviews, manage user lifecycle
• Define privileged roles in Azure AD, such as global admin, as well as non-global administrative roles, and enable Privileged Identity Management to track usage of roles.	• Install Azure AD Connect and Azure AD Connect Health	• Identify on-premises, SaaS and other Line of Business applications to see if they can be managed by Azure AD	• Enforce the use of Privileged Identity Management
• Configure Self-Service Password Reset for users	• Enable password hash sync and password writeback	• Integrate supported SaaS applications that exist in the Azure portal	• Complete access review for Azure AD directory roles in Privileged Identity Management
• Configure password policies, banned passwords and enable on-premises integration for password protection	• Assign licensing to users • Create plan for external user access • Decide on device management strategy	• Deploy and configure Azure AD Application Proxy to integrate access to on-premises applications	• Implement dynamic group membership policies • Deploy group-based application provisioning for SaaS applications
• Configure MFA and Conditional Access baseline	• Deploy Windows Hello for Business in organization		• Automate user provisioning and deprovisioning for HR systems and Azure AD
• Enable Azure AD Identity Protection to track risky sign-ins and compromised user passwords	• Deploy Passwordless authentication methods for users		

Enabling Controls
Assess usage and performance patterns from the captured alerts established during the preceding phases to validate the controls meet the objectives. Configure governance controls based on required modifications as indicated during the testing process.

NTT DATA Digital Trusted Identity Services Managed Services

Operational Support

Operational support to ensure Azure Active Directory is operating efficiently. We monitor for threats and provide remediation to help mitigate exposure to risk.

- Maintain Azure AD Connect servers and ADFS infrastructure
- Regularly execute and triage IdFix reports, ensuring healthy directory synchronizations
- Triage Azure AD Connect Health Alerts for Sync and ADFS
- Manage user identities, including:
  - » Group memberships
  - » Assignment of licenses
  - » Assign users to enterprise applications
  - » CRUD (create, read, update, delete) operations
  - » Manage access by external users
- Manage device joins and removal from Azure AD or Hybrid Azure AD
- Configure Conditional Access policies
- Monitor authentication logs for anomalies or login problems on:
  - » Azure AD App Proxy Connectors
  - » Passthrough Auth Agents
  - » Password Writeback Service
  - » On-premises password protection gateway

Optimization Support

Continual improvement efforts to consistently improve the client's security posture

On a monthly basis:
- Drive improvements to Identity Secure Score
- Manage lifecycle of SSO config for Azure AD
- Triage and investigate security and risk events
- Review and design catalogs and access packages for applications and resources
- Assign users to access packages in line with security policies
- Review approval workflows regularly to ensure the proper approvers are included
- Design and implement Conditional Access policies, if applicable

On a quarterly basis, review:
- Provisioned enterprise applications
- Access to directory by external identities
- Who has been granted access to privileged roles
- Steps for defining security gates for activation of privileged roles
- Consent grants to applications

Audit Support

Support client-let audit preparations for compliance or security program-related efforts

Audit assistance on up to a biannual basis. Such tasks may include:
- Review proper application of technical compliance controls in of Azure AD if customer is subject to regulation
- Ensure Azure AD audit logs, including sign-in activity and risk events are being archived to a SIEM for historical reference
- Export data from Azure AD upon request
- Off-band reporting per client-directed requirements

Why Partner With NTT DATA

Gold
Microsoft Partner
Azure Expert MSP

Gold Cloud Platform
SAP on Azure Advanced Specialization

Microsoft

A **Leader** in cyber resiliency (security consulting, strategy, incident response and business continuity)

NelsonHall, "NEAT report for Cyber Resiliency," June 6, 2019

Regulatory and Industry Compliance and Certifications

A **Leader** in the Gartner Magic Quadrant for Application Security Testing

Gartner, Inc. Magic Quadrant for Application Security Testing, April 29, 2020

- Microsoft Azure Expert MSP
- SAP on Azure Advanced Specialization
- 12 Gold Competencies, 4 Silver
- NTT & Microsoft Strategic Alliance
- CSA Corporate Member
- CNCF Silver member

- **3,500** cloud architects and engineers
- **500+** cloud clients
- **5,000+** cloud migrations
- **420+** Azure certifications
- **4,300** experts on Microsoft technologies

3,000+ security experts

6.1+ trillion logs analyzed annually

9 SOCs and **7** RandD centers

6.2 billion attacks defended annually

150+ million identities managed

A **Leader** in public cloud transformation, globally

ISG, "Provider Lens Quadrant Report for Cloud Transformation/Operation Services and XaaS 2020," November 2019

Application Modernization:

- **9,500** app clients, globally
- **1,000+** DevOps build and release (CI/CD) engineers
- **200+** Agile certified resources