STEEL DRUM 2017 L'VIV

INTRODUCTION TO MICROSOFT CLOUD SECURITY SCENARIOS – AZURE IAAS PLATFORM.

MAY 2017

IGOR SHASTITKO

IGOR SHASTITKO

Living in Bratislava, Slovakia

ROLE

- Senior Infrastructure/ Security Consultant
- Contractor/Independent consultant
- igorsh@outlook.com
- +421944905459

BACKGROUND

- Computer Science
- MCSE/MCT
- Geek ☺

WORK

- Microsoft Partners
- Microsoft Learning Centers
- Microsoft MCS (10 years)

PLEASURE

- Family
- Video Blogging youtube.com/iwalker2000
- Gadgets & technologies

Microsoft

Adgenda for today

Describe & discuss possible Cloud Security projects portfolio & some technical questions

CLOUD SECURITY PORTFOLIO

- Azure IaaS & hybrid infra security opportunities
- Hybrid Identity opportunities
- Mobile devices & data protection

EMS: MOBILE DEVICES & DATA PROTECTION

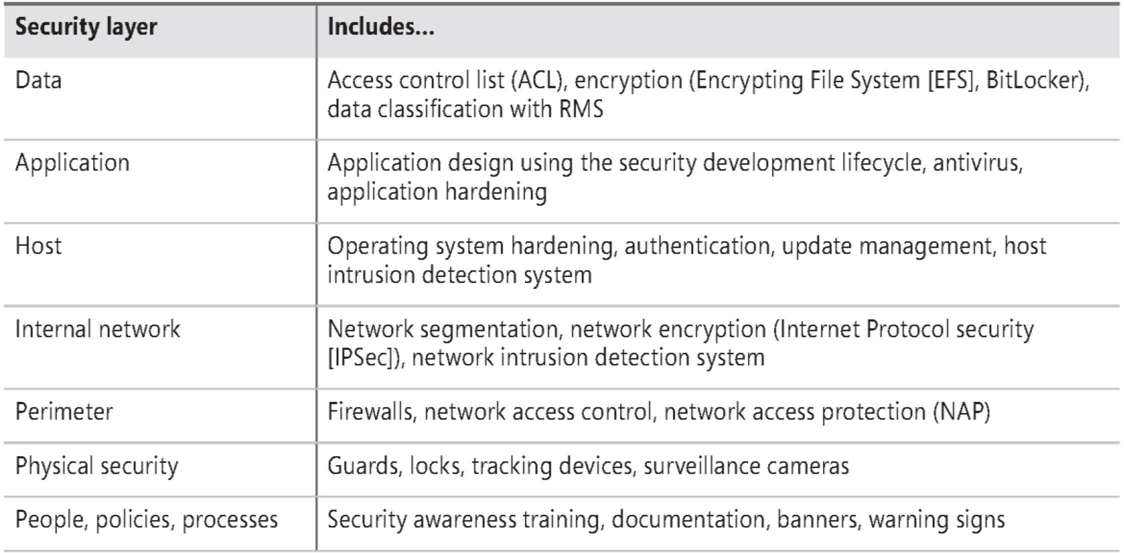
- EMS discussion
- MDM considerations
- RMS/Azure IP considerations

EMS: HYBRID IDENTITY

- EMS discussion
- Identify cloud/hybrid identity opportunity
- Cloud identity considerations

Before we start ANY Cloud/Security project

Defense-in-Depth MUST NECESSARILY BE implemented for on-premises infrastructure before any other projects



Security layer	Includes...
Data	Access control list (ACL), encryption (Encrypting File System [EFS], BitLocker), data classification with RMS
Application	Application design using the security development lifecycle, antivirus, application hardening
Host	Operating system hardening, authentication, update management, host intrusion detection system
Internal network	Network segmentation, network encryption (Internet Protocol security [IPSec]), network intrusion detection system
Perimeter	Firewalls, network access control, network access protection (NAP)
Physical security	Guards, locks, tracking devices, surveillance cameras
People, policies, processes	Security awareness training, documentation, banners, warning signs

- Start any new security project's discussion with Defense-in-Depth methodology/strategy
- Cloud (and hybrid cloud especially) solutions are just reflection of customer on-premises infra's security
- Most common attacks to the cloud start with on-premises' breaches

Threats against cloud deployments and infrastructure

New types of threats can be related to characteristics of the public cloud only, or to issues introduced by connectivity between on-premises environments and the public cloud.

ATTACKS AGAINST CLOUD ADMINISTRATORS

Targeted attacks against on-premises and cloud infrastructures alike often focus on IT administrators. The intent is to take control of an email account that has a high probability of containing credentials that can be used to gain access to the public cloud administrator portal.

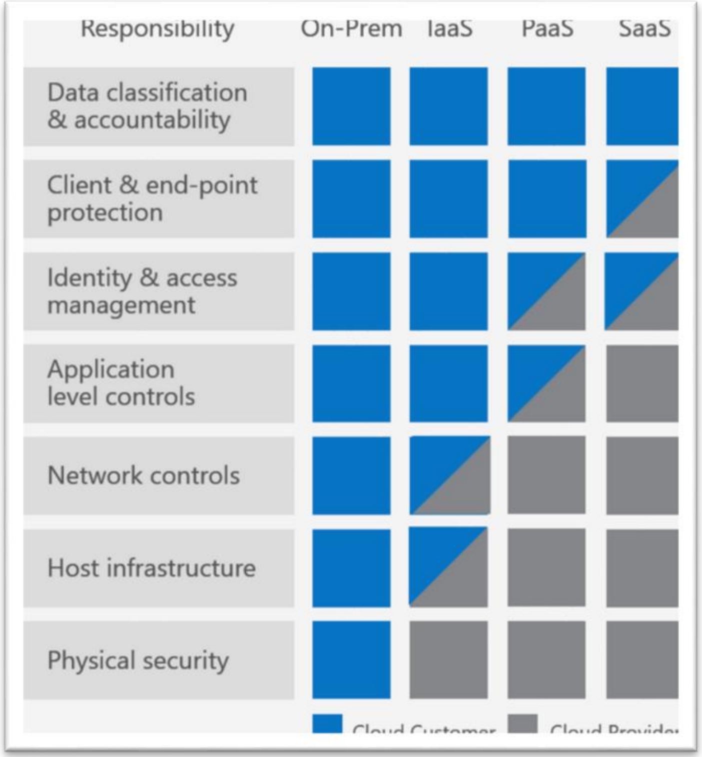
PIVOT BACK ATTACKS

A pivot back attack occurs when an attacker compromises a public cloud resource to obtain information that they then use to attack the resource provider's on-premises environment. Public facing endpoints in the cloud are often under constant brute force attack through protocols such as Remote Desktop Protocol (RDP) and Secure Shell (SSH).

https://www.microsoft.com/security/sir/default.aspx

Azure Security Infrastructure

Start to discuss this topics with customers in any hybrid/public cloud Azure Security project



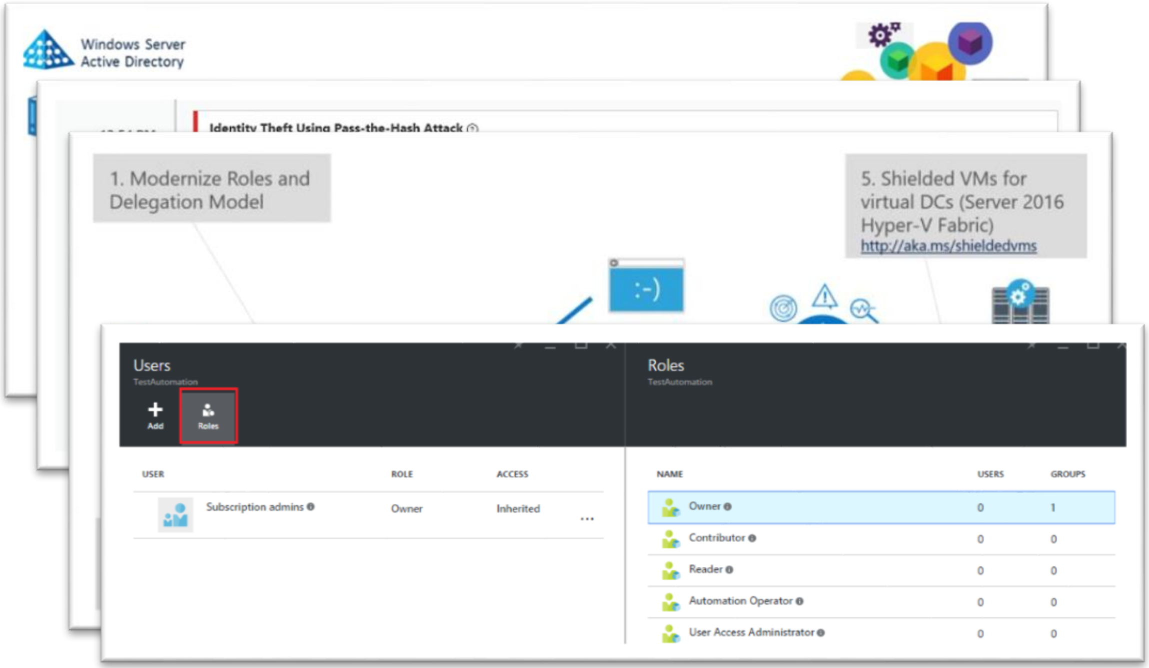
Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	🟦⬛
Identity & access management	🟦	🟦	🟦⬛	🟦⬛
Application level controls	🟦	🟦	🟦⬛	⬛
Network controls	🟦	🟦⬛	⬛	⬛
Host infrastructure	🟦	🟦⬛	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider

MANDATORY ACTIONS

- Admin access protection in Azure IaaS
- Azure IaaS virtual networks/network access protection to Azure IaaS
- Data protection in Azure
- Antivirus/antimalware protection in Azure IaaS
- Monitoring of security for Azure IaaS, VMs, hybrid infra

Admin access protection



Windows Server Active Directory

Identity Theft Using Pass-the-Hash Attack

1. Modernize Roles and Delegation Model

5. Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric) http://aka.ms/shieldedvms

Users

TestAutomation

USER	ROLE	ACCESS
Subscription admins	Owner	Inherited

Roles

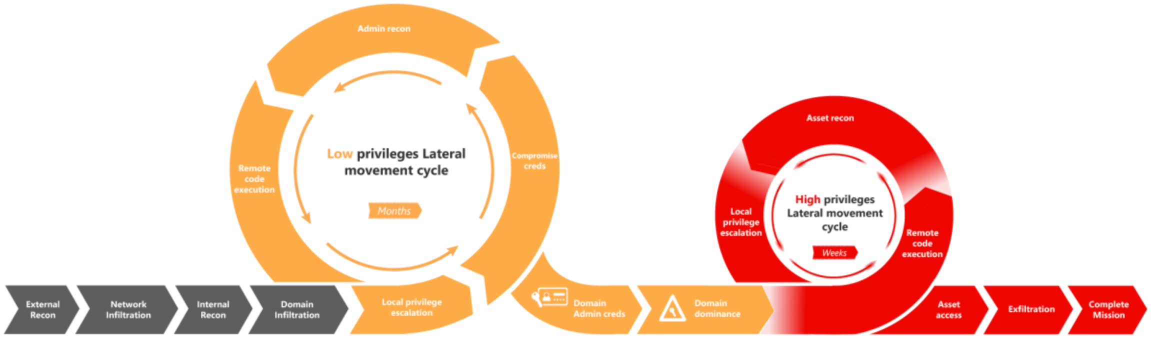
TestAutomation

NAME	USERS	GROUPS
Owner	0	1
Contributor	0	0
Reader	0	0
Automation Operator	0	0
User Access Administrator	0	0

- Hybrid Identity solution/project
- Modernization of existing local identity infrastructure with modern technologies, e.g. authentication silos, Microsoft ATA etc.
- Modernization of existing administration procedures, processes and on-premises admin account protection (PAW)
- Planning Role Based Access Control (RBAC) and procedures in general

Cyber Kill CHAIN attack

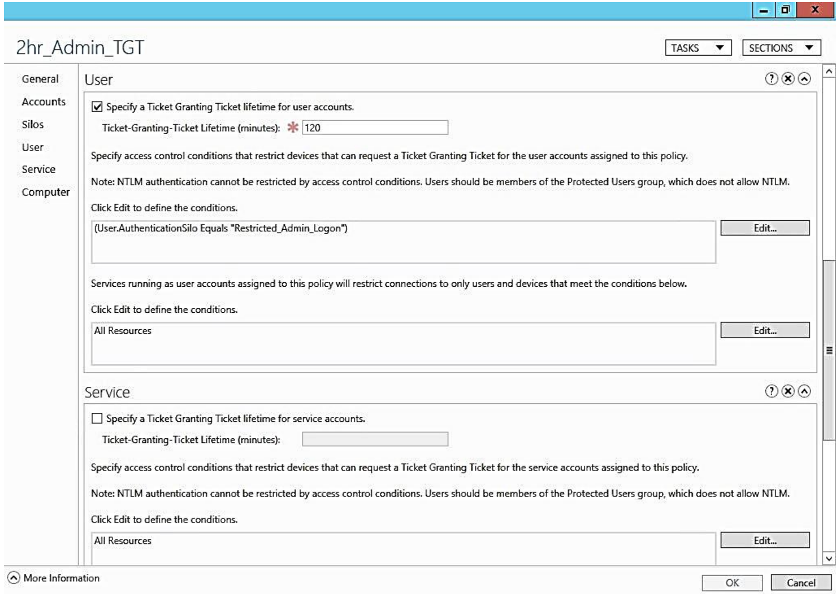
New types of attacks have a few stages that could be prevented by monitoring & countermeasures



- **Reconnaissance** - Account enumeration
- **Compromised Credential** - Abnormal working hours or location
- **Lateral Movement** - Abnormal authentication or resource access
- **Privilege Escalation** – Log Audit
- **Domain Dominance** - Remote execution

Protect administrative accounts on-premises

Authentication Policies and Authentication Policy Silos as good way to modernization AD



2hr_Admin_TGT

User

☑ Specify a Ticket Granting Ticket lifetime for user accounts.

Ticket-Granting-Ticket Lifetime (minutes): * 120

Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the user accounts assigned to this policy.

Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the Protected Users group, which does not allow NTLM.

Click Edit to define the conditions.

(User.AuthenticationSilo Equals "Restricted_Admin_Logon")

Services running as user accounts assigned to this policy will restrict connections to only users and devices that meet the conditions below.

Click Edit to define the conditions.

All Resources

Service

□ Specify a Ticket Granting Ticket lifetime for service accounts.

Ticket-Granting-Ticket Lifetime (minutes):

Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the service accounts assigned to this policy.

Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the Protected Users group, which does not allow NTLM.

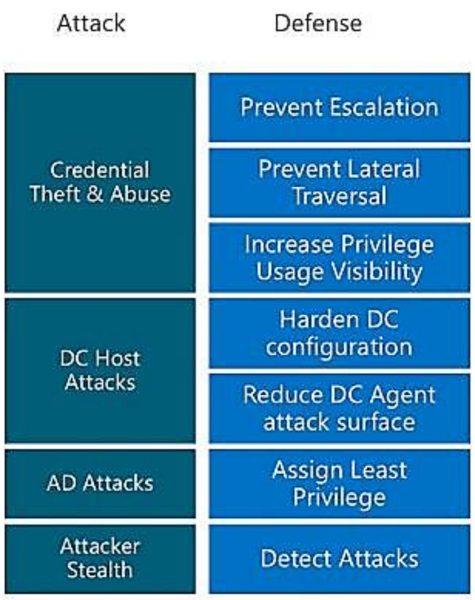
Click Edit to define the conditions.

All Resources

- Good point to start modernization on-premises
- An **authentication policy silo controls** which **accounts can be restricted** by the silo and defines the authentication policies to apply to the members.
- An **authentication policy** defines the Kerberos protocol ticket-granting ticket (TGT) **lifetime properties** and authentication **access control conditions** for an account type.
  - The **TGT lifetime** for the account, which is set to be non-renewable.
  - The **criteria that device accounts need to meet** to sign in with a password or a certificate.
  - The **criteria that users and devices need to meet** to authenticate to services running as part of the account.
- Required Windows Server 2012 R2 or later

Modernization of existing local identity infrastructure with modern technologies

Protection on-premises again modern attack types - Securing privileged access & PAW



Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
DC Host Attacks	Harden DC configuration
	Reduce DC Agent attack surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks

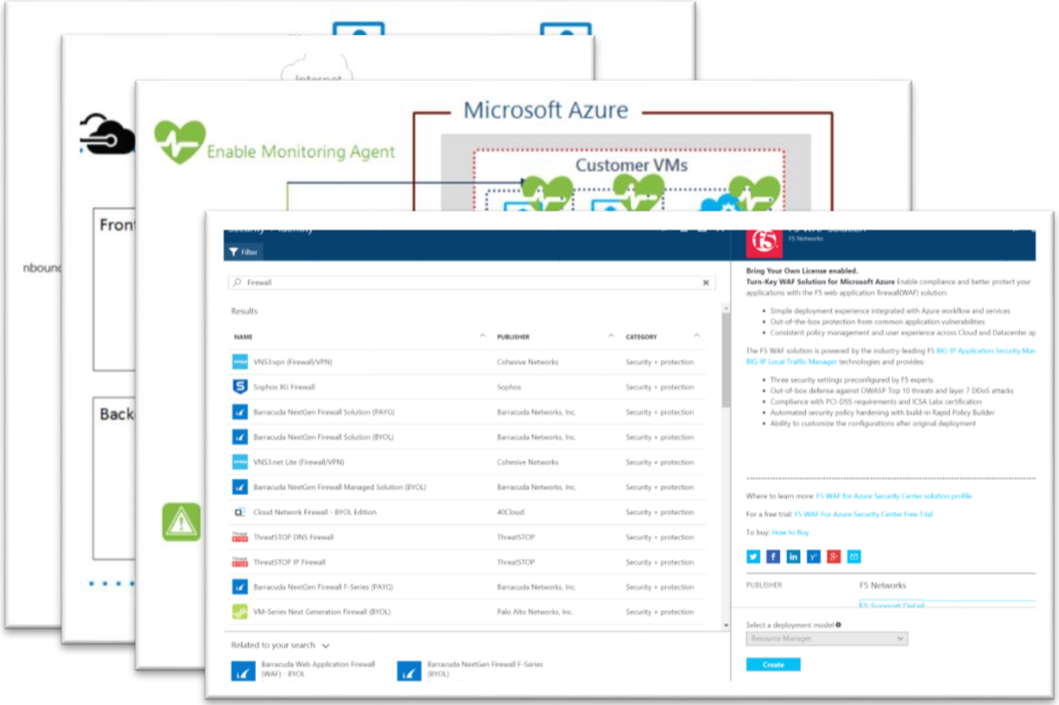
- Security Privileged Access Roadmap: Stage 1
  - **Separate Admin** account for admin tasks
  - **Privileged Access Workstations** (PAWs) Phase 1: Active Directory admins
  - **Unique** Local Admin **Passwords** for **Workstations**
  - **Unique** Local Admin **Passwords** for **Servers**
- Security Privileged Access Roadmap: Stage 2
  - **PAW** Phases 2 and 3: all **admins** and additional **hardening**
  - Time-bound privileges (**no permanent administrators**)
  - **Multi-factor** for time-bound elevation
  - **Just Enough Admin** (JEA) for DC Maintenance
  - **Lower attack surface** of Domain and DCs
  - **Attack Detection**
- Security Privileged Access Roadmap: Stage 3
  - Modernize **Roles** and **Delegation Model**
  - **Smartcard** or Passport Authentication for **all admins**
  - **Admin Forest** for Active Directory administrators
  - **Code Integrity** Policy for DCs (Server 2016)
  - **Shielded VMs** for virtual DCs (Server 2016 Hyper-V Fabric)

https://aka.ms/privsec

Virtual Networks protection in Azure

Safe and extend your Network Engineers experience with Azure Projects

- Remote Access to IaaS/VMs & hybrid connections solutions
- Network architecture and Network Security Groups planning in Azure IaaS
- VM network security audit
- Virtual Network Security Appliances – well known network security solutions in Azure Marketplace



Firewall

Results

NAME	PUBLISHER	CATEGORY
VNS3:vpn (Firewall/VPN)	Cohesive Networks	Security + protection
Sophos XG Firewall	Sophos	Security + protection
Barracuda NextGen Firewall Solution (PAYG)	Barracuda Networks, Inc.	Security + protection
Barracuda NextGen Firewall Solution (BYOL)	Barracuda Networks, Inc.	Security + protection
VNS3:net Lite (Firewall/VPN)	Cohesive Networks	Security + protection
Barracuda NextGen Firewall Managed Solution (BYOL)	Barracuda Networks, Inc.	Security + protection
Cloud Network Firewall - BYOL Edition	40Cloud	Security + protection
ThreatSTOP DNS Firewall	ThreatSTOP	Security + protection
ThreatSTOP IP Firewall	ThreatSTOP	Security + protection
Barracuda NextGen Firewall F-Series (PAYG)	Barracuda Networks, Inc.	Security + protection
VM-Series Next Generation Firewall (BYOL)	Palo Alto Networks, Inc.	Security + protection

Related to your search

Barracuda Web Application Firewall (WAF) - BYOL

Barracuda NextGen Firewall F-Series (BYOL)

Bring Your Own License enabled.
Turn-Key WAF Solution for Microsoft Azure Enable compliance and better protect your applications with the F5 web application firewall(WAF) solution:

- Simple deployment experience integrated with Azure workflow and services
- Out-of-the-box protection from common application vulnerabilities
- Consistent policy management and user experience across Cloud and Datacenter ap

The F5 WAF solution is powered by the industry-leading F5 BIG-IP Application Security Man BIG-IP Local Traffic Manager technologies and provides:

- Three security settings preconfigured by F5 experts
- Out-of-box defense against OWASP Top 10 threats and layer 7 DDoS attacks
- Compliance with PCI-DSS requirements and ICSA Labs certification
- Automated security policy hardening with build-in Rapid Policy Builder
- Ability to customize the configurations after original deployment

Where to learn more: F5 WAF for Azure Security Center solution profile

For a free trial: F5 WAF For Azure Security Center Free Trial

To buy: How to Buy

PUBLISHER F5 Networks

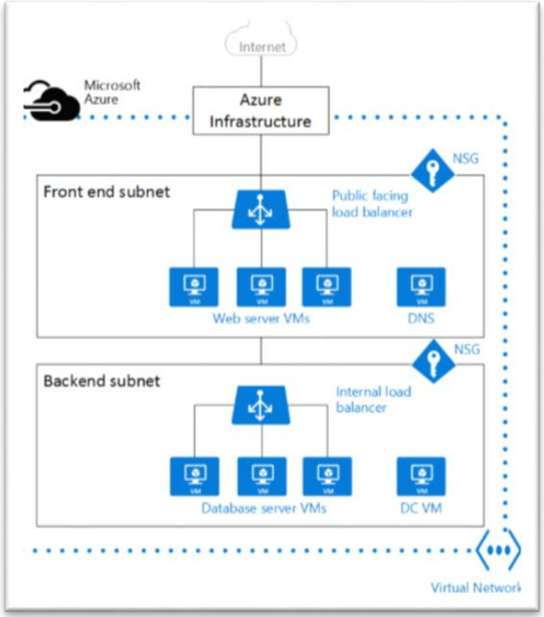
F5 Support Detail

Select a deployment model: Resource Manager

Create

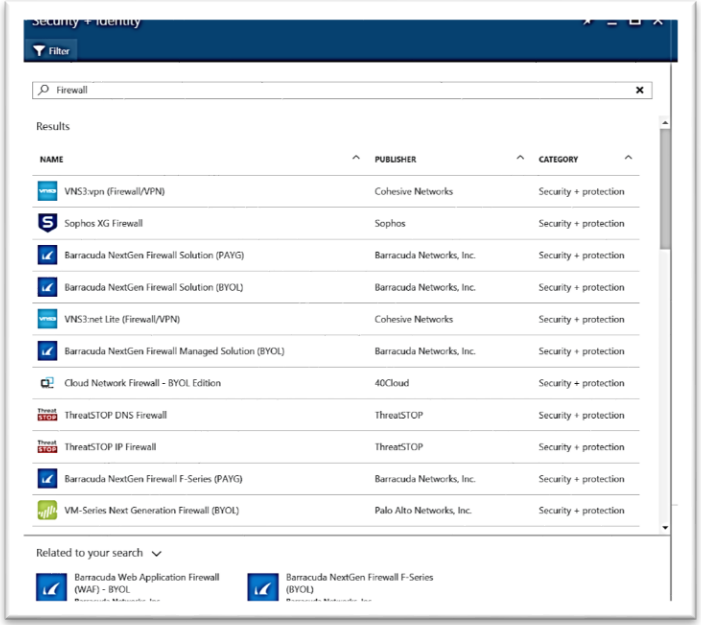
Microsoft

Virtual Networks protection’s Best Practices



- Subnet your networks based on security zones.
- Use Network Security Groups carefully.
- Use site-to-site VPN to connect Azure Virtual Networks.
- Configure host-based firewalls on infrastructure as a service (IaaS) virtual machines.
- Configure User Defined Routes to control traffic.
- Require forced tunneling.

Virtual Networks protection's Best Practices



Security + Identity

Firewall

Results

NAME	PUBLISHER	CATEGORY
VNS3:vpn (Firewall/VPN)	Cohesive Networks	Security + protection
Sophos XG Firewall	Sophos	Security + protection
Barracuda NextGen Firewall Solution (PAYG)	Barracuda Networks, Inc.	Security + protection
Barracuda NextGen Firewall Solution (BYOL)	Barracuda Networks, Inc.	Security + protection
VNS3:net Lite (Firewall/VPN)	Cohesive Networks	Security + protection
Barracuda NextGen Firewall Managed Solution (BYOL)	Barracuda Networks, Inc.	Security + protection
Cloud Network Firewall - BYOL Edition	40Cloud	Security + protection
ThreatSTOP DNS Firewall	ThreatSTOP	Security + protection
ThreatSTOP IP Firewall	ThreatSTOP	Security + protection
Barracuda NextGen Firewall F-Series (PAYG)	Barracuda Networks, Inc.	Security + protection
VM-Series Next Generation Firewall (BYOL)	Palo Alto Networks, Inc.	Security + protection

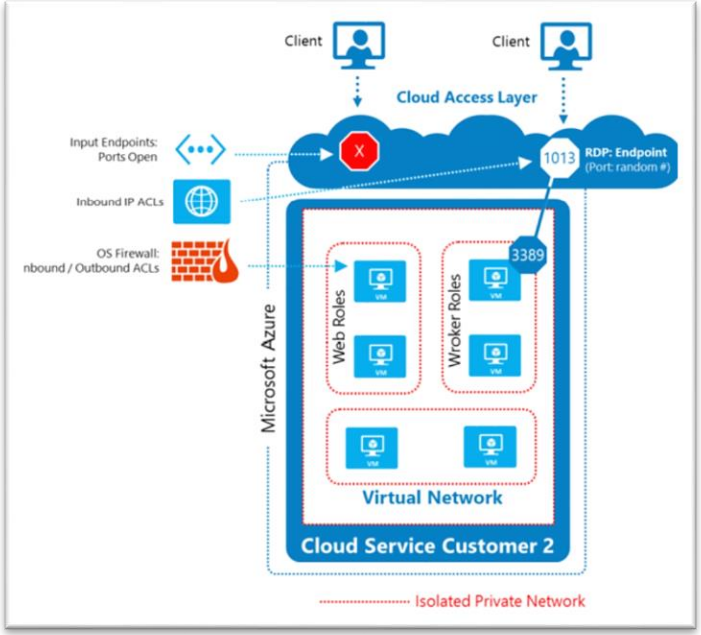
Related to your search

Barracuda Web Application Firewall (WAF) - BYOL

Barracuda NextGen Firewall F-Series (BYOL)

- Deploy virtual network security appliances - network security capabilities provided by virtual network security appliances include:
  - Firewalling
  - Intrusion detection and prevention
  - Vulnerability management
  - Application control
  - Network-based anomaly detection
  - Web filtering
  - Antivirus protection
  - Botnet protection
- Create perimeter networks for Internet-facing devices.
- Use ExpressRoute.

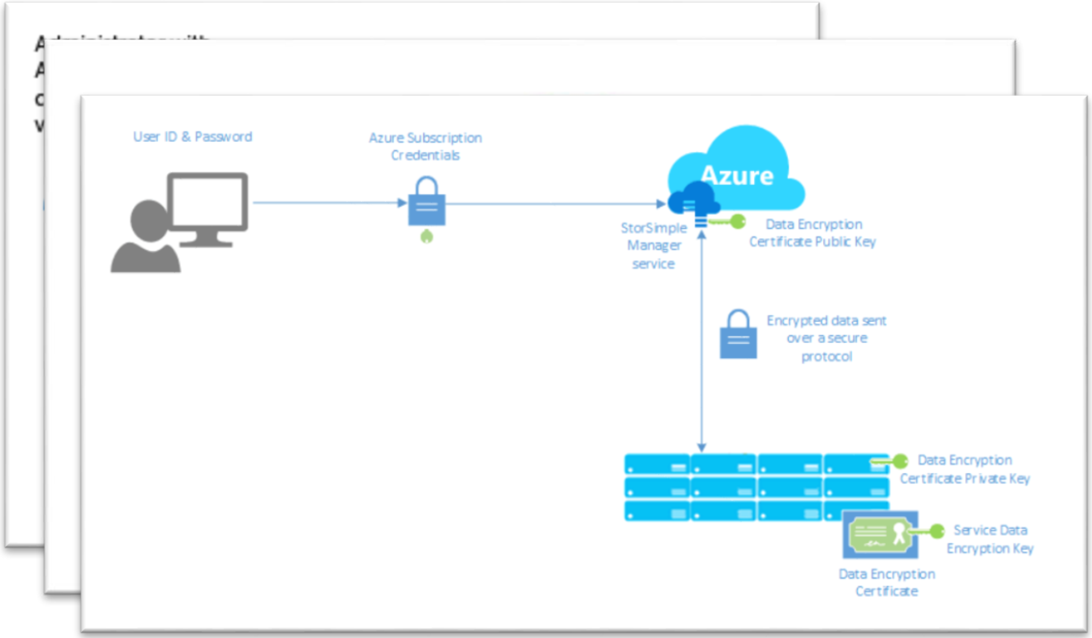
Virtual Networks protection’s Best Practices



- Optimize uptime and performance.
  - HTTP-based load balancing
  - External load balancing
  - Internal load balancing
  - Global load balancing
- Disable management protocols to virtual machines. Disable access to WinRM, RDP and SSH protocols. Other options can have to be used to access VMs for remote management:
  - Point-to-site VPN
  - Site-to-site VPN
  - ExpressRoute
- Enable Azure Security Center. Azure Security Center helps optimize and monitor network security by:
  - Providing network security recommendations.
  - Monitoring the state of your network security configuration.
  - Alerting you to network-based threats both at the endpoint and network levels.

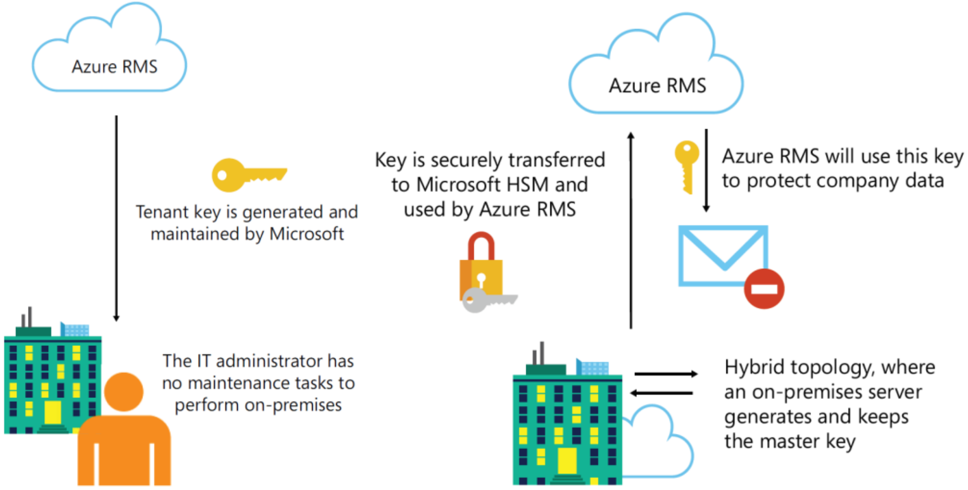
Data protection in Azure

Build the customer trust to store data in Azure


User ID & Password
Azure Subscription Credentials
Azure
StorSimple Manager service
Data Encryption Certificate Public Key
Encrypted data sent over a secure protocol
Data Encryption Certificate Private Key
Service Data Encryption Key
Data Encryption Certificate

- Help customer to understand data protection and encryption in Azure IaaS
- Azure Key Vault/BYOK discussion
- Plan, Design & Implement VMs/Storage/SQL encryption
- StorSimple as the part of solution

Select Azure RMS keys’ ownership



Tenant key is generated and maintained by Microsoft

The IT administrator has no maintenance tasks to perform on-premises

Key is securely transferred to Microsoft HSM and used by Azure RMS

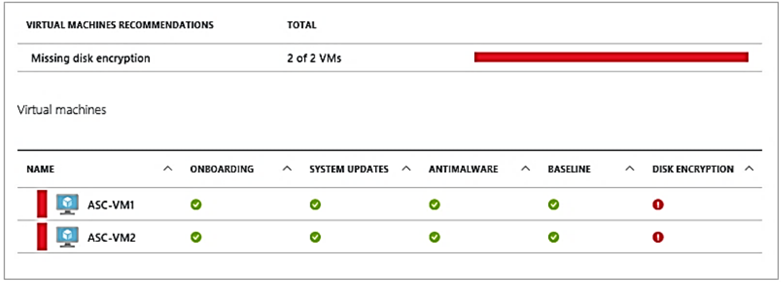
Azure RMS will use this key to protect company data

Hybrid topology, where an on-premises server generates and keeps the master key

Key operation	Default option (managed by Microsoft)	BYOK (managed by the company)
Revoke your tenant key	No (automatic)	No (automatic)
Re-key your tenant key	Yes	Yes
Back up and recover your tenant key	No	Yes
Export your tenant key	Yes	No*
Respond to a breach	Yes	Yes

***** If you use BYOK, you cannot export your tenant key from Azure RMS. The copy in Azure RMS is non-recoverable

Azure Disk Encryption for Windows and Linux IaaS VMs



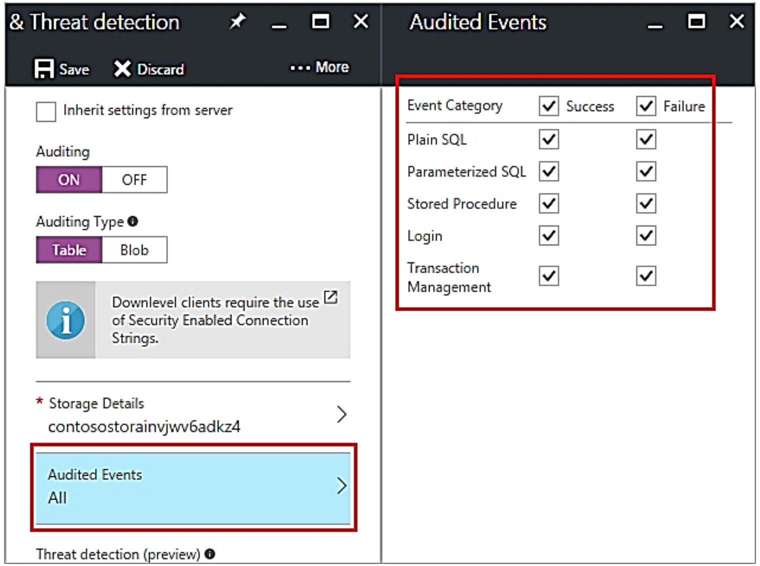
VIRTUAL MACHINES RECOMMENDATIONS	TOTAL
Missing disk encryption	2 of 2 VMs

Virtual machines

NAME	ONBOARDING	SYSTEM UPDATES	ANTIMALWARE	BASELINE	DISK ENCRYPTION
ASC-VM1	✓	✓	✓	✓	❗
ASC-VM2	✓	✓	✓	✓	❗

- The solution is **integrated** with **Azure Key Vault**
- Ensures that all data on the virtual machine disks are **encrypted at rest in Azure storage**.
- Enabling encryption on **new IaaS VMs that are created from pre-encrypted Virtual Hard Disk** (VHD) and encryption keys
- Encryption on **new IaaS VMs** that are created from the **Azure Marketplace images**
- Encryption on **existing IaaS VMs** that are running in Azure
- **Disabling encryption** on **Windows IaaS VMs**
- **Disabling** encryption on **data drives** for **Linux IaaS VMs**

Securing Azure SQL Database



☐ Inherit settings from server

Auditing: [✓ ON] OFF

Auditing Type: [✓ Table] Blob

Downlevel clients require the use of Security Enabled Connection Strings.

* Storage Details
contosostorainvjwv6adkz4

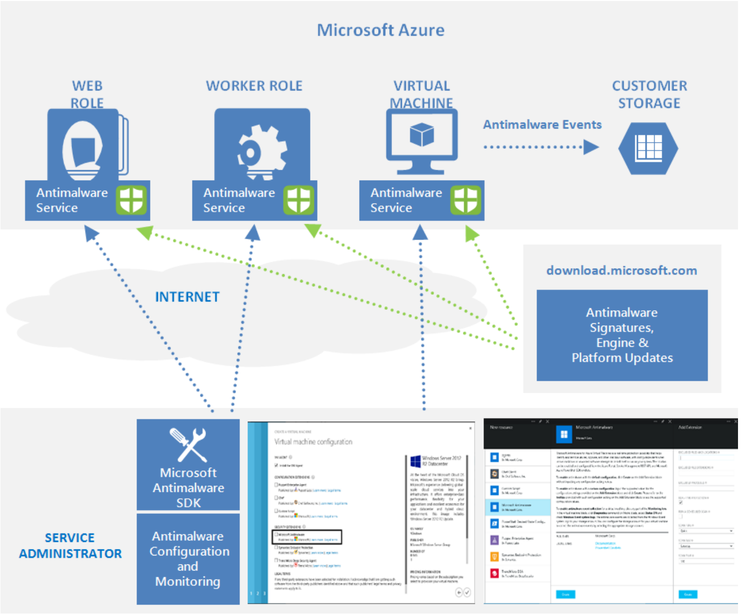
Audited Events
All

Threat detection (preview)

Event Category	☑ Success	☑ Failure
Plain SQL	☑	☑
Parameterized SQL	☑	☑
Stored Procedure	☑	☑
Login	☑	☑
Transaction Management	☑	☑

- Developers! Developers! Developers!
- Azure SQL Firewall
- Transparent Data Encryption (TDE)
- SQL Always Encrypted
- Row-level security
- Dynamic Data Masking
- Azure SQL Database auditing
- Some features are not applied to services like Azure SQL Data Warehouse

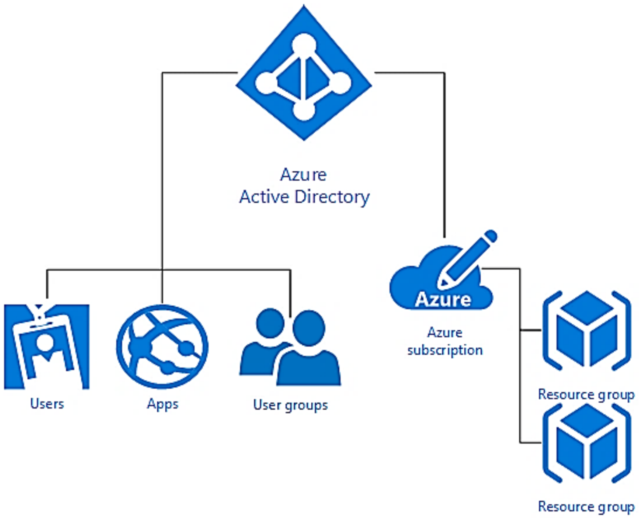
VMs OS security management best practices



- **Hardening VMs OS** with **Security Compliance Manager** and **Microsoft Security guide**
- **Microsoft Antimalware in Azure** or other integrated solutions/Security extensions
- Microsoft **Antimalware** For **Azure Cloud Services**
- Developers! Developers! Developers!

Microsoft

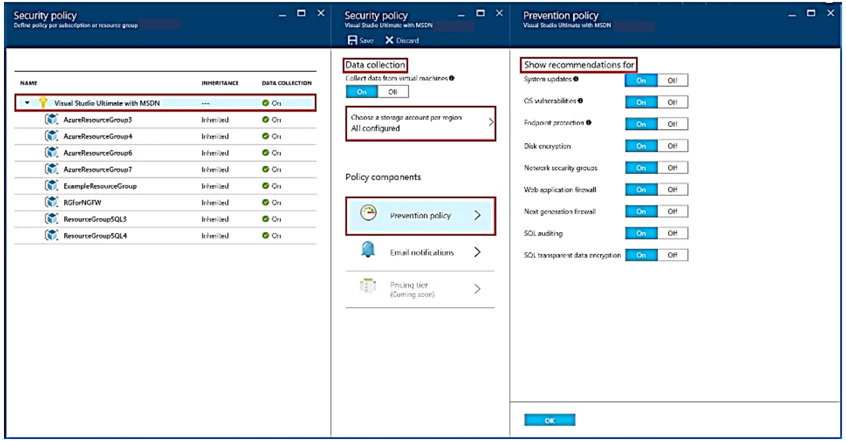
Azure IaaS security management



- Planning and deploy **Azure Security Center**
- **Role Based Access Control** for Azure IaaS
- **Audit log & collection** and Power BI
- Security monitoring with **Operations Management Suite** (OMS)

Azure Security Center

Security Center helps prevent, detect, and respond to threats



Security policy

Define policy per subscription or resource group [redacted]

NAME	INHERITANCE	DATA COLLECTION
Visual Studio Ultimate with MSDN	---	✓ On
AzureResourceGroup3	Inherited	✓ On
AzureResourceGroup4	Inherited	✓ On
AzureResourceGroup6	Inherited	✓ On
AzureResourceGroup7	Inherited	✓ On
ExampleResourceGroup	Inherited	✓ On
RGforNGFW	Inherited	✓ On
ResourceGroupSQL3	Inherited	✓ On
ResourceGroupSQL4	Inherited	✓ On

Security policy

Visual Studio Ultimate with MSDN [redacted]

Data collection

Collect data from virtual machines: [✓ On] Off

Choose a storage account per region: All configured

Policy components

- Prevention policy
- Email notifications
- Pricing tier (Coming soon)

Prevention policy

Visual Studio Ultimate with MSDN [redacted]

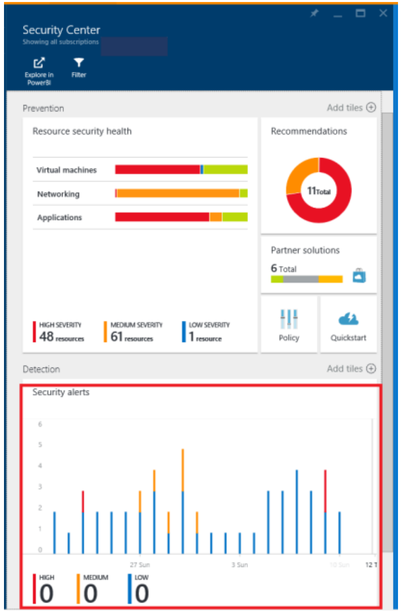
Show recommendations for

System updates	[✓ On] Off
OS vulnerabilities	[✓ On] Off
Endpoint protection	[✓ On] Off
Disk encryption	[✓ On] Off
Network security groups	[✓ On] Off
Web application firewall	[✓ On] Off
Next generation firewall	[✓ On] Off
SQL auditing	[✓ On] Off
SQL transparent data encryption	[✓ On] Off

- **Security Policy** for Azure subscriptions and resource groups for security data collection
- **Security recommendations**
  - Provisioning antimalware to help identify and remove malicious software
  - Configuring network security groups and rules to control traffic to VMs
  - Provisioning of web application firewalls to help defend against attacks that target your web applications
  - Deploying missing system updates
  - Addressing OS configurations that do not match the recommended baselines
- **Resource health**

Azure Security Center

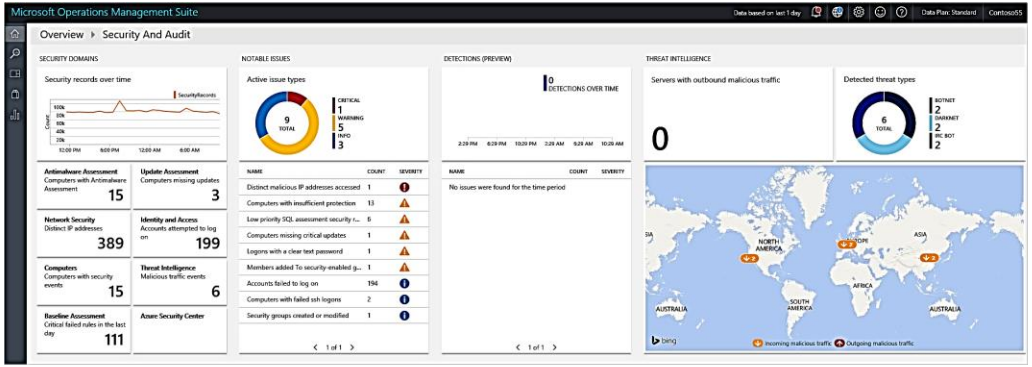
Security Center helps prevent, detect, and respond to threats



- **Security alerts** - automatically collects, analyzes, and integrates log data from your Azure resources, the network, and partner solutions like antimalware programs and firewalls.
  - Compromised VMs communicating with known malicious IP addresses
  - Advanced malware detected by using Windows error reporting
  - Brute force attacks against VMs
  - Security alerts from integrated antimalware programs and firewalls
- **Partner solutions** lets you monitor at a glance the health status of your partner solutions integrated with your Azure subscription.

Monitoring risk and health of VMs/hybrid infra

Security and Audit dashboard in Azure Operational Insights



Microsoft Operations Management Suite

Data based on last 1 day | Data Plan: Standard | Contoso55

Overview ▸ Security And Audit

SECURITY DOMAINS

Security records over time

Antimalware Assessment
Computers with Antimalware Assessment
15

Update Assessment
Computers missing updates
3

Network Security
Distinct IP addresses
389

Identity and Access
Accounts attempted to log on
199

Computers
Computers with security events
15

Threat Intelligence
Malicious traffic events
6

Baseline Assessment
Critical failed rules in the last day
111

Azure Security Center

NOTABLE ISSUES

Active issue types

NAME	COUNT	SEVERITY
Distinct malicious IP addresses accessed	1	❗
Computers with insufficient protection	13	⚠
Low priority SQL assessment security r...	6	⚠
Computers missing critical updates	1	⚠
Logons with a clear text password	1	⚠
Members added To security-enabled g...	1	⚠
Accounts failed to log on	194	ℹ
Computers with failed ssh logons	2	ℹ
Security groups created or modified	1	ℹ

‹ 1 of 1 ›

DETECTIONS (PREVIEW)

NAME	COUNT	SEVERITY
No issues were found for the time period		

‹ 1 of 1 ›

THREAT INTELLIGENCE

Servers with outbound malicious traffic

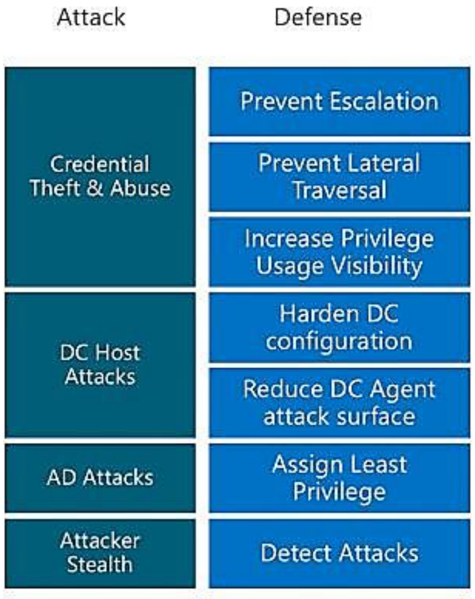
0

Detected threat types

FOCUS AREAS

- Security and Compliance
- Identity and Access
- Antimalware assessment
- Threat Intelligence
- Availability and Business Continuity
- Performance and Scalability

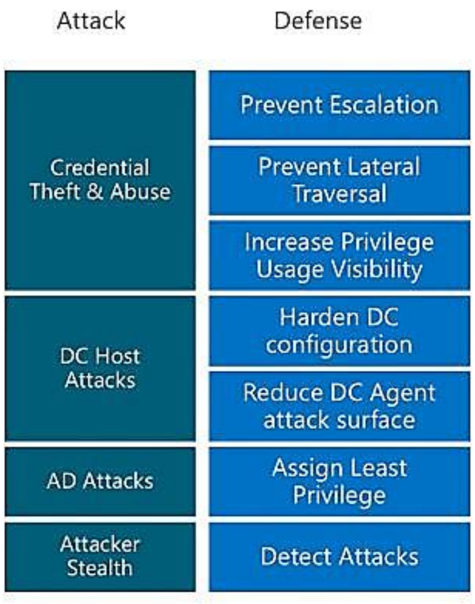
Azure IaaS/on-premises infra security resources



Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
DC Host Attacks	Harden DC configuration
	Reduce DC Agent attack surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks

- **Securing Privileged Access** - https://aka.ms/privsec
- **Privileged Access Workstations** – http://aka.ms/cyberpaw
- **Azure Role-Based Access Control (RBAC)** - https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure
- **Azure Network Security Groups (NSG) – Best Practices and Lessons Learned** - https://blogs.msdn.microsoft.com/igorpag/2016/05/14/azure-network-security-groups-nsg-best-practices-and-lessons-learned/
- **Securing Remote Access to Azure Virtual Machines over the Internet** - https://blogs.msdn.microsoft.com/azuresecurity/2015/09/08/securing-remote-access-to-azure-virtual-machines-over-the-internet/
- **Configure forced tunneling using the Azure Resource Manager deployment model** - https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm
- **Microsoft cloud services and network security** - https://docs.microsoft.com/en-us/azure/best-practices-network-security

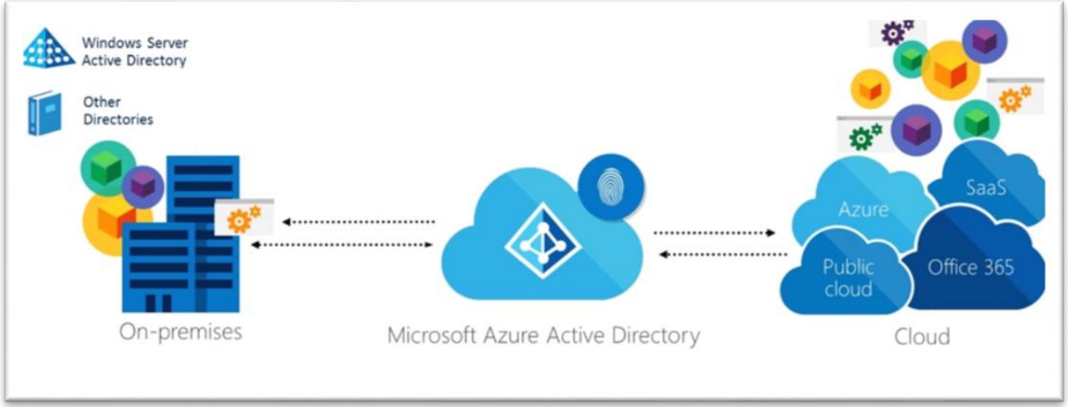
Azure IaaS/on-premises infra security resources



Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
DC Host Attacks	Harden DC configuration
	Reduce DC Agent attack surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks

- **Encrypt an Azure Virtual Machine** - https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption
- **Azure Storage Service Encryption for Data at Rest** - https://docs.microsoft.com/en-us/azure/storage/storage-service-encryption
- **Overview of Azure SQL Database firewall rules** - https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure
- **Always Encrypted: Protect sensitive data in SQL Database and store your encryption keys in Azure Key Vault** - https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault
- **Dynamic Data Masking** - https://msdn.microsoft.com/library/mt130841.aspx
- **Get started with SQL database auditing** - https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing-get-started
- **Deploying Antimalware Solutions on Azure Virtual Machines** - https://azure.microsoft.com/en-us/blog/deploying-antimalware-solutions-on-azure-virtual-machines/
- **Azure Security Center planning and operations guide** - https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide
- **Azure Security Center Common Configuration Identifiers and Baseline Rules** - https://gallery.technet.microsoft.com/Azure-Security-Center-a789e335
- **Get insights from Azure Security Center data with Power BI** - https://docs.microsoft.com/en-us/azure/security-center/security-center-powerbi
- **Get started with Log Analytics** - https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-get-started
- **Monitoring and responding to security alerts in Operations Management Suite Security and Audit Solution** - https://docs.microsoft.com/en-us/azure/operations-management-suite/oms-security-responding-alerts

Cloud/Hybrid Identity Resources



- **Azure Active Directory Proof of Concept Playbook** - http://aka.ms/aadpocplaybook
- **Microsoft Hybrid Identity Design Considerations Guide** - https://docs.microsoft.com/en-us/azure/active-directory/active-directory-hybrid-identity-design-considerations-overview
- **Conditional Access to applications that are hosted on-premises -** https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-on-premises-setup

Microsoft