OWASP
AppSec EU
Belfast
8-12 May, 2017

Azure security best practices

Viktorija Almazova, IT Security Architect

WHY, I FEEL SAFER ALREADY....
"SECURITY GUARD"
imgflip.com

Developers are in a driver seat now

Azure security services

Azure security services

Azure security general

- Azure Security Center
- Azure Key Vault
- Azure Disk Encryption
- Log Analytics
- Azure Dev/Test Labs

Azure Storage Security

- Azure Storage Service Encryption
- StorSimple Encrypted Hybrid Storage
- Azure Client-Side Encryption
- Azure Storage Shared Access Signatures
- Azure Storage Account Keys
- Azure File Shares with SMB 3.0 Encryption
- Azure Storage Analytics

Backup and Disaster Recovery

- Azure Backup
- Azure Site Recovery

Azure Database Security

- Azure SQL Firewall
- Azure SQL Authentication
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing

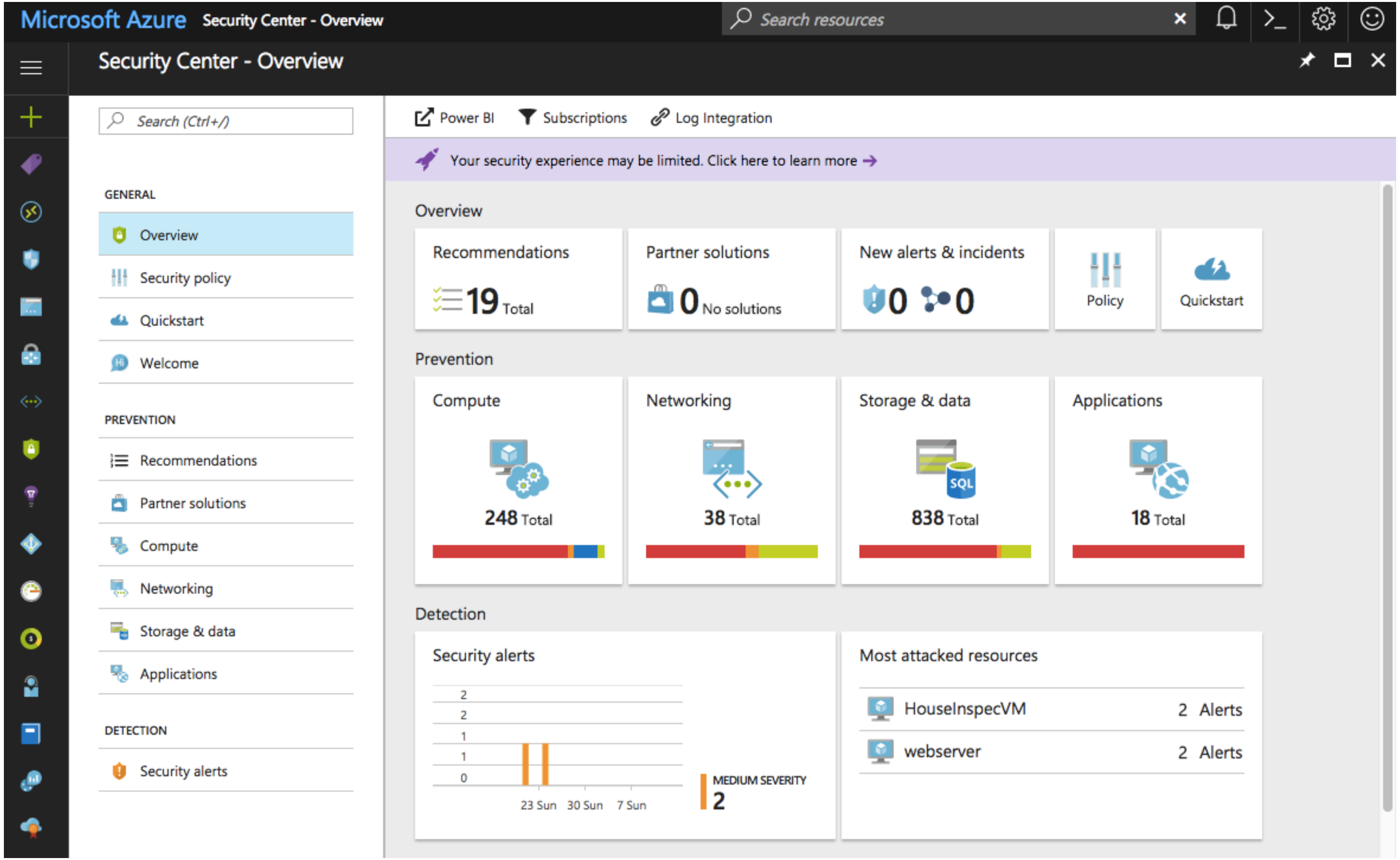
Azure Identity and Access Management

- Azure Role Based Access Control
- Azure Active Directory /B2C/B2B
- Azure Multi-Factor Authentication

Azure Networking

- Network Security Groups
- Azure VPN Gateway
- Azure Application Gateway
- Azure Load Balancer
- Azure Traffic Manager
- Azure Application Proxy

Azure security general



Microsoft Azure Security Center - Overview

Search resources

Security Center - Overview

Search (Ctrl+/)

GENERAL

- Overview
- Security policy
- Quickstart
- Welcome

PREVENTION

- Recommendations
- Partner solutions
- Compute
- Networking
- Storage & data
- Applications

DETECTION

- Security alerts

Power BI | Subscriptions | Log Integration

Your security experience may be limited. Click here to learn more →

Overview

Recommendations	Partner solutions	New alerts & incidents	Policy	Quickstart
19 Total	0 No solutions	0 0		

Prevention

Compute	Networking	Storage & data	Applications
248 Total	38 Total	838 Total	18 Total

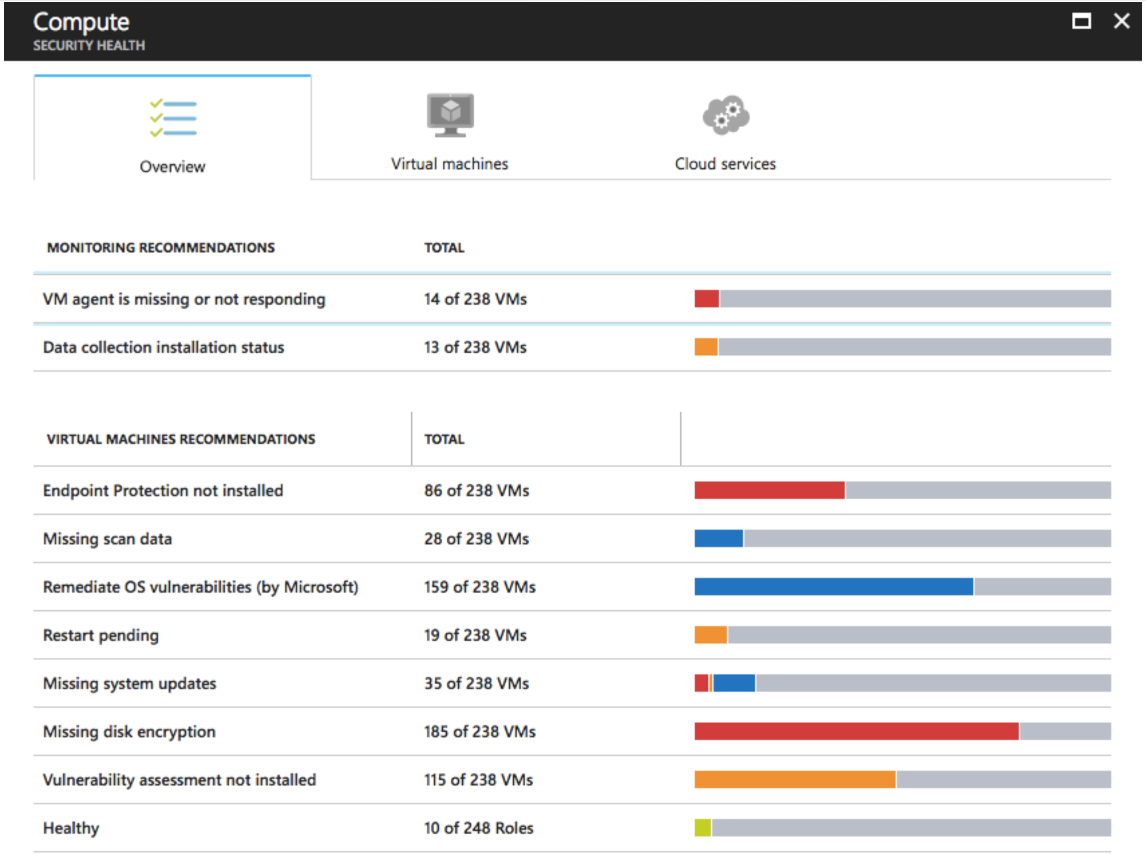
Detection

Security alerts

MEDIUM SEVERITY 2

Most attacked resources

HouseInspecVM	2 Alerts
webserver	2 Alerts



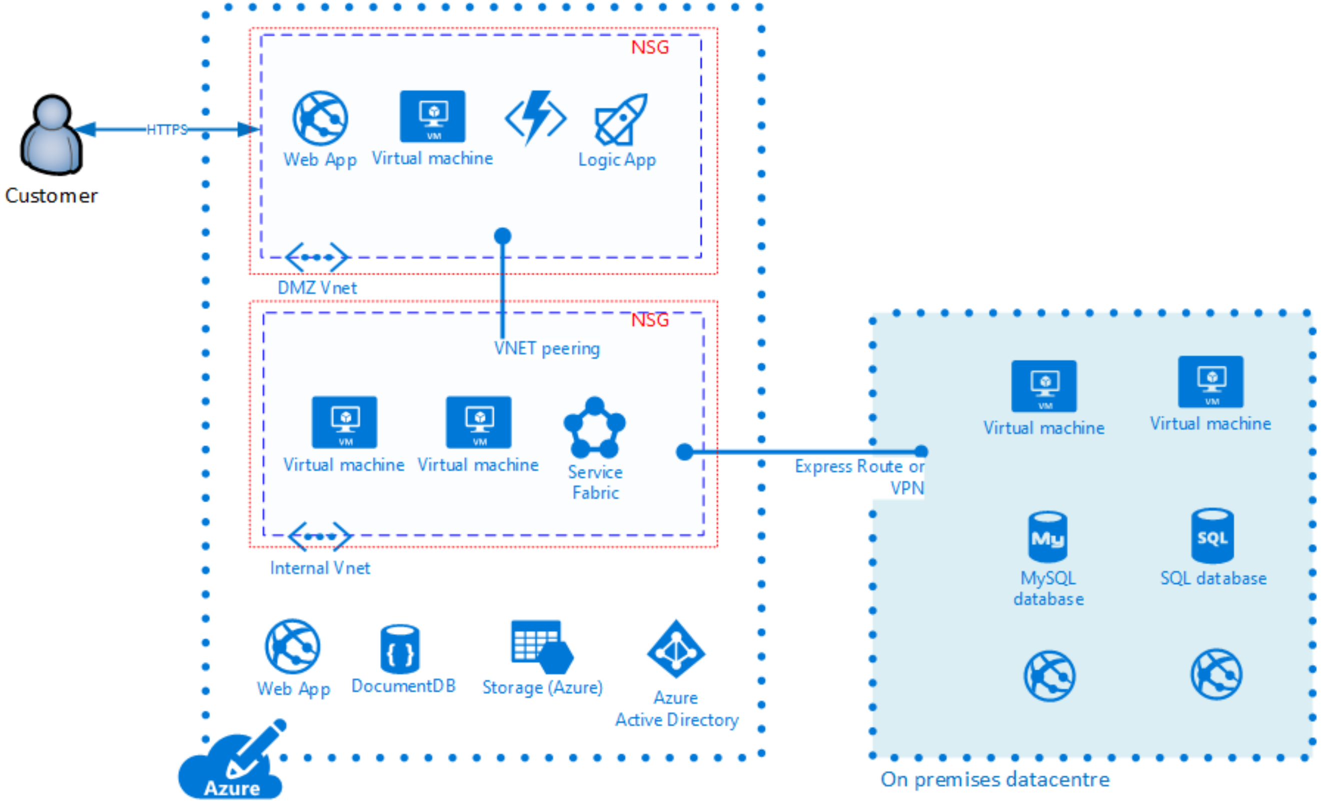
Compute

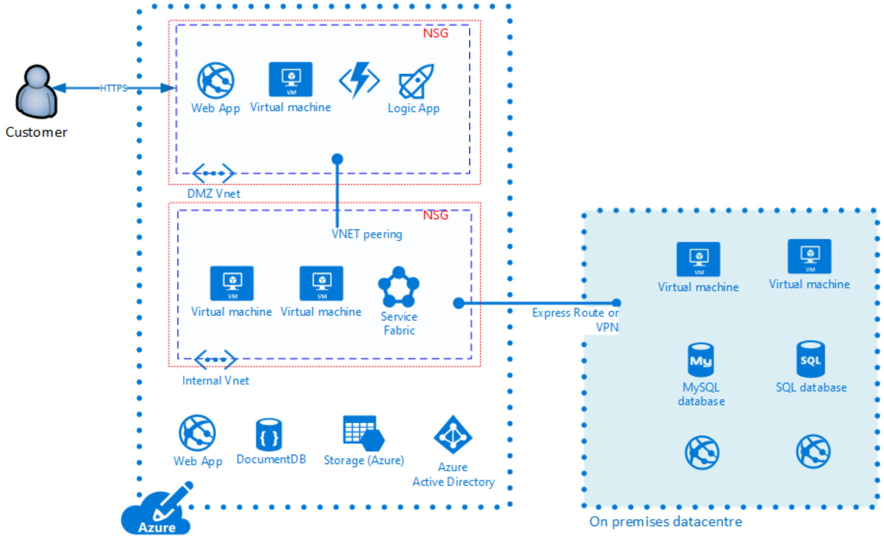
SECURITY HEALTH

MONITORING RECOMMENDATIONS	TOTAL
VM agent is missing or not responding	14 of 238 VMs
Data collection installation status	13 of 238 VMs

VIRTUAL MACHINES RECOMMENDATIONS	TOTAL
Endpoint Protection not installed	86 of 238 VMs
Missing scan data	28 of 238 VMs
Remediate OS vulnerabilities (by Microsoft)	159 of 238 VMs
Restart pending	19 of 238 VMs
Missing system updates	35 of 238 VMs
Missing disk encryption	185 of 238 VMs
Vulnerability assessment not installed	115 of 238 VMs
Healthy	10 of 248 Roles

Application architecture


Customer
HTTPS
NSG
Web App
Virtual machine
Logic App
DMZ Vnet
NSG
VNET peering
Virtual machine
Virtual machine
Service Fabric
Internal Vnet
Web App
DocumentDB
Storage (Azure)
Azure Active Directory
Azure
Express Route or VPN
Virtual machine
Virtual machine
MySQL database
SQL database
On premises datacentre



Some best practices:

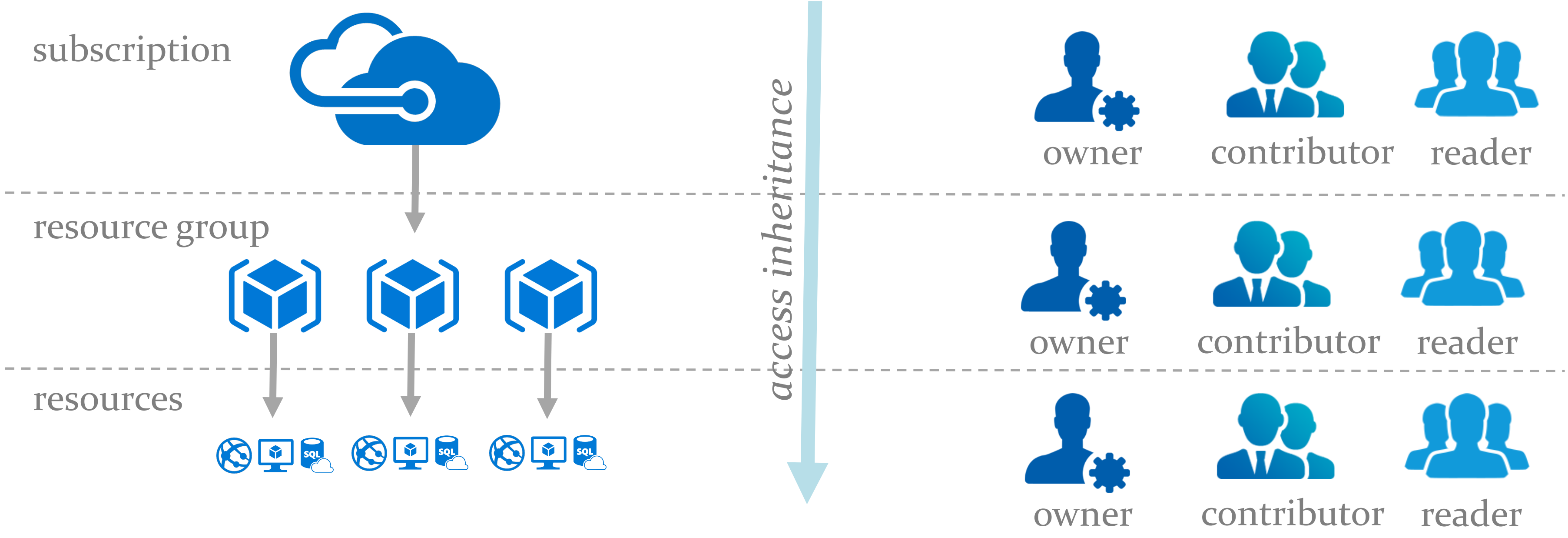
- Logically segment subnets
- Use Virtual network appliances
- Deploy DMZs for security zoning
- Avoid exposure to the Internet with dedicated WAN links
- Optimize uptime and performance
- Use global load balancing
- Disable RDP access to Azure Virtual Machines
- Enable Azure Security Center
- Extend your datacenter into Azure

Access control

Access control

- Manage an access to Azure resources with Role based control
- Implement authentication and authorization for web application
- Secure connections between application and services
- Azure Key Vault

Role based control in Azure



subscription

resource group

resources

access inheritance

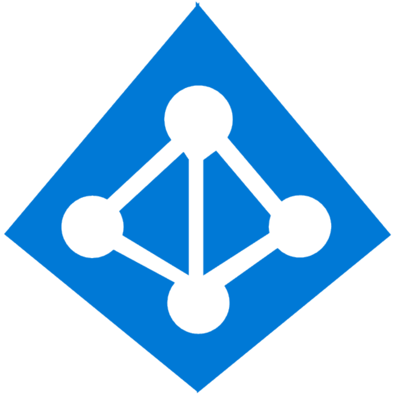
owner contributor reader

owner contributor reader

owner contributor reader

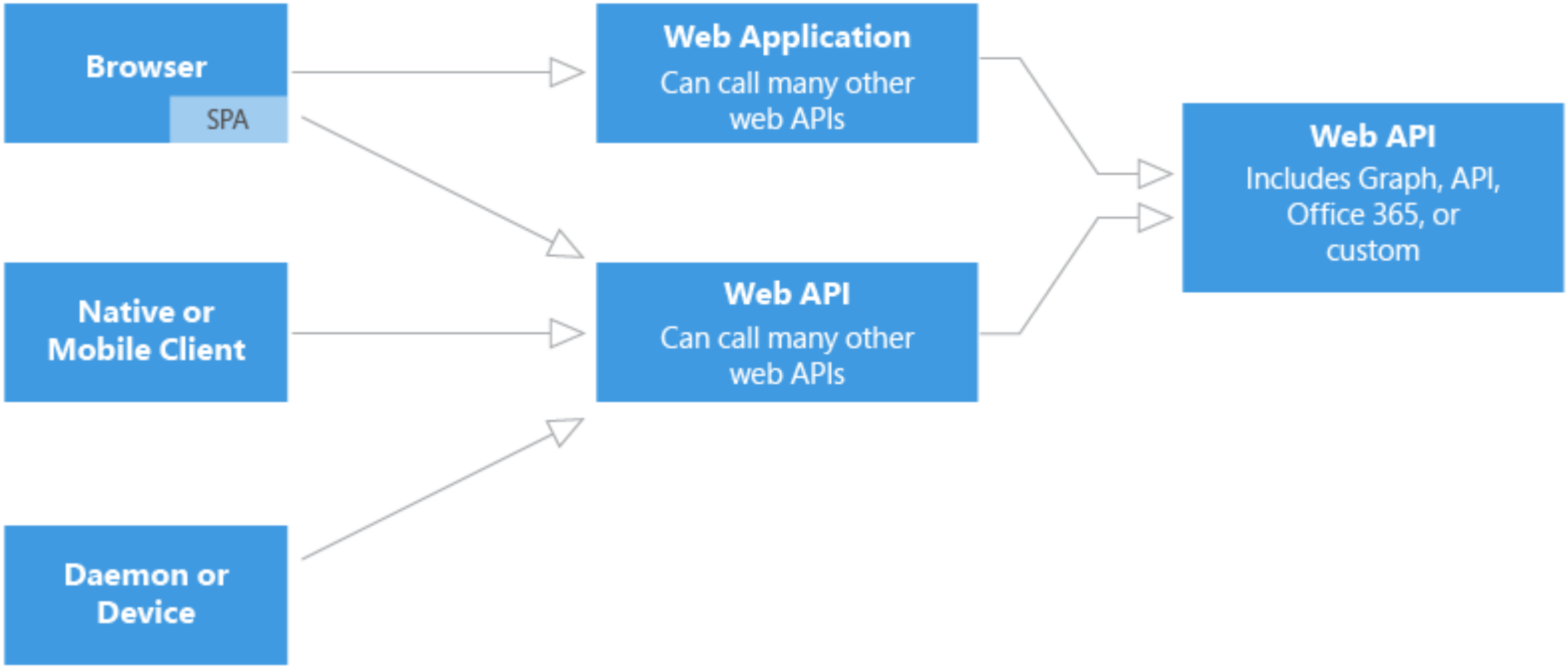
principle of least privilege

Azure Active Directory



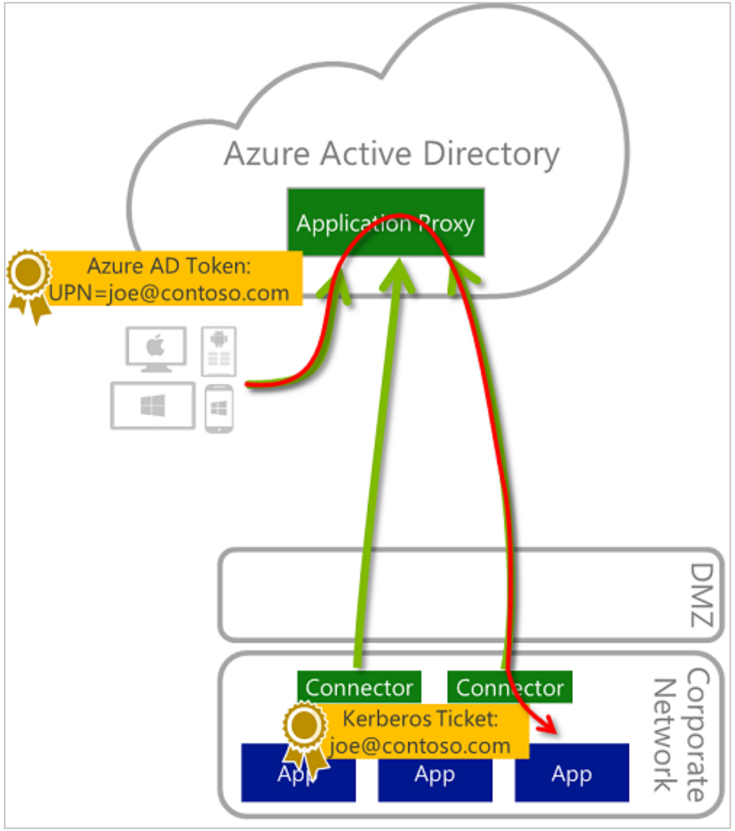
- AAD not MS AD – it is all about Identity
- For application developers AAD lets focus on application not user management

Application Types and Scenarios

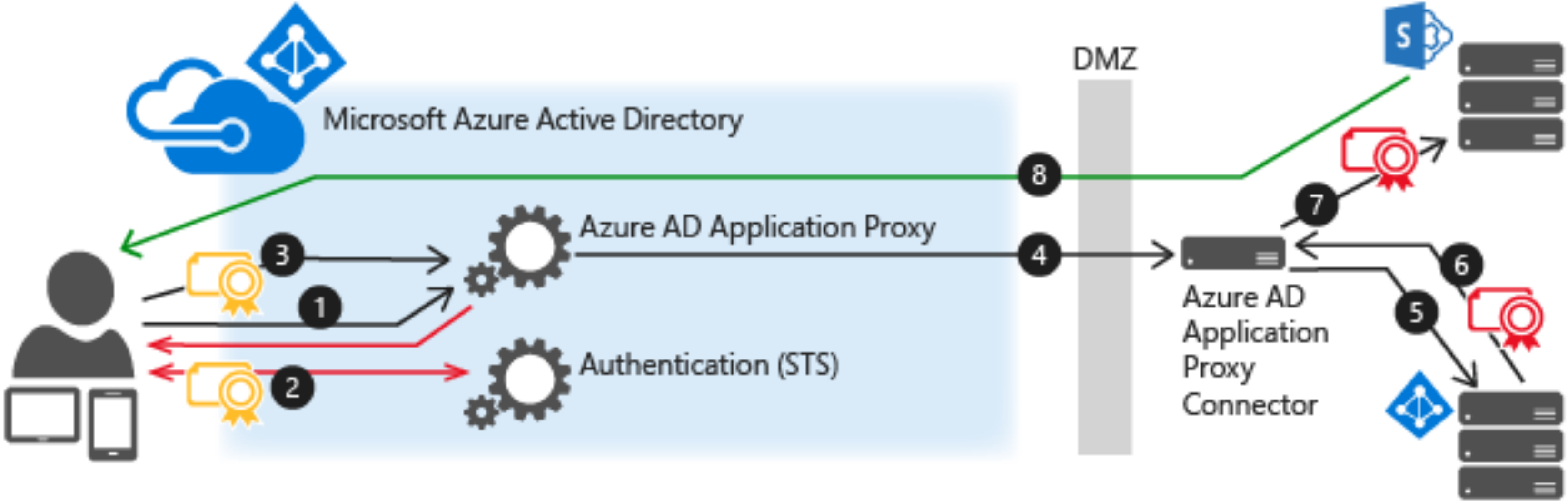

Browser
SPA
Web Application
Can call many other web APIs
Web API
Includes Graph, API, Office 365, or custom
Native or Mobile Client
Web API
Can call many other web APIs
Daemon or Device

https://docs.microsoft.com/en-us/azure/active-directory/active-directory-code-samples#web-browser-to-web-application

Azure Application Proxy



Azure Application Proxy

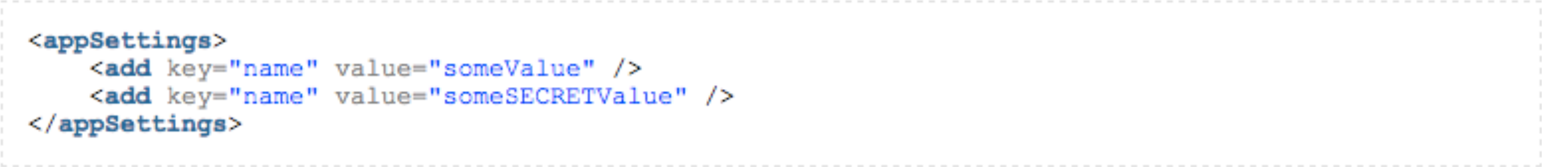

Microsoft Azure Active Directory
DMZ
8
Azure AD Application Proxy
3
4
7
6
1
5
Azure AD Application Proxy Connector
2
Authentication (STS)

Secure connections between application and services

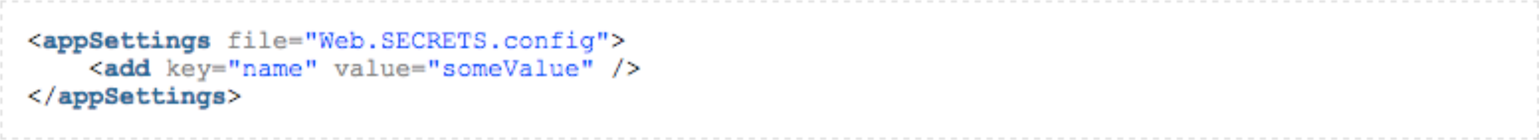
- Keep passwords and connection strings out of source
- Don't put private stuff in common configuration files
- Use Environment variables or User-level config options
- When deploying a web service to Azure use Application settings

Keep passwords and connection strings OUT

ASP.NET 4.6

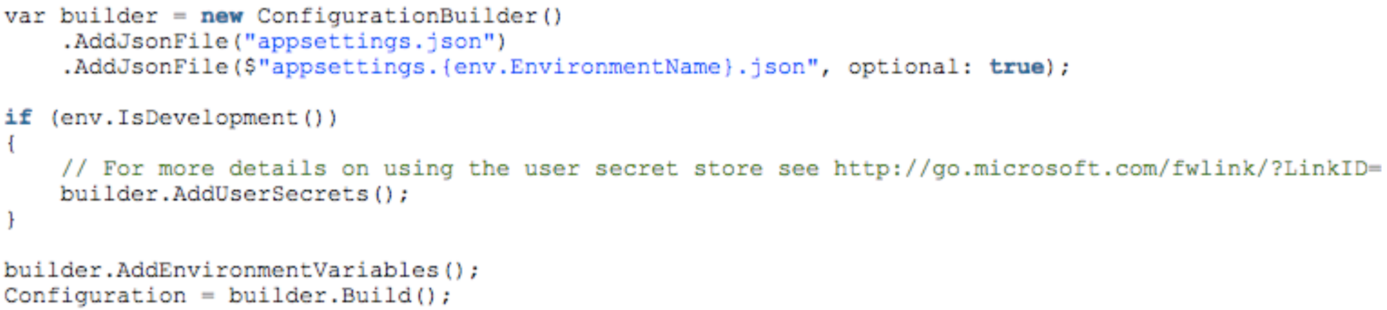


```
<appSettings>
    <add key="name" value="someValue" />
    <add key="name" value="someSECRETValue" />
</appSettings>
```



```
<appSettings file="Web.SECRETS.config">
    <add key="name" value="someValue" />
</appSettings>
```

ASP.NET 5

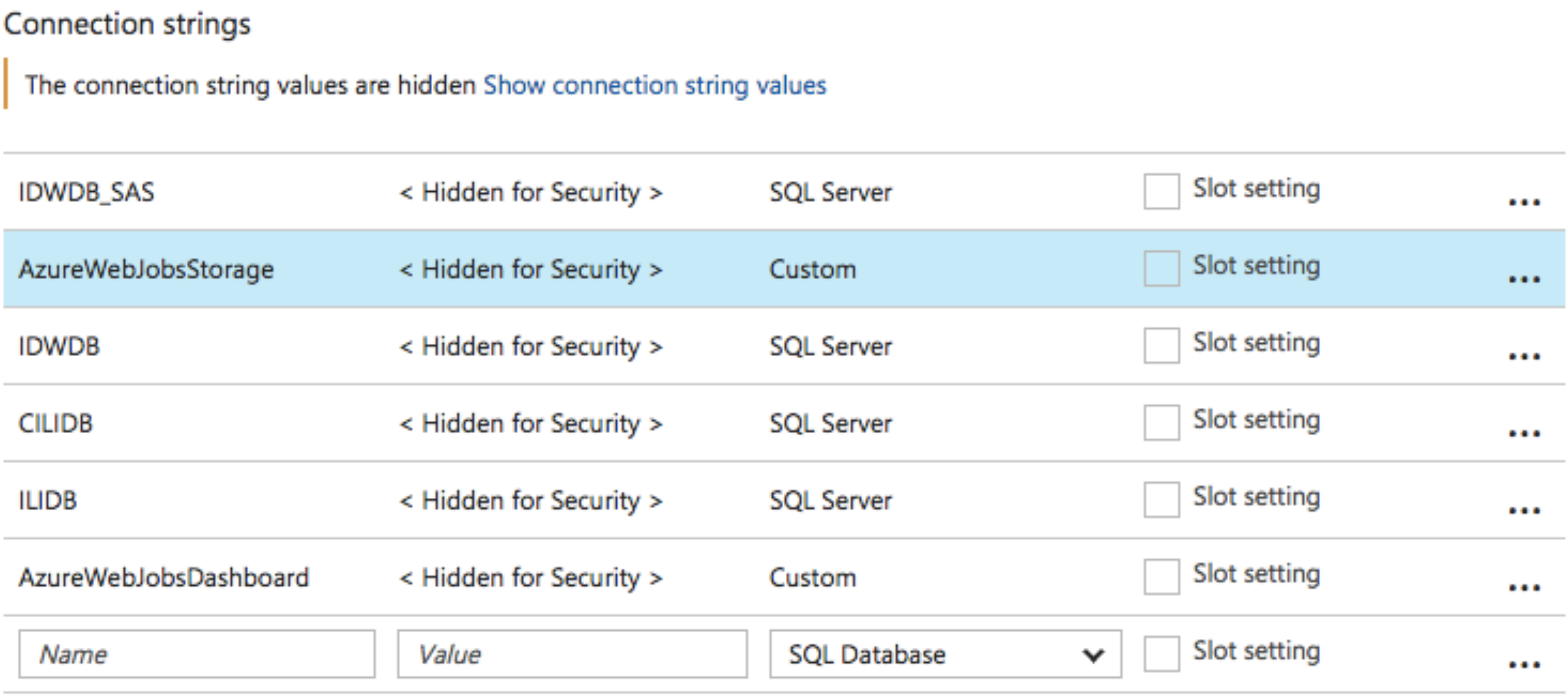


```
var builder = new ConfigurationBuilder()
    .AddJsonFile("appsettings.json")
    .AddJsonFile($"appsettings.{env.EnvironmentName}.json", optional: true);

if (env.IsDevelopment())
{
    // For more details on using the user secret store see http://go.microsoft.com/fwlink/?LinkID=
    builder.AddUserSecrets();
}

builder.AddEnvironmentVariables();
Configuration = builder.Build();
```

Secure connections between application and services



Connection strings

The connection string values are hidden Show connection string values

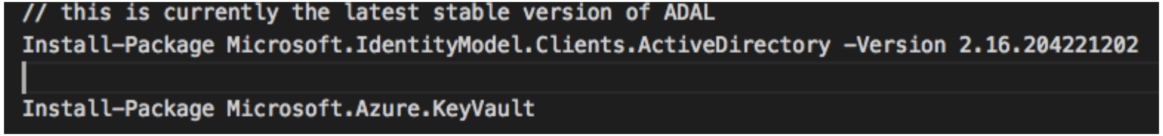
IDWDB_SAS	< Hidden for Security >	SQL Server	□ Slot setting	...
AzureWebJobsStorage	< Hidden for Security >	Custom	□ Slot setting	...
IDWDB	< Hidden for Security >	SQL Server	□ Slot setting	...
CILIDB	< Hidden for Security >	SQL Server	□ Slot setting	...
ILIDB	< Hidden for Security >	SQL Server	□ Slot setting	...
AzureWebJobsDashboard	< Hidden for Security >	Custom	□ Slot setting	...
Name	*Value*	SQL Database ⌄	□ Slot setting	...

Azure Key Vault

- Azure Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services
- Keys are stored in a vault and invoked by URI when needed
- Keys are safeguarded by Azure

Azure Key Vault

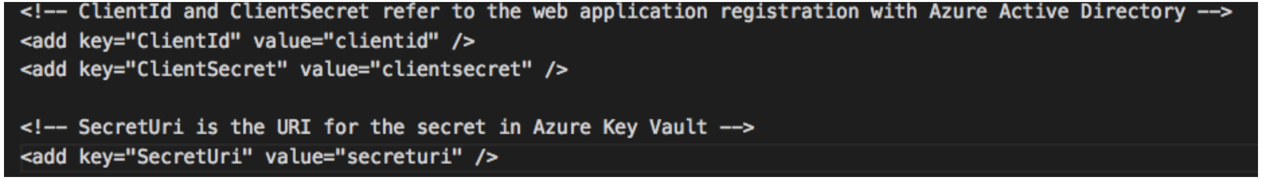
Add Nuget



```
// this is currently the latest stable version of ADAL
Install-Package Microsoft.IdentityModel.Clients.ActiveDirectory -Version 2.16.204221202

Install-Package Microsoft.Azure.KeyVault
```

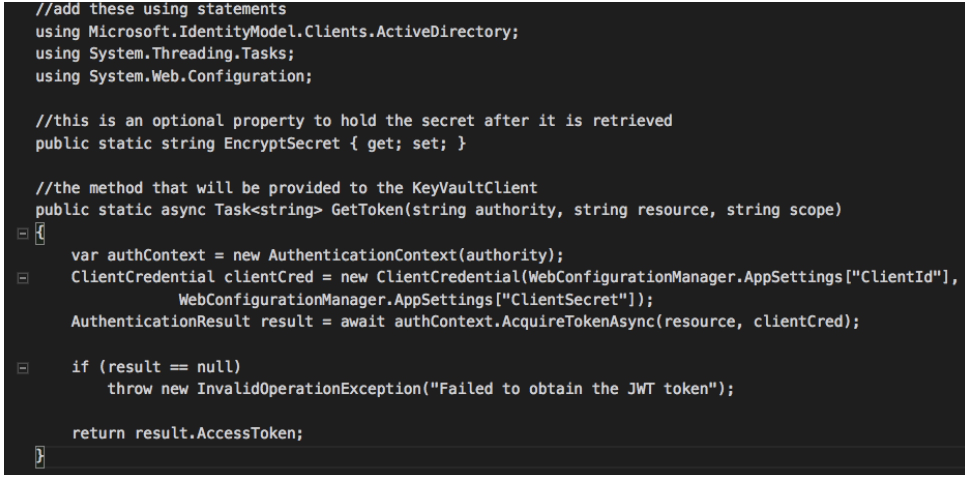
Modify web.config



```
<!-- ClientId and ClientSecret refer to the web application registration with Azure Active Directory -->
<add key="ClientId" value="clientid" />
<add key="ClientSecret" value="clientsecret" />

<!-- SecretUri is the URI for the secret in Azure Key Vault -->
<add key="SecretUri" value="secreturi" />
```

Add token to grab an access token



```
//add these using statements
using Microsoft.IdentityModel.Clients.ActiveDirectory;
using System.Threading.Tasks;
using System.Web.Configuration;

//this is an optional property to hold the secret after it is retrieved
public static string EncryptSecret { get; set; }

//the method that will be provided to the KeyVaultClient
public static async Task<string> GetToken(string authority, string resource, string scope)
{
    var authContext = new AuthenticationContext(authority);
    ClientCredential clientCred = new ClientCredential(WebConfigurationManager.AppSettings["ClientId"],
                WebConfigurationManager.AppSettings["ClientSecret"]);
    AuthenticationResult result = await authContext.AcquireTokenAsync(resource, clientCred);

    if (result == null)
        throw new InvalidOperationException("Failed to obtain the JWT token");

    return result.AccessToken;
}
```

Data protection

Azure data protection

Data isolation
Logical isolation segregates each customer's data from that of others is enabled by default

In-transit data protection
Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default

Data redundancy
Customers have multiple options for replicating data, including number of copies and number and location of replication data centers

At-rest data protection
Customers can implement a range of encryption options for virtual machines, storage, SQL, etc

Encryption
Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data

Data destruction
Strict standards for overwriting storage resources before reuse and the physical destruction of decommissioned hardware are by default

Azure data encryption

Virtual Machines – Windows and Linux

- Azure Disk Encryption - *<BitLocker [Windows], DM-Crypt [Linux]>*
- Partner Volume Encryption – *<CloudLink® SecureVM>*

SQL Server and SQL Database

- Transparent Data Encryption - *<SQL Server OR SQL Database>*
- Cell Level Encryption - *<SQL Server OR SQL Database>*
- Always Encrypted

Azure Storage – Blobs, Tables, Queues

- Application Level Encryption - *<Storage Client-Side encryption>*
- Cloud Integrated Storage - *<StorSimple>*

HDInsight

- HDInsight – *<Leverages Azure Storage, SQL Azure DB encryption>*

Azure Backup Service

- Azure Backup Service – *<Leverages Azure Disk Encryption>*

Keys Management

Azure Key Vault

<Keys and Secrets controlled by customers in their key vault>

Authentication to Key Vault

<Authentication to Key Vault is using Azure AD>

Application security

Application security

problems remains the same

Application security

- Changes thru deployment – templates and deployment pipeline
- Owasp Top 10
- Protect additionally with WAF and securing HTTP headers
- Scanning for security web app

QUESTIONS

A Long Time Ago in a Galaxy Far, Far Away…

Thank You to Our Sponsors

OWASP
AppSec EU
Belfast

CME Group

SYNOPSYS®

Hewlett Packard
Enterprise

ARXAN

BLACKDUCK

CHECKMARX

CITRIX®

FLEXERA
SOFTWARE

kiuwan

netsparker®

POSITIVE TECHNOLOGIES

RAPID7

Sonatype

Twistlock

Invest
Northern
Ireland

INTUITION
TechChannels

jscrambler

promon

WhiteHat
SECURITY.

MCSGROUP
INTELLIGENT RECRUITMENT SOLUTIONS

edgescan

Invest
Northern
Ireland

Allstate.
You're in good hands.