SOITRON
INSPIRÁRIUM

MODERNÍ DATOVÁ CENTRA

16. 3. 2022
9:00 - 10:30 hod.

- Čekáme na všechny účastníky. Začínáme v **9.05 hod**.
- Celý webinář bude nahráván
- Mikrofony jsou po dobu prezentace vypnuté (Mute)
- Dotazy můžete pokládat v průběhu prezentace pomocí **Q & A** (otázky a odpovědi)

CISCO Partner
Gold Certified

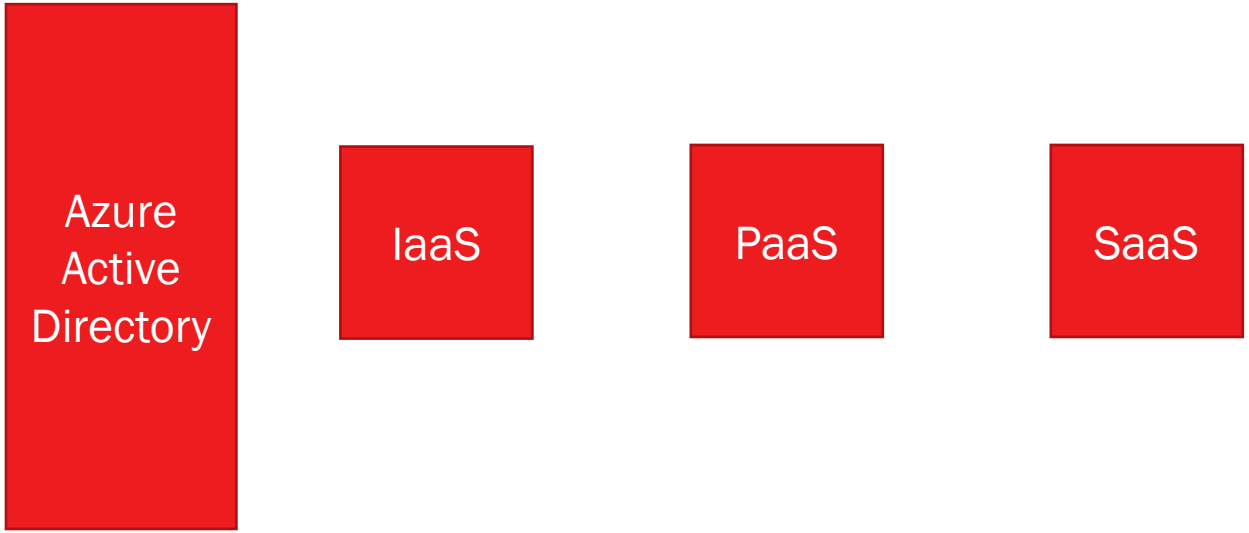
AGENDA – HYBRIDNÍ DATOVÁ CENTRA – ARCHITEKTURA / SPRÁVA A BEZPEČNOST 16.3.2022

- Architektura datových center (20 min)
  - Azure
  - Onprem datové centrum - nepřipravené a jeho nástrahy
  - Cloudifikované datové centrum (Azure Stack, HCI...)
- Přechod k hybridním scénářům (20 min)
  - SMB prostředí
  - Enterprise prostředí
  - Propojení datové vrstvy
- Management prostředí – live ukázky (20 minut)
  - Azure
  - Intersight
- Bezpečnost datových center (15 minut)
  - Azure governance
  - Zero Trust Model
- Vaše otázky ?

Architektura datových center

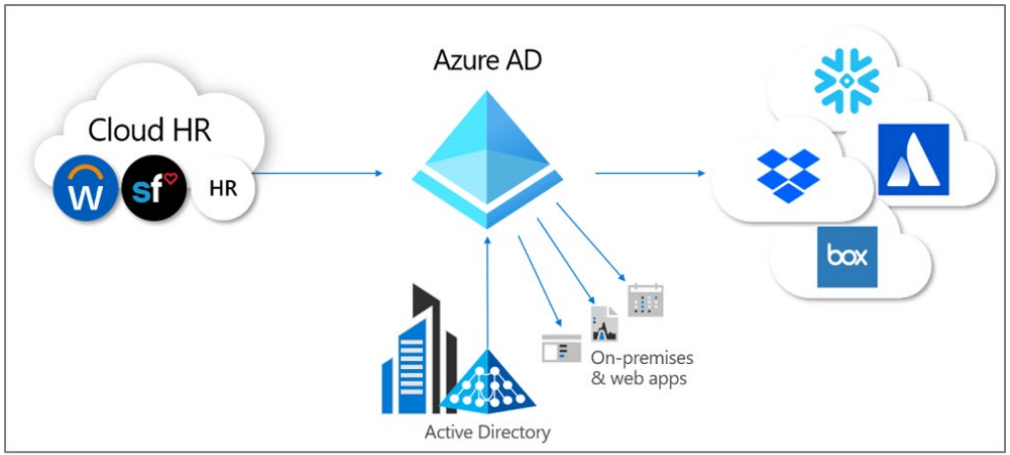
Azure

AZURE

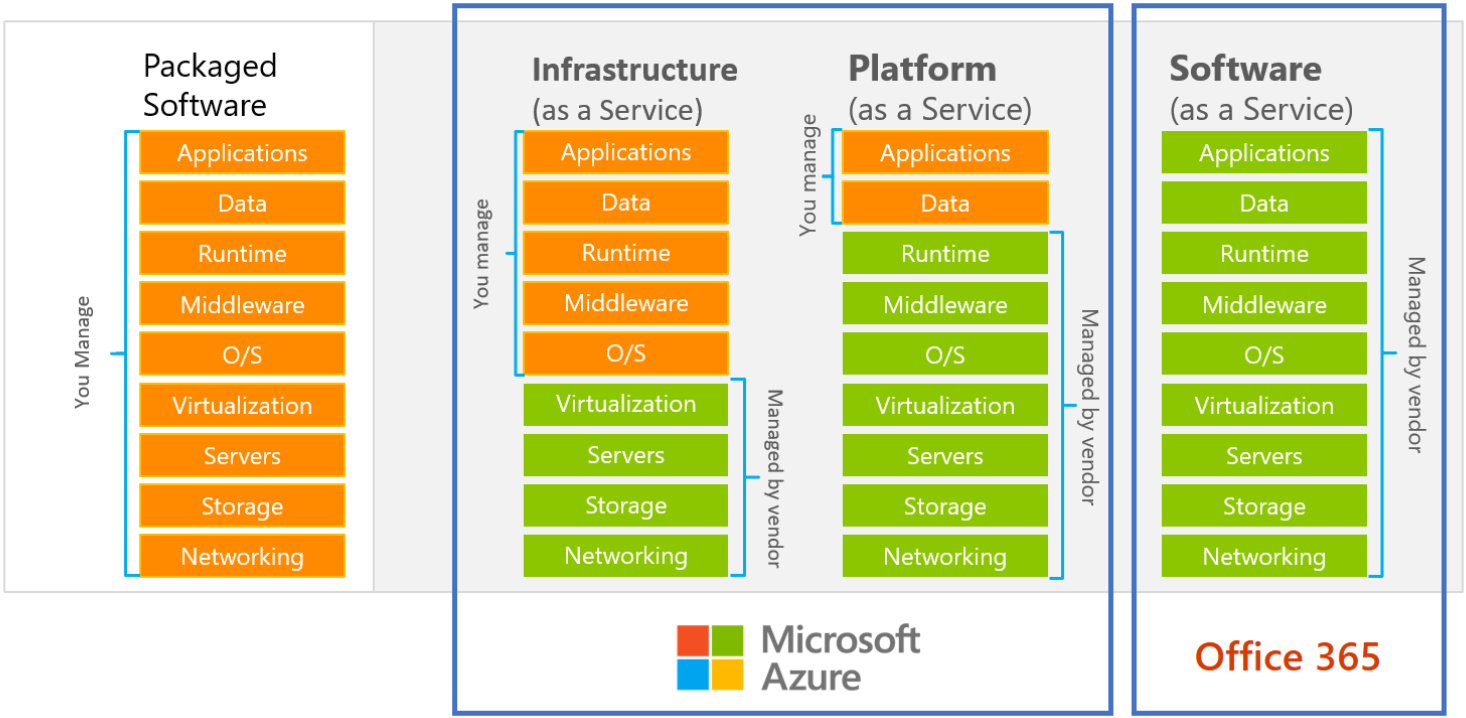


AZURE - AAD

- Čo je Azure Active Directory ?
- Dokáže nahradiť naše lokálne Active Directory ?
- Možnosti
  - Active Directory Domain Services
  - Active Directory
- Dôležité
  - Licenčný model
  - Aké benefity ponúka



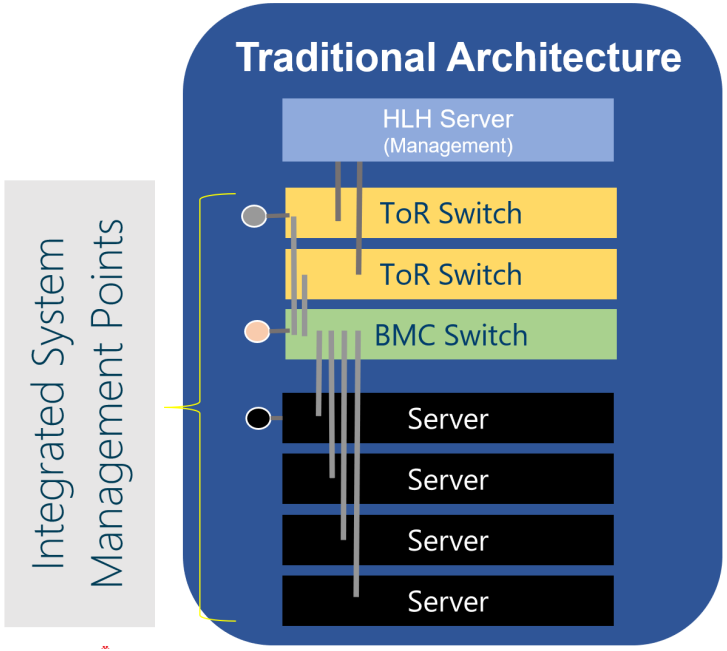
AZURE – IAAS, SAAS, PAAS



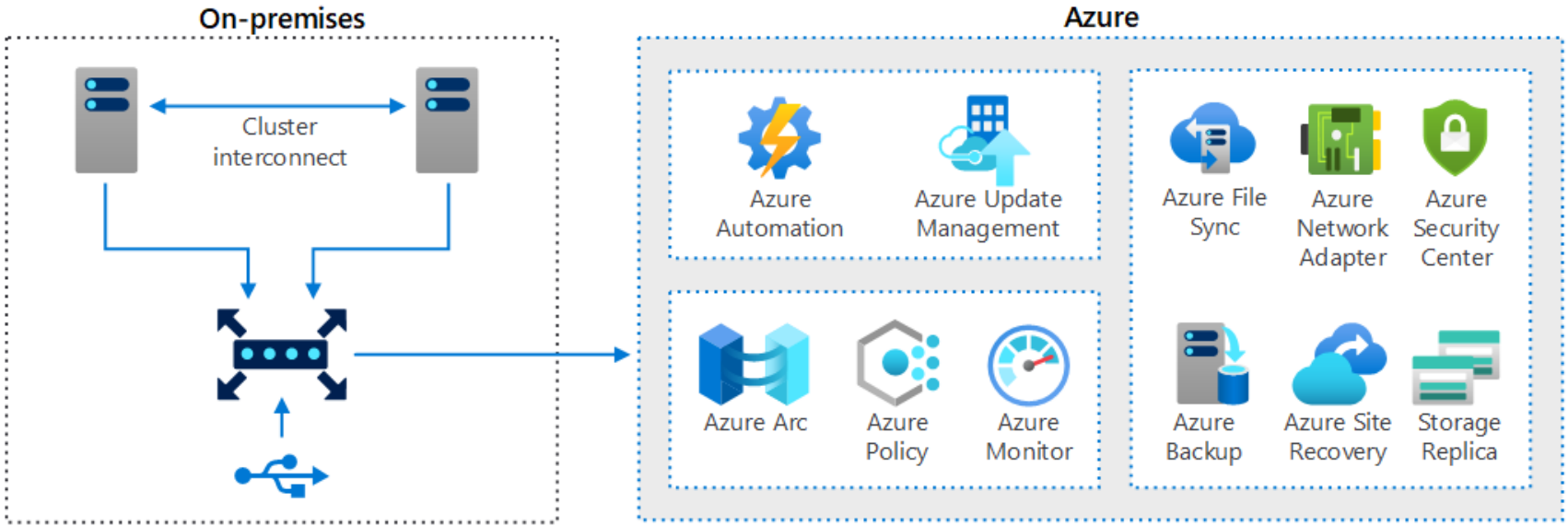
Onprem datové centrum

ONPREM DATOVÉ CENTRUM

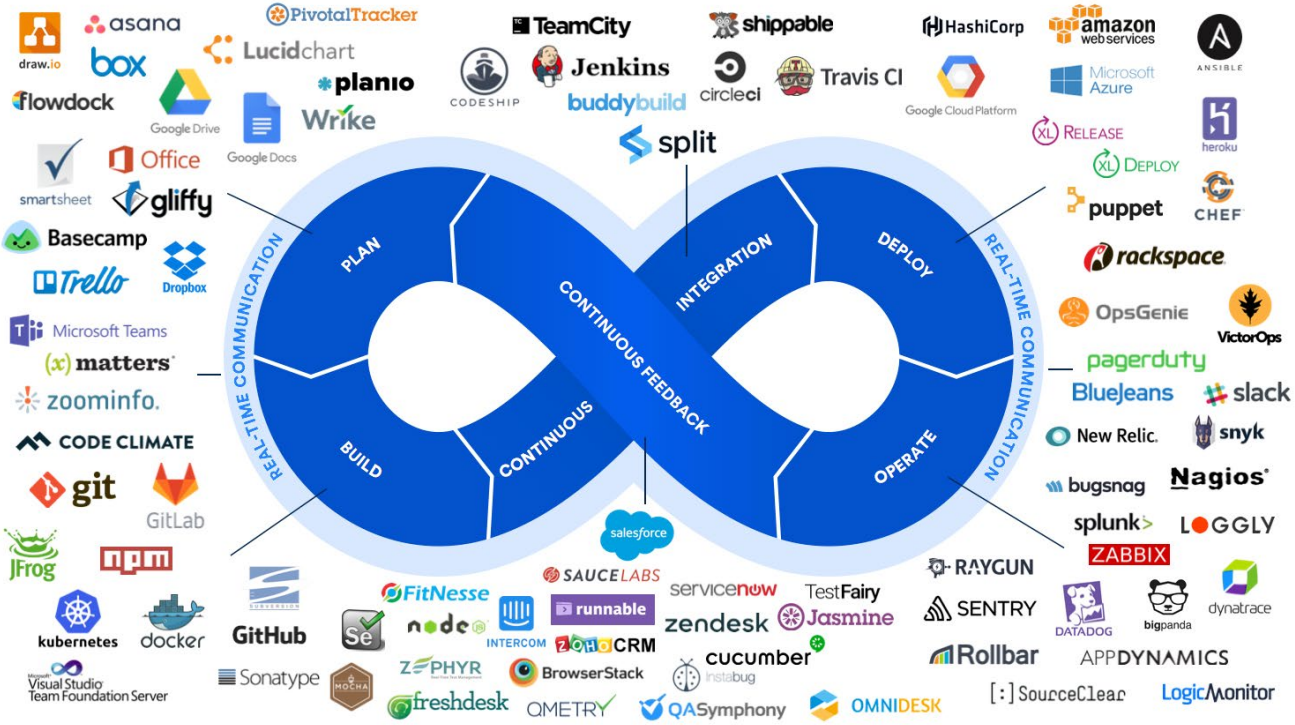
- Klasická infrastruktura ....



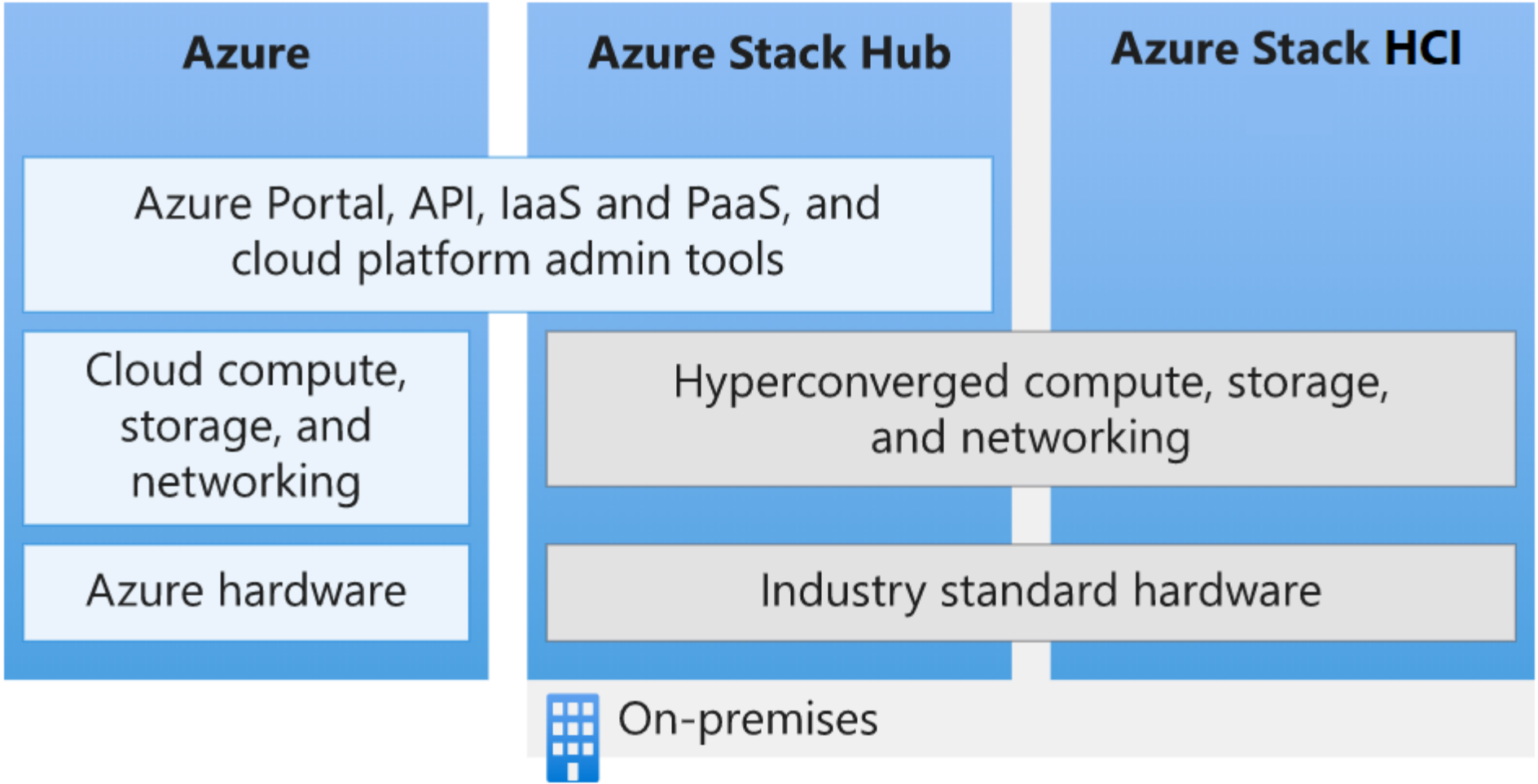
CLOUDIFIKOVANÉ DATOVÉ CENTRUM – HCI



CLOUDIFIKOVANÉ DATOVÉ CENTRUM – ŽIVOTNÍ CYKLUS

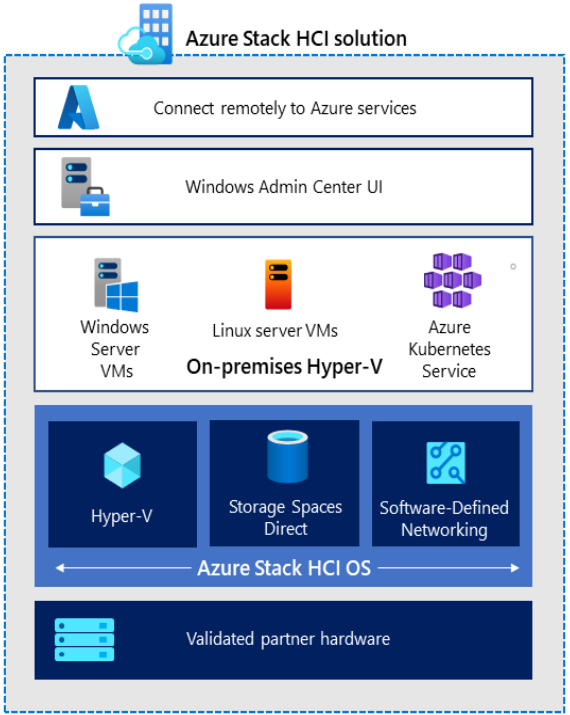


Azure Stack a HCI


Azure
Azure Stack Hub
Azure Stack HCI
Azure Portal, API, IaaS and PaaS, and cloud platform admin tools
Cloud compute, storage, and networking
Hyperconverged compute, storage, and networking
Azure hardware
Industry standard hardware
On-premises

AZURE HCI – HYPERKONVERGOVANÁ INFRAŠTRUKTÚRA

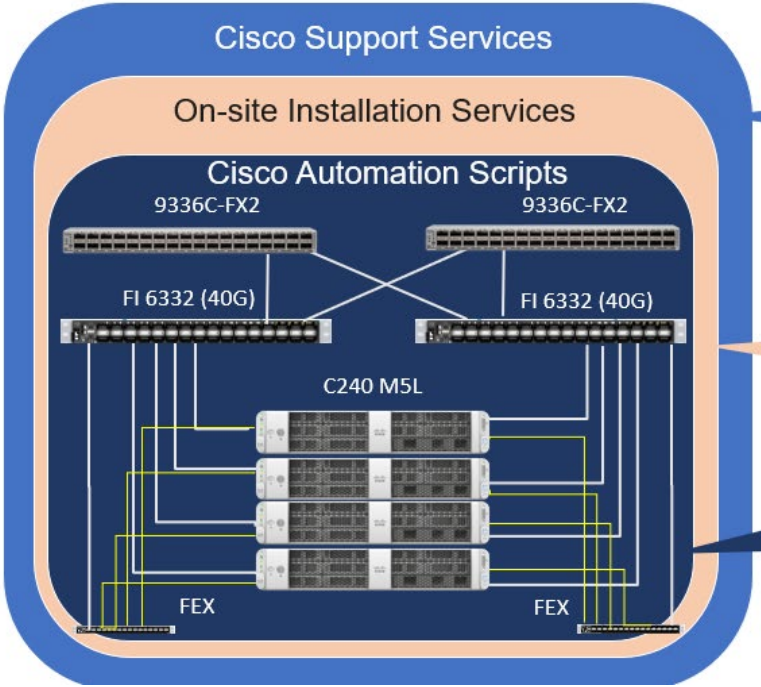
- Azure HCI vyžaduje permanentné pripojenie do Azure
- Po úvodnej inštalácii prebieha registrácia voči Azure (do 30 dní)



HW PRE AZURE STACK

- Inštalácia prebiaha na certfikovanom HW spoločnosti
- Zoznam společnosti
  - Cisco
  - Dell
  - HPE
  - Lenovo
- Aktualizácie prebiehajú na dvoch úrovniach
  - HW
  - Azure Stack
- Podpora je dostupná od
  - OEM vendor
  - Microsoft

AZURE STACK HUB



- Cisco/Microsoft poskytuje support

- Příprava a instalace Azure Stacku
- Integrace do prostředí Active direktory, Azure services
- Billing v prostředí Azure

- Service Profile Template Driven
- Automatizace nastavování služeb
- Snížení času deploymentu z hodin na minuty

AZURE STACK HUB - MODEL ZAPOJENIA

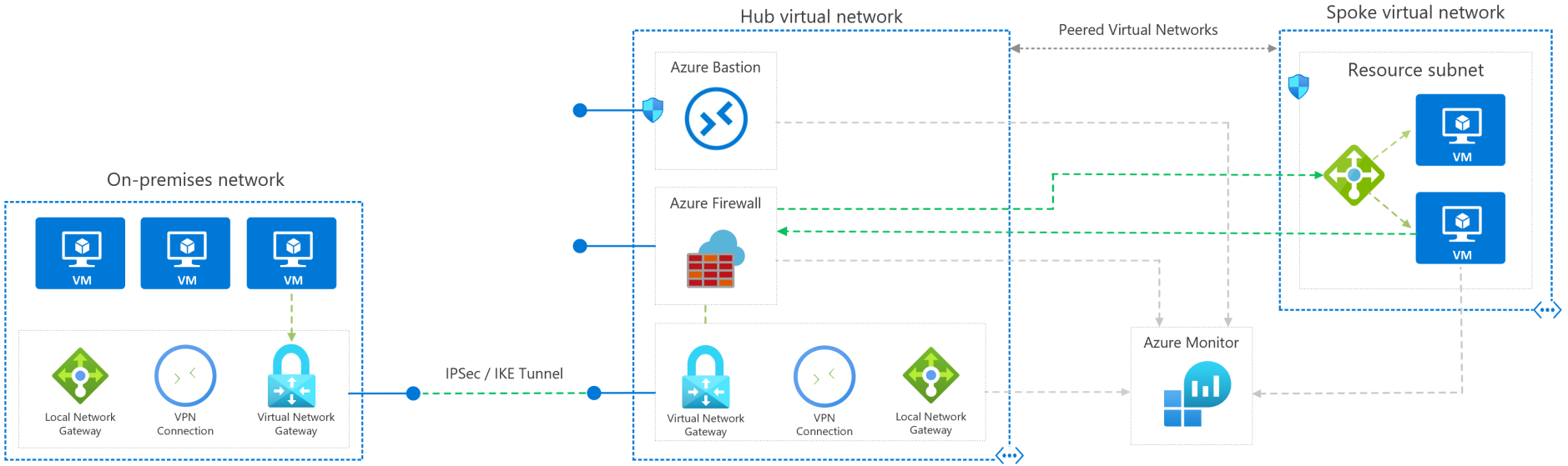
- Connected
  - 99,9% zapojeni
- Disconnected
  - Obmedzeni funkcionalit
  - Motivacia pre model zapojenia „Disconnected“
    - Spoločnosť so striktními bezpečnostními pravidlami
    - Latencia
    - Dat nesmú byť posielané do Azure
- Identity
  - AAD
  - ADFS

Přechod k hybridním scénářům

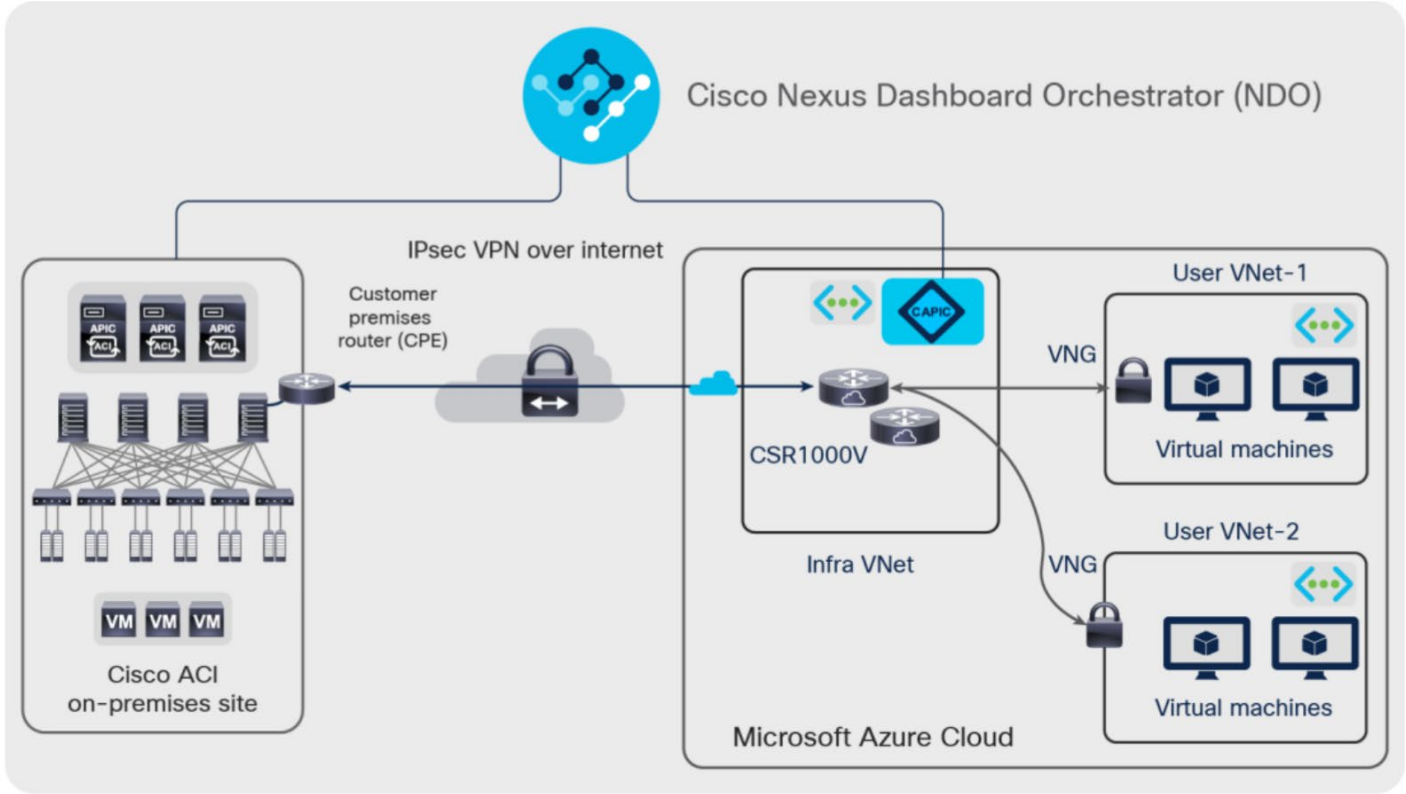
SMB PROSTREDIE

- Identifikovanie očakávaní
  - Zníženie nákladov
  - Zefektívnenie prevádzkovaných služieb
  - Zvýšenie bezpečnosti
  - iné
- Cieľ migrácie
  - Infraštruktúra
  - Aplikácie
- Plán
- Testovanie
- Migrácia

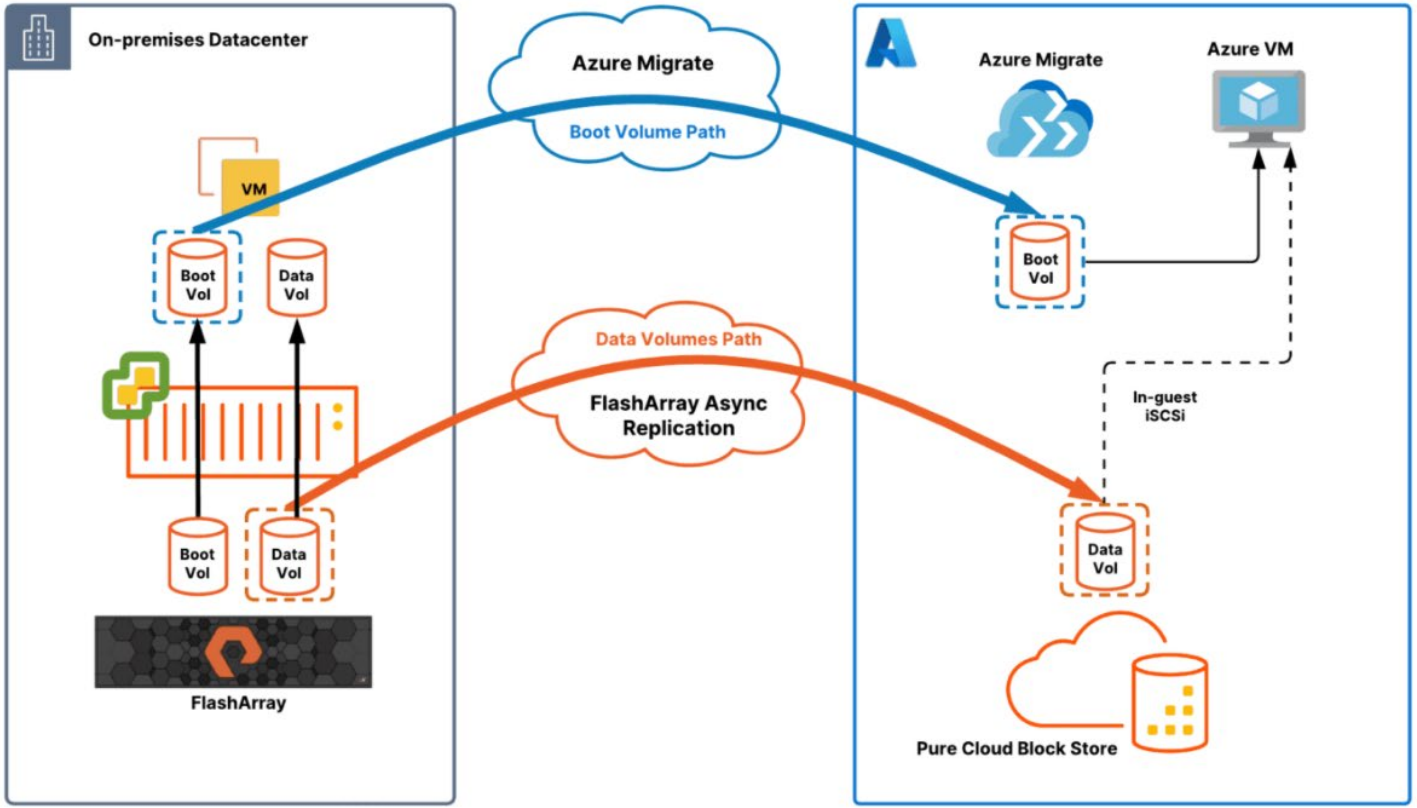
SMB PROSTREDIE



ENTERPRISE PROSTŘEDÍ

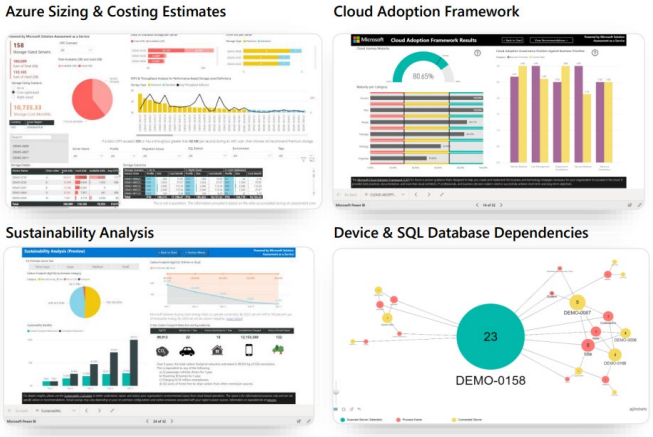


PROPOJENÍ DATOVÉ VRSTVY



ANALÝZA SOUČASNÉHO STAVU

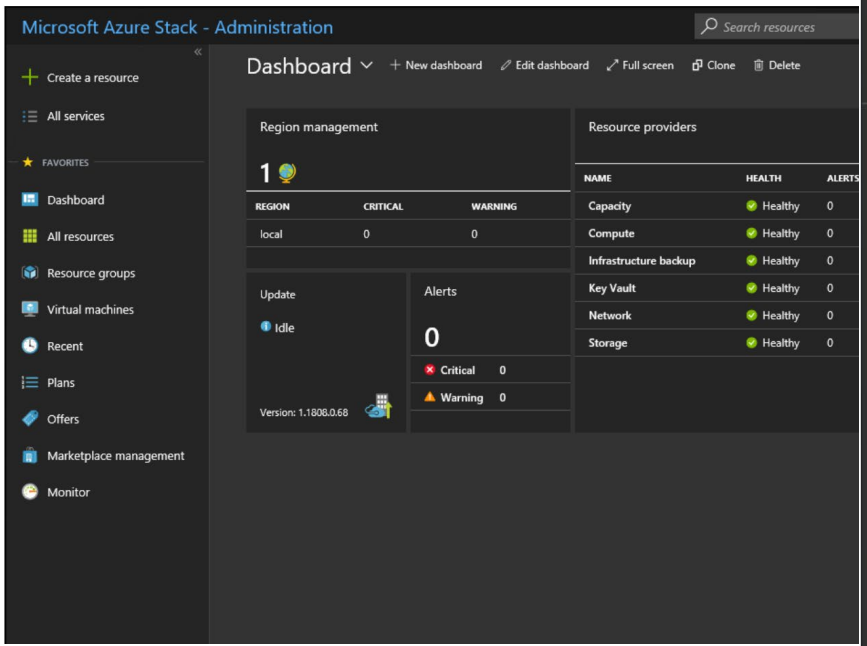
- Typy analýzy
  - Infrastructure & Database (3- 6 týdnů)
  - Modern work (2 týdny)
  - Security (2 týdny)
  - Application Modernization (1 týden)
  - Azure Foundation (3 - 4 týdny)

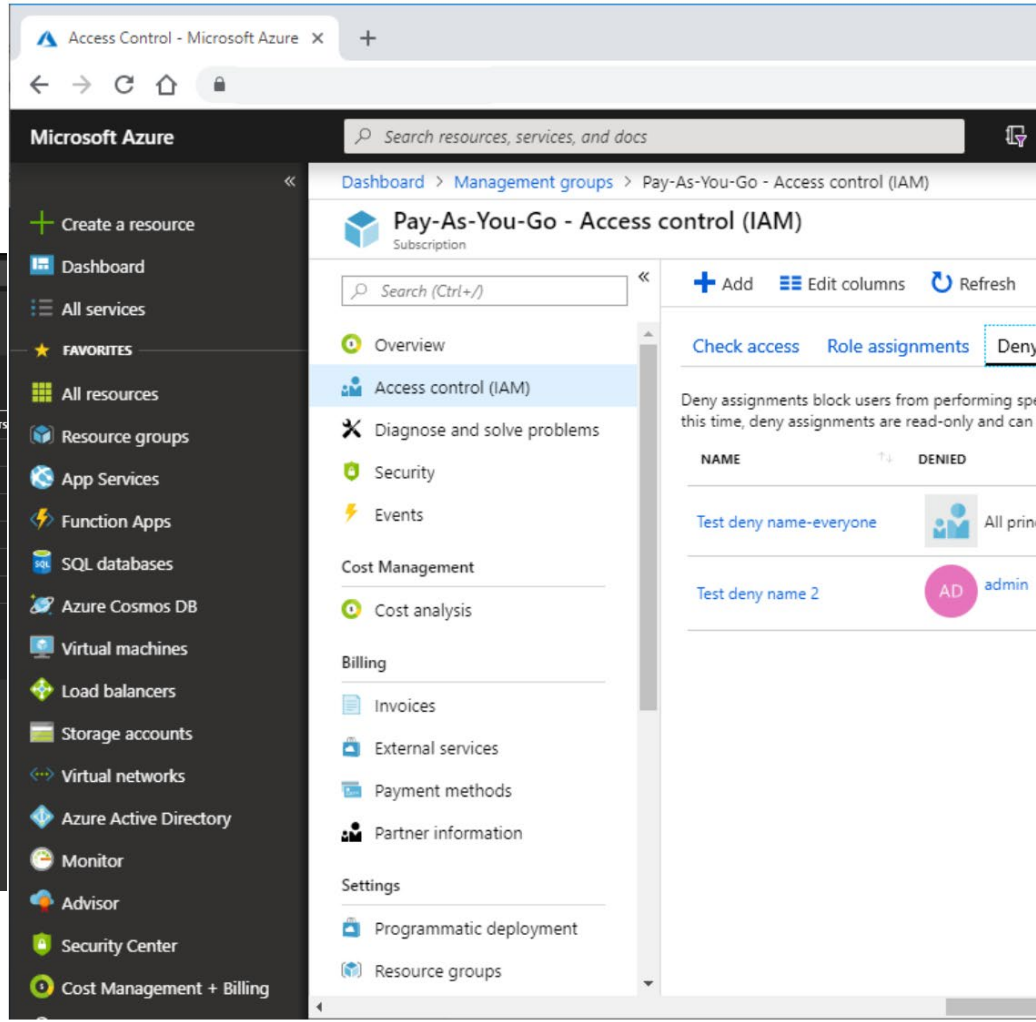


- Průběh analýzy
  - Na společné schůzce zjistíme vaše očekávání a potřeby.
  - Dohodneme vše potřebné a nasadíme analytický nástroj.
  - Vyhodnotíme získaná data.
  - Představíme výsledky včetně doporučení oblastí, které lze optimalizovat.
  - Celková doba trvání analýzy je 3 - 4 týdny

Management – live ukázky

AZURE A AZURE STACK HUB

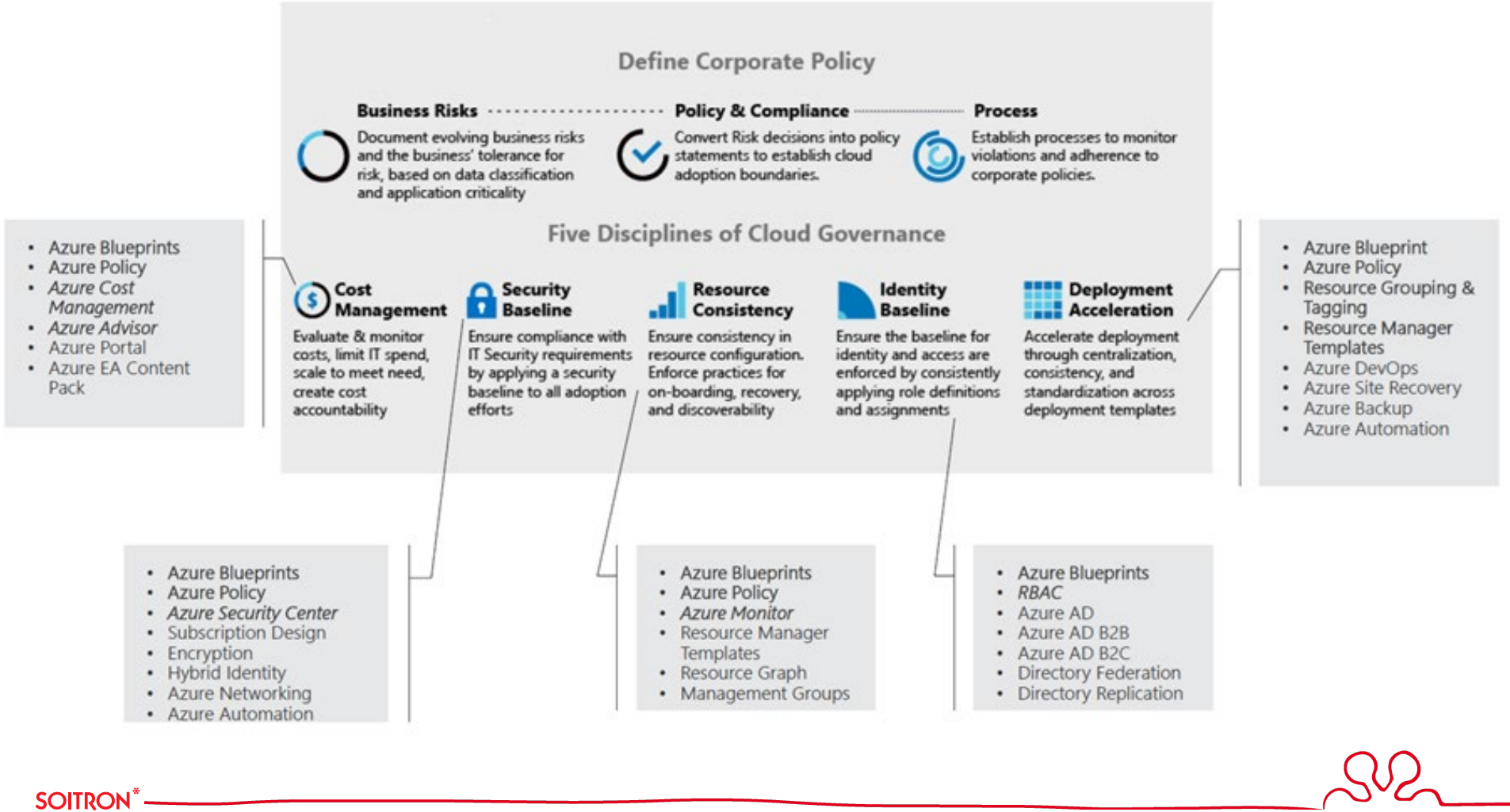




Bezpečnost datových center

AZURE GOVERNANCE

- Zásady správného řízení v cloudu představují iterativní process
- Poskytují mechanismy a postupy pro zajištění kontroly nad vašimi aplikacemi a prostředky v cloudu
- Zásady správného řízení v Azure jsou primárně implementované pomocí dvou služeb:
  - Azure Policy umožňuje vytvářet, přiřazovat a spravovat definice zásad k vynucení pravidel pro vaše prostředky. Tato funkce udržuje tyto prostředky v souladu s vašimi podnikovými standardy.
  - Azure Cost Management umožňuje sledovat využití cloudu a výdaje pro vaše prostředky v cloudu.
- Cost Management – náklady na cloudové služby
- Security Baseline – zajišťuje konzistentní aplikování technických požadavků na bezpečnost
- Identity Baseline – doplňují security baseline o konzistentní aplikování požadavků na autentizaci a autorizaci
- Resource Consistency – zajišťuje konzistentní konfiguraci prostředků v cloudu
- Deployment Acceleration – definuje zásady správného řízení konfigurace nebo nasazení prostředků v cloudu


Define Corporate Policy
Business Risks
Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality
Policy & Compliance
Convert Risk decisions into policy statements to establish cloud adoption boundaries.
Process
Establish processes to monitor violations and adherence to corporate policies.
Five Disciplines of Cloud Governance
Cost Management
Evaluate & monitor costs, limit IT spend, scale to meet need, create cost accountability
Security Baseline
Ensure compliance with IT Security requirements by applying a security baseline to all adoption efforts
Resource Consistency
Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability
Identity Baseline
Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments
Deployment Acceleration
Accelerate deployment through centralization, consistency, and standardization across deployment templates
Azure Blueprints
Azure Policy
Azure Cost Management
Azure Advisor
Azure Portal
Azure EA Content Pack
Azure Blueprint
Azure Policy
Resource Grouping & Tagging
Resource Manager Templates
Azure DevOps
Azure Site Recovery
Azure Backup
Azure Automation
Azure Blueprints
Azure Policy
Azure Security Center
Subscription Design
Encryption
Hybrid Identity
Azure Networking
Azure Automation
Azure Blueprints
Azure Policy
Azure Monitor
Resource Manager Templates
Resource Graph
Management Groups
Azure Blueprints
RBAC
Azure AD
Azure AD B2B
Azure AD B2C
Directory Federation
Directory Replication

ZERO TRUST MODEL

- Zero Trust architektura je soubor paradigmat kybernetické bezpečnosti, která posouvají statickou ochranu založenou na sítích a perimetrech směrem na uživatele, aktiva a zdroje.
- Architektura je založena na základě zásady „nikdy nedůvěřujte, vždy ověřujte a autorizujte“
  - Autorizace na základě dostupných dat včetně identity uživatele, lokality, zdraví zařízení, klasifikaci dat atp.
  - Použití principu Least Privilege Access
  - Omezení přístupu uživatelů pomocí Just In Time / Just Enough (JIT/JEA) a adaptivní politiky založené na riziku a ochraně dat.
  - Detekování a analýza hrozeb
- NIST SP 800-207
- CIS Benchmarks™
- The Comprehensive Playbook for Implementing Zero Trust Security
- Zero Trust Maturity Assessment Tool (https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool)

ZERO TRUST MATURITY ASSESSMENT TOOL REPORT

Implement multifactor authentication.

1. Multifactor authentication helps protect your applications by requiring users to confirm their identity using a second source of validation, such as a phone or token, before access is granted.
2. Azure Active Directory (Azure AD) can help you enable multifactor authentication for free.
3. Already have Azure AD? Start deploying today.

Enable passwordless authentication.

1. Passwordless authentication methods such as Windows Hello and Microsoft Authenticator provide a simpler and more secure authentication experience across the web and mobile devices. Based on the recently developed FIDO2 standard, these methods allow users to authenticate easily and securely without requiring a password.
2. Microsoft can help you adopt passwordless authentication today. Download the passwordless authentication datasheet to learn more.
3. If you already have Azure Active Directory (Azure AD), see how you can enable passwordless authentication today.

Implement single sign-on (SSO).

1. SSO not only strengthens security by removing the need to manage multiple credentials for the same person but also delivers a better user experience with fewer sign-in prompts.
2. Microsoft Azure Active Directory (Azure AD) provides an SSO experience to popular software as a service (SaaS) apps, on-premises apps, and custom-built apps that reside on any cloud for any user type and any identity.
3. Plan your SSO deployment.

Block legacy authentication.

1. One of the most common attack vectors for malicious actors is to use stolen or replayed credentials against legacy protocols, such as SMTP, that can't use modern security challenges.
2. Conditional access in Azure AD can help you block legacy authentication. See more information about Block Legacy Authentication.

Protect identities against compromise.

1. Real-time risk assessments can help protect against identity compromise at the time of login and during sessions.
2. Azure Identity Protection delivers real-time continuous detection, automated remediation, and connected intelligence to investigate risky users and sign-ins to address potential vulnerabilities.
3. Enable Identity Protection to get started. Bring in user session data from Microsoft Cloud App Security to enrich Azure AD with possible risky user behavior after they were authenticated.

Enrich your Identity and Access Management (IAM) solution with more data.

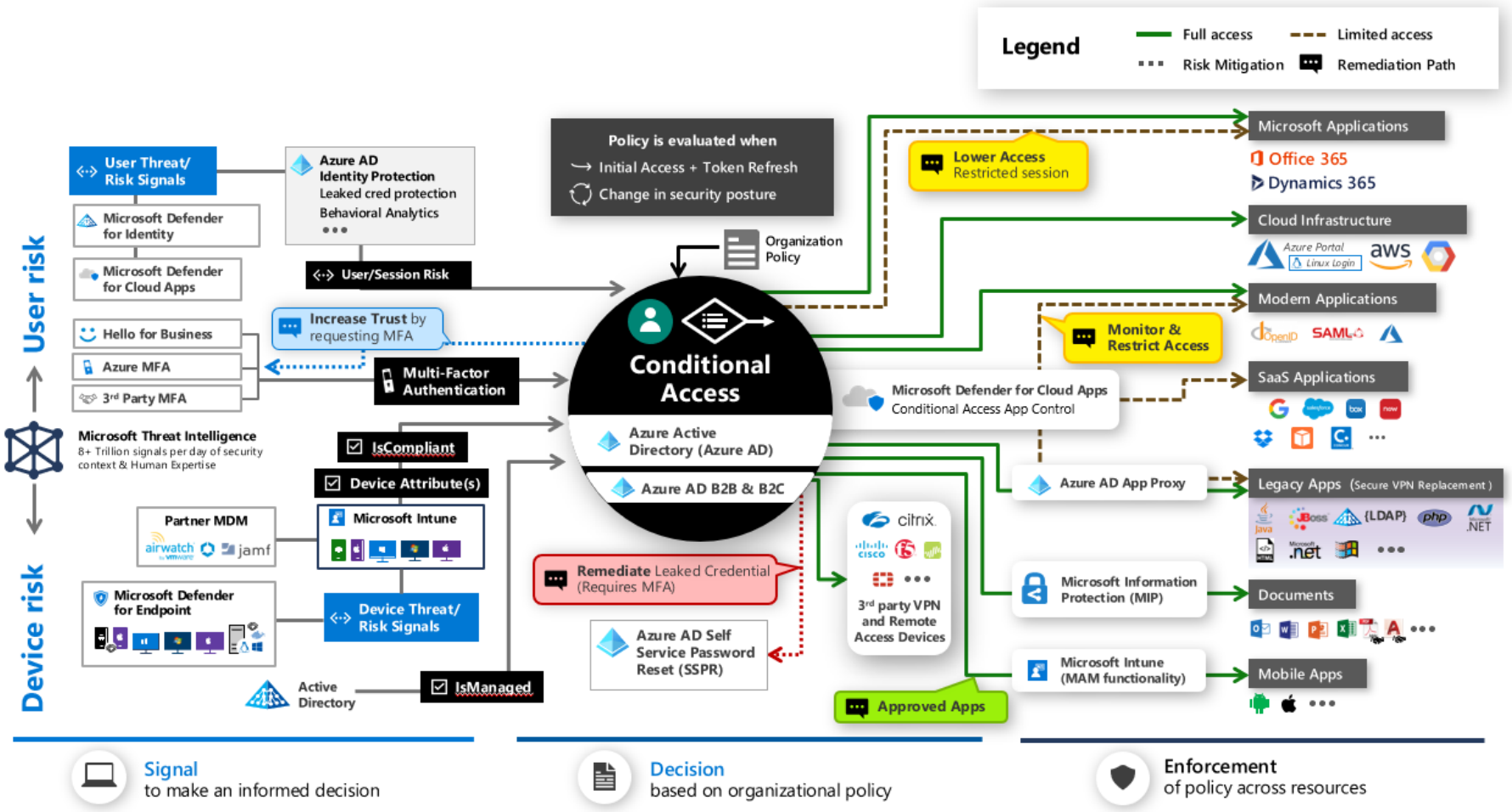
1. The more data you feed your IAM solution, the more you can improve your security posture with granular access decisions and better visibility into users accessing corporate resources, and the more you can tailor the end-user experience.
2. Azure Active Directory (Azure AD), Microsoft Cloud App Security, and Microsoft Defender for Endpoint all work together to provide enriched signal processing for better decision making.
3. Configure Conditional Access in Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Cloud App Security.

Fine-tune your access policies.

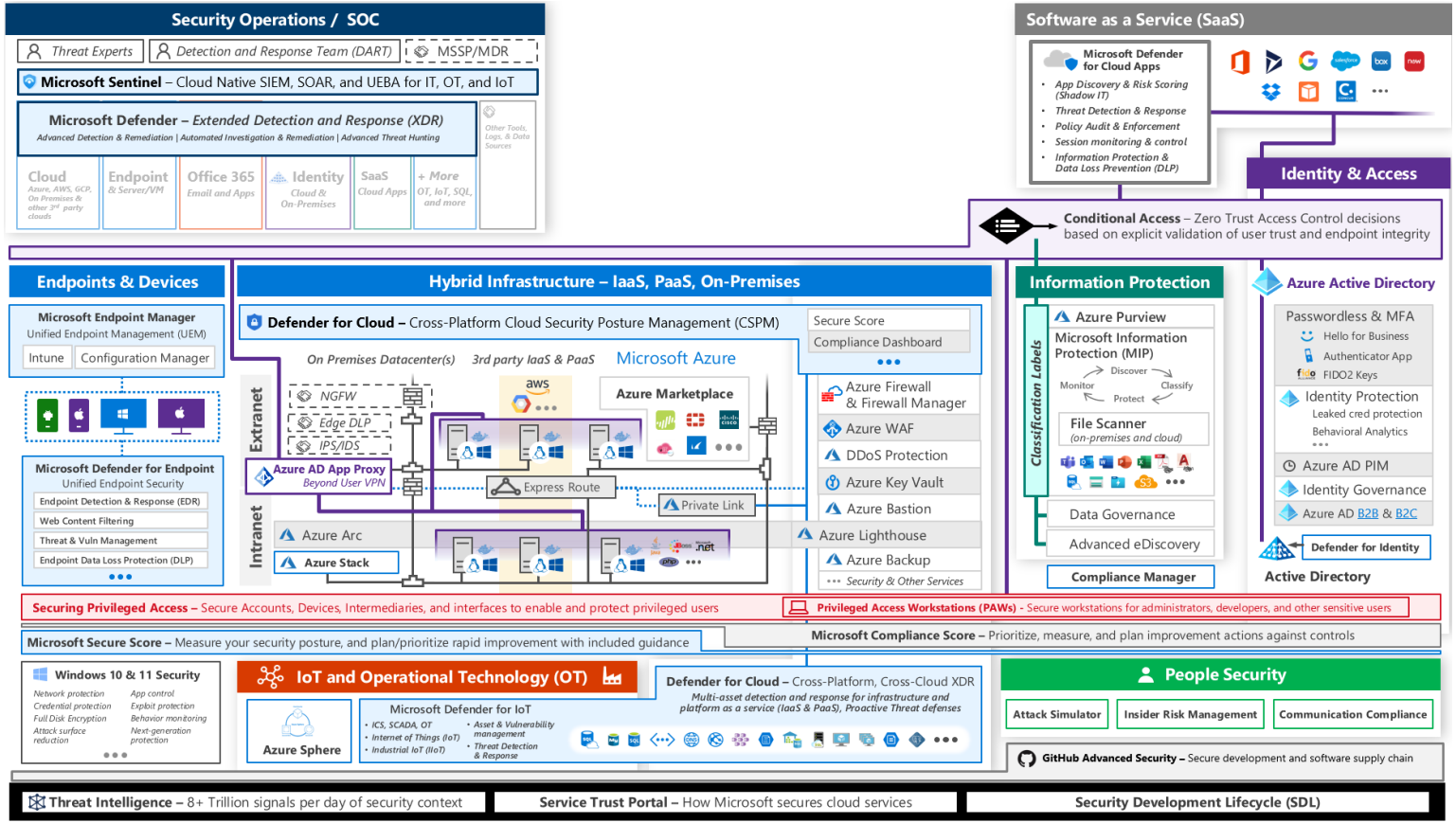
1. Enforce granular access control with risk-based adaptive access policies that integrate across endpoints, apps, and networks to better protect your data.
2. Conditional Access in Azure AD enables you to enforce fine-tuned adaptive access controls, such as requiring multi-factor authentication, based upon user context, device, location, and session risk information.
3. Fine-tune your Conditional Access policies.

Improve your identity security posture.

1. The identity secure score in Azure AD helps you assess your identity security posture by analyzing how well your environment aligns with Microsoft best-practice recommendations for security.
2. Get your identity secure score


Legend
Full access
Limited access
Risk Mitigation
Remediation Path
User risk
Device risk
User Threat/ Risk Signals
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
User/Session Risk
Hello for Business
Azure MFA
3rd Party MFA
Increase Trust by requesting MFA
Multi-Factor Authentication
Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise
IsCompliant
Device Attribute(s)
Partner MDM
Microsoft Intune
Microsoft Defender for Endpoint
Device Threat/ Risk Signals
Active Directory
IsManaged
Policy is evaluated when
Initial Access + Token Refresh
Change in security posture
Organization Policy
Conditional Access
Azure Active Directory (Azure AD)
Azure AD B2B & B2C
Remediate Leaked Credential (Requires MFA)
Azure AD Self Service Password Reset (SSPR)
Lower Access
Restricted session
Monitor & Restrict Access
Microsoft Defender for Cloud Apps
Conditional Access App Control
Azure AD App Proxy
citrix
3rd party VPN and Remote Access Devices
Approved Apps
Microsoft Applications
Office 365
Dynamics 365
Cloud Infrastructure
Azure Portal
Linux Login
aws
Modern Applications
SaaS Applications
Legacy Apps (Secure VPN Replacement)
Microsoft Information Protection (MIP)
Documents
Microsoft Intune (MAM functionality)
Mobile Apps
Signal
to make an informed decision
Decision
based on organizational policy
Enforcement
of policy across resources

REFERENČNÍ ARCHITEKTURA KYBERNETICKÉ BEZPEČNOSTI V CLOUDU



OTÁZKY?

KONTAKTY

Soitron s.r.o.

Pekařská 621/7

155 00 Praha 5

tel.: +420 266 199 918

e-mail: info@soitron.cz
web: www.soitron.com

SOITRON*