Azure Security Overview

Maxime Coquerel - MVP Azure

Disclamer

“*Tous les posts de cette présentation ne reflètent que mon opinion et non celle de mes employeurs et clients.*“

Remerciements

Merci à l’équipe OWASP Québec ainsi qu’au Cégep Sainte Foy!

Speaker

Maxime Coquerel

Cloud Architect

Email : max.coquerel@live.fr

Blog : zigmax.net (Since 2012)

Github : https://github.com/zigmax

Twitter : @zig_max

Open Source Contributor (Kubernetes / OpenStack).

Session Agenda / Goal

- Introduction
- Compliance & Gouvernance
- Gestion des identités
- Chiffrement et voûte de mots de passe
- Infrastructure
- Azure Security Center
- Investigation
- Conclusion


54 regions worldwide
140 available in 140 countries
West Central US
West US 2
West US
US Gov Arizona
US Gov Texas
South Central US
US Gov Iowa, Central US
Canada East
Canada Central
North Central US
US DoD East
East US, East US 2, US Gov Virginia
US DoD Central
Norway West
Norway East
West Europe
Germany West Central
UK West
Germany No rth
North Europe
Germany No rtheast
UK South
Germany Central
France Central
Switzerland No rth
France South
Switzerland West
China No rth, China No rth 2
Korea Central
Korea South
Japan East
Japan West
China East, China East 2
East Asia
UAE North
UAE Central
West India
Central India
South India
Southeast Asia
Brazil South
South Africa No rth
South Africa West
Australia East
Australia Central, Australia Central 2
Australia Southeast
Available region
Announced region
Availability Zone(s) p resent
* Two Azure Government Secret region locations undisclosed

Data Breach


DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013
14,644,949,623
ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.
DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

Data Breach - Facebook

Notable Data Breaches

- **Facebook** >
- Government of India/Aadhaar >
- Exactis >
- Under Armour >
- Twitter >

Facebook

2018-04-04

Score: 10.0

2,100,000,000 Records

Facebook revealed that malicious actors could have abused its search and account recovery capabilities to scrape public profile information from most of its more than 2 billion users. The social networking platform discovered that bad actors had the option of submitting phone numbers and email addresses to locate users' public profiles and obtain personal information off them. As Facebook's CTO Mike Schroepfer explained at the time, "Given the scale and sophistication of the activity we've seen, we believe most people on Facebook [over 2 billion users] could have had their public profile scraped in this way." The tech giant responded by disabling the feature and changing its account recovery process to reduce the risk of scraping.

Data Breach - Government of India/Aadhaar

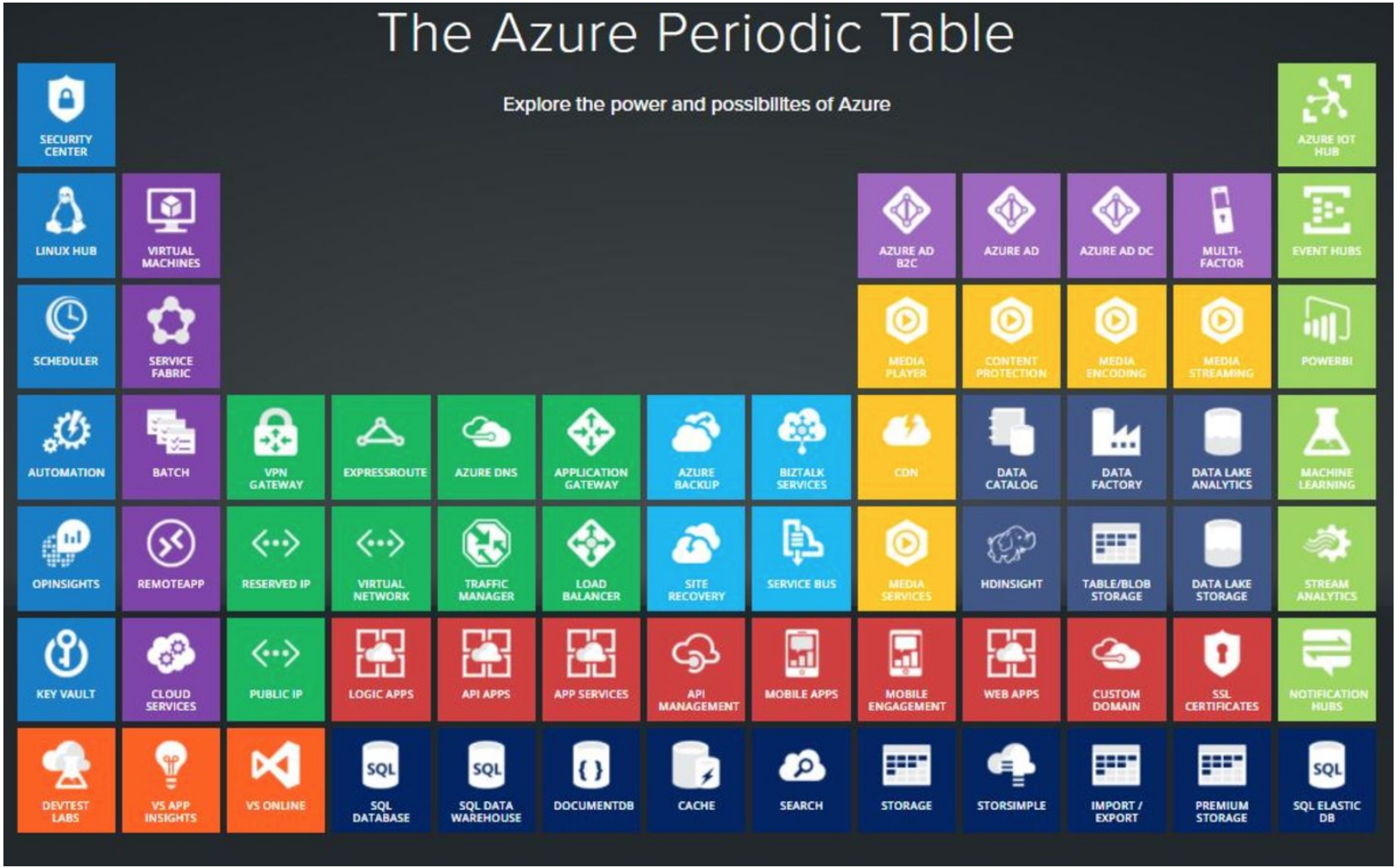
Government of India/Aadhaar

2018-01-03

Score: 10.0

1,200,000,000 Records

An anonymous service allowed anyone with 500 rupees to access all 1.2 billion Indian citizens' personal information. In January 2018, the Tribune News Service paid to access a service being offered by anonymous sellers over WhatsApp. Reporters found they could use the service to enter any Aadhaar number, a 12-digit unique identifier assigned to every Indian citizen, and retrieve personal information stored by the Unique Identification Authority of India on any of India's 1.1 billion citizens including their name, address, photo, phone number and email address. An additional 300 rupees yielded access to software through which anyone could print an ID card for any Aadhaar number.


The Azure Periodic Table
Explore the power and possibilites of Azure
SECURITY CENTER
AZURE IOT HUB
LINUX HUB
VIRTUAL MACHINES
AZURE AD B2C
AZURE AD
AZURE AD DC
MULTI-FACTOR
EVENT HUBS
SCHEDULER
SERVICE FABRIC
MEDIA PLAYER
CONTENT PROTECTION
MEDIA ENCODING
MEDIA STREAMING
POWERBI
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

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 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

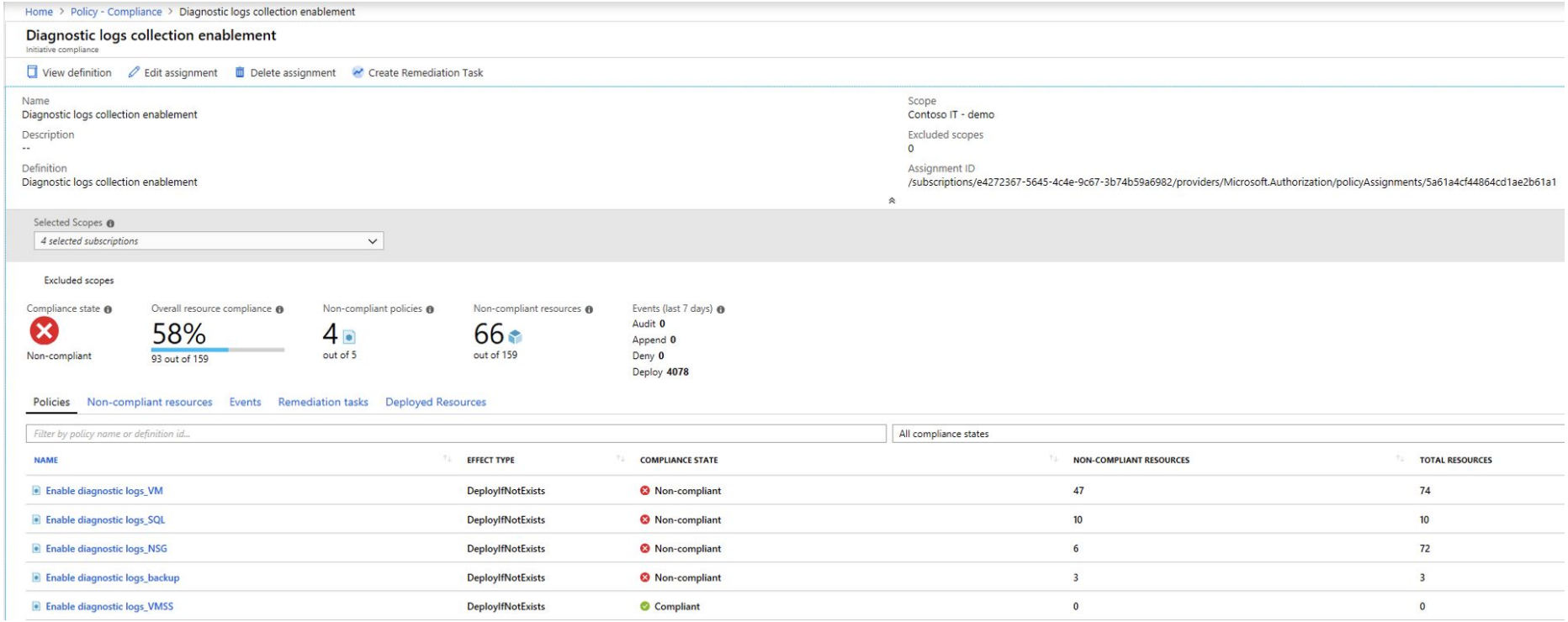
- Real time remediation
- Remediation on existing resources (NEW)

Remediation

https://github.com/Azure/azure-policy |

Source: Microsoft Ignite - BRK3085

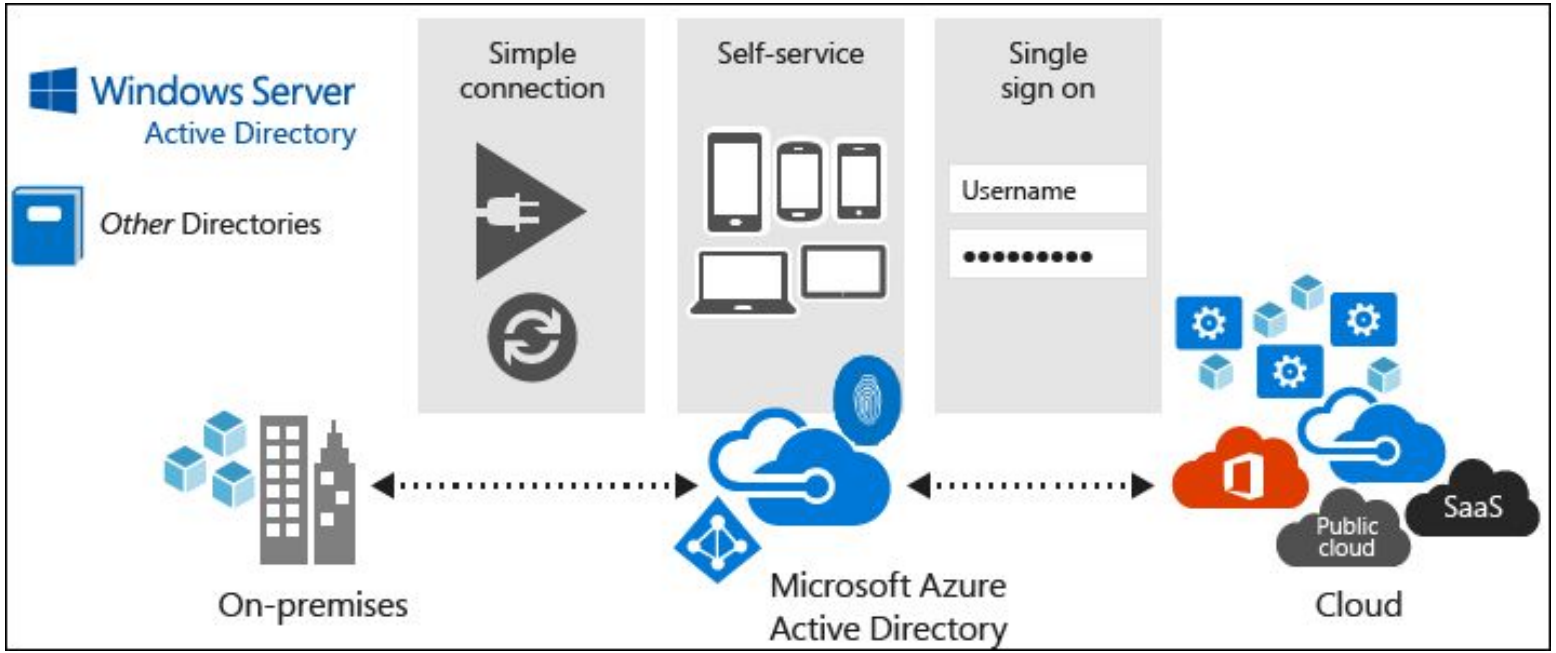
Azure Policy



Azure Policy - Demo

Gestion des identités

Azure AD


Windows Server
Active Directory
Other Directories
Simple connection
Self-service
Single sign on
Username
On-premises
Microsoft Azure Active Directory
Public cloud
SaaS
Cloud

Azure B2C

Customers

Social IDs

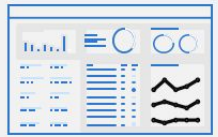
Business & Government IDs

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

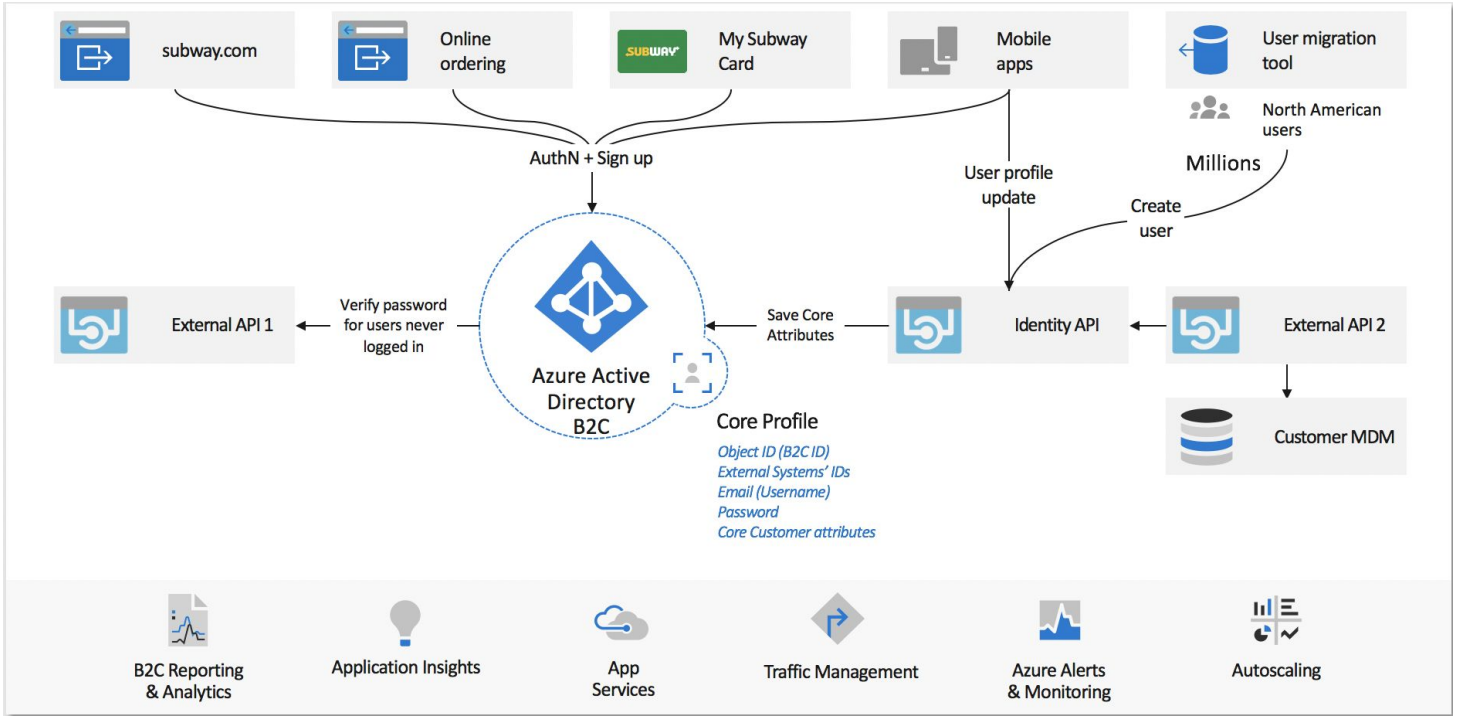


Analytics

CRM and Marketing Automation

Source : Microsoft Ignite 2018 - BRK3240

Azure B2C - Example Subway

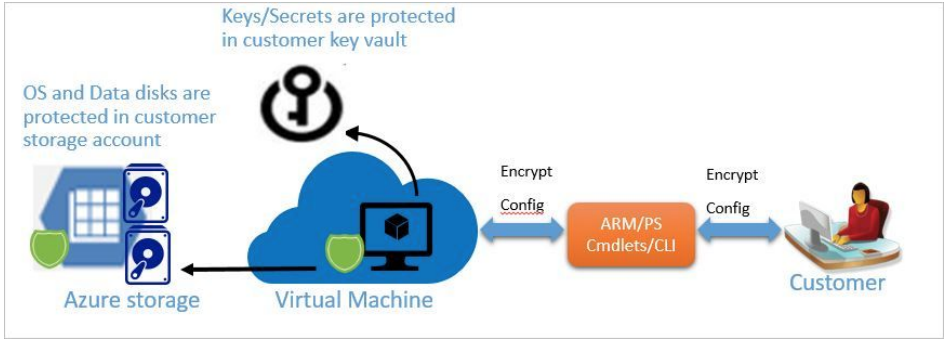


Source : Microsoft Ignite 2018 - BRK3240

Chiffrement & Voûte de mots de passe

Azure Disk Encryption

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



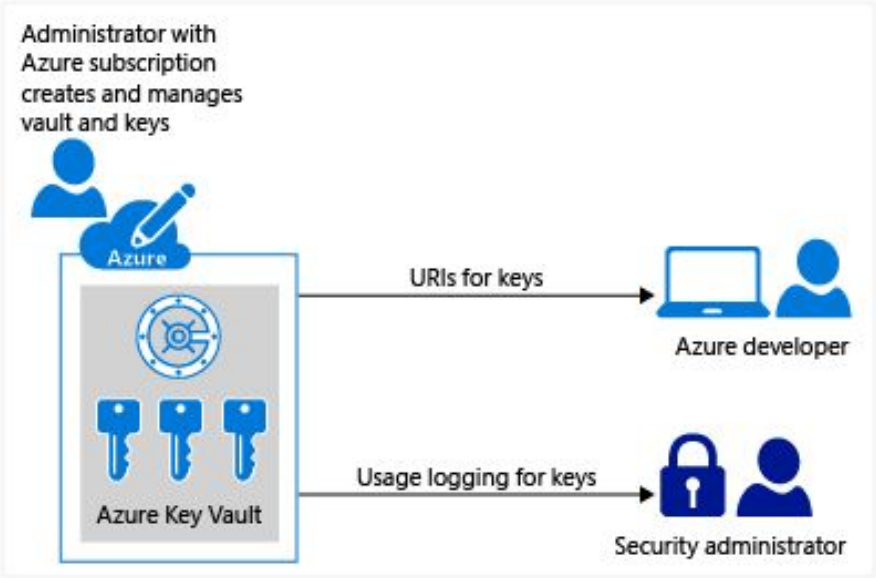
Howto : Azure Disk Encryption

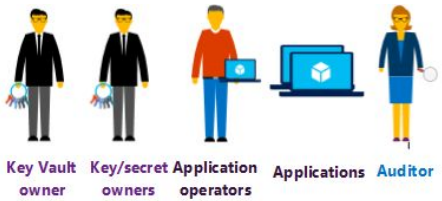
http://zigmax.net/azure-chiffrer-une-machine-virtuelle-azure-disk-encryption/

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

Infrastructure

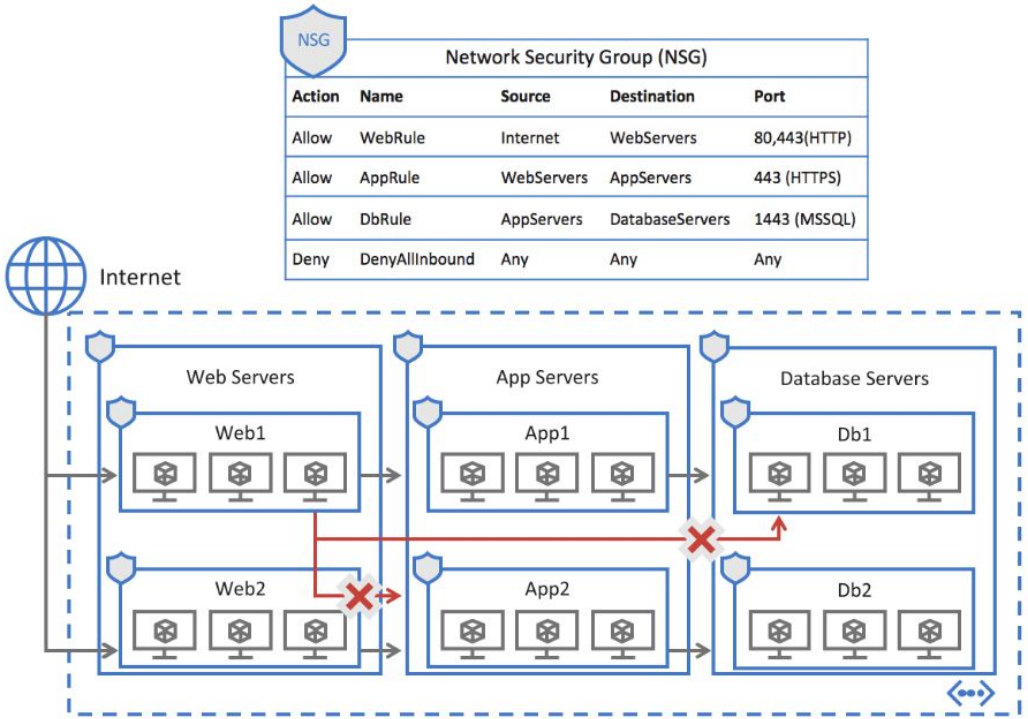
Network and Application Security Group (NSG)

Network Security Groups

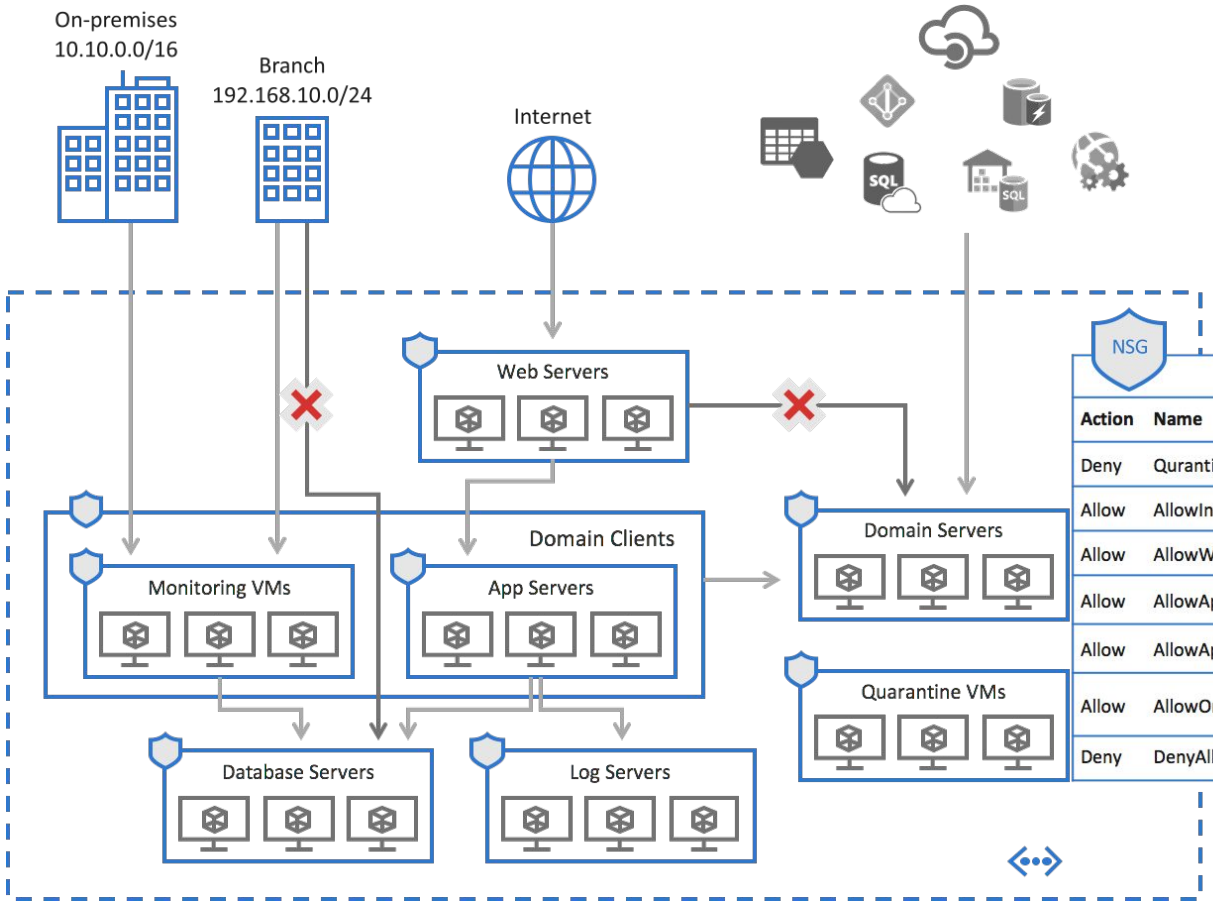
- Protects your workloads with distributed ACLs
- Simplified configuration with augmented security rules
- Enforced at every host, applied on multiple subnets

Application Security Groups

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



Source Microsoft Ignite 2018 - BRK4029



NSG

Network Security Group (NSG)

Action	Name	Source	Destination	Port
Deny	QurantineVMs	Any	**QurantineVMs**	Any
Allow	AllowInternetToWebServers	Internet	WebServers	80,443(HTTP)
Allow	AllowWebToApp	WebServers	AppServers	443 (HTTPS)
Allow	AllowAppToDb	AppServers	DatabaseServers	1443 (MSSQL)
Allow	AllowAppToLogServers	AppServers	LogServers	8089
Allow	AllowOnPrem	10.10.0.0/16 192.168.10.0/24	MonitoingVMs	80 (HTTP)
Deny	DenyAllInbound	Any	Any	Any

Azure Firewall

Cloud native stateful Firewall as a Service

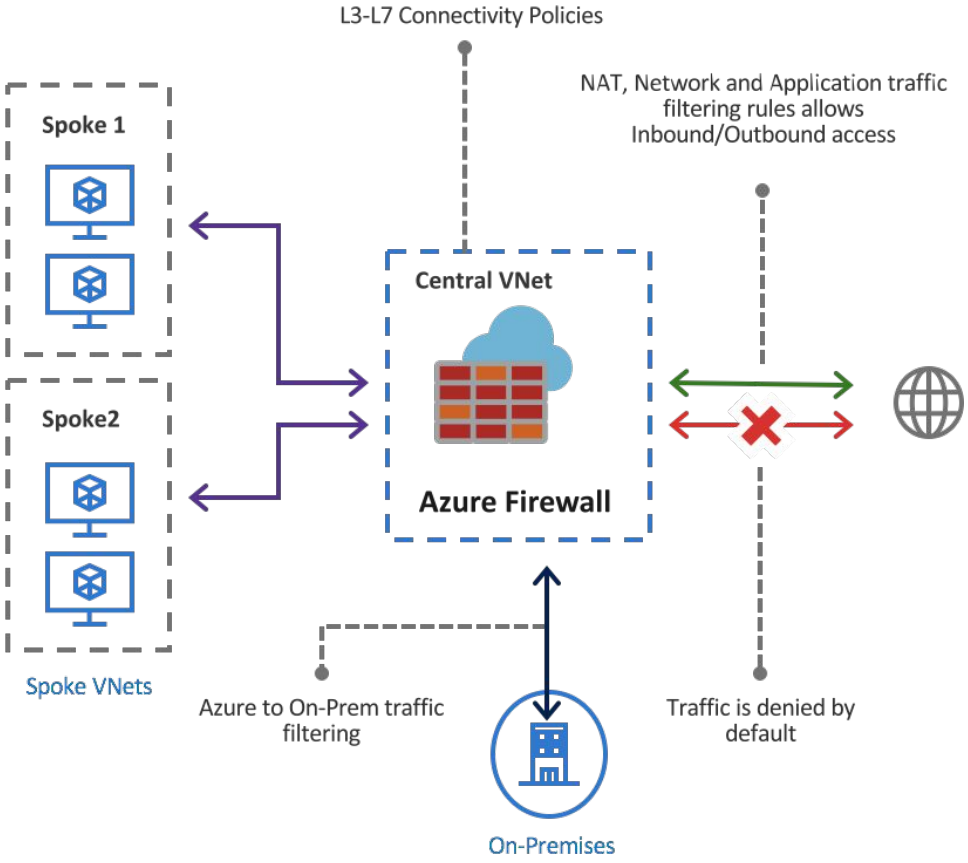
- Built-in High Availability and Auto Scale
- Network and Application traffic filtering
- Centralized policy across VNets and Subscriptions

Complete VNET protection

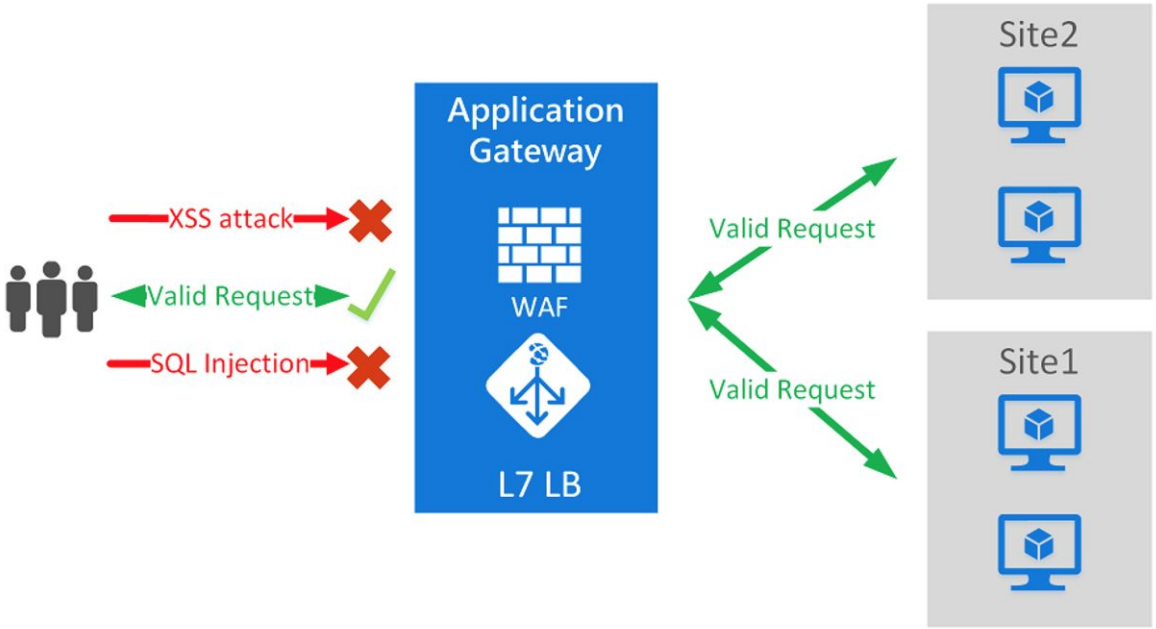
- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)

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)

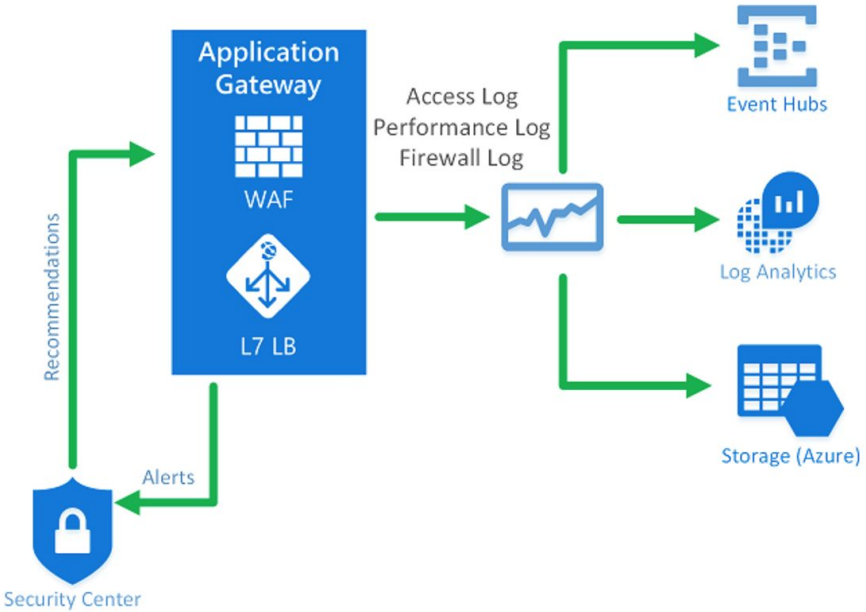


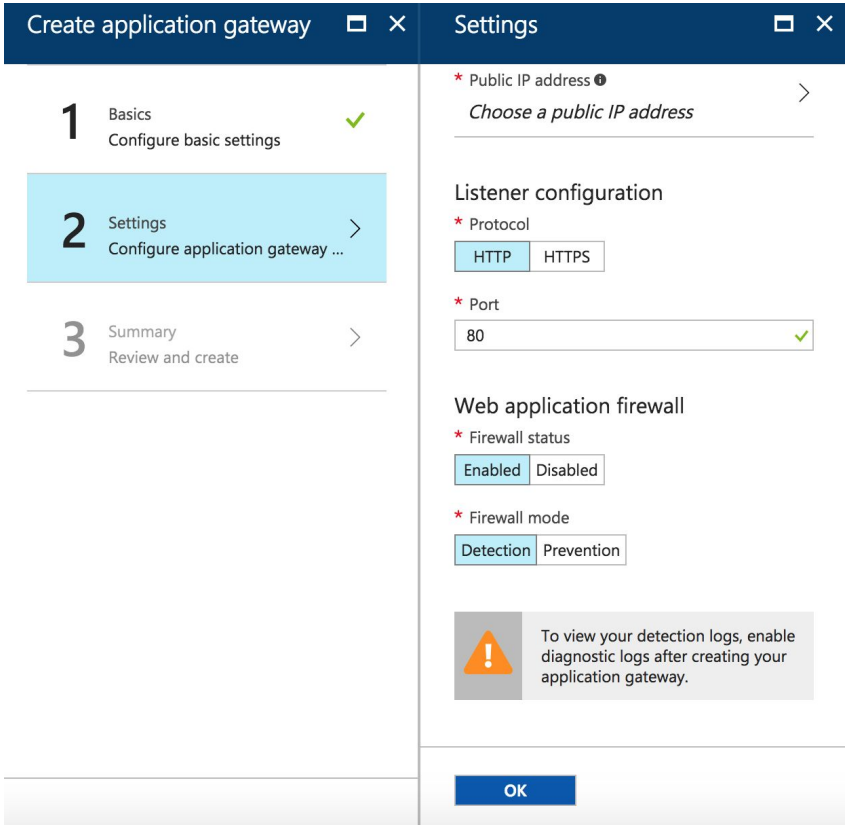
OWASP_3.0

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

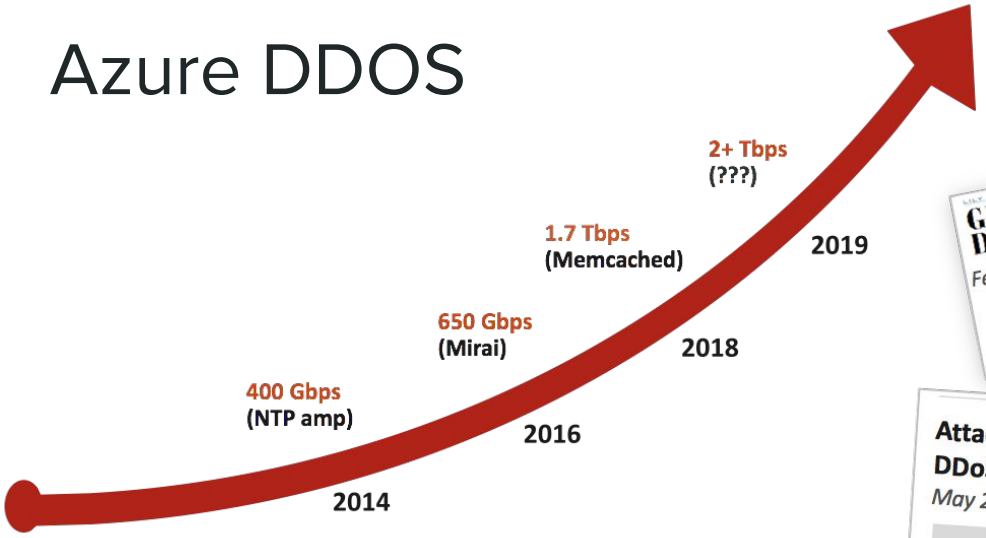
Azure WAF

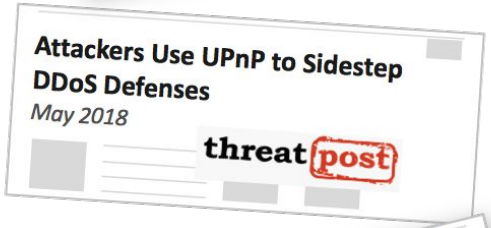

Application Gateway
WAF
L7 LB
Access Log
Performance Log
Firewall Log
Event Hubs
Log Analytics
Storage (Azure)
Recommendations
Alerts
Security Center


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

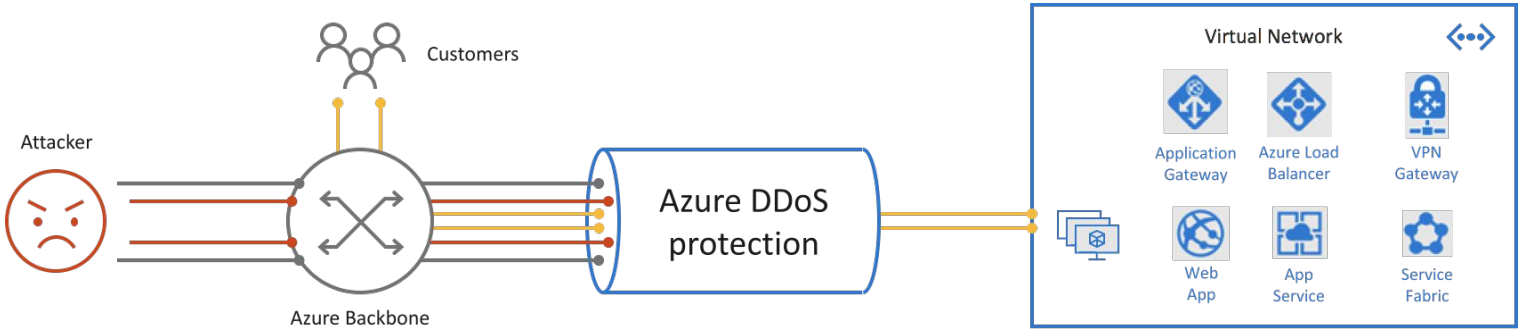
Attack Downtime

35%

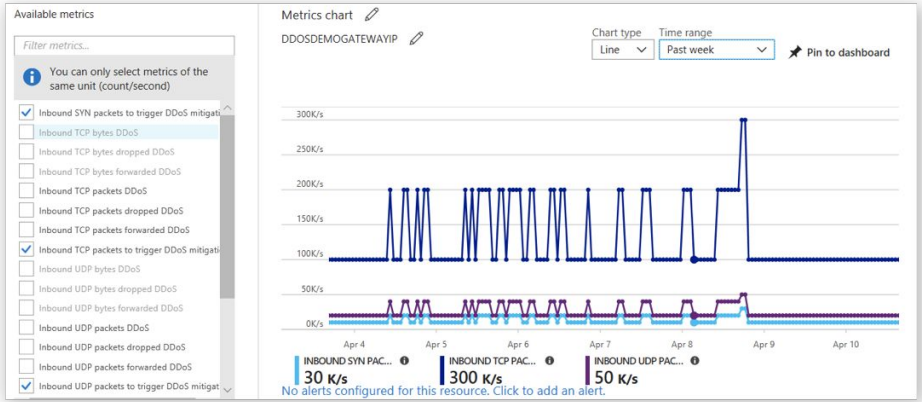
Businesses impacted

Source : Microsoft Ignite 2018 - BRK4029

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

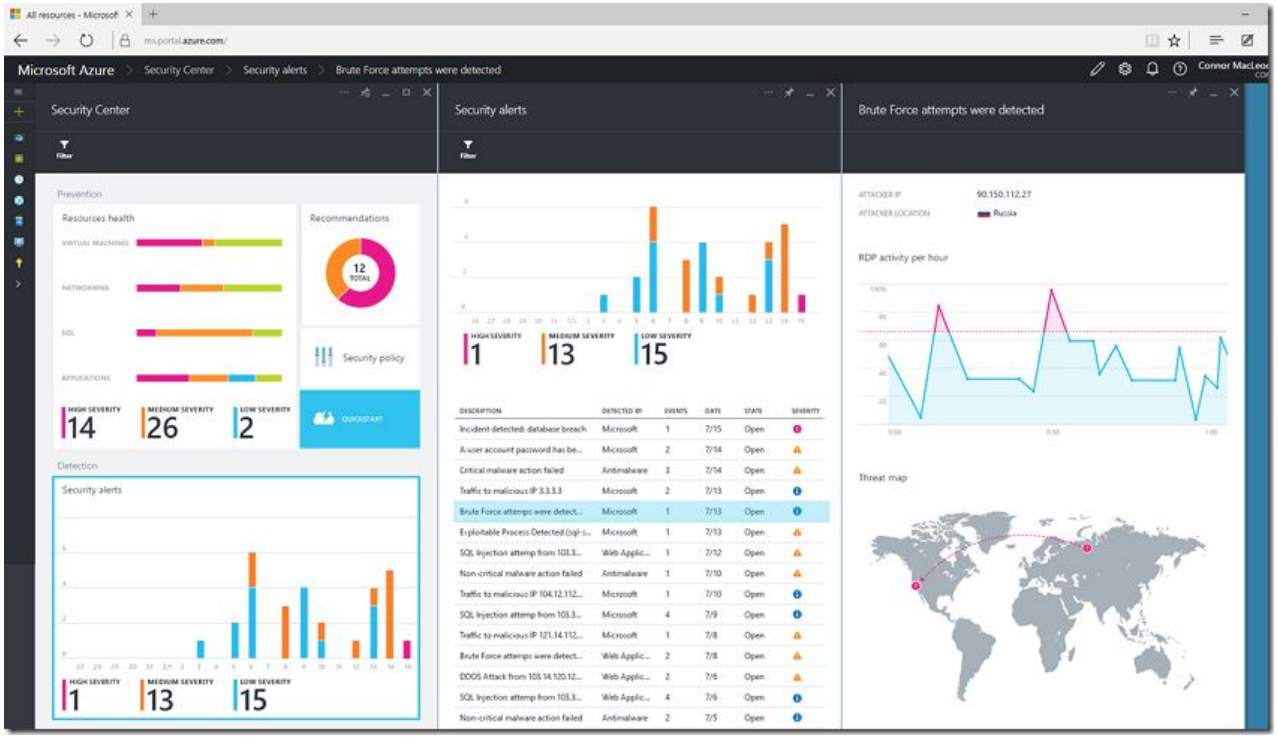


Azure Security Center

Azure Security Center

- Integrated threat intelligence
- Behavioral analytics
- Anomaly detection

Azure Security Center



Prevention policy

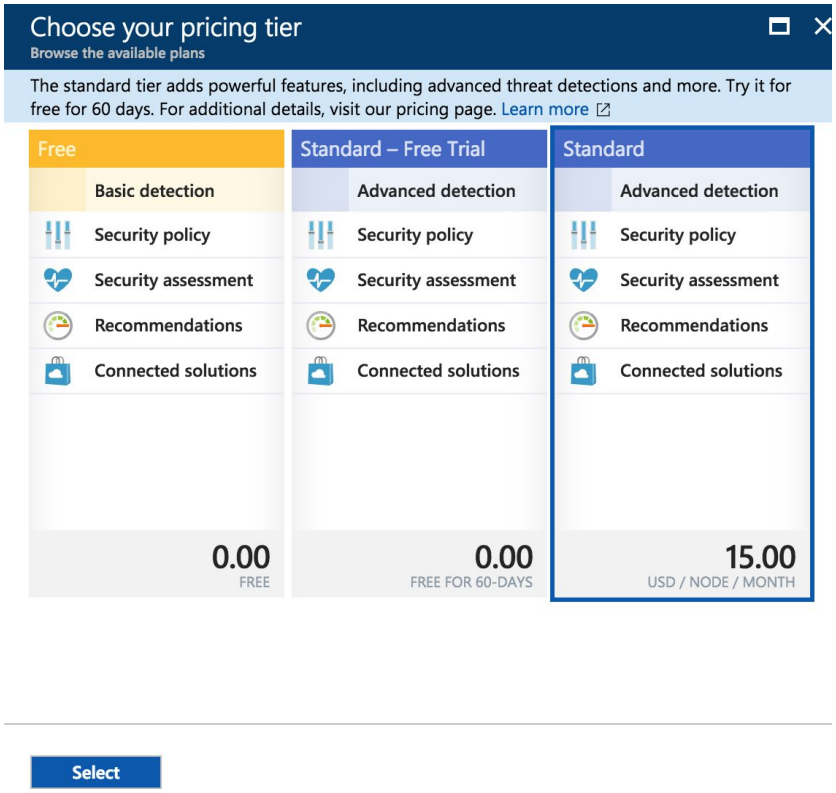
Microsoft Azure Sponsorship

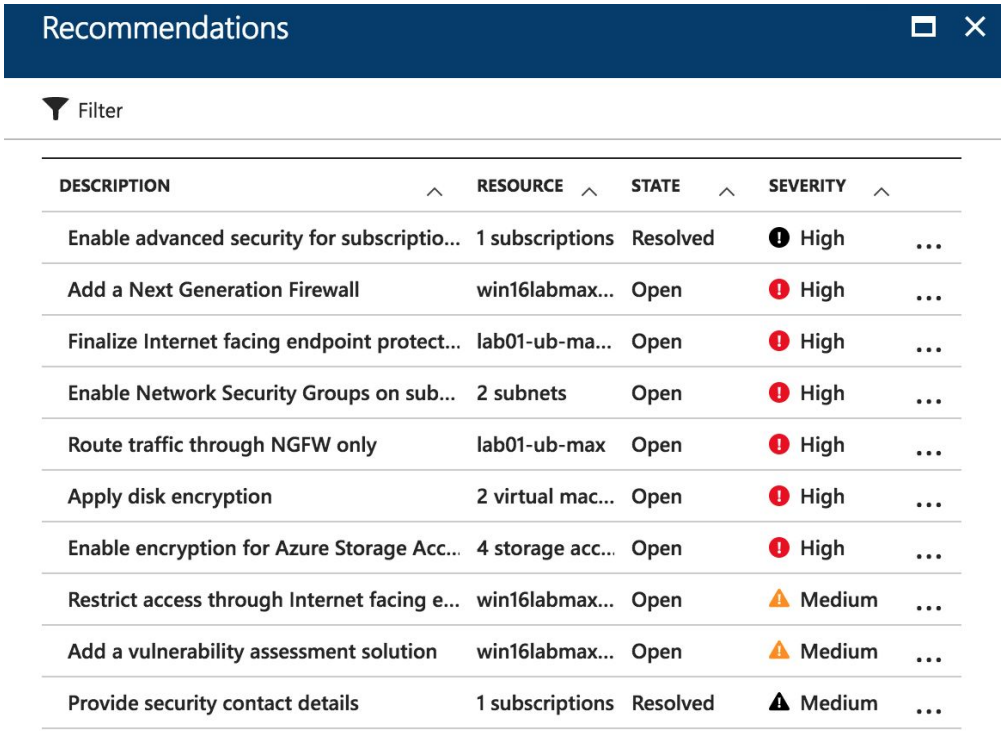
Show recommendations for

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





Azure Security Center

lab01-ub-max-nsg

Edit inbound rules

Network security group info

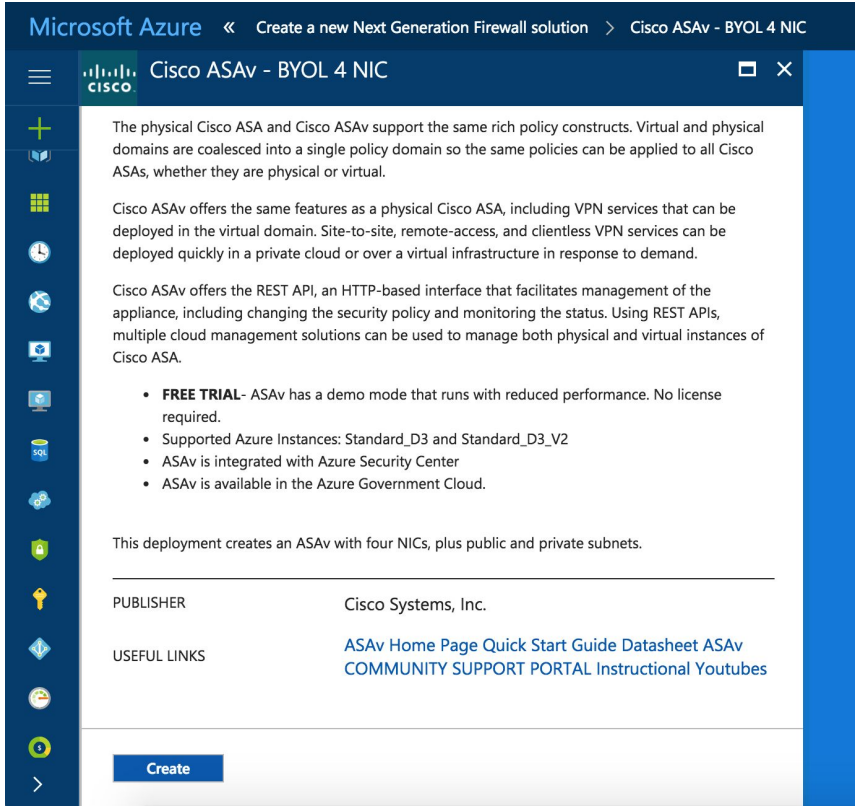
NETWORK SECURITY GROUP	lab01-ub-max-nsg
LOCATION	eastus
DESCRIPTION	Your NSG has inbound rules that open access to 'Any' or 'Internet' which might enable attackers to access your resources. We recommend that you edit the below inbound rules to restrict access to a specified set of sources.

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



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.

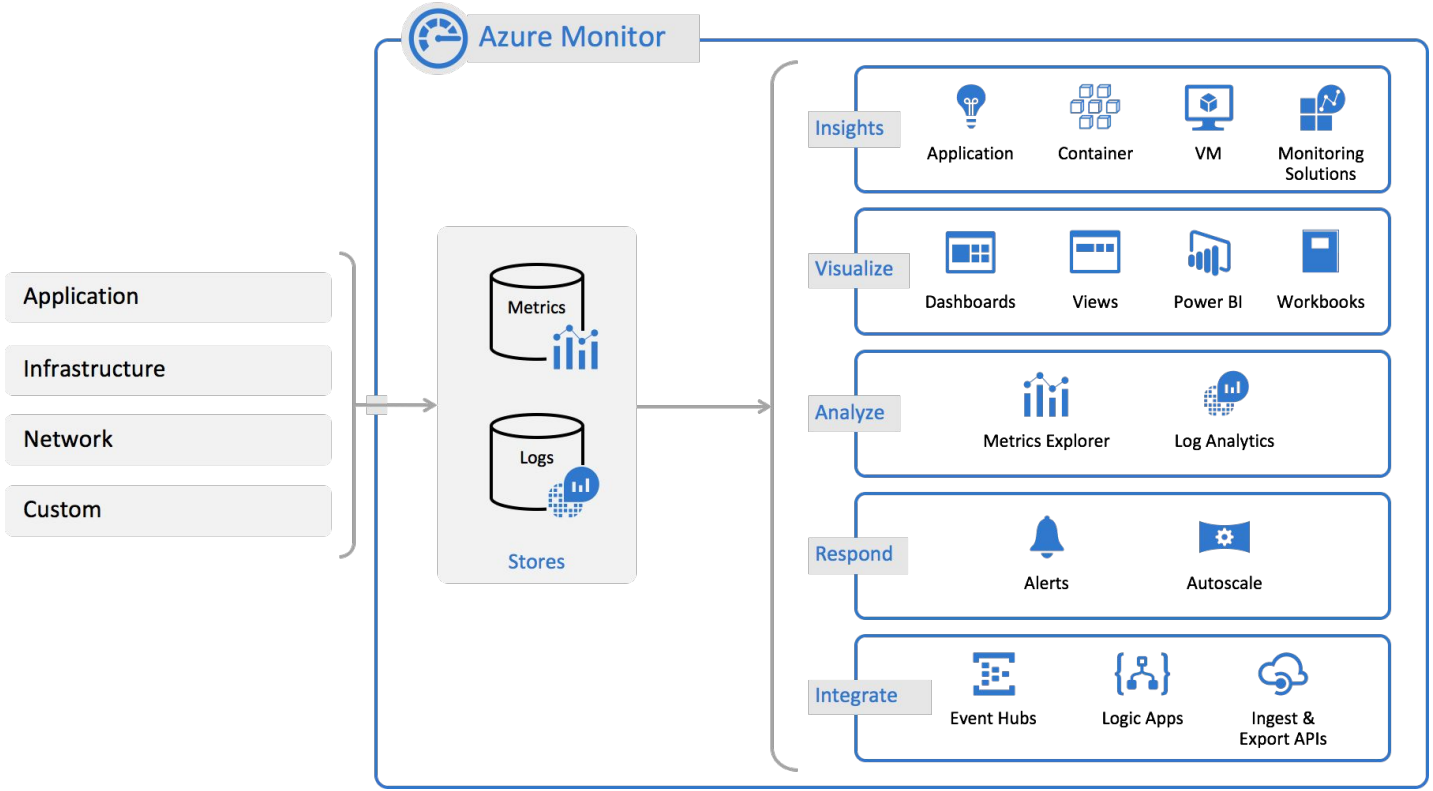
Search:

Reporter	Date	Comment	Categories
infosky.net	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 ... show more	DDoS Attack
doyoucheck.com	14 hours ago	ssh intrusion attempt	SSH
Anonymous	25 Jun 2017	Brute force SSH login	Brute-Force SSH
cutkit.eu	25 Jun 2017	SSH brute force	Brute-Force SSH
blueSh4rk	25 Jun 2017	unauthorized ssh connection attempt	Brute-Force SSH
blog.demees.net	25 Jun 2017	ssh-bruteforce	SSH
infosky.net	25 Jun 2017	SSH/22 MH Probe, BF -	Brute-Force SSH
infosky.net	25 Jun 2017	SSH/22 MH Probe, BF -	Brute-Force SSH

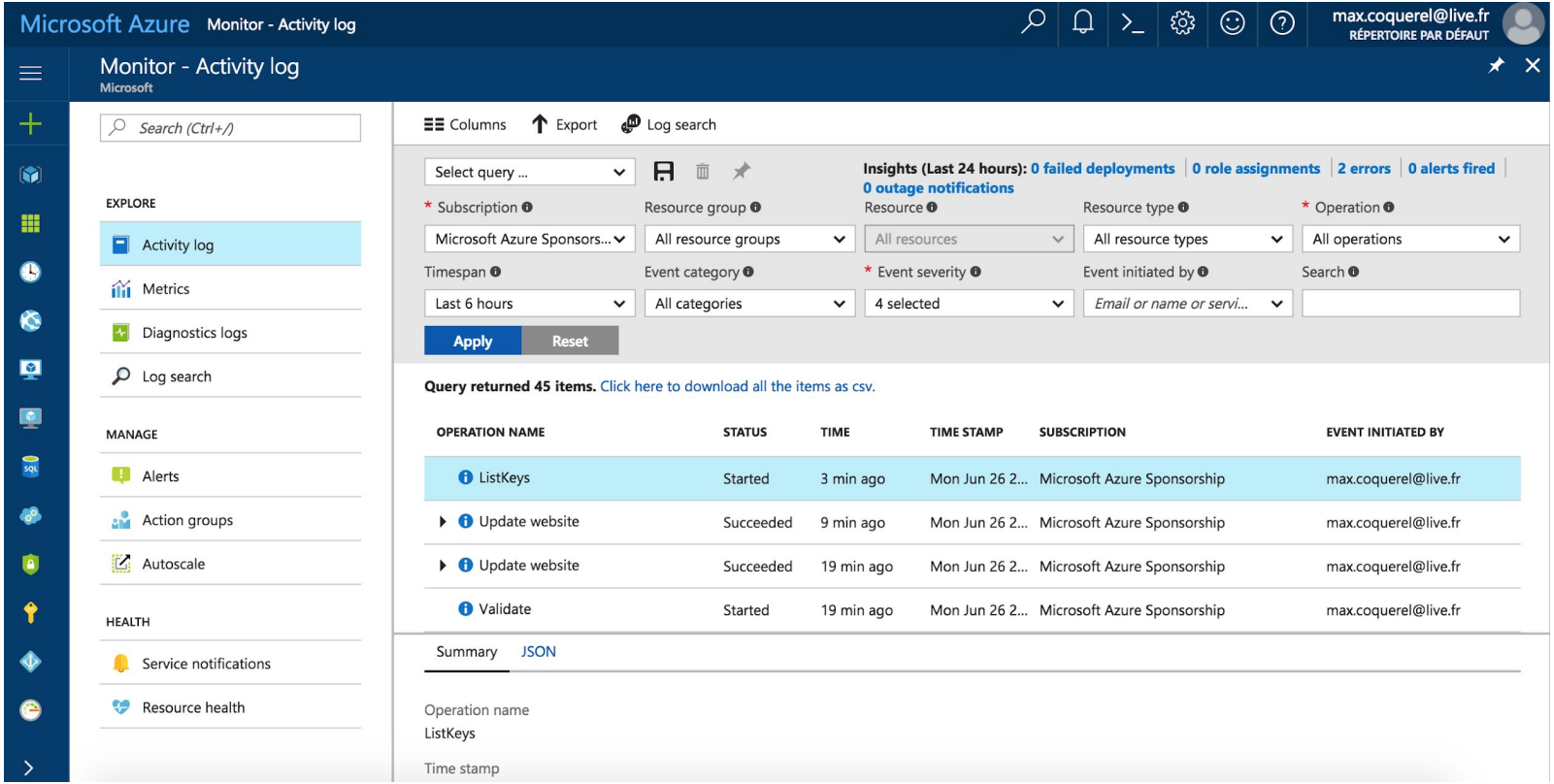
Azure Security Center - Demo

Investigation

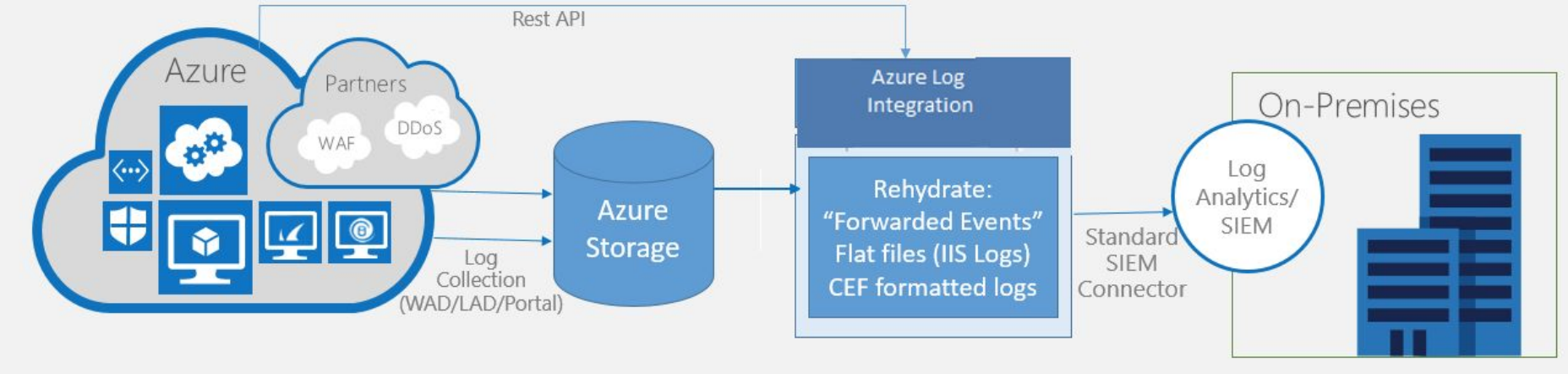
Azure Monitor



Forensic investigation (Logs)



Azure SIEM (IBM QRadar + Splunk)



Howto Azure with IBM QRadar: http://zigmax.net/azure-siem-ibm-qradar/

Conclusion

> Compliance …. **Azure Policy**

> Identity Management … **Azure Active Directory**

> No flat networks … **Network Security Group**

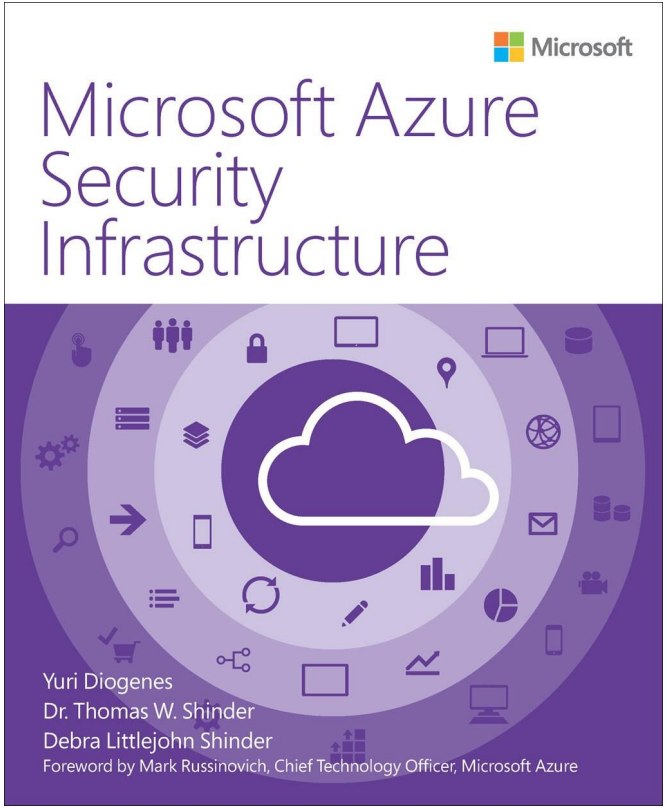
> Manage secrets … **Azure Key Vault**

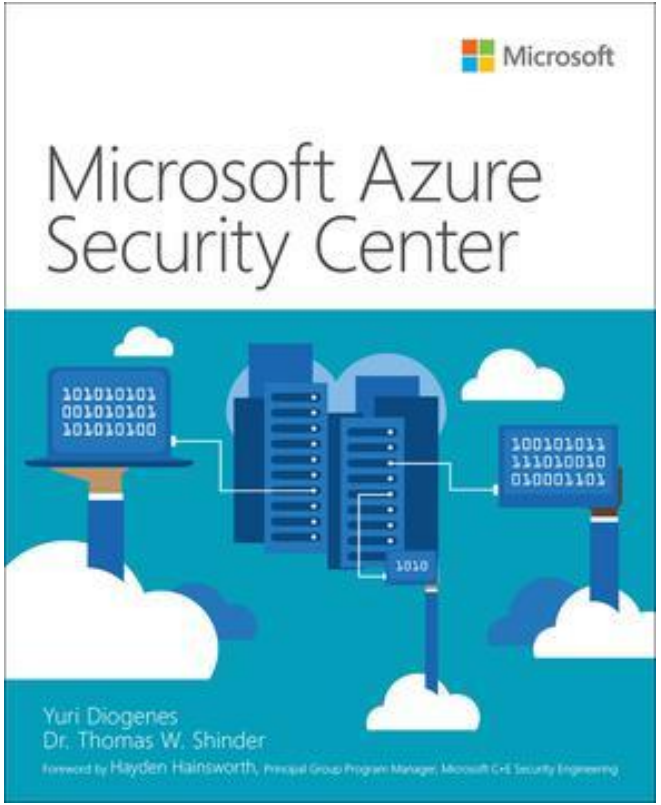
> Firewall / WAF …. **Azure Firewall / Azure WAF**

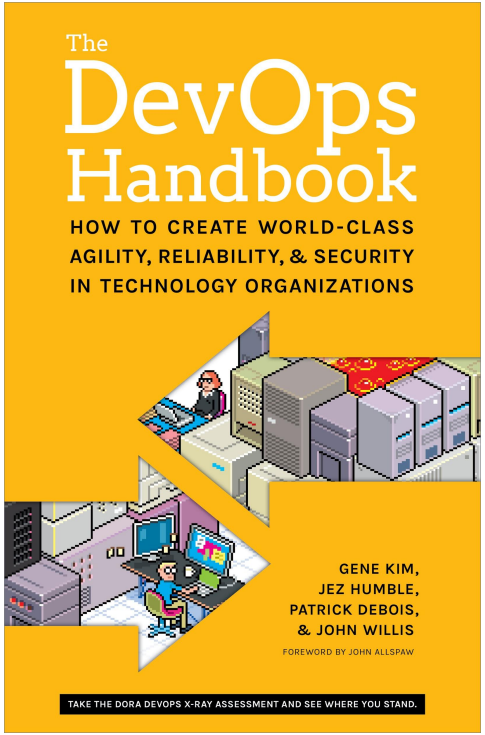
> Threat Analytics - **Azure Security Center**

> Have fun :) !

Books


Microsoft
Microsoft Azure Security Infrastructure
Yuri Diogenes
Dr. Thomas W. Shinder
Debra Littlejohn Shinder
Foreword by Mark Russinovich, Chief Technology Officer, Microsoft Azure


Microsoft
Microsoft Azure Security Center
Yuri Diogenes
Dr. Thomas W. Shinder
Foreword by Hayden Hainsworth, Principal Group Program Manager, Microsoft C+E Security Engineering


The
DevOps Handbook
HOW TO CREATE WORLD-CLASS AGILITY, RELIABILITY, & SECURITY IN TECHNOLOGY ORGANIZATIONS
GENE KIM,
JEZ HUMBLE,
PATRICK DEBOIS,
& JOHN WILLIS
FOREWORD BY JOHN ALLSPAW
TAKE THE DORA DEVOPS X-RAY ASSESSMENT AND SEE WHERE YOU STAND.

Technical Ressources

Microsoft Learn - https://docs.microsoft.com/fr-fr/learn/

Microsoft Virtual Academy (FR) - https://stanislas.io/2016/04/26/41/

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 2018 - https://myignite.techcommunity.microsoft.com/

Questions / Talks