

# Azure Security Overview

---

Maxime Coquerel - MVP Azure



# # Speaker

Maxime Coquerel

Director Cloud Security Architect

Email : [max.coquerel@live.fr](mailto:max.coquerel@live.fr)

Blog : [zigmax.net](https://zigmax.net) (Since 2012)

Github : <https://github.com/zigmax>

Twitter : [@zig\\_max](https://twitter.com/zig_max)

Open Source Contributor (Kubernetes / VSCode).



# Disclaimer

*“Any views or opinions expressed in this presentation are those of the presenter and not necessarily represent the view and opinions of my employer, its ownership, management or its employees .”*

Thank you!

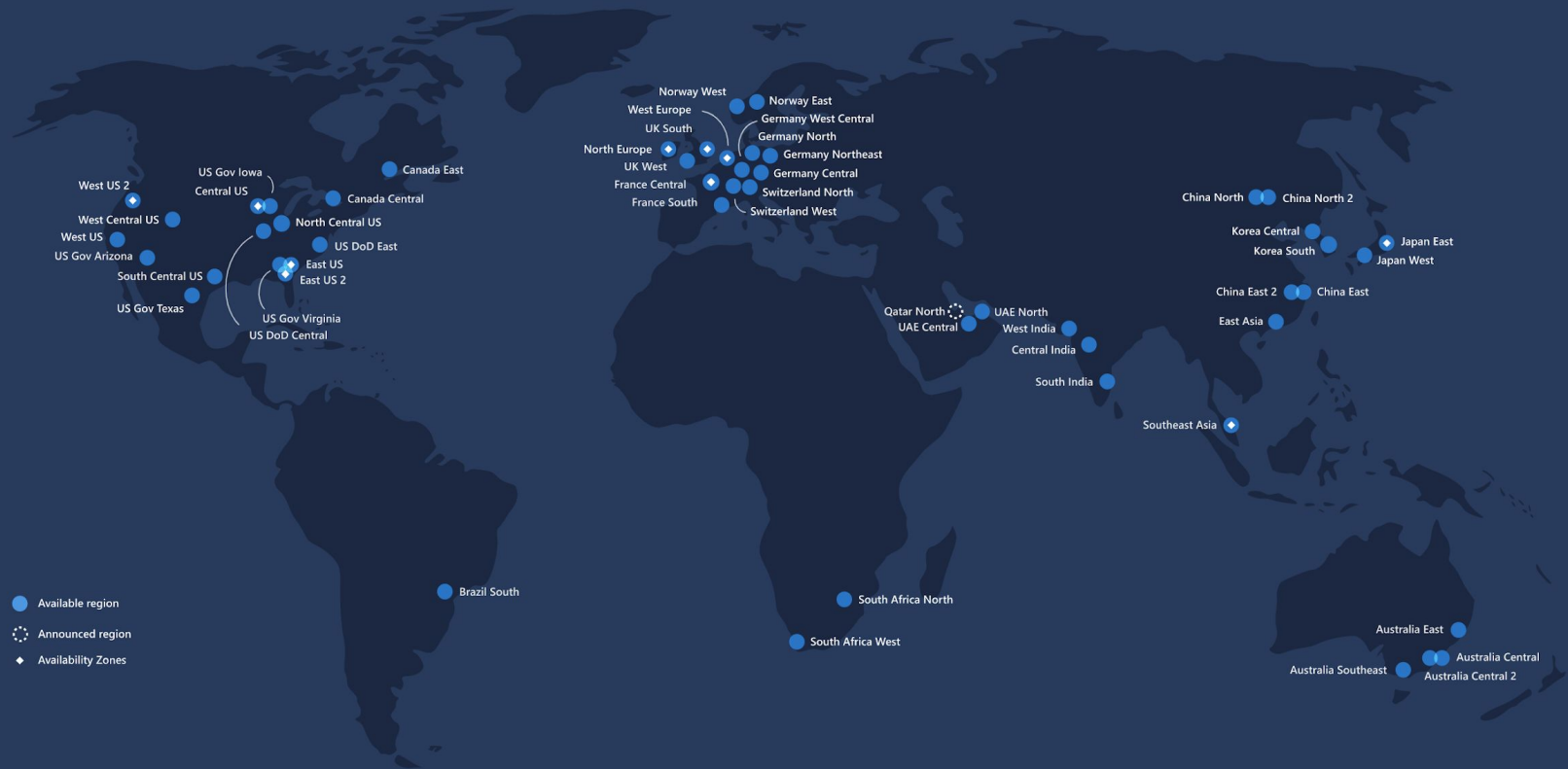


# Session Agenda / Goal

- Introduction
- Compliance & Gouvernance
- Identities Management
- Encryption & Vault
- Infrastructure
- Azure Sentinel
- Azure Security Center
- Investigation
- Conclusion



55 regions worldwide 140 available in 140 countries



\* Two Azure Government Secret region locations undisclosed

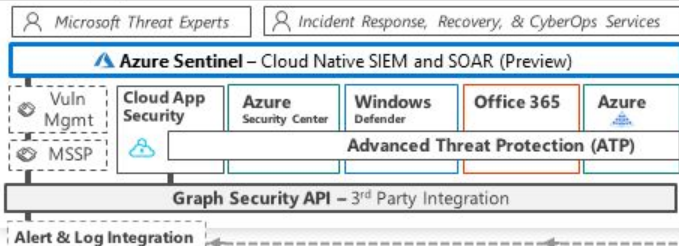
# The Azure Periodic Table

Explore the power and possibilities of Azure

Explore the power and possibilities of Azure														AZURE IOT HUB
SECURITY CENTER								AZURE AD B2C	AZURE AD	AZURE AD DC	MULTI-FACTOR	EVENT HUBS		
LINUX HUB	VIRTUAL MACHINES								MEDIA PLAYER	CONTENT PROTECTION	MEDIA ENCODING	MEDIA STREAMING	POWERBI	
SCHEDULER	SERVICE FABRIC								CDN	DATA CATALOG	DATA FACTORY	DATA LAKE ANALYTICS	MACHINE LEARNING	
AUTOMATION	BATCH	VPN GATEWAY	EXPRESSROUTE	AZURE DNS	APPLICATION GATEWAY	AZURE BACKUP	BIZTALK SERVICES	CDN	DATA CATALOG	DATA FACTORY	DATA LAKE ANALYTICS	MACHINE LEARNING		
OPINSIGHTS	REMOTEAPP	RESERVED IP	VIRTUAL NETWORK	TRAFFIC MANAGER	LOAD BALANCER	SITE RECOVERY	SERVICE BUS	MEDIA SERVICES	HDINSIGHT	TABLE/BLOB STORAGE	DATA LAKE STORAGE	STREAM ANALYTICS		
KEY VAULT	CLOUD SERVICES	PUBLIC IP	LOGIC APPS	API APPS	APP SERVICES	API MANAGEMENT	MOBILE APPS	MOBILE ENGAGEMENT	WEB APPS	CUSTOM DOMAIN	SSL CERTIFICATES	NOTIFICATION HUBS		
DEVTEST LABS	VS APP INSIGHTS	VS ONLINE	SQL DATABASE	SQL DATA WAREHOUSE	DOCUMENTDB	CACHE	SEARCH	STORAGE	STORSIMPLE	IMPORT / EXPORT	PREMIUM STORAGE	SQL ELASTIC DB		



## Security Operations Center (SOC)



## Cybersecurity Reference Architecture

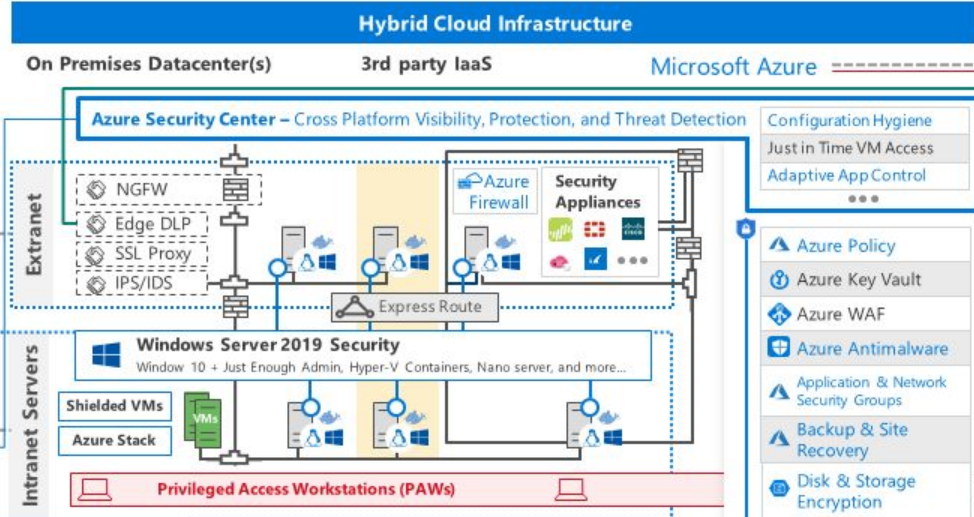
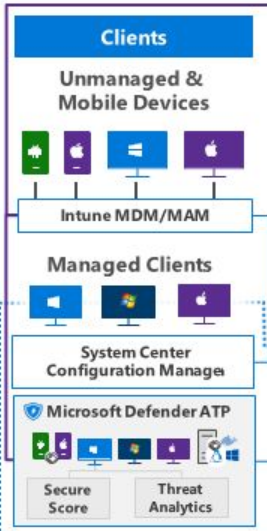
May 2018 – <https://aka.ms/MCRA> | [Video Recording](#) | [Strategies](#)

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. [Securing Privileged Access](#)
2. [Office 365 Security](#)
3. [Rapid Cyberattacks \(Wannacrypt/Petva\)](#)



Security Development Lifecycle (SDL)

## Software as a Service

Office 365

Secure Score  
Customer Lockbox

Dynamics 365

**Information Protection**

**Conditional Access – Identity Perimeter Management**

Cloud App Security

**Azure Information Protection (AIP)**

Discover  
Classify  
Protect  
Monitor

Hold Your Own Key (HYOK)

**AIP Scanner**

Office 365

Data Loss Protection  
Data Governance  
eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Compliance Manager

**Identity & Access**

**Azure Active Directory**

Azure AD Identity Protection  
Leaked cred protection  
Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Microsoft

Trust Center

Intelligent Security Graph



# **Compliance & Gouvernance**

# The Trusted Cloud

Azure has the deepest and most comprehensive compliance coverage in the industry

## GLOBAL



ISO 27001



ISO 27018



ISO 27017



ISO 22301



ISO 9001



SOC 1  
Type 2



SOC 2  
Type 2



SOC 3



CSA STAR  
Self-Assessment



CSA STAR  
Certification



CSA STAR  
Attestation

## US GOV



Moderate  
JAB P-ATO



High  
JAB P-ATO



DoD DISA  
SRG Level 2



DoD DISA  
SRG Level 4



DoD DISA  
SRG Level 5



SP 800-171



FIPS 140-2



Section 508  
VPAT



ITAR



CJIS



IRS 1075

## INDUSTRY



PCI DSS  
Level 1



CDSA



MPAA



FACT UK



Shared  
Assessments



FISC Japan



HIPAA /  
HITECH Act



HITRUST



GxP  
21 CFR Part 11



MARS-E



IG Toolkit UK



FERPA



GLBA



FFIEC

## REGIONAL



Argentina  
PDPA



EU  
Model Clauses



UK  
G-Cloud



China  
DJCP



China  
GB 18030



China  
TRUCS



Singapore  
MTCS



Australia  
IRAP/CCSL



New Zealand  
GCIO



Japan My  
Number Act



ENISA  
IAF



Japan CS  
Mark Gold



Spain  
ENS



Spain  
DPA



India  
MeitY



Canada  
Privacy Laws



Privacy  
Shield



Germany IT  
Grundschutz  
workbook

# Microsoft Trust Center

We build our Trusted Cloud on four foundational principles



## Security

We build our services from the ground up to help safeguard your data



## Privacy

Our policies and processes help keep your data private and in your control



## Compliance

We provide industry-verified conformity with global standards



## Transparency

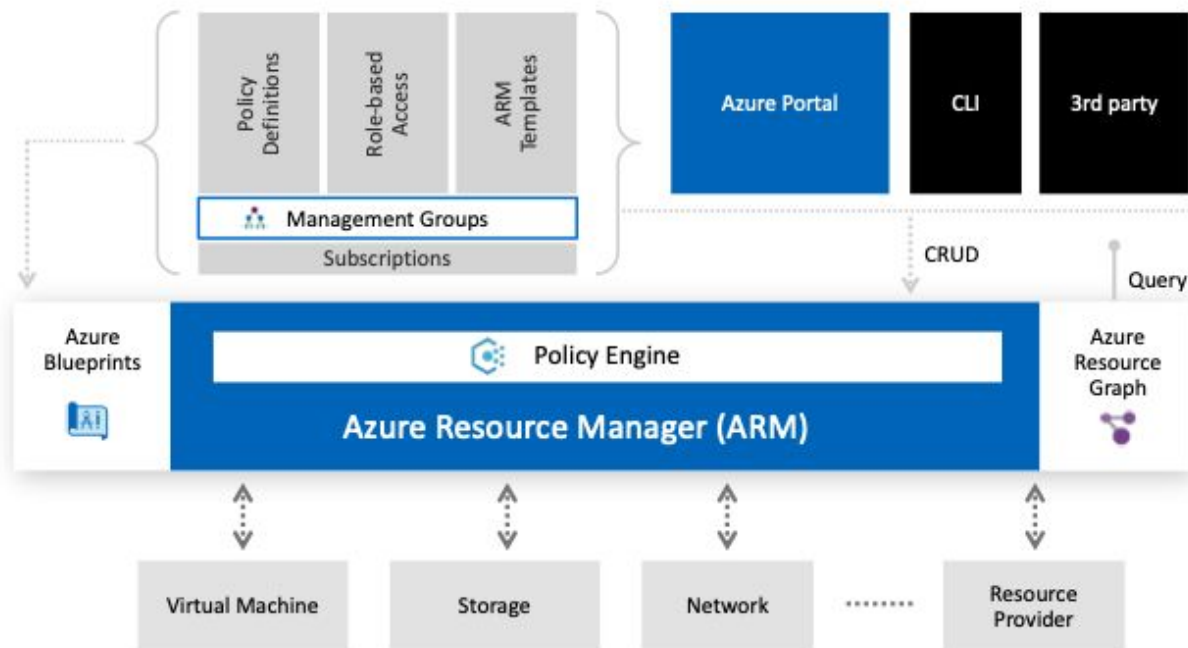
We make our policies and practices clear and accessible to everyone

<https://www.microsoft.com/en-us/trustcenter/default.aspx>

# Azure Governance Architecture

Providing control over the cloud environment, without sacrificing developer agility

- 1. Environment factory**  
Deploy and update cloud environments in a repeatable manner using composable artifacts
- 2. Policy-based control**  
Real-time enforcement, compliance assessment and remediation at scale
- 3. Resource visibility**  
Query, explore & analyze cloud resources at scale



# Introducing Azure Management Groups

Efficiently apply governance controls and manage groups of Azure subscriptions



1 Ensure compliance

2 Empower DevOps

3 Manage costs

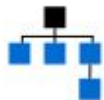


## Simplify subscription management

Group subscriptions into logical groups

Inherit properties that apply to all subscriptions

View aggregated information above the subscription level



## Fit your organization

Create a flexible hierarchy that can be updated quickly

Mirror the hierarchy to the organizational model that works for you

Scale up or down depending on the organizational needs



## Apply controls at scale

Leverage Azure Resource Manager (ARM) objects that integrate with other Azure services

Azure services:

Azure Policy

RBAC

Azure Cost Management

Azure Blueprints

Azure Security Center

# Management Group & subscription modeling strategy



1 Ensure compliance

2 Empower DevOps

3 Manage costs



Org Management Group



Prod RBAC + Policy



App A  
Prod



App B  
Prod



App D  
Prod



Shared services  
(Prod)



Pre-Prod RBAC + Policy



App A  
Pre-Prod



App B  
Pre-Prod



App C  
Pre-Prod



Shared services  
(Pre-Prod)

Microsoft  
recommended

# Azure Policy



- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy (**NEW**)

## Enforcement & Compliance



- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and aggregate policy states with policy initiative
- Exclusion Scope

## Apply policies at scale



- Real time remediation
- Remediation on existing resources (**NEW**)

## Remediation



# Azure Policy

[Home](#) > [Policy - Compliance](#) > Diagnostic logs collection enablement

## Diagnostic logs collection enablement

Initiative compliance

[View definition](#) [Edit assignment](#) [Delete assignment](#) [Create Remediation Task](#)

Name

Diagnostic logs collection enablement

Description

--

Definition

Diagnostic logs collection enablement

Scope

Contoso IT - demo

Excluded scopes

0

Assignment ID

/subscriptions/e4272367-5645-4c4e-9c67-3b74b59a6982/providers/Microsoft.Authorization/policyAssignments/5a61a4cf44864cd1ae2b61a1

Selected Scopes

4 selected subscriptions

Excluded scopes

Compliance state



Non-compliant

Overall resource compliance

58%

93 out of 159

Non-compliant policies

4

out of 5

Non-compliant resources

66

out of 159

Events (last 7 days)

Audit 0

Append 0

Deny 0

Deploy 4078

[Policies](#) [Non-compliant resources](#) [Events](#) [Remediation tasks](#) [Deployed Resources](#)

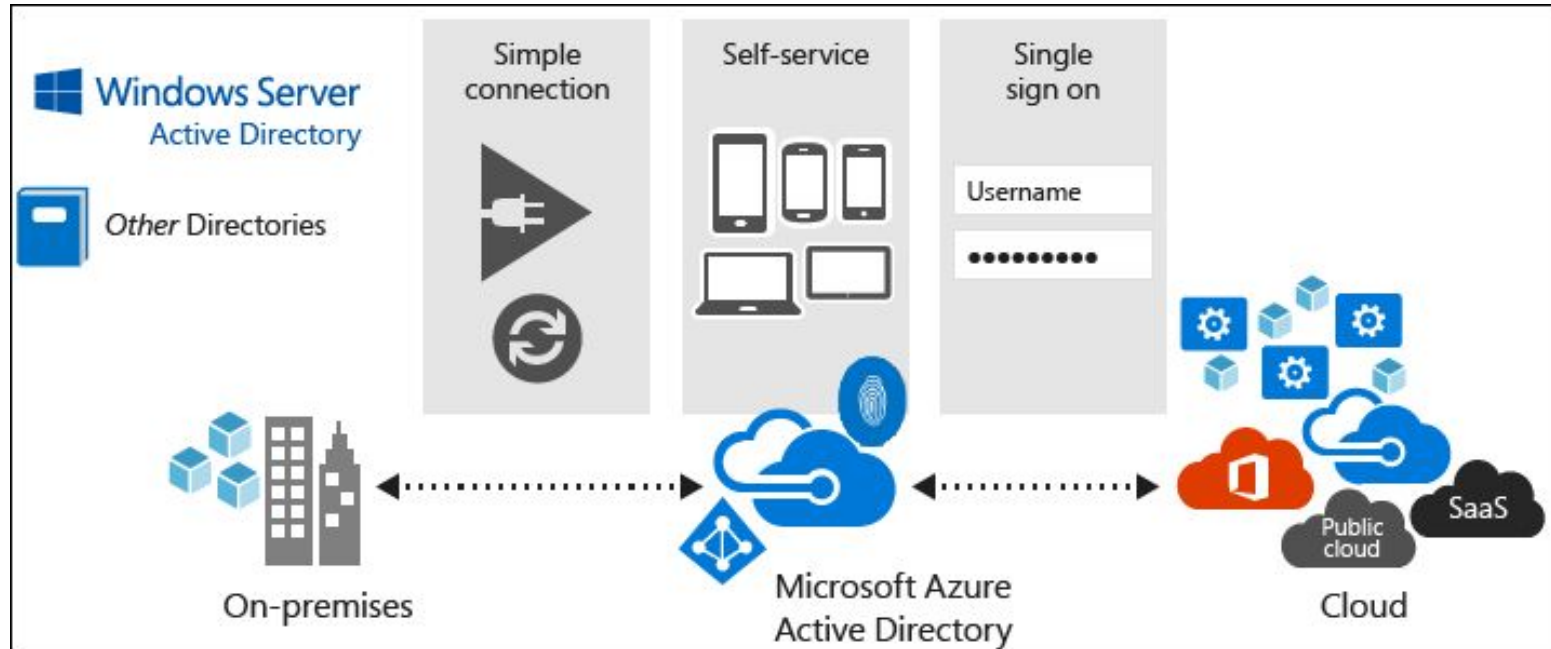
Filter by policy name or definition id...

All compliance states

NAME	EFFECT TYPE	COMPLIANCE STATE	NON-COMPLIANT RESOURCES	TOTAL RESOURCES
<a href="#">Enable diagnostic logs_VM</a>	DeployIfNotExists	Non-compliant	47	74
<a href="#">Enable diagnostic logs_SQL</a>	DeployIfNotExists	Non-compliant	10	10
<a href="#">Enable diagnostic logs_NSG</a>	DeployIfNotExists	Non-compliant	6	72
<a href="#">Enable diagnostic logs_backup</a>	DeployIfNotExists	Non-compliant	3	3
<a href="#">Enable diagnostic logs_VMSS</a>	DeployIfNotExists	Compliant	0	0

# **Identities Management**

# Azure AD



# Azure B2C

## Customers

### Social IDs



### Business & Government IDs



## Azure Active Directory B2C

- ➔ Provide branded (white-label) registration and login experiences
- ➔ Securely authenticate your customers using their preferred identity provider
- ➔ Capture login, preference, and conversion data for customers

## Business



### Apps & APIs

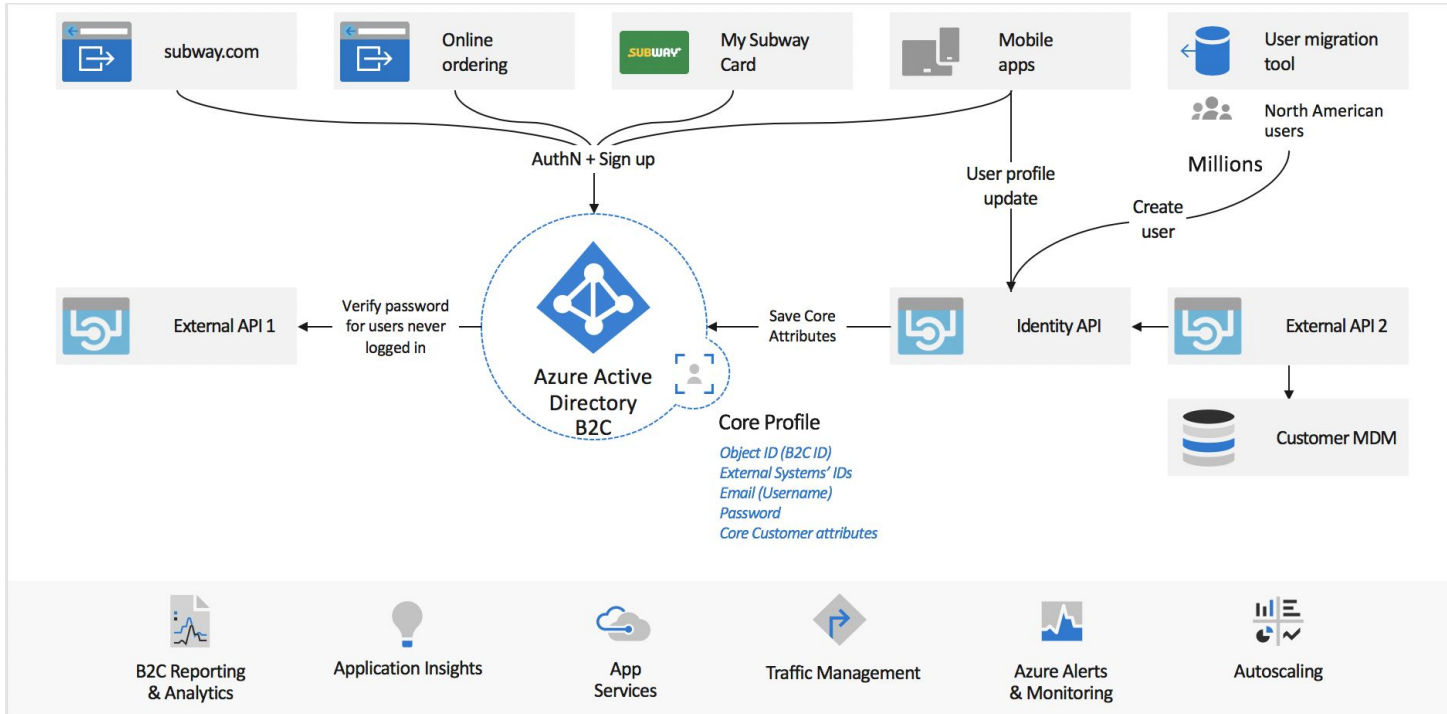


### Analytics



### CRM and Marketing Automation

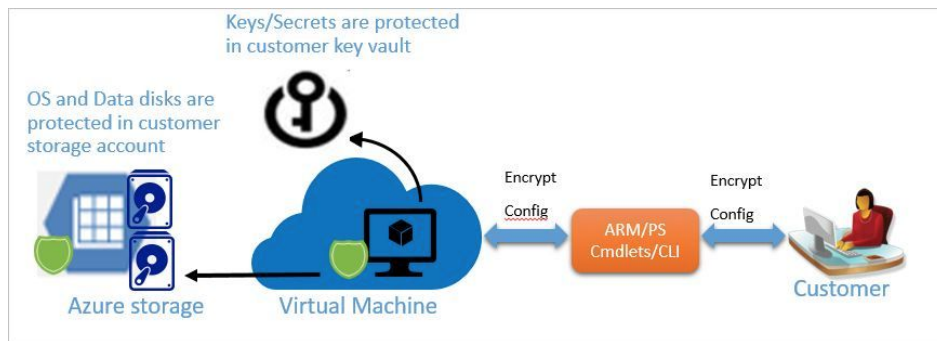
# Azure B2C - Example Subway



# **Encryption & Vault**

# Azure Disk Encryption

- Need Azure Key Vault / Azure AAD /
- Based on Windows : BitLocker / Linux : DM-CRYPT



Howto : Azure Disk Encryption

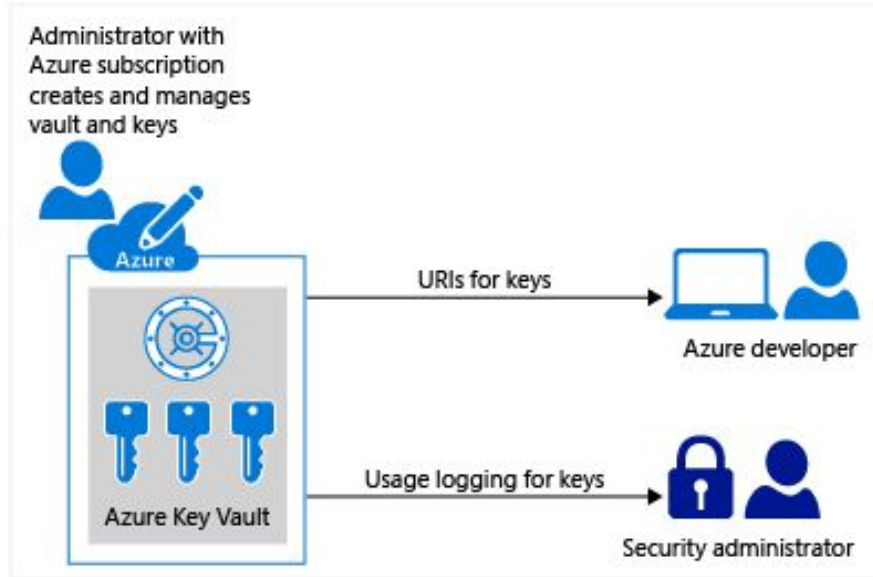
<http://zigmax.net/azure-chiffre-une-machine-virtuelle-azure-disk-encryption/>

Official Documentation :

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption>



# Azure Key Vault



- 1.....Creates a key vault.
- 2.....Authorizes applications and users for specific operations.
- 3.....Add keys and secrets to key vault.
- 4.....Configure application with URI of key or secret or entire vault
- 5.....Use secrets and keys in the key vault.  
Or, less commonly, add / update keys and secrets in the key vault.
- 6..... Monitors key vault logs.
- 7.....Update keys and secrets as needed.
- 8.....Updates permissions as needed.
- 9.....Delete key or secret when no longer needed.
- 10.....Deletes key vault when no longer needed.

Example : [https://github.com/zigmax/azureqc17-security/tree/master/AzureKeyVault\\_Demo](https://github.com/zigmax/azureqc17-security/tree/master/AzureKeyVault_Demo)

# Infrastructure

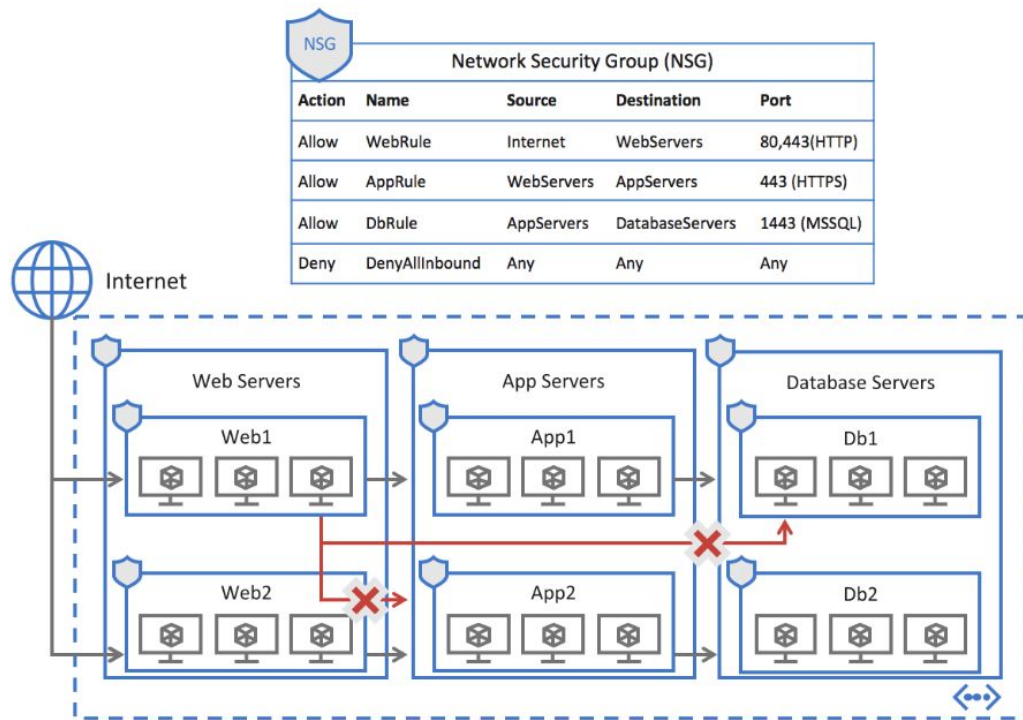
# Network and Application Security Group (NSG)

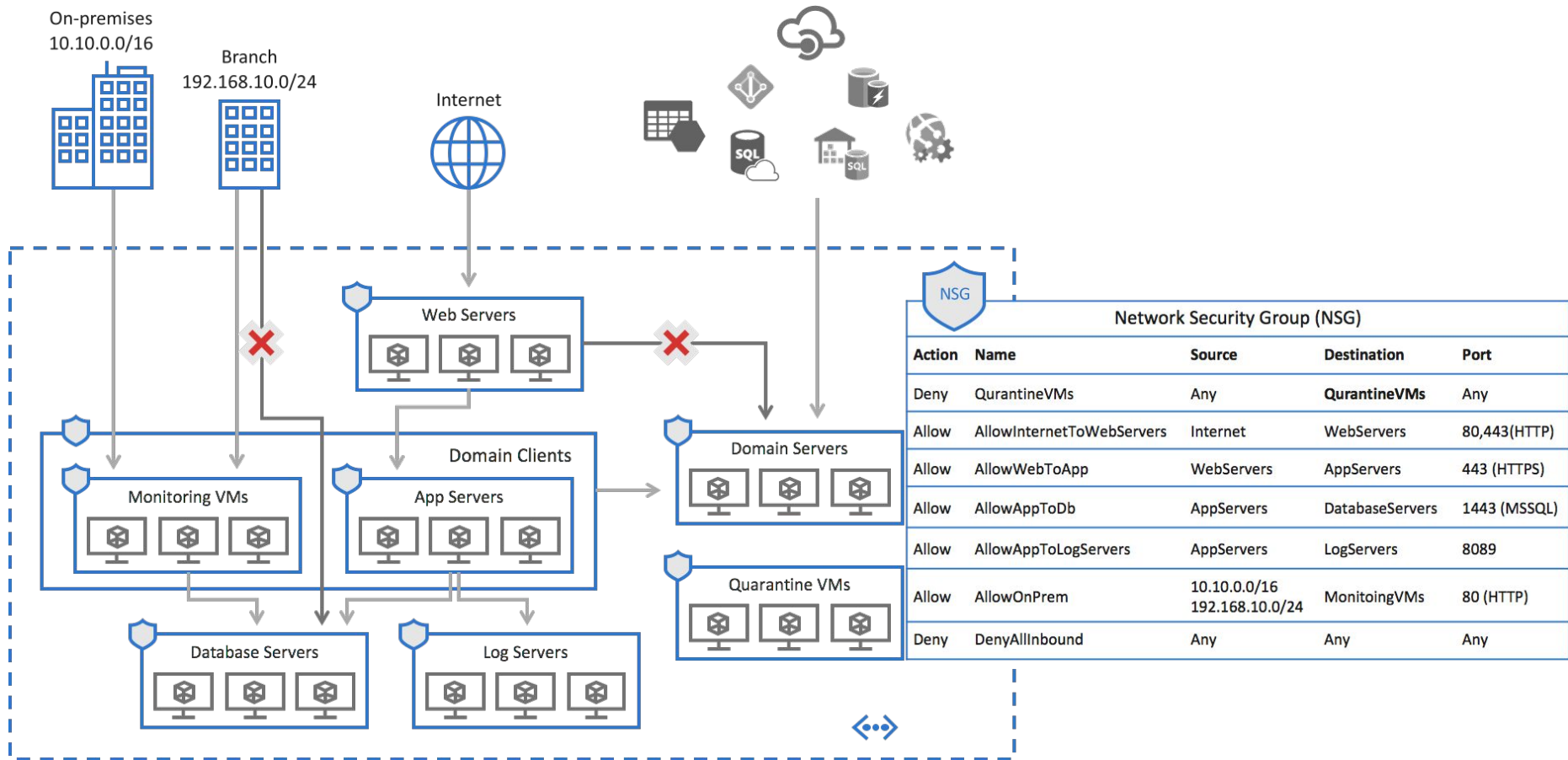
## Network Security Groups

- Protects your workloads with distributed ACLs
- Simplified configuration with augmented security rules
- Enforced at every host, applied on multiple subnets

## Application Security Groups

- Micro-segmentation for dynamic workloads
- Named monikers for groups of VMs
- Removes management of IP addresses





# Azure Firewall

## Cloud native stateful Firewall as a Service

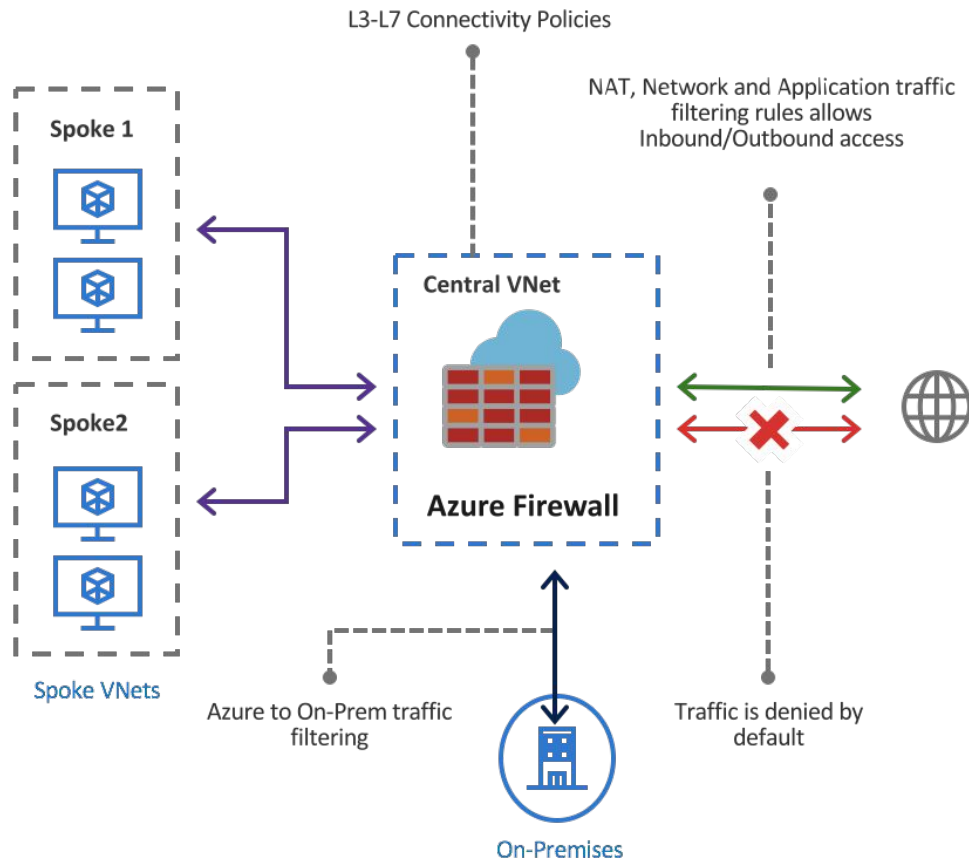
- Built-in High Availability and Auto Scale
- Network and Application traffic filtering
- Centralized policy across VNets and Subscriptions

## Complete VNET protection

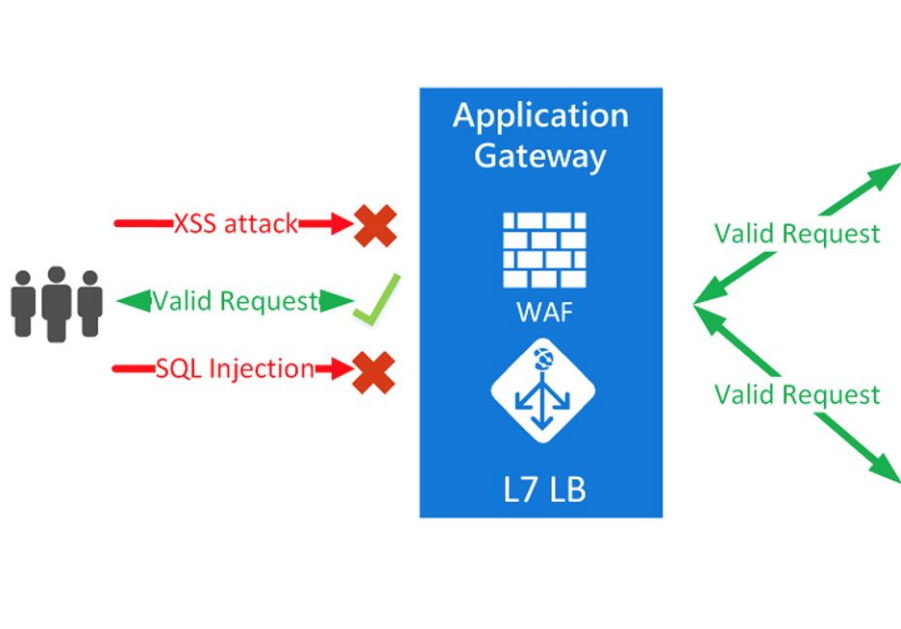
- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)

## Centralized logging

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or SIEM



# Azure Web Application Firewall (WAF)

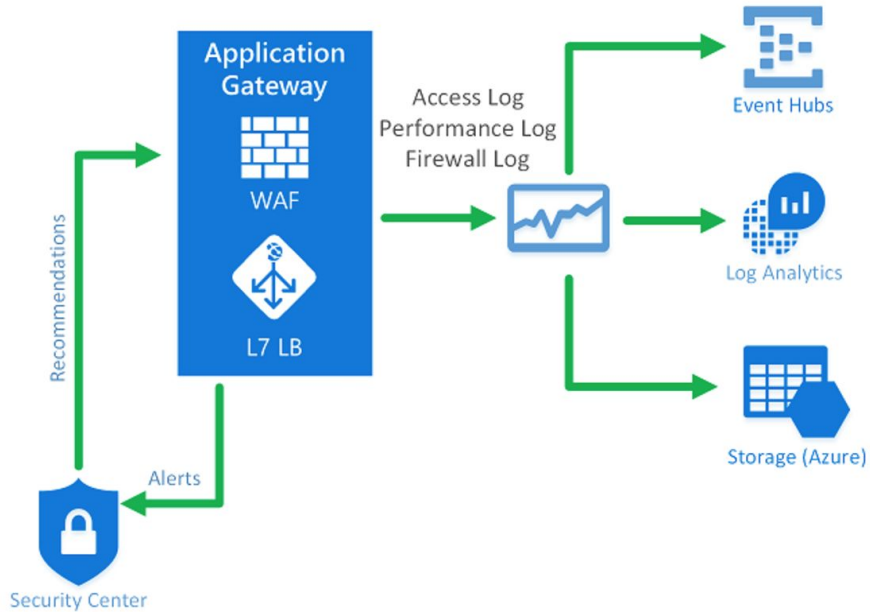


## OWASP\_3.0

The 3.0 core rule set provided has 13 rule groups as shown in the following table. Each of these rule groups contains multiple rules, which can be disabled.

RuleGroup	Description
<b>REQUEST-910-IP-REPUTATION</b>	Contains rules to protect against known spammers or malicious activity.
<b>REQUEST-911-METHOD-ENFORCEMENT</b>	Contains rules to lock down methods (PUT, PATCH< ..)
<b>REQUEST-912-DOS-PROTECTION</b>	Contains rules to protect against Denial of Service (DoS) attacks.
<b>REQUEST-913-SCANNER-DETECTION</b>	Contains rules to protect against port and environment scanners.
<b>REQUEST-920-PROTOCOL-ENFORCEMENT</b>	Contains rules to protect against protocol and encoding issues.
<b>REQUEST-921-PROTOCOL-ATTACK</b>	Contains rules to protect against header injection, request smuggling, and response splitting
<b>REQUEST-930-APPLICATION-ATTACK-LFI</b>	Contains rules to protect against file and path attacks.
<b>REQUEST-931-APPLICATION-ATTACK-RFI</b>	Contains rules to protect against Remote File Inclusion (RFI)

# Azure WAF



Create application gateway

1 Basics  
Configure basic settings

2 Settings  
Configure application gateway ...

3 Summary  
Review and create

Settings

\* Public IP address ⓘ  
Choose a public IP address

Listener configuration

\* Protocol  
HTTP HTTPS

\* Port  
80

Web application firewall

\* Firewall status  
Enabled Disabled

\* Firewall mode  
Detection Prevention

⚠

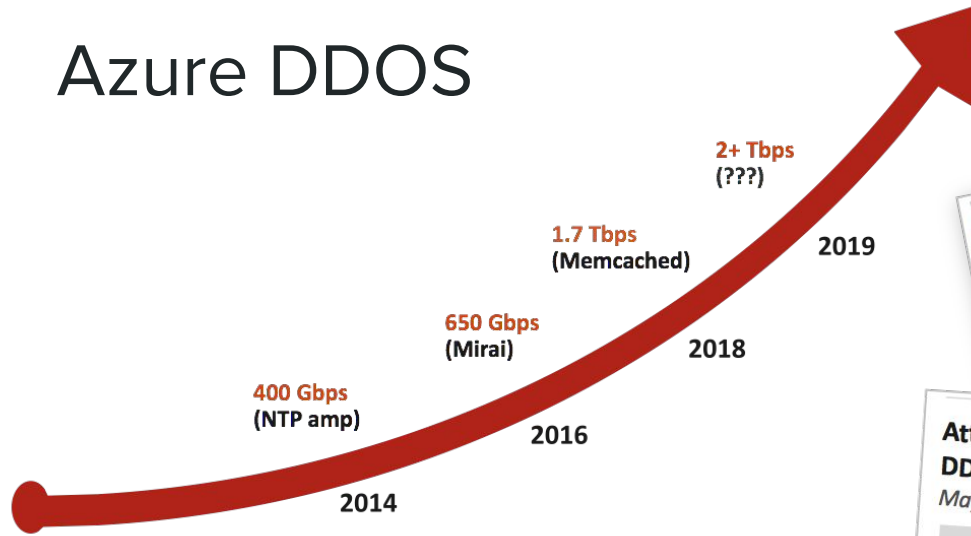
To view your detection logs, enable diagnostic logs after creating your application gateway.

OK

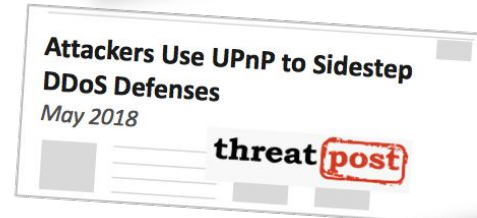


# DDoS Attack Trends

## Azure DDOS



- Continued growth in frequency, size, sophistication, and impact
- Often utilized as 'cyber smoke screen' to mask infiltration attacks
- Botnet networks enable massive scale weaponization



### Attack Frequency

58%

Vs. 2017

### Attack Size

1.7 Tbps

Peak

4X

> 50Gbps

### Attack Vectors

56%

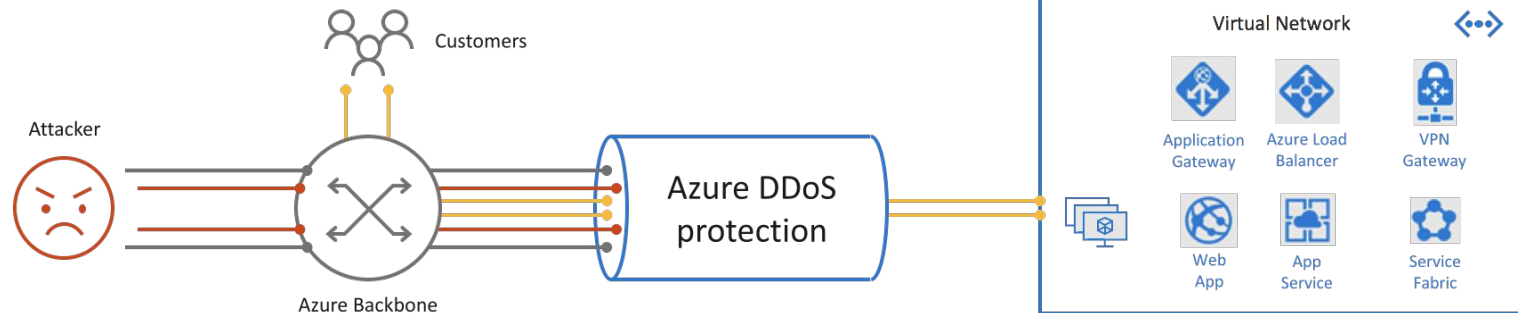
Multi-vector

### Attack Downtime

35%

Businesses impacted

# Azure DDoS Standard Protection



- Protection for your virtual network resources
- Automatic mitigation for 60+ network layer attacks
- Adaptive tuning via application traffic profiling and machine learning algorithms
- Real time monitoring and alerting in Azure Monitor
- Integration with WAF for application layer protection



# **Azure Sentinel (SIEM)**

# Azure Sentinel



# Integration Example - O365 with Azure Sentinel

The screenshot displays the Azure Sentinel interface. On the left is a navigation pane with options like 'Create a resource', 'Home', 'Dashboard', 'All services', and a 'FAVORITES' section listing various Azure services. The main area shows a breadcrumb trail: 'Home > Azure Sentinel workspaces > Azure Sentinel - Cases > Case'. Below this, the 'Case' details are shown for Case ID '2aba73bb-6bd8-4b67-95ed-6f2dc997c353 - PREVIEW'. The case title is 'Anomalous Login followed by Suspicious O365 Mailbox Forwarding'. It has a 'High' severity, 'New' status, and is 'Unassigned'. The description states: 'This is an indication of a sign in by Lee Gu from an unusual location (Chisinau, Chisinau, MD) followed by a suspicious inbox forwarding rule being set on a user's inbox. This may indicate that the account is compromised, and that the mailbox is being used to exfiltrate information from your organization. The user Lee Gu (LeeG@M365x387926.OnMicrosoft.com) created or updated an inbox forwarding rule that forwards all incoming email to the external address pwnme83js0dk9@gmail.com.' It also shows the last modification time as '02/27/19, 02:09 PM' and the creation time as '02/26/19, 02:00 PM'. An 'Investigate' button is at the bottom. On the right, there are tabs for 'Alerts' and 'Entities'. The 'Alerts' tab is active, showing a search bar and a table of alerts.

ALERT NAME	PRO...	CREA...	TIME...
Anonymous IP address	Microsoft	02/26/19...	2/26/201
Suspicious inbox forwarding	Microsoft	02/26/19...	2/26/201

## Azure Sentinel - Incidents

Selected workspace: 'contoso77' - PREVIEW



Refresh



Last 24 hours



Actions

### General

News &amp; guides

Overview

Logs

### Threat management

Incidents

Workbooks (new)

Dashboards

Hunting

Notebooks

### Configuration

Data connectors

Analytics

Playbooks

Community

Workspace settings

**119**  
OPEN INCIDENTS **119**  
NEW INCIDENTS **0**  
IN PROGRESS

### Open Incidents By Severity

  
■ CRITICAL (0) ■ HIGH (15) ■ MEDIUM (62) ■ LOW (40) ■ INFORMATIONAL (2)

SEVERITY : Informational, Low, Medium, High, Critical

STATUS : New, In Progress

PRODUCT NAME : All

	INCIDENT...	TITLE	ALERTS	PRODUC...	CREATED TIME	OWNER	STATUS
<input checked="" type="checkbox"/>	17758	Suspicious Volume Shadow Copy ...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17757	Suspicious command execution	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17756	Suspicious process executed	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17755	Suspicious double extension file e...	1	Azure Secur...	09/14/19, 11:34 PM	Unassigned	New
	17743	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 10:40 PM	Unassigned	New
	17741	Suspicious authentication activity	1	Azure Secur...	09/14/19, 10:33 PM	Unassigned	New
	17729	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 09:40 PM	Unassigned	New
	17716	Time Series Anomaly detection for...	1	Azure Senti...	09/14/19, 08:40 PM	Unassigned	New
	17714	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:34 PM	Unassigned	New
	17713	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17712	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17711	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17710	Suspicious authentication activity	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New
	17709	Suspicious authentication activitv	1	Azure Secur...	09/14/19, 08:33 PM	Unassigned	New

## Suspicious Volume Shadow Copy Activity

Incident Id: 17758

High  
SEVERITYNew  
STATUSUnassigned  
OWNER

### Description

Analysis of host data has detected a shadow copy deletion activity on the resource. Volume Shadow Copy (VSC) is an important artifact that stores data snapshots. Some malware and specifically Ransomware, targets VSC to sabotage backup strategies.

### Tags

+

### Last update time

09/14/19, 11:34 PM

### Creation time

09/14/19, 11:34 PM

### Close reason

N/A

[Investigate \(Now available!\)](#)[View full details](#)

» Home &gt; Azure Sentinel - Hunting

## Azure Sentinel - Hunting

Selected workspace: 'CyberSecurityDemo' - PREVIEW

🔍 Search (Ctrl+/)

+ New Query

🔄 Refresh

🕒 Last 24 hours

## General

📊 Overview

📋 Logs

## Threat management

🔒 Cases

📊 Dashboards

👤 User profiles (Coming soon)

## Hunting

## Configuration

📖 Getting started

📊 Data collection

🔒 Security analytics

📖 Playbooks

👤 Community

⚙️ Workspace Settings

🌐 19  
Total Queries🌐 106  
Total Results

## Queries

🔍 Search queries

✕

FAVORITES: All

PROVIDER: All

DATA SOURCES: All

TACTICS: All

🌟	QUERY	📄 DESCRIPTION	PROVIDER	📄 DATA SOURCE	📄 RESULTS	📄 TACTICS
🌟	New processes observed in last 24 h...	Shows new processes observed in the last ...	Microsoft	SecurityEvent	103	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄 📅 📆 📇 📈 📉 📊 📋 📅 📌 📁 📂 📃 📄
🌟	Azure AD signins from new locations	New AzureAD signin locations today versu...	Microsoft	SigninLogs	3	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
🌟	Processes executed from binaries hid...	Process executed from binary hidden in Ba...	Microsoft	SecurityEvent	0	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
🌟	Processes executed from base-encod...	Finding base64 encoded PE files header se...	Microsoft	SecurityEvent	0	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
🌟	Anomalous Azure AD apps based on ...	This query over Azure AD sign-in activity h...	Microsoft	SigninLogs	0	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Summary of users creating new user ...	New user accounts may be an attacker pro...	Microsoft	OfficeActivity	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	User and Group enumeration	The query finds attempts to list users or gr...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Summary of failed user logons by rea...	A summary of failed logons can be used to...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Hosts with new logons	Shows new accounts that have logged ont...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Malware in the recycle bin	Finding attackers hiding malware in the re...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Masquerading files	Malware writers often use windows system...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Accounts and User Agents associated...	Summary of users/user agents associated ...	Microsoft	OfficeActivity	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Office365 authentications	Shows authentication volume by user age...	Microsoft	OfficeActivity	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Summary of users created using unc...	Summarizes users of uncommon & undocu...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Powershell downloads	Finds PowerShell execution events that co...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Script usage summary (cscript.exe)	Daily summary of vbs scripts run across th...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Sharepoint downloads	Shows volume of documents uploaded to ...	Microsoft	OfficeActivity	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Uncommon processes/files - bottom ...	Shows the rarest processes seen running f...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄
★	Summary of user logons by logon type	Comparing successful and unsuccessful lo...	Microsoft	SecurityEvent	--	🔍 🔄 📊 📋 📅 📌 📁 📂 📃 📄

## New processes observed in last 24 hours

Microsoft  
Provider🌐 103  
Results📊 SecurityEvent  
Data Source

## Description

Shows new processes observed in the last 24 hours versus the previous 30 days. These new processes could be benign new programs installed on hosts; however, especially in normally stable environments, these new processes could provide an indication of an unauthorized/malicious binary that has been installed and run. Reviewing the wider context of the logon sessions in which these binaries ran can provide a good starting point for identifying possible attacks.

## Query Information

```
let start=datetime("2019-02-23T10:41:10.127Z");
let end=datetime("2019-02-24T10:41:10.127Z");
let processEvents=SecurityEvent
| where TimeGenerated > start and TimeGenerated < en
| where EventID==4688
| project TimeGenerated, ComputerName=Computer,Acco
```

[View query result >](#)

## Entities

## Tactics

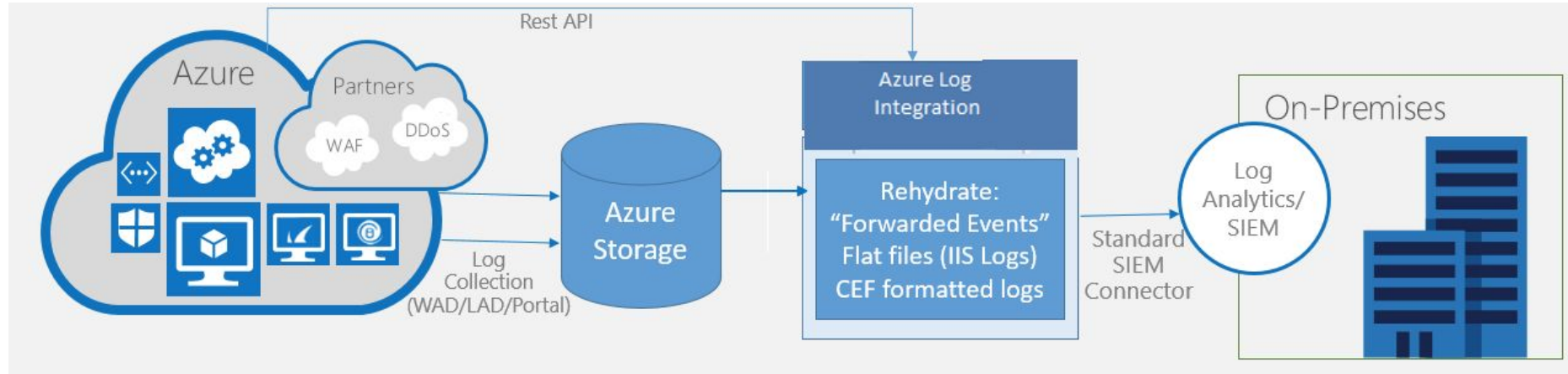
## Execution

The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.  
[read more...](#)

Run Query



# Azure SIEM (IBM QRadar + Splunk)



How to Azure with IBM QRadar: <https://zigmax.net/azure-siem-ibm-qradar/>

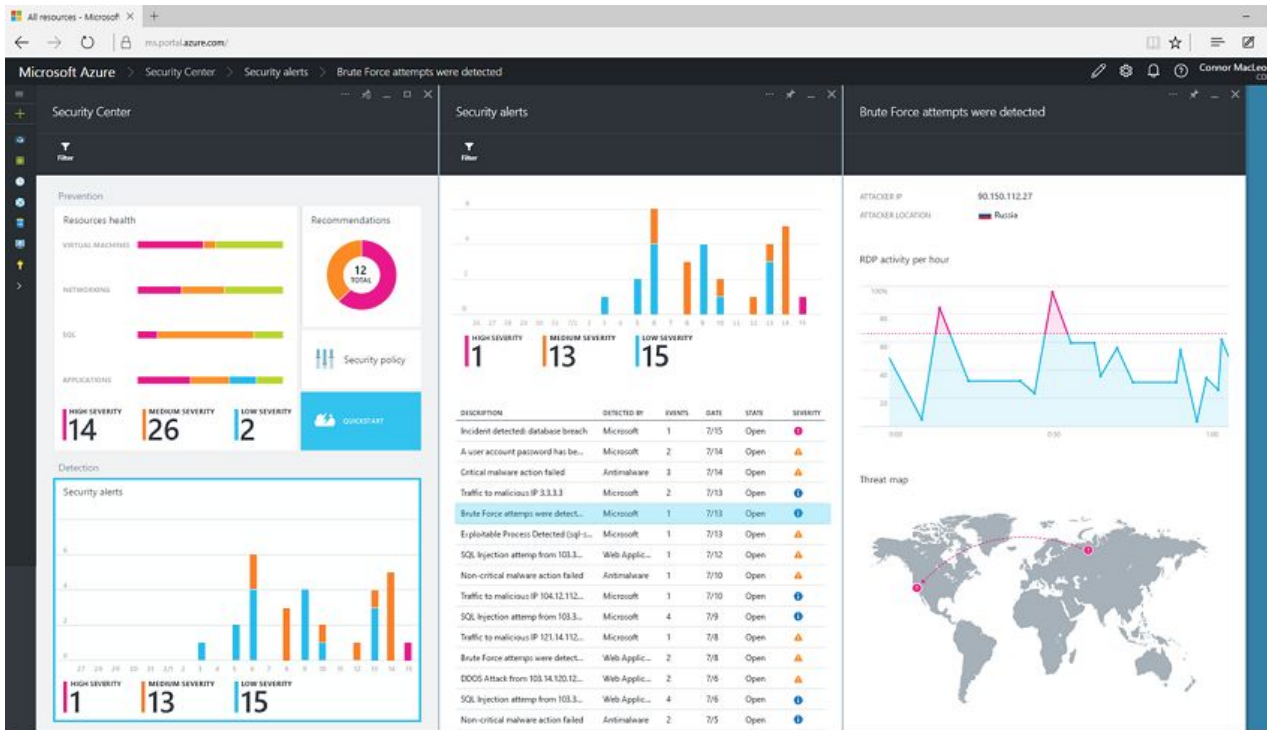
# **Azure Security Center**

# Azure Security Center



- Integrated threat intelligence
- Behavioral analytics
- Anomaly detection
- Advanced Threat Protection

# Azure Security Center



## Prevention policy

Microsoft Azure Sponsorship

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

Vulnerability Assessment ☒ On ☐ Off

Storage Encryption ☒ On ☐ Off

SQL auditing & Threat detection ☒ On ☐ Off

SQL Encryption ☒ On ☐ Off













OK

# Azure Security Center

## Choose your pricing tier

Browse the available plans

The standard tier adds powerful features, including advanced threat detections and more. Try it for free for 60 days. For additional details, visit our pricing page. [Learn more](#)

Free	Standard – Free Trial	Standard
Basic detection	Advanced detection	Advanced detection
 Security policy	 Security policy	 Security policy
 Security assessment	 Security assessment	 Security assessment
 Recommendations	 Recommendations	 Recommendations
 Connected solutions	 Connected solutions	 Connected solutions
0.00 FREE	0.00 FREE FOR 60-DAYS	15.00 USD / NODE / MONTH

## Recommendations

Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY	
Enable advanced security for subscription...	1 subscriptions	Resolved	High	...
Add a Next Generation Firewall	win16labmax...	Open	High	...
Finalize Internet facing endpoint protect...	lab01-ub-ma...	Open	High	...
Enable Network Security Groups on sub...	2 subnets	Open	High	...
Route traffic through NGFW only	lab01-ub-max	Open	High	...
Apply disk encryption	2 virtual mac...	Open	High	...
Enable encryption for Azure Storage Acc...	4 storage acc...	Open	High	...
Restrict access through Internet facing e...	win16labmax...	Open	Medium	...
Add a vulnerability assessment solution	win16labmax...	Open	Medium	...
Provide security contact details	1 subscriptions	Resolved	Medium	...

Select

# Azure Security Center

lab01-ub-max-nsg

🛡️ Edit inbound rules

## Network security group info

NETWORK SECURITY GROUP lab01-ub-max-nsg

LOCATION eastus

DESCRIPTION Your NSG has inbound rules that open access to 'Any' or 'Internet' which might enable attackers to access your resources. We recommend that you edit the below inbound rules to restrict access to a specified set of sources.

## Related inbound rules

PRIORITY	NAME	SOURCE	SERVICE	ACTIONS
1000	default-allow-ssh	*	TCP	Allow

## Associated with

NAME	VIRTUAL MACHINE
 lab01-ub-max642	lab01-ub-max

Microsoft Azure << Create a new Next Generation Firewall solution > Cisco ASAv - BYOL 4 NIC

Cisco ASAv - BYOL 4 NIC



The physical Cisco ASA and Cisco ASAv support the same rich policy constructs. Virtual and physical domains are coalesced into a single policy domain so the same policies can be applied to all Cisco ASAs, whether they are physical or virtual.

Cisco ASAv offers the same features as a physical Cisco ASA, including VPN services that can be deployed in the virtual domain. Site-to-site, remote-access, and clientless VPN services can be deployed quickly in a private cloud or over a virtual infrastructure in response to demand.

Cisco ASAv offers the REST API, an HTTP-based interface that facilitates management of the appliance, including changing the security policy and monitoring the status. Using REST APIs, multiple cloud management solutions can be used to manage both physical and virtual instances of Cisco ASA.

- **FREE TRIAL**- ASAv has a demo mode that runs with reduced performance. No license required.
- Supported Azure Instances: Standard\_D3 and Standard\_D3\_V2
- ASAv is integrated with Azure Security Center
- ASAv is available in the Azure Government Cloud.

This deployment creates an ASAv with four NICs, plus public and private subnets.

PUBLISHER Cisco Systems, Inc.

USEFUL LINKS [ASAv Home Page](#) [Quick Start Guide](#) [Datasheet](#) [ASAv COMMUNITY SUPPORT PORTAL](#) [Instructional Youtube](#)

Create

# Azure Security Center - Alert

TCP packet, no conn, denied

10.1.0.4



## DESCRIPTION

%ASA-6-106015: Deny TCP (no connection) from 124.243.216.102/11207 to 10.1.0.4/22 flags RST on interface management

## DETECTION TIME

Monday, June 26, 2017, 9:20:00 PM

## SEVERITY

Low

## STATE

Active

## ATTACKED RESOURCE

10.1.0.4

## SUBSCRIPTION

[Microsoft Azure Sponsorship](#)  
(7db5e03c-f3c2-48b1-b326-aa53faaaafc3)

## DETECTED BY

Cisco ASAv

## ACTION TAKEN

Blocked

## ENVIRONMENT

Azure

## RESOURCE TYPE

Azure Resource

## HIT COUNT

1

## SOURCE IPS

124.243.216.102

Secure <https://www.abuseipdb.com/check/124.243.216.102>

## IP Abuse Reports for 124.243.216.102:

This IP address has been reported a total of **26** times. 124.243.216.102 was first reported on 18 Jun 2017. The most recent report was **2 hours ago**.

**Recent Reports:** We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Search:

Reporter	Date	Comment	Categories
✓ <a href="#">infosky.net</a>	2 hours ago	SSH/22 MH Probe, BF -	Brute-Force SSH
Anonymous	6 hours ago	Jun 26 14:30:16 ns sshd\[20408\]: pam_unix(sshd:auth \\\): authentication failure\; logname= uid=0 eui ... <a href="#">show more</a>	DDoS Attack
✓ <a href="#">doyoucheck.com</a>	14 hours ago	ssh intrusion attempt	SSH
Anonymous	25 Jun 2017	Brute force SSH login	Brute-Force SSH
✓ <a href="#">cutkit.eu</a>	25 Jun 2017	SSH brute force	Brute-Force SSH
<a href="#">blueSh4rk</a>	25 Jun 2017	unauthorized ssh connection attempt	Brute-Force SSH
✓ <a href="#">blog.demees.net</a>	25 Jun 2017	ssh-bruteforce	SSH
✓ <a href="#">infosky.net</a>	25 Jun 2017	SSH/22 MH Probe, BF -	Brute-Force SSH
✓ <a href="#">infosky.net</a>	25 Jun 2017	SSH/22 MH Probe, BF -	Brute-Force SSH


# Azure Security Center - Demo





# Advanced Threat Protection

[Home](#) > [Security Center - Pricing & settings](#) > [Settings - Pricing tier](#)

 **Settings - Pricing tier**  
Microsoft Azure Sponsorship

Settings

Pricing tier

Data Collection

Email notifications


Threat detection

Workflow automation (Preview)

Continuous export (Preview)







Save

Free (for Azure resources only)	Standard
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Azure Secure Score	✓ Azure Secure Score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

 **Pricing will apply to: 1 resources in this subscription**

^

 Select pricing tier by resource type

Resource Type	Resource Quantity	Pricing	Plan
 Virtual machines	0 VMs and VMSS instances	\$15/Server/Month	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
 App Service	0 instances	\$15/Instance/Month	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
 PaaS SQL servers	0 resources	\$15/Server/Month	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
 SQL servers on VMs (Preview)	0 SQL servers on VMs	FREE during prev... ⓘ	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
 Storage accounts	1 Storage accounts	\$0.02/10K Transactions	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
 Kubernetes Services (Preview)	0 Kubernetes services' cores	\$2/VM core/Month	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled



# Advanced Threat Protection

[Home](#) > [Security Center - Overview](#) > [Security alerts](#) > PREVIEW - Privileged container detected

## PREVIEW - Privileged container detected



 Filter

	Attacked Resource <span>↑↓</span>	Count <span>↑↓</span>	Activity time <span>↑↓</span>	Environme... <span>↑↓</span>	State <span>↑↓</span>	Severity <span>↑↓</span>	
	AKSDMOMAX	1	11/22/19, 02:51 PM	Azure	Active	 Low	...

# Advanced Threat Protection

... > Security alerts > PREVIEW - Privileged container detected > PREVIEW - Privileged container detected

PREVIEW - Privileged container detected

AKSDEMOMAX

Learn more

## General information

DESCRIPTION	Kubernetes audit log analysis detected a new privileged container. A privileged container has access to the node's resources and breaks the isolation between containers. If compromised, an attacker can use the privileged container to gain access to the node.
ACTIVITY TIME	Friday, November 22, 2019, 2:51:54 PM
SEVERITY	<div><div></div>Low</div>
STATE	Active
ATTACKED RESOURCE	AKSDEMOMAX
SUBSCRIPTION	Microsoft Azure Sponsorship (7db5e03c-f3c2-48b1-b326-aa53faaaafc3)
DETECTED BY	<div><div></div>Microsoft</div>
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	<div><div></div>Kubernetes Service</div>

... > Security alerts > PREVIEW - Privileged container detected > PREVIEW - Privileged container detected

PREVIEW - Privileged container detected

AKSDEMOMAX

Learn more

DETECTED BY	<div><div></div>Microsoft</div>
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	<div><div></div>Kubernetes Service</div>
CONTAINER NAME	nsenter
CONTAINER IMAGE	alexexiled/nsenter:2.34
NAMESPACE	default
POD NAME	maxime-nsenter-aks-nodepool1-29366245-vmss000000

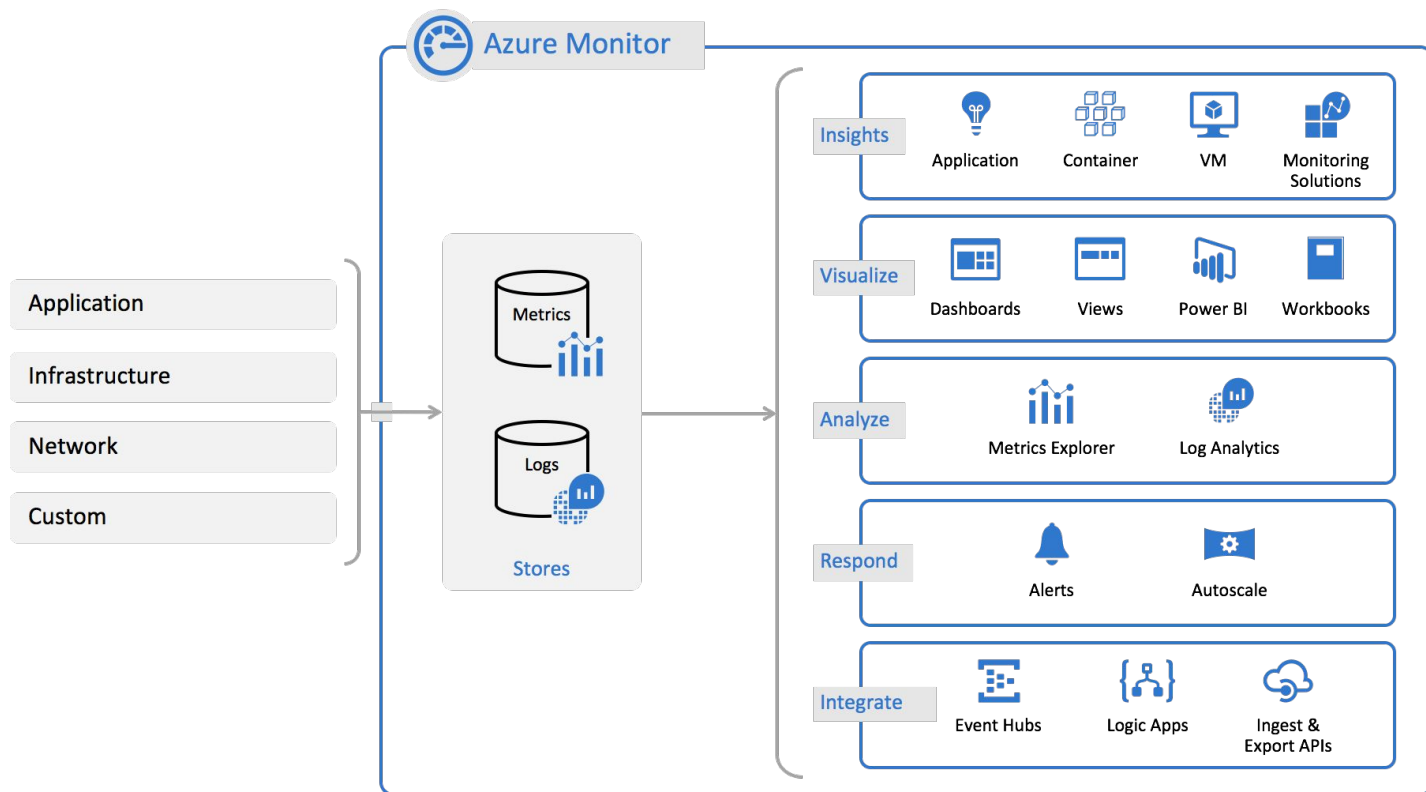
Remediation steps

REMEDIATION STEPS

Find the container in the alert details.  
If the container doesn't need to run in privileged mode, remove the privileges from the container.  
If the container is not legitimate, escalate the alert to the information security team.

# Investigation

# Azure Monitor



# Forensic investigation (Logs)

Microsoft Azure Monitor - Activity log

max.coquerel@live.fr  
RÉPERTOIRE PAR DÉFAUT

Monitor - Activity log  
Microsoft

Search (Ctrl+/)

EXPLORE

- Activity log
- Metrics
- Diagnostics logs
- Log search

MANAGE

- Alerts
- Action groups
- Autoscale

HEALTH

- Service notifications
- Resource health

Columns Export Log search

Select query ...

Insights (Last 24 hours): 0 failed deployments | 0 role assignments | 2 errors | 0 alerts fired | 0 outage notifications

\* Subscription ⓘ Resource group ⓘ Resource ⓘ Resource type ⓘ \* Operation ⓘ

Microsoft Azure Sponsors... All resource groups All resources All resource types All operations

Timespan ⓘ Event category ⓘ \* Event severity ⓘ Event initiated by ⓘ Search ⓘ

Last 6 hours All categories 4 selected Email or name or servi...

Apply Reset

Query returned 45 items. [Click here to download all the items as csv.](#)

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
ListKeys	Started	3 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr
Update website	Succeeded	9 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr
Update website	Succeeded	19 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr
Validate	Started	19 min ago	Mon Jun 26 2...	Microsoft Azure Sponsorship	max.coquerel@live.fr

Summary JSON

Operation name  
ListKeys

Time stamp



NEW

# Exam AZ-500: Microsoft Azure Security Technologies

Candidates for this exam are Microsoft Azure security engineers who implement security controls, maintain the security posture, manages identity and access, and protects data, applications, and networks...

[More](#)

**Fulfills requirements for:** [Microsoft Certified: Azure Security Engineer Associate](#)

## Skills measured

### [Manage identity and access](#)

Implement platform protection

Manage security operations

Secure data and applications

### **Manage identity and access (20-25%)**

#### **Configure Microsoft Azure Active Directory for workloads**

- create App registration
- configure App registration permission scopes
- manage App registration permission consent
- configure multi-factor authentication settings
- manage Microsoft Azure AD directory groups
- manage Microsoft Azure AD users
- install and configure Microsoft Azure AD Connect
- configure authentication methods
- implement conditional access policies
- configure Microsoft Azure AD identity protection

#### **Configure Microsoft Azure AD Privileged Identity Management**

- monitor privileged access
- configure access reviews
- activate Privileged Identity Management

#### **Configure Microsoft Azure tenant security**

- transfer Microsoft Azure subscriptions between Microsoft Azure AD tenants
- manage API access to Microsoft Azure subscriptions and resources

# Watching: Secure cloud resources with Azure

From the course: **Microsoft Azure Security Center: Securing Cloud Resources**



142



1,178



...

Microsoft Azure

Search resources, services, and docs

Home > Security Center > Just in time VM access > JIT VM access configuration > Add port configuration

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

Virtual machines

Virtual networks

Key vaults

Automation Accounts

Security Center

Management groups

Policy

Azure Active Directory

SQL servers

SQL databases

Monitor

Storage accounts

Log Analytics workspaces

Enable JIT on 1 VMs

STATE SEVERITY

Open High

JIT VM access configuration

MyWindowsVM1

+ Add Save Discard

Configure the ports for which the just in time VM access will be applicable

PORT	PROT...	ALLOWED SOUR...	IP RANGE	TIME RANGE (H...
22 (Recommended)	Any	Per request	N/A	3 hours
3389 (Recommended)	Any	Per request	N/A	3 hours
5985 (Recommended)	Any	Per request	N/A	3 hours
5986 (Recommended)	Any	Per request	N/A	3 hours

Add port configuration

\* Port

22

Protocol

Any TCP UDP

Allowed source IPs

Per request CIDR block

IP addresses

Max request time

23 (hours)

0:19 / 0:55

1x CC

## Introduction

- Secure cloud resources with Azure 55s

What you should know  
1m 17s

## 1. Getting Started with Azure Security Center (ASC)

Azure Security Center console  
4m 11s

Prerequisites and onboarding resources  
4m 16s

Management groups  
1m 52s

Azure Policy and compliance  
4m 30s

Azure Policy in action  
4m 0s

Logging and monitoring  
6m 17s

Security threat alerts  
2m 14s

Alert validation  
2m 36s

Planning and operations  
4m 1s



## Vous regardez : Découvrir Azure Policy

Dans le cours : Microsoft Azure : La sécurité

31 150

Vue d'ensemble Contenu Transcriptions Notes

### 3. Assurer la conformité

Découvrir Azure Policy  
1 min 1 sec

Assigner une stratégie  
2 min 31 sec

Valider le bon fonctionnement de la stratégie  
1 min 36 sec

Connaître le résultat de la non-conformité  
1 min 16 sec

### 4. Aborder la sécurité de l'infrastructure

Découvrir Network Security Groups  
1 min 9 sec

Mettre en œuvre Network Security Groups  
5 min 15 sec

Créer une passerelle applicative  
3 min 39 sec

Configurer Application Gateway  
4 min 52 sec

Mettre en place le pare-feu  
3 min 3 sec

### 5. Administrer les identités

Gérer les identités avec Azure Active Directory  
5 min 16 sec

Créer un groupe

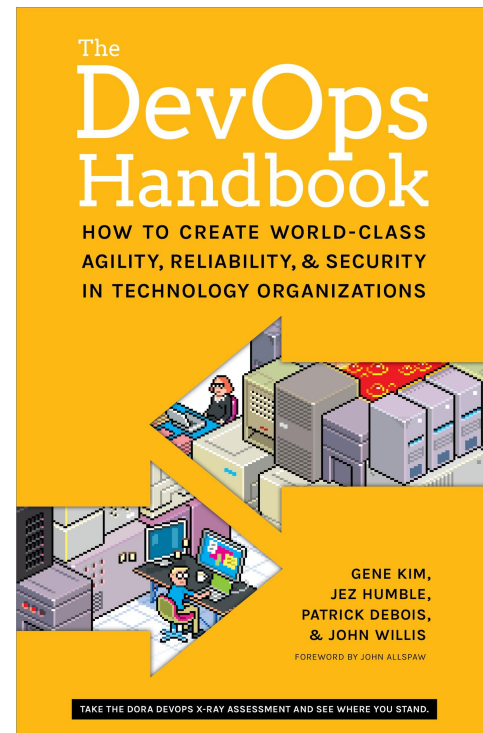
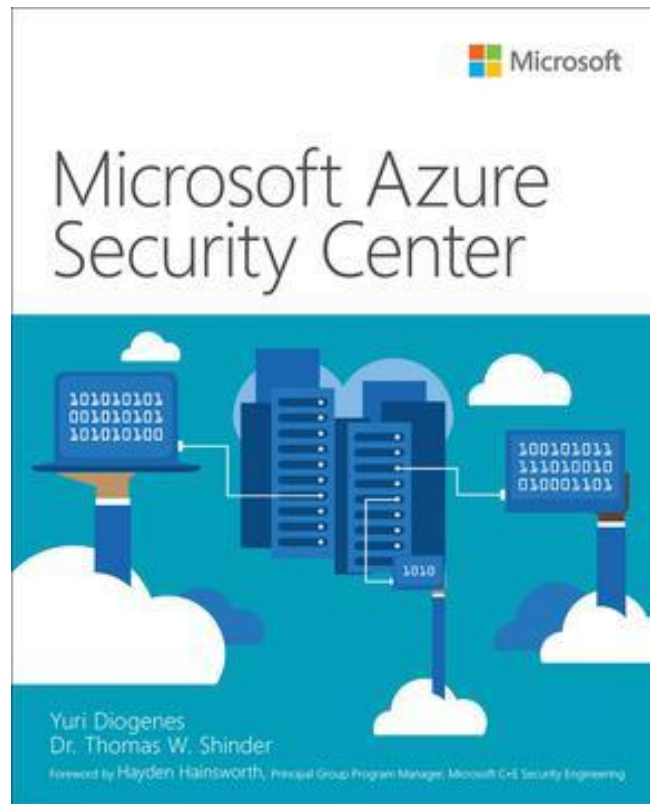
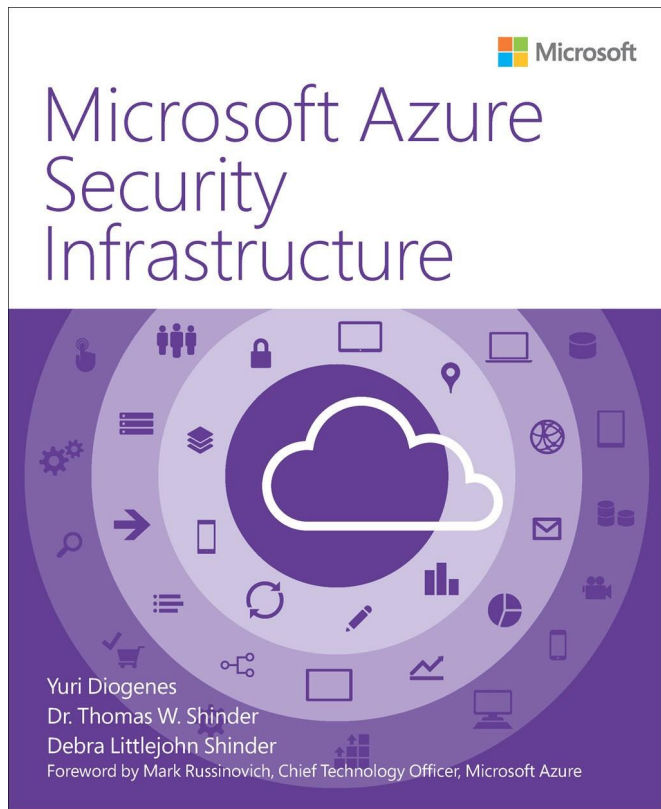
Aide/Commentaires

# Conclusion

- > Compliance .... **Azure Policy / Management Group**
- > Identity Management ... **Azure Active Directory**
- > No flat networks ... **Network Security Group**
- > Manage secrets ... **Azure Key Vault**
- > Firewall / WAF .... **Azure Firewall / Azure WAF**
- > SIEM .... **Azure Sentinel**
- > Threat Analytics - **Azure Security Center**



# Books



# Technical Resources

Microsoft Learn - <https://docs.microsoft.com/en-us/learn/>

AZ-500 Prep Guide -

<https://stanislas.io/2019/04/25/preparation-guide-for-microsoft-az-500-microsoft-azure-security-technologies-certification/>

Microsoft Technical Community Content

<https://github.com/Microsoft/TechnicalCommunityContent>

Azure Security Blog - <https://azure.microsoft.com/en-us/blog/topics/security/>

Maxime Blog - <http://zigmax.net>

Microsoft Ignite 2019 - <https://myignite.techcommunity.microsoft.com/>

Questions / Talks