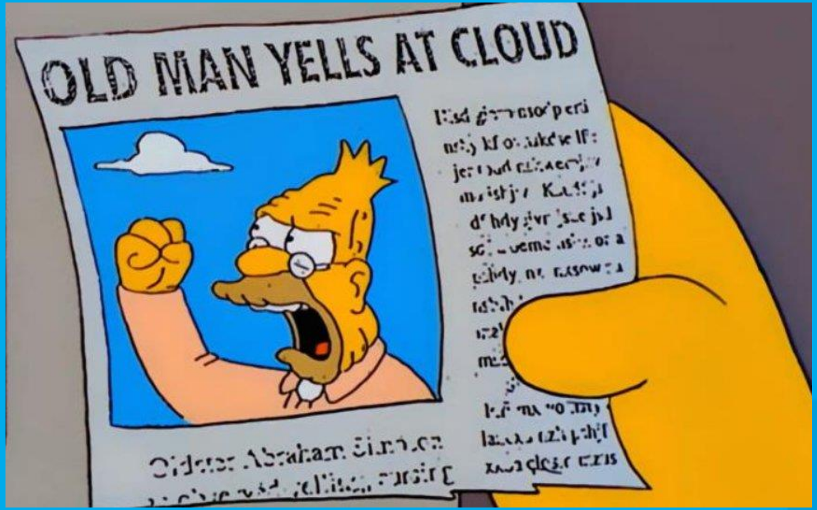
Securing Azure Services The Right Way

Dimitar Grozdanov



Azure Saturday 2019

macedonian.net user group

azuresaturday.mk

Sponsors

HASELT

MCA

SORSIX

INTERWORKS®

Symphony Solutions

netcetera
Software matters

seavus®

iBORN

Supporters

Swarmtix

IT.mk

Cloud security is a shared responsibility

MICROSOFT'S COMMITMENT

Securing and managing the cloud foundation

- Physical assets
- Datacenter operations
- Cloud infrastructure

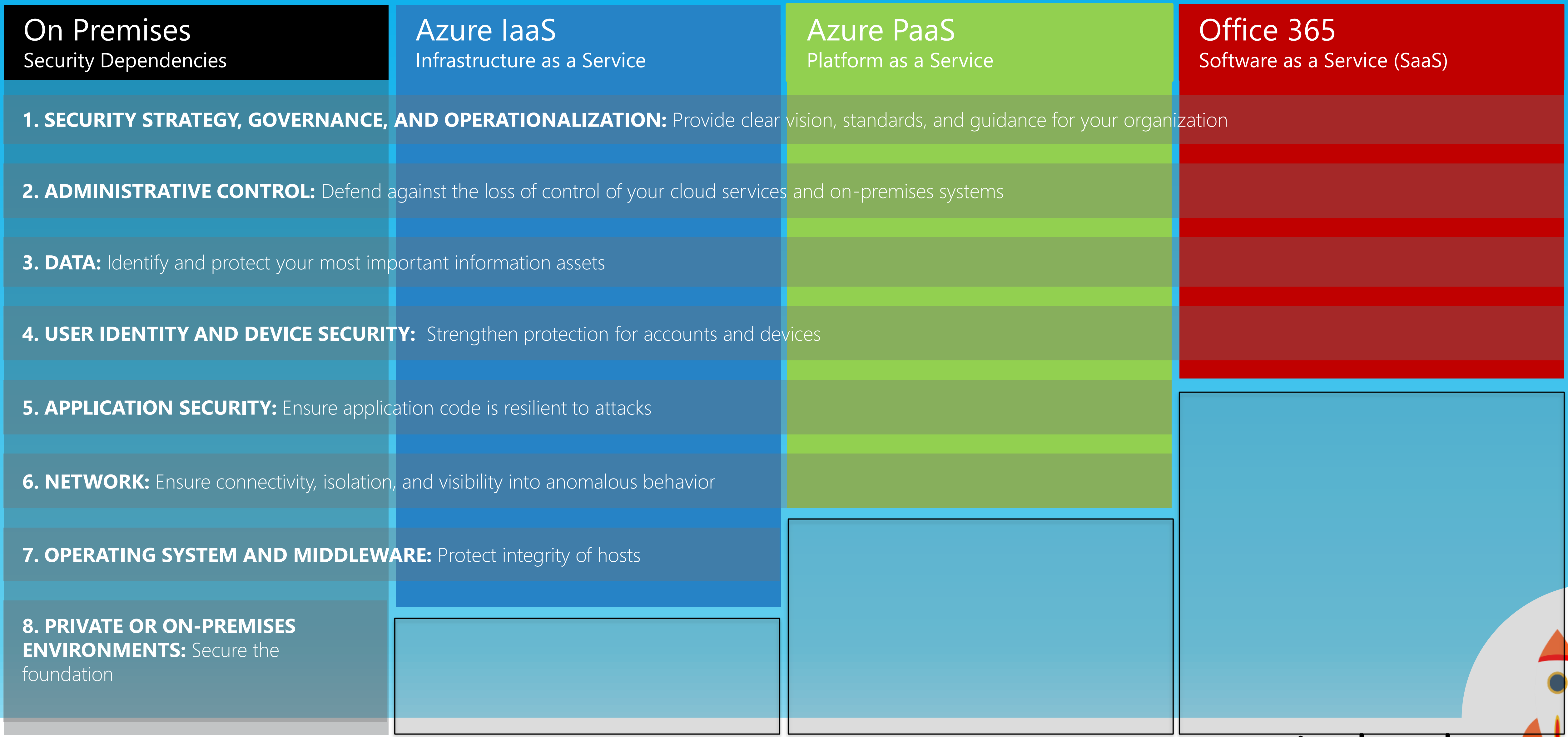
SHARED RESPONSIBILITY

Securing and managing your cloud resources

- Virtual machines, networks & services
- Applications
- Data

VARIES ACROSS IAAS, PAAS, SAAS

Service responsibility matrix



On Premises
Security Dependencies

Azure IaaS
Infrastructure as a Service

Azure PaaS
Platform as a Service

Office 365
Software as a Service (SaaS)

1. SECURITY STRATEGY, GOVERNANCE, AND OPERATIONALIZATION: Provide clear vision, standards, and guidance for your organization

2. ADMINISTRATIVE CONTROL: Defend against the loss of control of your cloud services and on-premises systems

3. DATA: Identify and protect your most important information assets

4. USER IDENTITY AND DEVICE SECURITY: Strengthen protection for accounts and devices

5. APPLICATION SECURITY: Ensure application code is resilient to attacks

6. NETWORK: Ensure connectivity, isolation, and visibility into anomalous behavior

7. OPERATING SYSTEM AND MIDDLEWARE: Protect integrity of hosts

8. PRIVATE OR ON-PREMISES ENVIRONMENTS: Secure the foundation

macedonian.net user group

azuresaturday.mk

Azure Compliance

The largest compliance portfolio in the industry

- ISO 27001
- SOC 1 Type 2
- SOC 2 Type 2
- PCI DSS Level 1
- Cloud Controls Matrix
- ISO 27018
- Content Delivery and Security Association
- Shared Assessments

- FedRAMP JAB P-ATO
- HIPAA / HITECH
- FIPS 140-2
- 21 CFR Part 11
- FERPA
- DISA Level 2
- CJIS
- IRS 1075
- ITAR-ready
- Section 508 VPAT

- European Union Model Clauses
- EU Safe Harbor
- United Kingdom G-Cloud
- China Multi Layer Protection Scheme
- China GB 18030
- China CCCPPF
- Singapore MTCS Level 3
- Australian Signals Directorate
- New Zealand GCIO
- Japan Financial Services
- ENISA IAF

Abundance of Azure services

Compute

- Virtual Machines
- Virtual Machine Scale Sets
- Cloud Services
- Containers
- Container Registry
- Container Service

Networking

- Virtual Network
- Azure DNS
- Application Gateway
- Traffic Manager
- ExpressRoute
- Load Balancer

Data & Storage

- Disk Storage
- Blob Storage
- File Storage
- Queue Storage
- Table Storage
- StorSimple

Web & Mobile

- Web Apps
- Mobile Apps
- Logic Apps
- Content Delivery Network

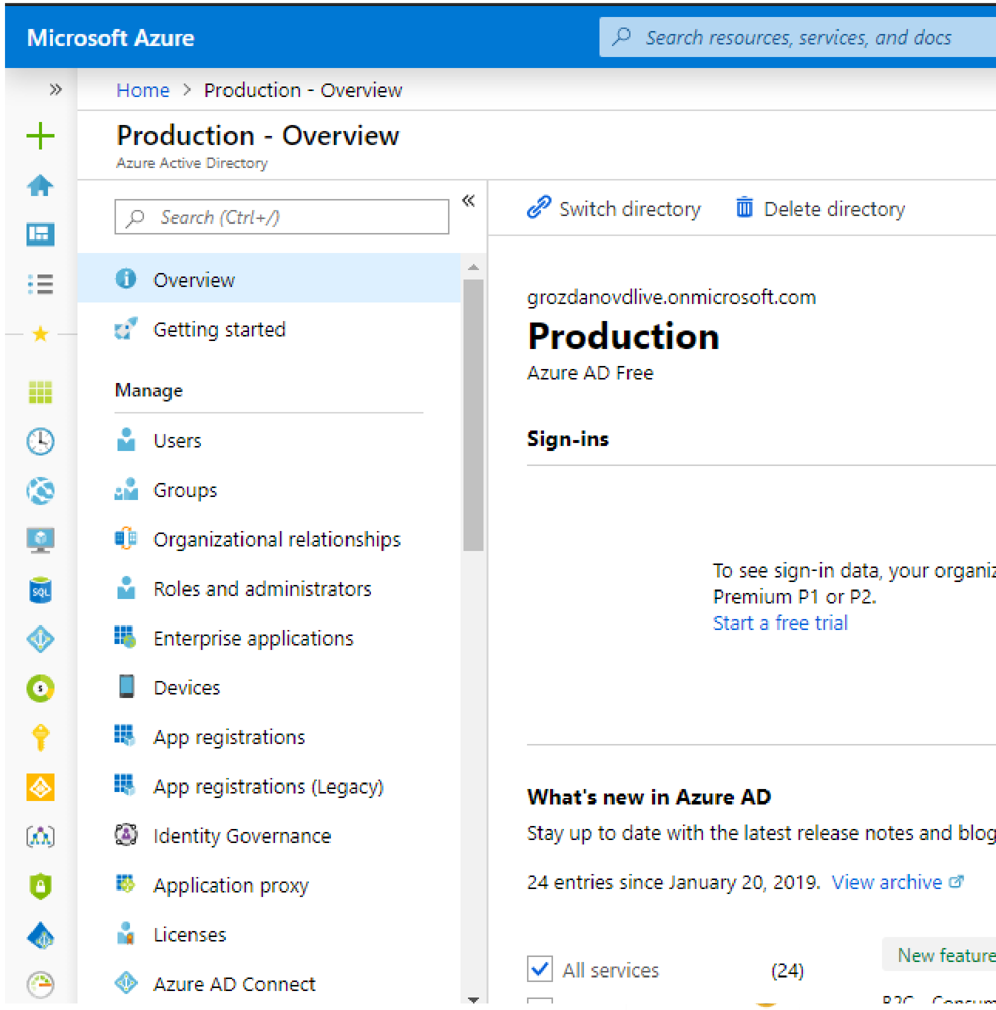
Other services

- Azure AD
- Azure AD DS
- Azure B2C
- MFA
- Automation
- Backup
- Site Recovery
- Log Analytics
- Azure Monitor
- Azure Advisor
- Key Vault
- Network Watcher
- Azure Security Center

Identity and Access Management

Overview of Azure Active Directory

- Microsoft-managed
- A platform as a service offering
- Multitenant by design
- Employs internet-friendly protocols (OAuth 2.0, OpenID, WS-*)
- Supports users, groups, applications, and devices
- No organizational units, No GPO-based computer or user management Includes built-in MFA support
- No support for forests:
  - Relies on federations to extend scope of authentication



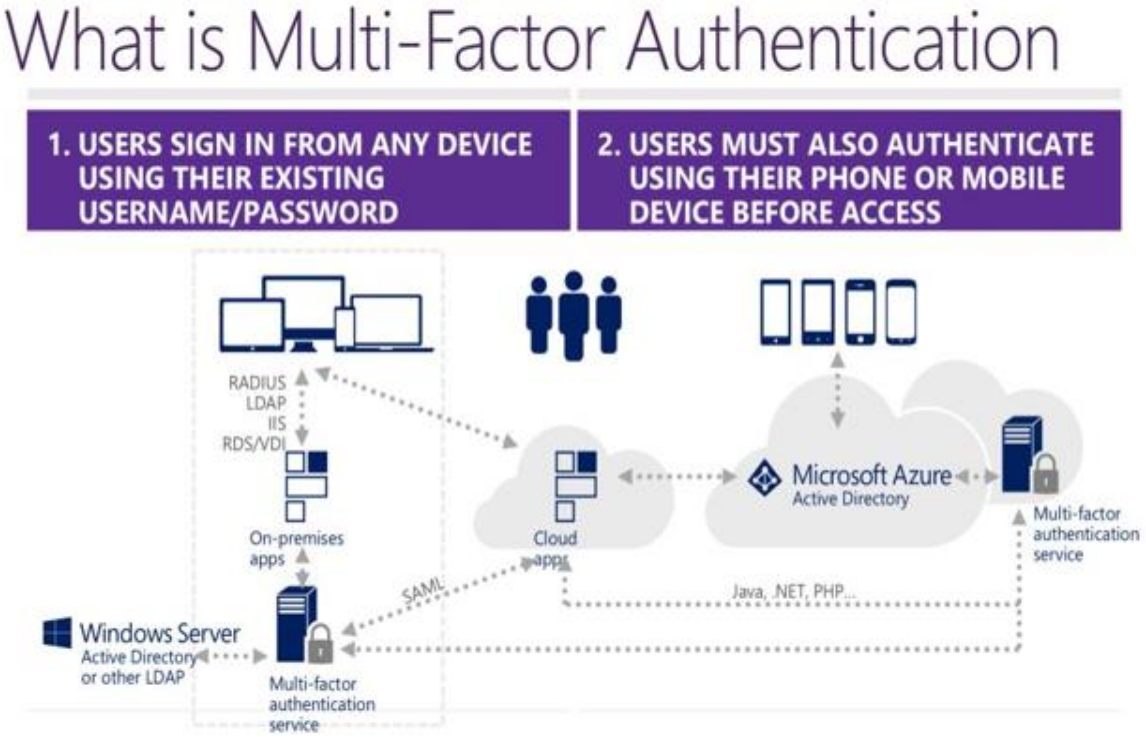
To see sign-in data, your organi
Premium P1 or P2.

Stay up to date with the latest release notes and blog

24 entries since January 20, 2019.

Multi-factor for time-bound elevation

- Azure MFA supplies added security for your identities by requiring two or more elements for full authentication
- These elements fall into three categories:
  - Something you know: password or answer to security question
  - Something you possess: mobile app or token device
  - Something you are: biometric property such as fingerprint
- Using Azure MFA increases identity security by limiting the impact of credential exposure

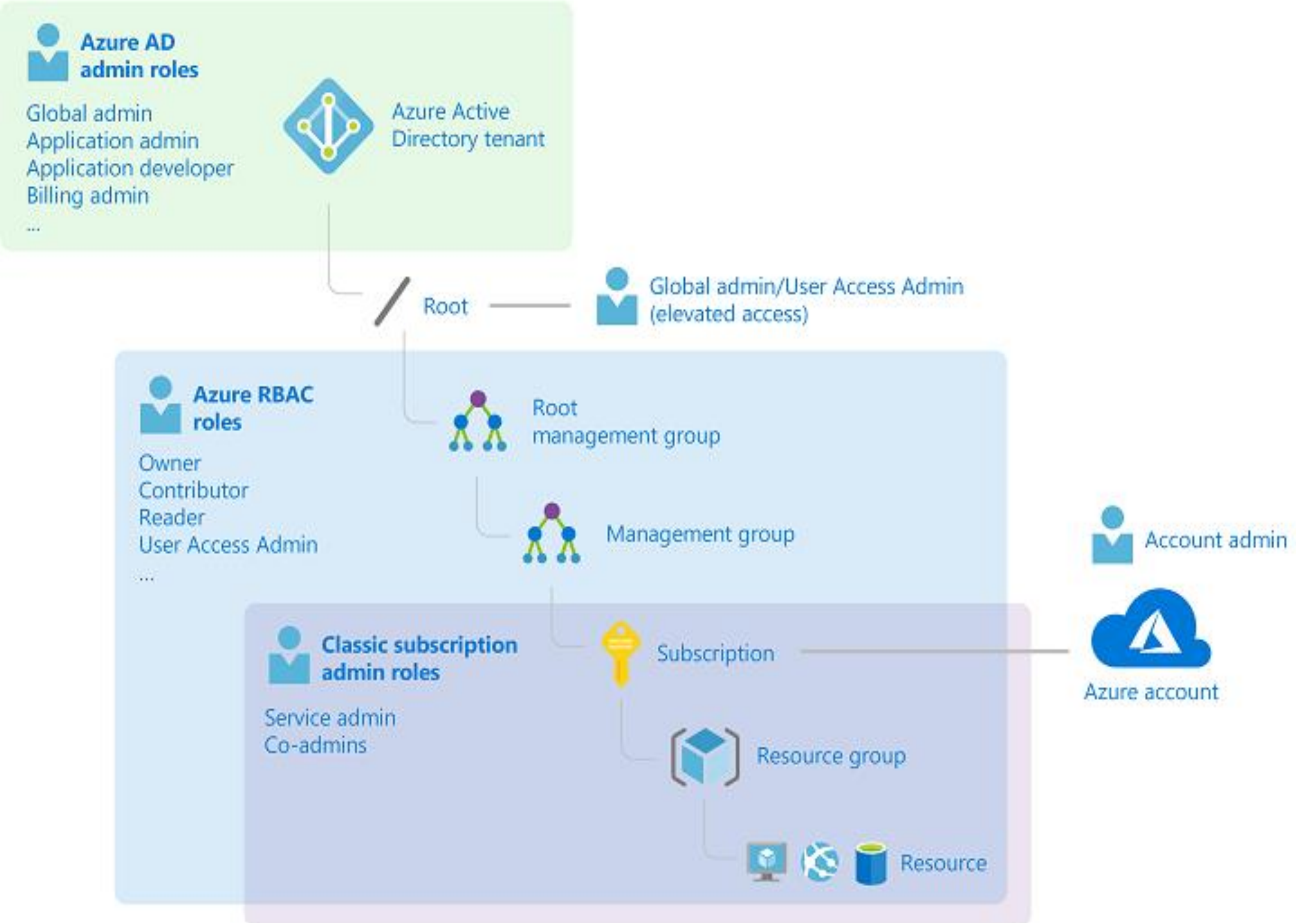


What is Multi-Factor Authentication

1. USERS SIGN IN FROM ANY DEVICE USING THEIR EXISTING USERNAME/PASSWORD

2. USERS MUST ALSO AUTHENTICATE USING THEIR PHONE OR MOBILE DEVICE BEFORE ACCESS

Admin roles and scope

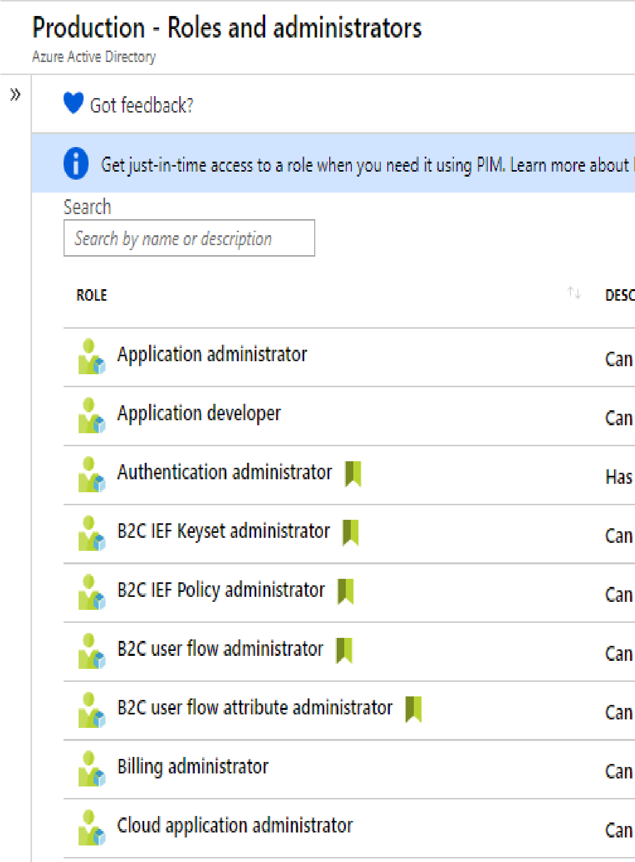


Role Assignment

- **Users**: From the same Azure AD and same subscription

- **Groups**: If a role is assigned to a group, a user receives the rights of the role when added to the group. The user also automatically loses access to the resource after getting removed from the group

- **Service principals**: Services can be granted access to Azure resources by assigning roles to the Azure AD service principal representing that service (auth is done by using certificates)



Production - Roles and administrators

Azure Active Directory

Got feedback?

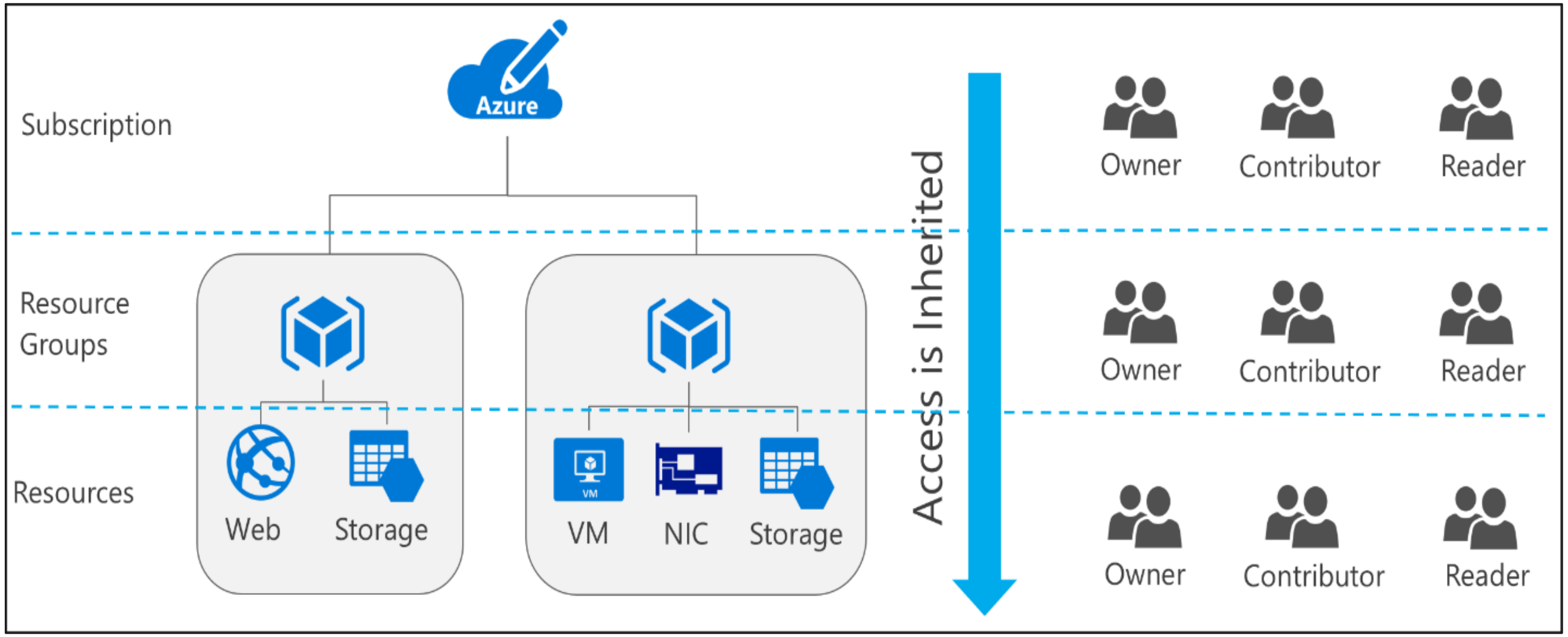
Get just-in-time access to a role when you need it using PIM. Learn more about

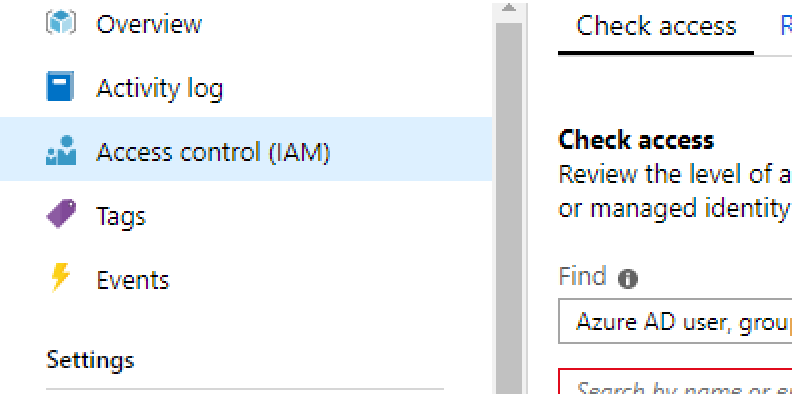
Search

Search by name or description

ROLE	DESC
Application administrator	Can
Application developer	Can
Authentication administrator	Has
B2C IEF Keyset administrator	Can
B2C IEF Policy administrator	Can
B2C user flow administrator	Can
B2C user flow attribute administrator	Can
Billing administrator	Can
Cloud application administrator	Can

Role Base Access Control (RBAC) Concepts





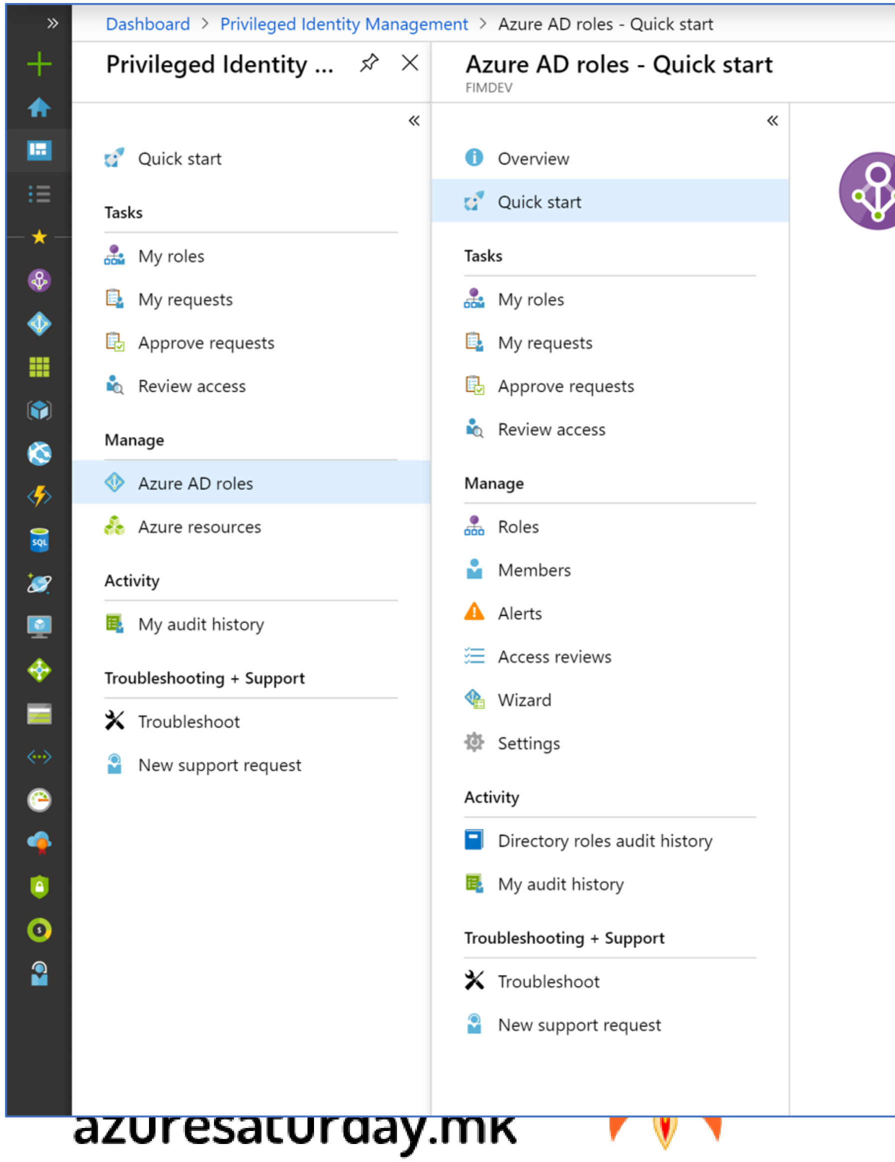
Check access
Review the level of a
or managed identity

Find
Azure AD user, grou
Search by name or e

1. Define what actions are allowed and/or denied
2. Associate the role with a user, group or service principal
3. Scope to a subscription, a resource group, or specific resources

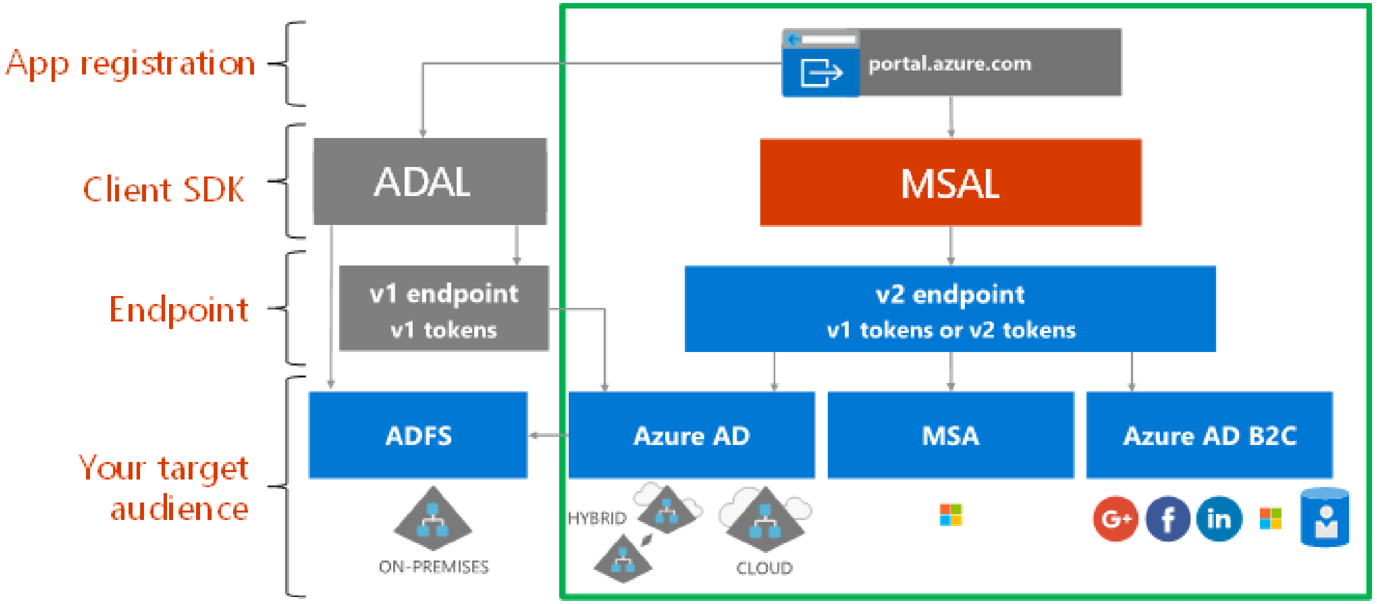
Azure AD Privileged Identity Management

- Service that enables you to manage, control, and monitor access to important resources in your organization
- Key features of PIM allow you to:
  - Provide just-in-time privileged access to Azure AD
  - Assign time-bound access to resources
  - Require approval to activate privileged roles
  - Enforce multi-factor authentication (MFA) for role activation
  - Use justification to understand why users activate roles
  - Get notifications when privileged roles are activated
  - Conduct access reviews to ensure users still need roles
  - Download audit history



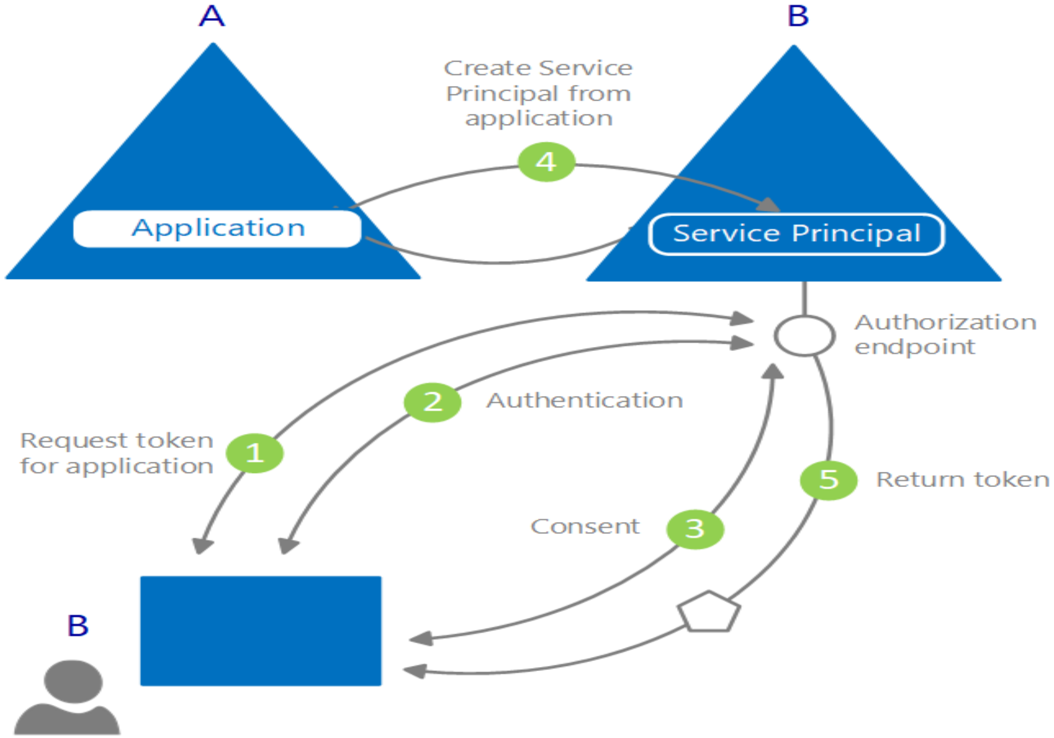
Manage app registration

- The Microsoft identity platform has two endpoints (v1.0 and v2.0) and two sets of client libraries to handle these endpoints
- Azure AD supports five primary application scenarios:
  - Single-page application (SPA)
  - Web browser to web application
  - Native application to web API
  - Web application to web API
  - Daemon or server application to web API



Manage app registration (cont.)

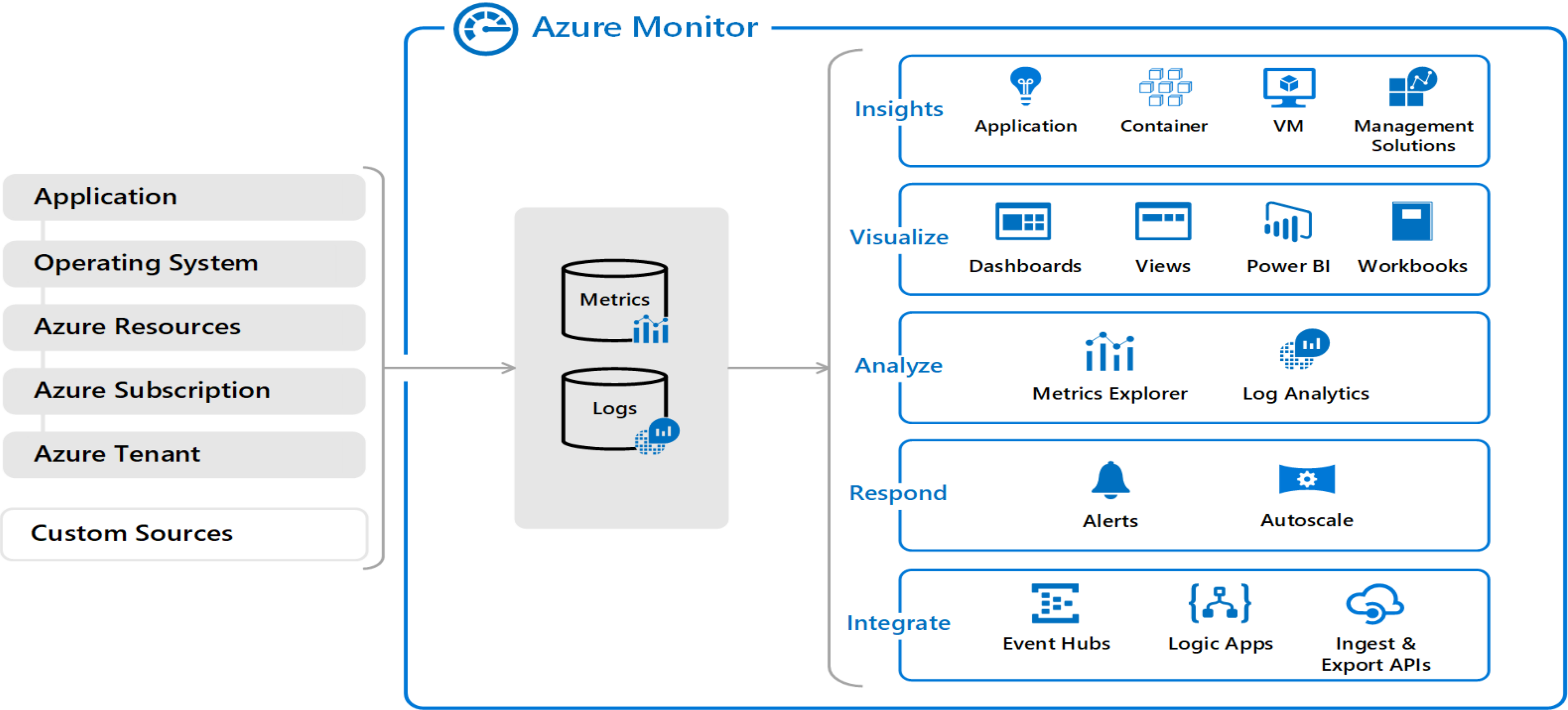
- Any application that outsources authentication to Azure AD must be registered in a directory
- Registration involves telling Azure AD about the application, including the URL where it’s located, the URL to send replies to after authentication, the URI to identify your application, and more
- Azure AD represents applications following a specific model that's designed to fulfill two main functions
  - Identify the app according to the authentication protocols it supports
  - Handle user consent during token request time and facilitate the dynamic provisioning of apps across tenants



Infrastructure and Services Security

Overview of elasticity and scalability

- DevOps has completely changed the way applications are developed and maintained
- Cloud applications typically encounter variable workloads and peaks in activity
- You can use Azure Monitor to understand how your applications are performing
- Azure Monitor Autoscale helps to enable the elastic scale feature of the cloud



Understand virtualization

- Virtualization creates a simulated, or virtual, computing environment, as opposed to a physical environment
- Each virtual machine can then interact independently and run different operating systems or applications
- There are four main categories of virtualization:
  - Desktop virtualization
  - Network virtualization
  - Software virtualization
  - Storage virtualization
- VM's are part of the IaaS part of Azure

IaaS/PaaS Building blocks

- Virtual Network
  - IP addresses and Subnets, Network Security Groups, Service Endpoints, Local/Regional Connectivity
- Network Load Balancer
  - Load-balance incoming internet traffic to your VMs
  - Load-balance traffic across VMs inside a virtual network
  - Port forward traffic to a specific port on specific VMs
  - Provide outbound connectivity for VMs inside your virtual network
- Firewall
  - WAF, SQL Azure, Storage, Network
- Traffic Manager
  - DNS based traffic routing (Performance, Priority, Weight, Geography)
- Virtual network gateways
  - Hybrid, Routing / Forced Tunneling, P2S, S2S, ExpressRoute
- Protection (ATP, DDoS, Sentinel)
  - Anti-virus/IPS, SIEM
- Certificate Management (Key Vault, Encryption, SPN, SSL/TLS)
- Storage
  - SAS, Firewall, Virus protection, DDoS

Understand containers

- A container is a modified runtime environment that prevents a program from accessing protected resources
- A container interacts directly with the host operating system (OS) and augments the containment functions
- A container does not use virtualization
- Several options exist within Azure

Configure container security

- Networking in a container deployment is a special area that you must address in security scenarios
- Containers are not inherently vulnerable
- The kernel is shared among all containers and the host
- An attacker who gains access to a container should not be able to gain access to other containers or the host

Understand serverless computing

- Serverless computing is the abstraction of servers, infrastructure, and operating systems
- Azure Functions is a serverless application platform
- Azure Logic Apps allows developers to add workflows to support their Azure functions
- Serverless computing generally encompasses three things:
  - Abstraction of servers
  - Event-driven scale
  - Microbilling

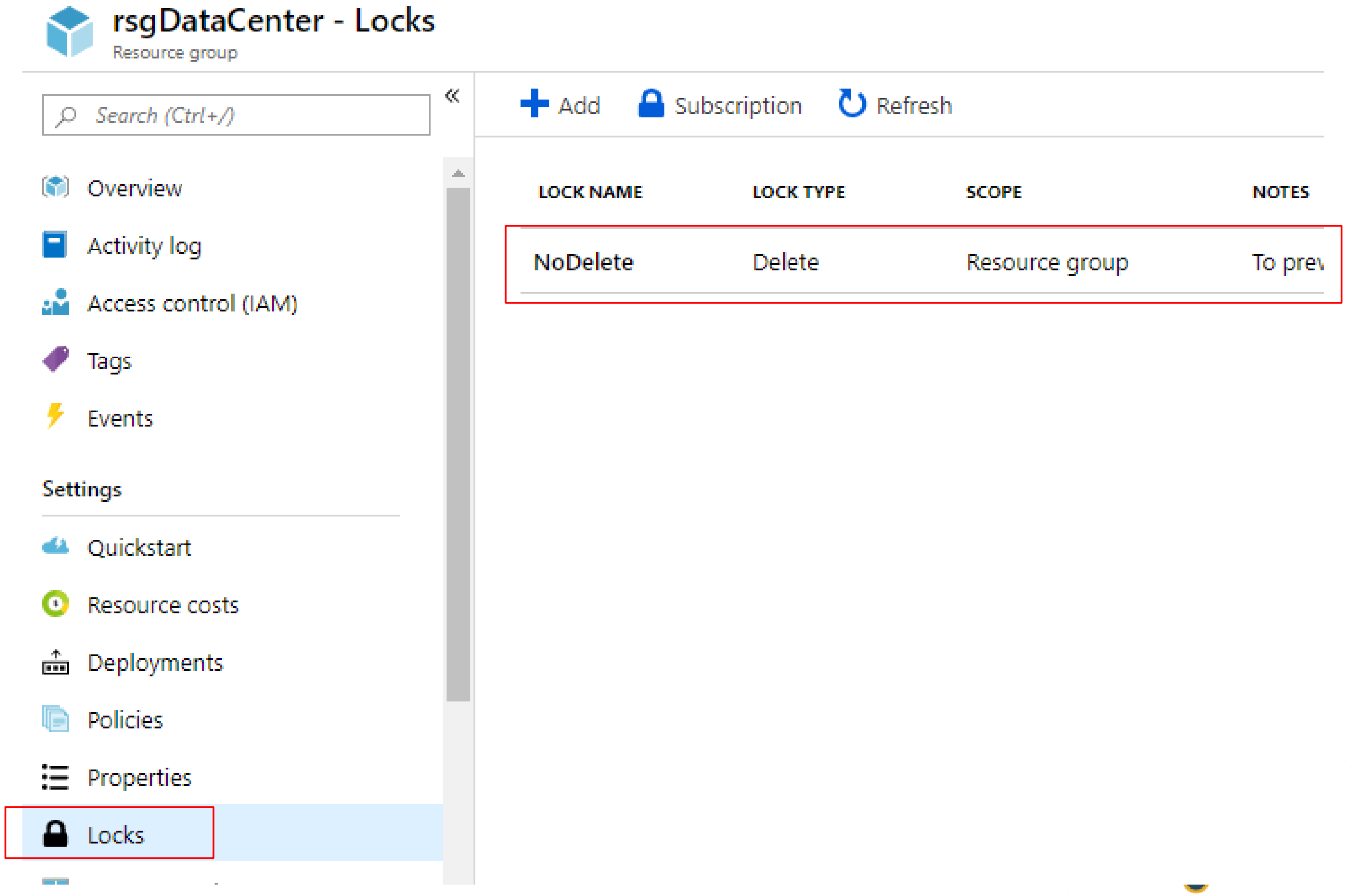
Configure security for serverless computing

- Serverless computing moves the responsibility for server management from the application owner to the platform provider
- However, there are some security issues and challenges in serverless computing, as you're still responsible for:
  - Your application code
  - Data management
  - Data encryption
  - Identity management
  - Authentication/authorization
  - Configuration of services and role-based access control (RBAC)

Platform Security Tools

Azure resource locks

- Management locks help you prevent accidental deletion or modification of your Azure resources
- You can manage these locks from within the Azure portal
- When you apply a lock at a parent scope, all resources within that scope inherit the same lock



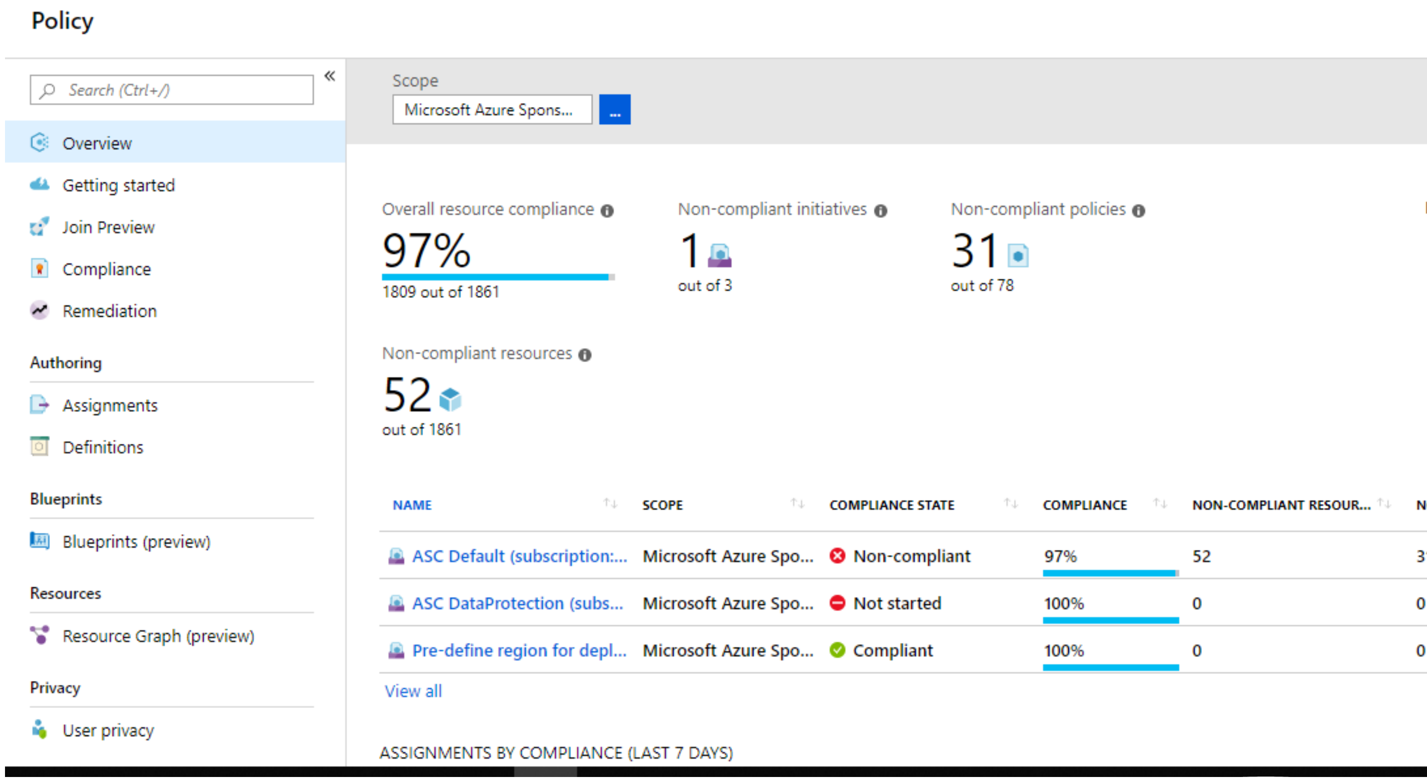
rsgDataCenter - Locks

Resource group

LOCK NAME	LOCK TYPE	SCOPE	NOTES
NoDelete	Delete	Resource group	To prev

Azure Policy

- Azure Policy is a service in Azure that you use to create, assign and, manage policies
- Azure Policy runs evaluations and scans for non-compliant resources
- Advantages:
  - Enforcement and compliance
  - Apply policies at scale
  - Remediation



Policy

Scope: Microsoft Azure Spons...

Overall resource compliance: 97%, 1809 out of 1861

Non-compliant initiatives: 1, out of 3

Non-compliant policies: 31, out of 78

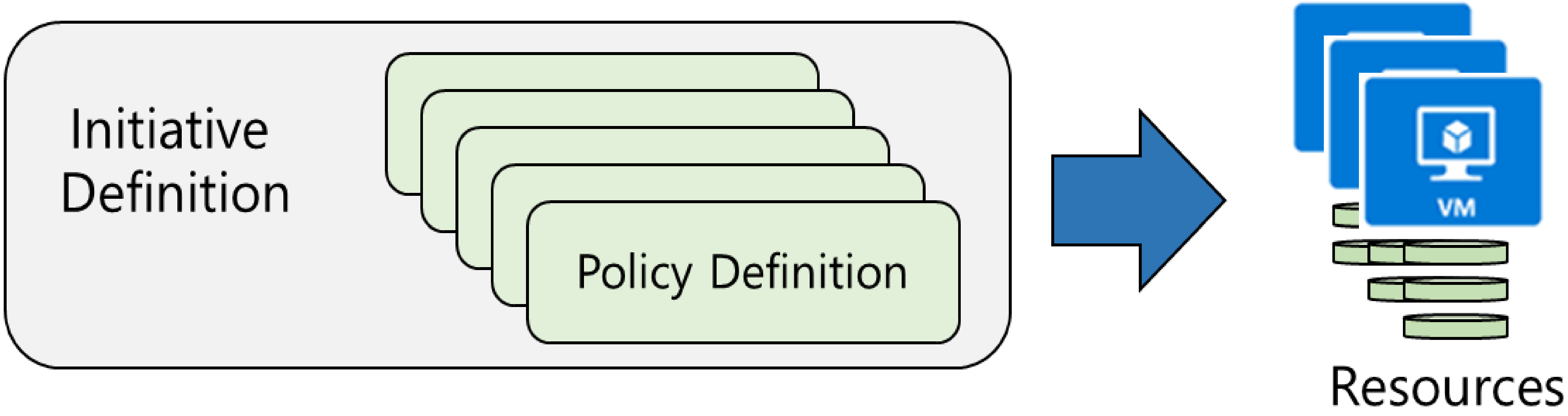
Non-compliant resources: 52, out of 1861

NAME	SCOPE	COMPLIANCE STATE	COMPLIANCE	NON-COMPLIANT RESOUR...	N
ASC Default (subscription:...	Microsoft Azure Spo...	✗ Non-compliant	97%	52	3
ASC DataProtection (subs...	Microsoft Azure Spo...	⊖ Not started	100%	0	0
Pre-define region for depl...	Microsoft Azure Spo...	✓ Compliant	100%	0	0

View all

ASSIGNMENTS BY COMPLIANCE (LAST 7 DAYS)

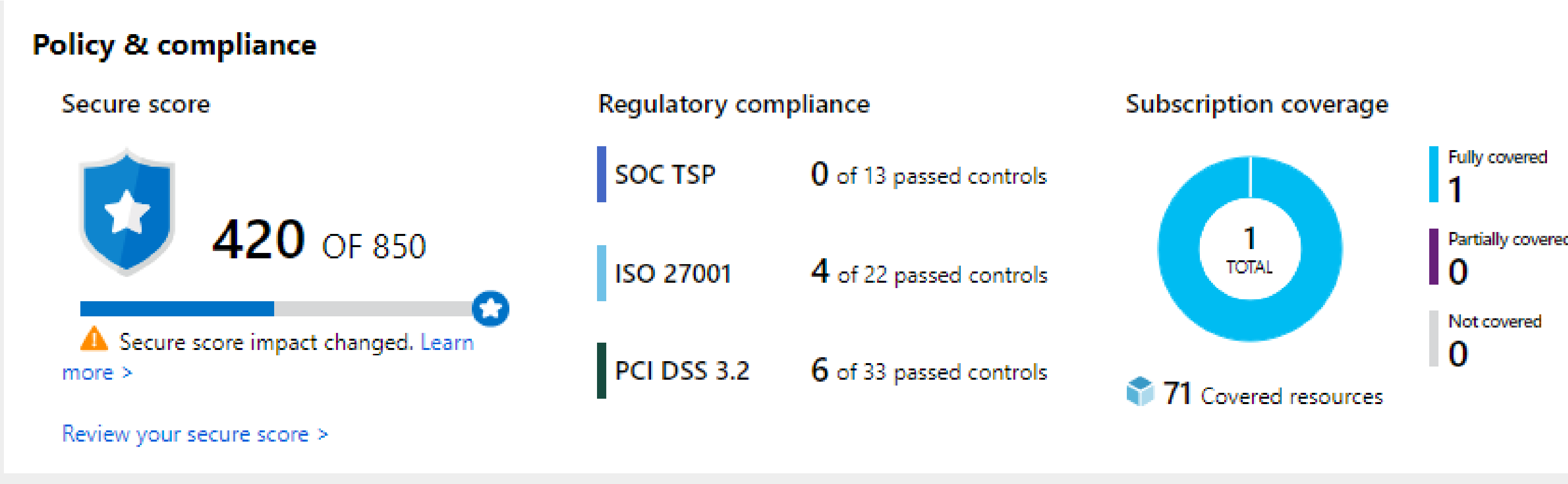
Implementing Azure Policy



1. Browse Policy Definitions
2. Create Initiative Definitions
3. Scope the Initiative Definition
4. View Policy evaluation results

Configure centralized policy management by using Azure Security Center

- You can enable or disable recommendations for:
  - System updates
  - OS vulnerabilities
  - Endpoint protection
  - Disk encryption
  - Network security groups
  - Web application firewall
  - Vulnerability Assessment
  - NGFW
  - SQL auditing & Threat detection
  - SQL Encryption



Policy & compliance

Secure score

420 OF 850

⚠ Secure score impact changed. Learn more >

Review your secure score >

Regulatory compliance

SOC TSP	0 of 13 passed controls
ISO 27001	4 of 22 passed controls
PCI DSS 3.2	6 of 33 passed controls

Subscription coverage

1 TOTAL

Fully covered 1

Partially covere 0

Not covered 0

71 Covered resources

Create a platform security baseline

- The Microsoft cybersecurity group in conjunction with CIS developed best practices to help establish security baselines
- A variety of security standards can help cloud service customers achieve workload security when using cloud services
- CIS has the following implementation levels:
  - Level 1. Recommended minimum security settings
  - Level 2. Recommended for highly secure environments

Create an IAM baseline

Some common recommendations for IAM protection baselines include:

- Restricting access to the Azure AD admin portal
- Enabling MFA
- Properly managing guests
- Managing password security
- Managing member and guest invitation capabilities
- Disabling application options

Create an Azure SQL Database baseline

Microsoft SQL Server policy recommendations include:

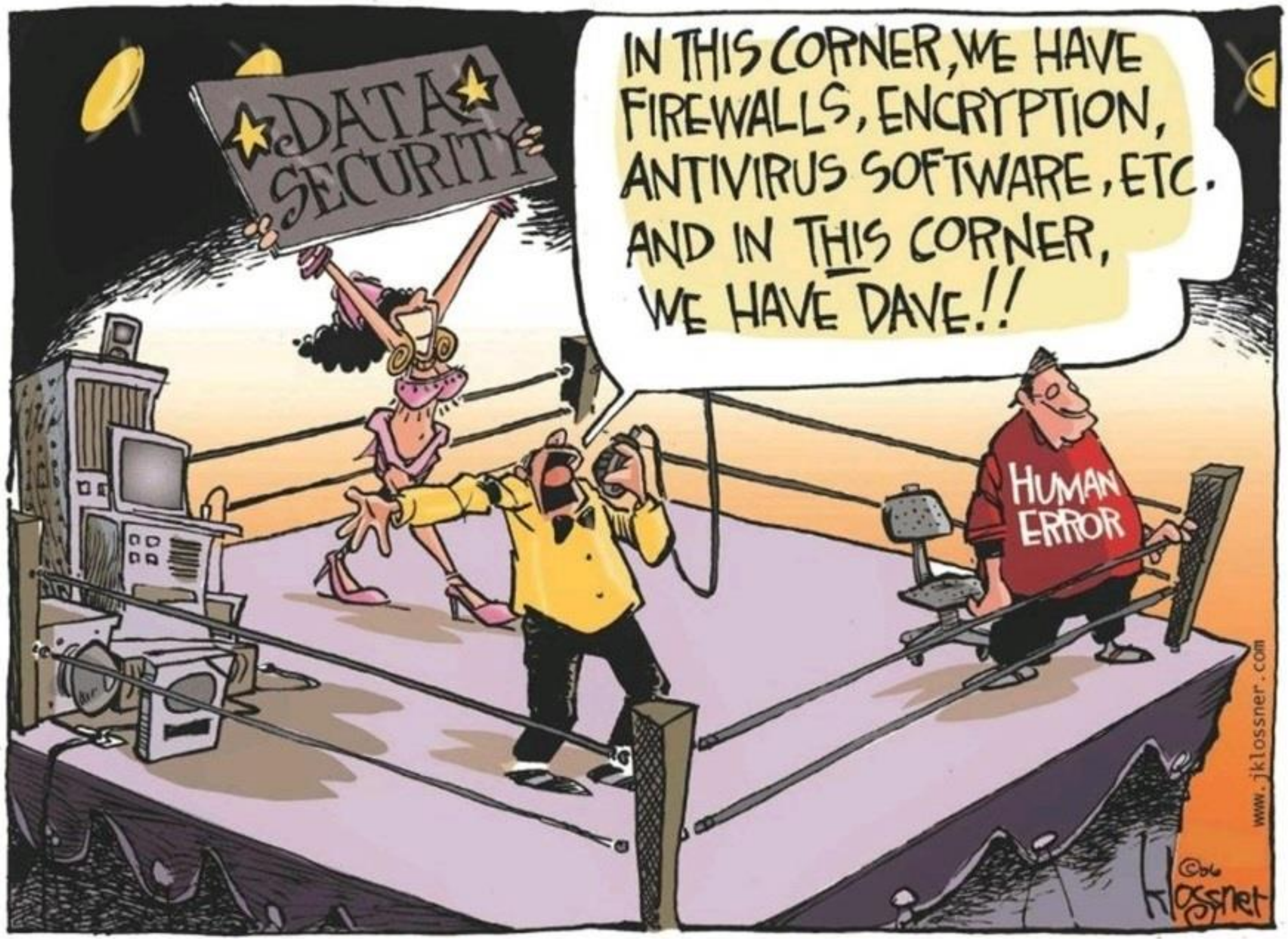
- Enable auditing
- Enable a threat detection service
- Enable all threat detection types
- Enable the option to send security alerts
- Enable the email service and co-administrators
- Configure audit retention for more than 90 days
- Configure threat detection retention for more than 90 days
- Configure Azure AD administration

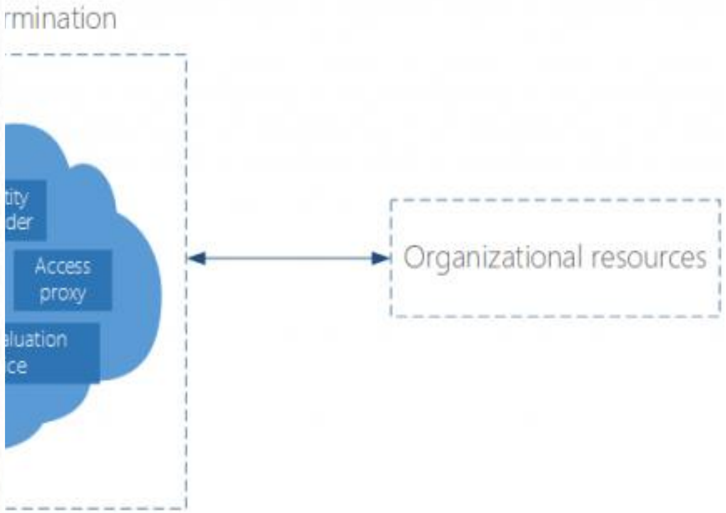
Demo

Security Center Overview

Zero Trust Model

- M
- Im
- M
- Se


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner


rmination

tity
der

Access
proxy

aluation
ce

Organizational resources

Simplify security with Azure services

<table>
<tr><th>Identity & access management</th><th>Data protection</th><th>Network security</th><th>Threat protection</th><th>Security management</th></tr>
<tr><td>Azure Active Directory</td><td>Encryption (Disks, Storage, SQL)</td><td>VNET, VPN, NSG</td><td colspan="2">Azure Security Center</td></tr>
<tr><td>Multi-Factor Authentication</td><td>Azure Key Vault</td><td>Application Gateway (WAF), Azure Firewall</td><td>Microsoft Antimalware for Azure</td><td>Azure Log Analytics</td></tr>
<tr><td>Role Based Access Control</td><td>Confidential Computing</td><td>DDoS Protection Standard</td><td></td><td></td></tr>
<tr><td>Azure Active Directory (Identity Protection)</td><td></td><td>ExpressRoute</td><td></td><td></td></tr>
</table>

+ Partner Solutions

Q&A

Thank you