OWASP and Cloud Security

[Your Name]
[Your Title]

Microsoft

Objectives

Threats

Landscape

What is the Cloud

Services

Shared Controls

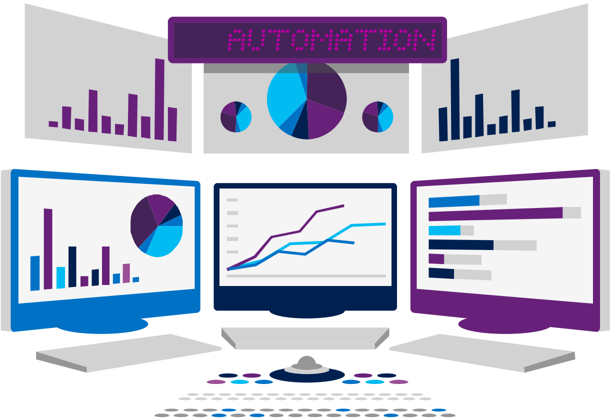
OWASP TOP 10

Vulnerabilities

The Cloud Can Protect You!

About Mike

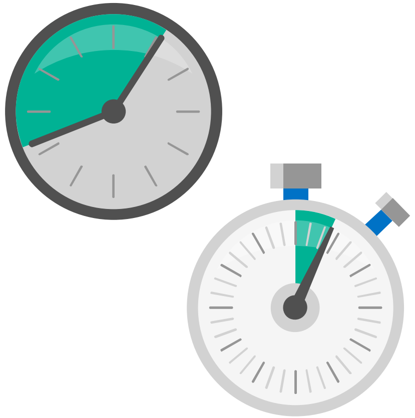
- Cloud Solution Architect. MCSD Certified on Azure
- Technical Evangelist
- Software Engineer with 15+ Yrs of Experience
- 8 years at Microsoft, 2 years in consulting
- AWS, Rackspace and Azure Experience
- http://github.com/michaelsrichter
- http://twitter.com/michaelsrichter
- https://www.linkedin.com/in/mikerichter



Schedule

Threats

Cloud



Injection

Broken Authentication

XSS

Direct Object References

Security Misconfiguration

Sensitive Data Exposure

Access Control

CSRF

Components

Redirects and Forwards

Q&A

Threats

The threat landscape today

PREMERA BLUE CROSS

January 2015

11M

Records

Names, dates of birth, emails, SSNs, bank account, medical and financial information

SONY®

November 2014

100TB

Data

Documents, SSNs, email, passwords, unpublished scripts, marketing plans, financial and legal information

THE HOME DEPOT

September 2014

55M

Credit Cards

Adobe

October 2014

152M

Records

User name and hashed passwords + 2.8M encrypted credit cards

ebay

May 2014

145M

Records

Customer names, passwords, email addresses, physical addresses, phone numbers, dates of birth

TARGET

December 2013

110M

Records

40M credit card, 70M customer details

The threat landscape today

$400B Estimated Annual Global Damages

The Target breach

Targeted corporate network

Total “kill chain” failure

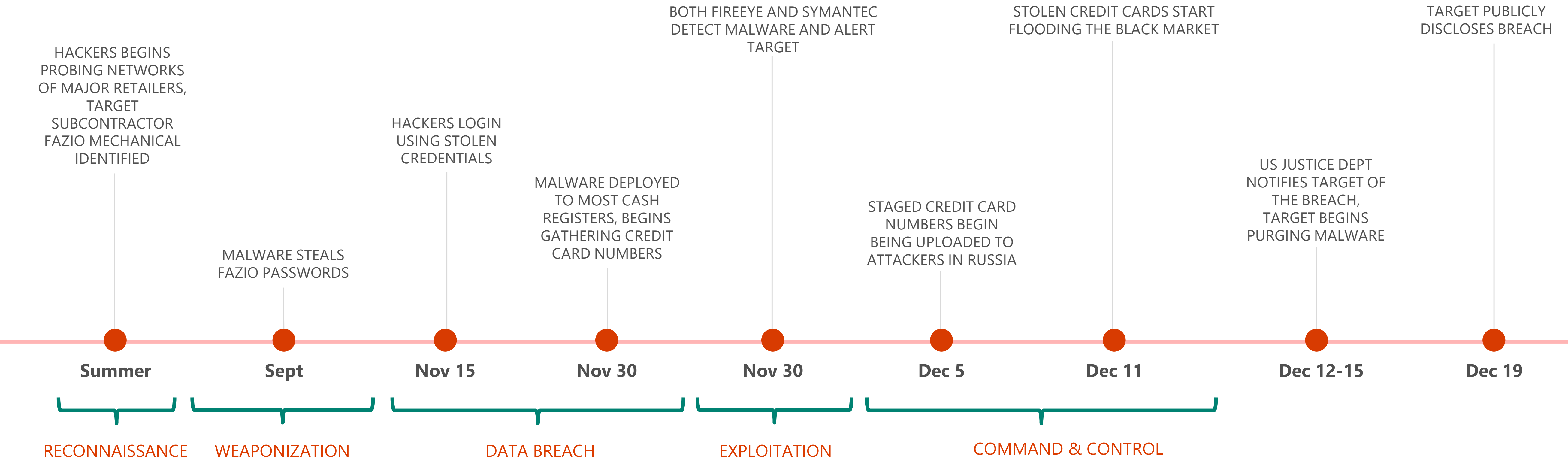
Multiple alerts ignored

40M
credit cards compromised

70M
PII records exposed

CEO
of Target resigned

Anatomy of an attack



Summer: HACKERS BEGINS PROBING NETWORKS OF MAJOR RETAILERS, TARGET SUBCONTRACTOR FAZIO MECHANICAL IDENTIFIED

Sept: MALWARE STEALS FAZIO PASSWORDS

Nov 15: HACKERS LOGIN USING STOLEN CREDENTIALS

Nov 30: MALWARE DEPLOYED TO MOST CASH REGISTERS, BEGINS GATHERING CREDIT CARD NUMBERS

Nov 30: BOTH FIREEYE AND SYMANTEC DETECT MALWARE AND ALERT TARGET

Dec 5: STAGED CREDIT CARD NUMBERS BEGIN BEING UPLOADED TO ATTACKERS IN RUSSIA

Dec 11: STOLEN CREDIT CARDS START FLOODING THE BLACK MARKET

Dec 12-15: US JUSTICE DEPT NOTIFIES TARGET OF THE BREACH, TARGET BEGINS PURGING MALWARE

Dec 19: TARGET PUBLICLY DISCLOSES BREACH

RECONNAISSANCE

WEAPONIZATION

DATA BREACH

EXPLOITATION

COMMAND & CONTROL

- X Fazio was running “free” malware software
- X Multi-factor authentication was not used to secure logins
- X Multiple alerts about malware were ignored
- X It took days after being notified of the breach to remediate and restore Target systems
- X Insufficient network segmentation allowed hackers to access sensitive systems
- X No restrictions were in place to block internet connections or upload locations

Insights from the Target breach

Cybersecurity is a boardroom problem

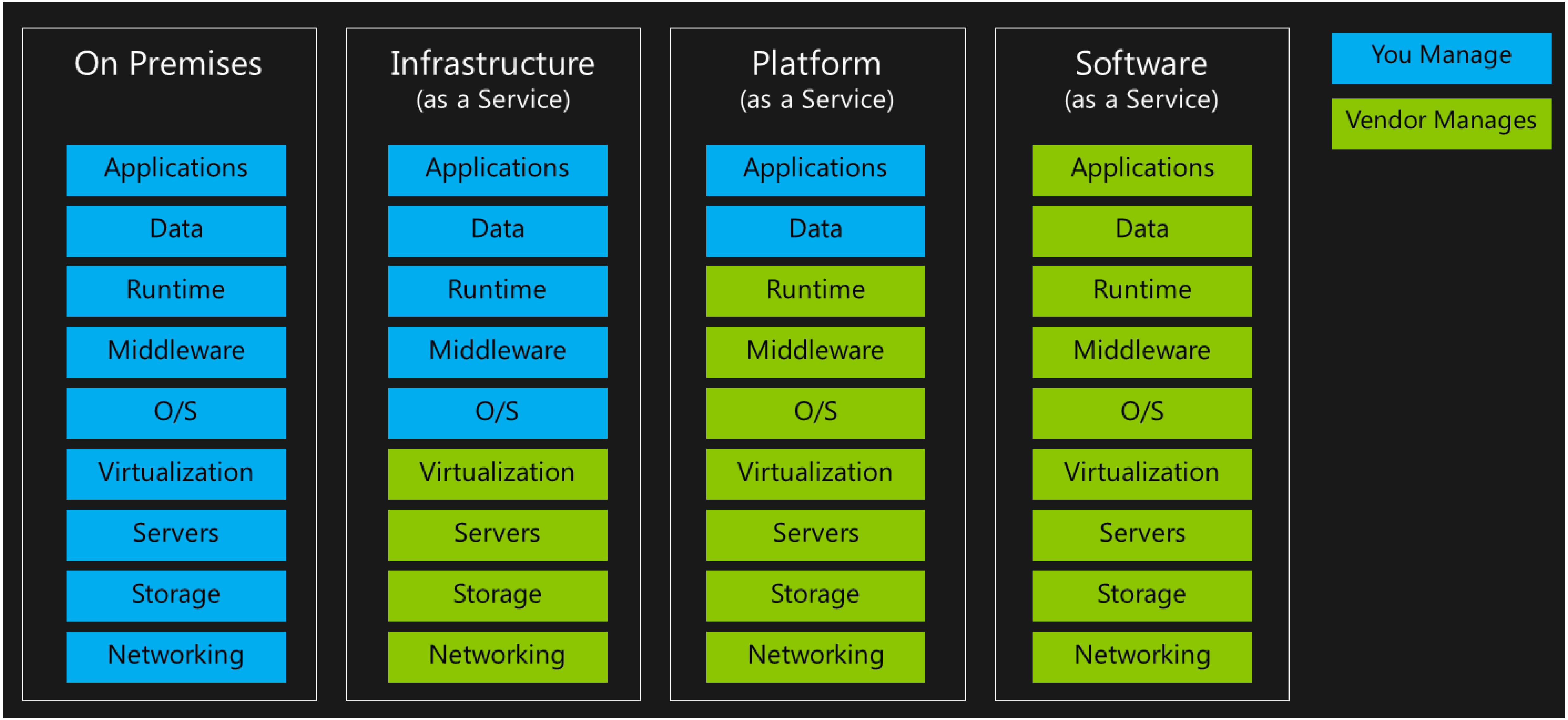
Traditional approaches are no longer effective

Signals create a lot of noise

On-premises is not safer than the cloud

Cloud

Cloud

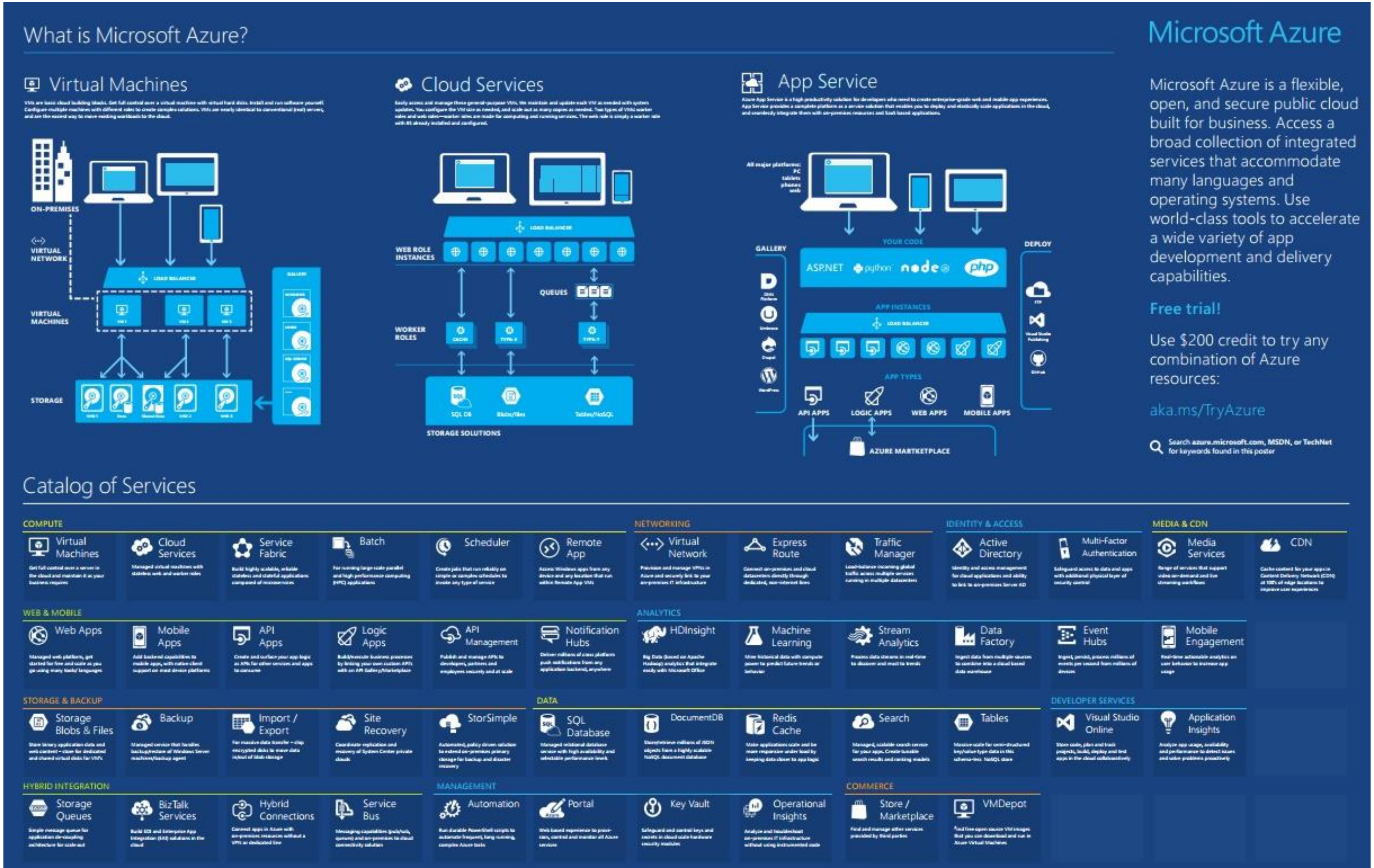


On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟦 Applications	🟦 Applications	🟦 Applications	🟩 Applications
🟦 Data	🟦 Data	🟦 Data	🟩 Data
🟦 Runtime	🟦 Runtime	🟩 Runtime	🟩 Runtime
🟦 Middleware	🟦 Middleware	🟩 Middleware	🟩 Middleware
🟦 O/S	🟦 O/S	🟩 O/S	🟩 O/S
🟦 Virtualization	🟩 Virtualization	🟩 Virtualization	🟩 Virtualization
🟦 Servers	🟩 Servers	🟩 Servers	🟩 Servers
🟦 Storage	🟩 Storage	🟩 Storage	🟩 Storage
🟦 Networking	🟩 Networking	🟩 Networking	🟩 Networking

🟦 You Manage

🟩 Vendor Manages

Cloud – Microsoft Azure



What is Microsoft Azure?

Virtual Machines

VMs are basic cloud building blocks. Get full control over a virtual machine with virtual hard disks. Install and run software yourself. Configure multiple machines with different roles to create complex solutions. VMs are nearly identical to conventional (real) servers, and are the easiest way to move existing workloads to the cloud.

Cloud Services

Easily access and manage these general-purpose VMs. We maintain and update each VM as needed with system updates. You configure the VM size as needed, and scale out as many copies as needed. Two types of VMs: worker roles and web roles—worker roles are made for computing and running services. The web role is simply a worker role with IIS already installed and configured.

App Service

Azure App Service is a high productivity solution for developers who need to create enterprise-grade web and mobile app experiences. App Service provides a complete platform as a service solution that enables you to deploy and elastically scale applications in the cloud, and seamlessly integrate them with on-premises resources and SaaS based applications.

Microsoft Azure

Microsoft Azure is a flexible, open, and secure public cloud built for business. Access a broad collection of integrated services that accommodate many languages and operating systems. Use world-class tools to accelerate a wide variety of app development and delivery capabilities.

Free trial!

Use $200 credit to try any combination of Azure resources:

aka.ms/TryAzure

Search azure.microsoft.com, MSDN, or TechNet for keywords found in this poster

Catalog of Services

COMPUTE

Virtual Machines
Get full control over a server in the cloud and maintain it as your business requires

Cloud Services
Managed virtual machines with stateless web and worker roles

Service Fabric
Build highly scalable, reliable stateless and stateful applications composed of microservices

Batch
For running large scale parallel and high performance computing (HPC) applications

Scheduler
Create jobs that run reliably on simple or complex schedules to invoke any type of service

Remote App
Access Windows apps from any device and any location that run within Remote App VMs

NETWORKING

Virtual Network
Provision and manage VPNs in Azure and securely link to your on-premises IT infrastructure

Express Route
Connect on-premises and cloud datacenters directly through dedicated, non-internet lines

Traffic Manager
Load-balance incoming global traffic across multiple services running in multiple datacenters

IDENTITY & ACCESS

Active Directory
Identity and access management for cloud applications and ability to link to on-premises Server AD

Multi-Factor Authentication
Safeguard access to data and apps with additional physical layer of security control

MEDIA & CDN

Media Services
Range of services that support video-on-demand and live streaming workflows

CDN
Cache content for your apps in Content Delivery Network (CDN) at 100's of edge locations to improve user experiences

WEB & MOBILE

Web Apps
Managed web platform, get started for free and scale as you go using many tools/ languages

Mobile Apps
Add backend capabilities to mobile apps, with native client support on most device platforms

API Apps
Create and surface your app logic as APIs for other services and apps to consume

Logic Apps
Build/execute business processes by linking your own custom APIs with an API Gallery/Marketplace

API Management
Publish and manage APIs to developers, partners and employees securely and at scale

Notification Hubs
Deliver millions of cross platform push notifications from any application backend, anywhere

ANALYTICS

HDInsight
Big Data (based on Apache Hadoop) analytics that integrate easily with Microsoft Office

Machine Learning
Mine historical data with compute power to predict future trends or behavior

Stream Analytics
Process data streams in real-time to discover and react to trends

Data Factory
Ingest data from multiple sources to combine into a cloud based data warehouse

Event Hubs
Ingest, persist, process millions of events per second from millions of devices

Mobile Engagement
Real-time actionable analytics on user behavior to increase app usage

STORAGE & BACKUP

Storage Blobs & Files
Store binary application data and web content – close for dedicated and shared virtual disks for VM's

Backup
Managed service that handles backup/restore of Windows Server machines/backup agent

Import / Export
For massive data transfer – ship encrypted disks to move data in/out of blob storage

Site Recovery
Coordinate replication and recovery of System Center private clouds

StorSimple
Automated, policy driven solution to extend on-premises primary storage for backup and disaster recovery

DATA

SQL Database
Managed relational database service with high availability and selectable performance levels

DocumentDB
Store/retrieve millions of JSON objects from a highly scalable NoSQL document database

Redis Cache
Make applications scale and be more responsive under load by keeping data closer to app logic

Search
Managed, scalable search service for your apps. Create tunable search results and ranking models

Tables
Massive scale for semi-structured key/value type data in this schema-less NoSQL store

DEVELOPER SERVICES

Visual Studio Online
Store code, plan and track projects, build, deploy and test apps in the cloud collaboratively

Application Insights
Analyze app usage, availability and performance to detect issues and solve problems proactively

HYBRID INTEGRATION

Storage Queues
Simple message queue for application de-coupling architecture for scale out

BizTalk Services
Build EDI and Enterprise App Integration (EAI) solutions in the cloud

Hybrid Connections
Connect apps in Azure with on-premises resources without a VPN or dedicated line

Service Bus
Messaging capabilities (pub/sub, queues) and on-premises to cloud connectivity solution

MANAGEMENT

Automation
Run durable PowerShell scripts to automate frequent, long running, complex Azure tasks

Portal
Web based experience to provision, control and monitor all Azure services

Key Vault
Safeguard and control keys and secrets in cloud scale hardware security modules

Operational Insights
Analyze and troubleshoot on-premises IT infrastructure without using instrumented code

COMMERCE

Store / Marketplace
Find and manage other services provided by third parties

VMDepot
Find free open source VM images that you can download and run in Azure Virtual Machines

Cloud – Microsoft Azure

Can I trust Microsoft Azure? **YES**

- Most Compliant Public Cloud
- Azure Trust Center
- Security, Privacy, Transparency
- Threats - DDos, Assume Breach, Penetration Testing

The Real Question is

- Can you trust your Datacenter?

OWASP Top 10

OWASP Top 10 | 1. Injection

Vulnerability

Allowing Untrusted Data

Dynamic SQL

Impact

Data Loss or Corruption

Stolen Data

Denial of Access

Prevention

Parameterized Queries

Input Validation

```
String query = "SELECT * FROM
accounts WHERE custID='" +
request.getParameter("id") + "'";
```

Cloud Solution

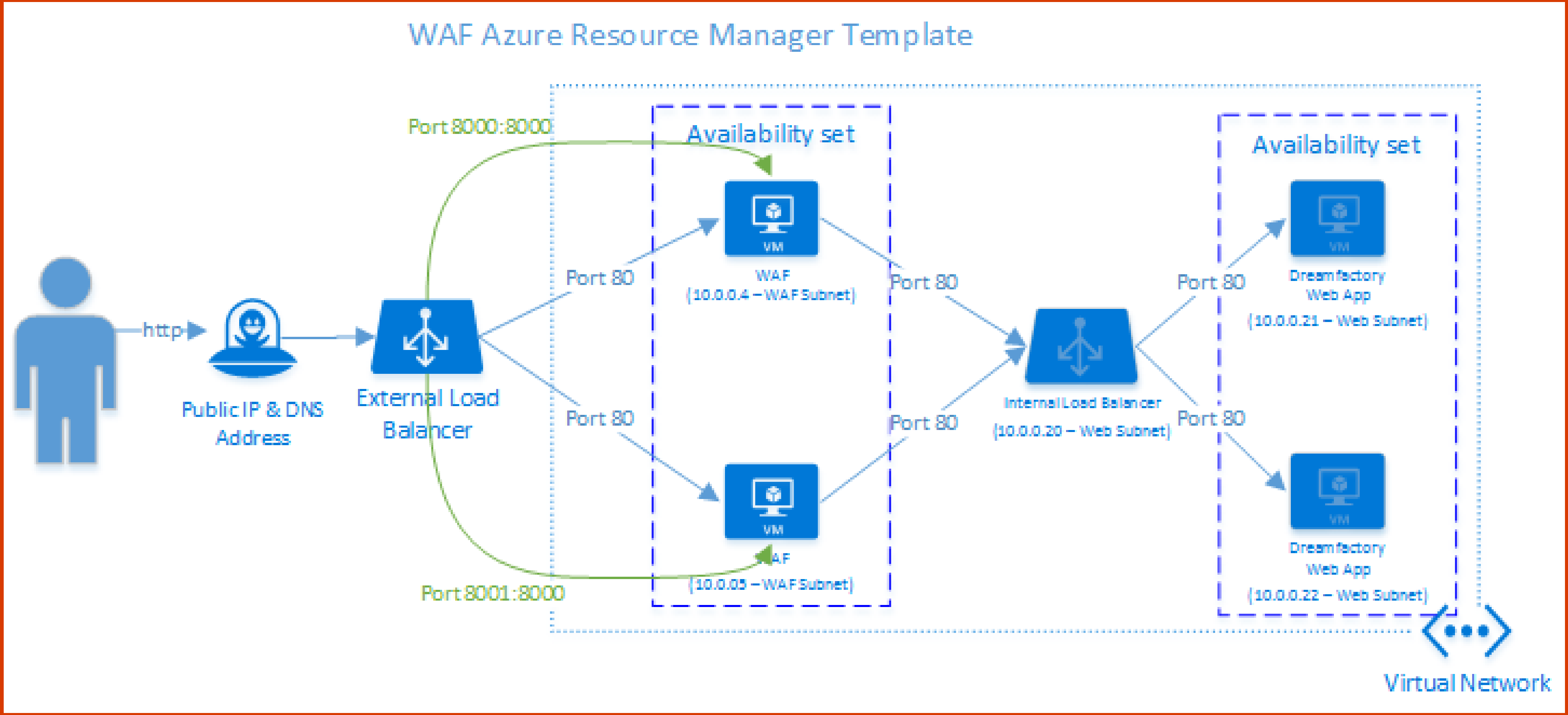
Web Application Firewall

- PaaS – Web Apps
  - Open Source – **ModSecurity**
- IaaS –
  - ARM Templates, Immutable Infrastructure
  - Vendors – **Barracuda Networks**

Demo: ModSecurity

Demo: Barracuda

WAF for Immutable Infrastructure



OWASP Top 10 | 1. Injection

Vulnerability

Allowing Untrusted Data

Dynamic SQL

Impact

Data Loss or Corruption

Stolen Data

Denial of Access

Prevention

Parameterized Queries

Input Validation

```
String query = "SELECT * FROM
accounts WHERE custID='" +
request.getParameter("id") + "'";
```

Cloud Solution

Web Application Firewall

- PaaS – Web Apps
  - Open Source – **ModSecurity**
- IaaS –
  - ARM Templates, Immutable Infrastructure
  - Vendors – **Barracuda Networks**

OWASP Top 10 | 2. Broken Authentication

Vulnerability

Unprotected Authentication Credentials

Exposed Session IDs

Passwords sent without HTTPS

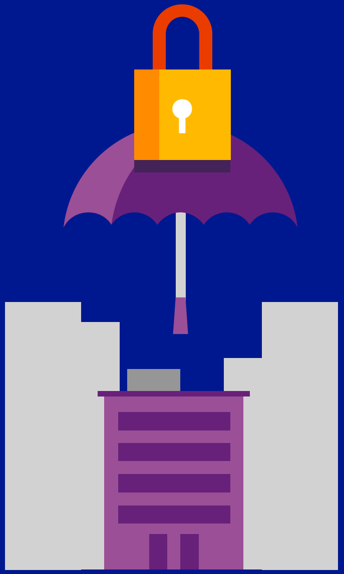
Impact

Hacked Accounts

Exposure

Prevention

Use Industry Standard Authentication practices and techniques.



Cloud Solution

Identity As a Service

Industry Standards – OAuth, Saml, WS Federation

Multi-Factor Authentication

Azure Active Directory

Azure Active Directory B2C

Demo: Azure Active Directory

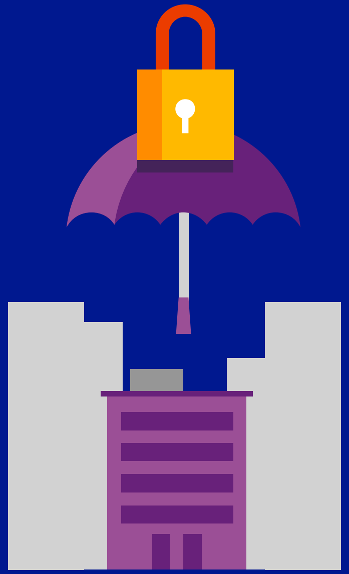
OWASP Top 10 | 2. Broken Authentication

Vulnerability

Unprotected Authentication Credentials

Exposed Session IDs

Passwords sent without HTTPS



Impact

Hacked Accounts

Exposure

Prevention

Parameterized Queries

Input Validation

Cloud Solution

Identity As a Service

Industry Standards – OAuth, Saml, WS Federation

Multi-Factor Authentication

Azure Active Directory

Azure Active Directory B2C***

OWASP Top 10 3. XSS

Vulnerability

Echoing unverified, unescaped user data

```
(String) page += "<input
name='creditcard'
type='TEXT' value='" +
request.getParameter("CC") +
"'>";
```

Impact

Deface Website

Hijack User Sessions

Insert Hostile Content

Redirect Users

Cloud Solution

Web Application Firewall

- Open Source – **ModSecurity**
- Vendors – **Barracuda Networks**

Prevention

Proper Escaping

“Whitelist” Validation

OWASP Top 10 4. Direct Object References

Vulnerability

Failing to verify user authorization for requested resources

```
String query = "SELECT * FROM accts WHERE
account = ?";
PreparedStatement pstmt =
connection.prepareStatement(query , ...
);
pstmt.setString( 1,
request.getParameter("acct"));
ResultSet results = pstmt.executeQuery();
```

```
http://example.com/app/accountInfo?acct=n
otmyacct
```

Impact

Compromised Data

Prevention

Check Access

Indirect Object References

Cloud Solution

Micro Services

API Management

- Authentication
- Rate Limiting / Throttling
- Quotas
- Caching
- Health Monitoring

Azure Rights Management

Azure Active Directory Groups (See #7 Access Control)

OWASP Top 10 5. Security Misconfiguration

Vulnerability

Access to Default Accounts

Unused Pages

Unpatched Flaws

Unprotected Files

Impact

Compromised System

Data Loss and Modification

Prevention

Proper Configuration

Automation

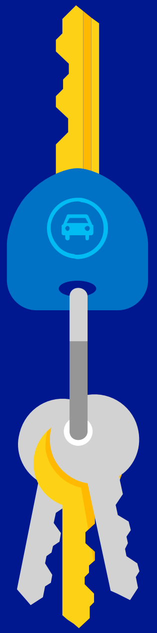
Devops

Cloud Solution

Role Based Access Control (RBAC)

DevOps (Staging Slots)

Application Settings



Demo: App Settings and RBAC

OWASP Top 10 6. Sensitive Data Exposure

Vulnerability

Data stored/transmitted in clear text

Weak Cryptography

Weak Key Management

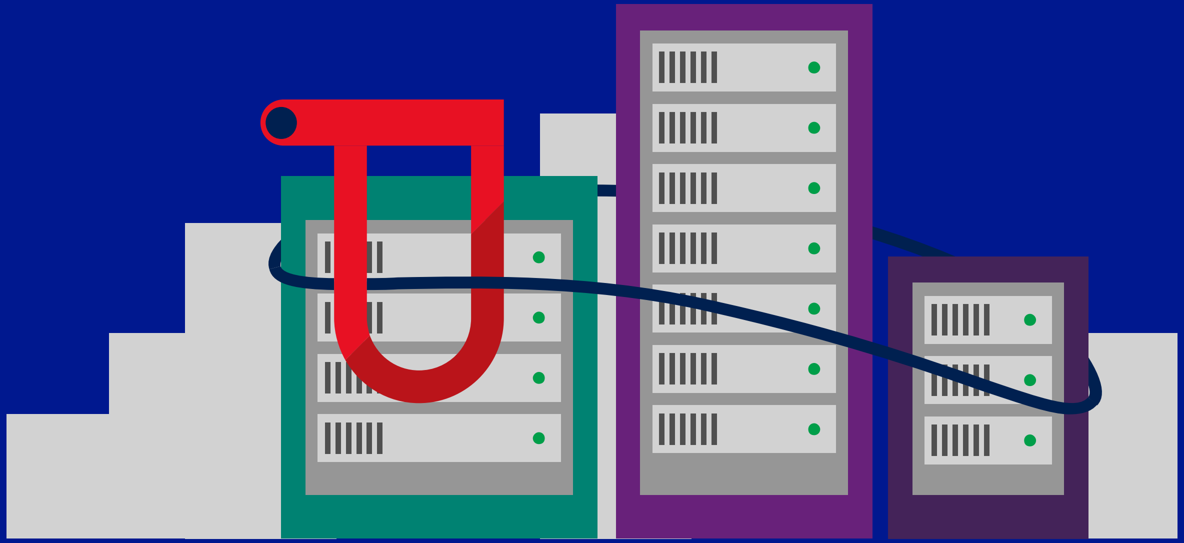
Impact

Compromised Sensitive Data

Compromised Credentials

Prevention

Encrypt Data in transit and at rest



Cloud Solution

https

Database Encryption

Always Encrypted

Rights Management

Dynamic Data Masking

Key Rotation

SAS Tokens

HSM (Azure Key Vault)

OWASP Top 10 7. Missing Function Level Access Control

Vulnerability

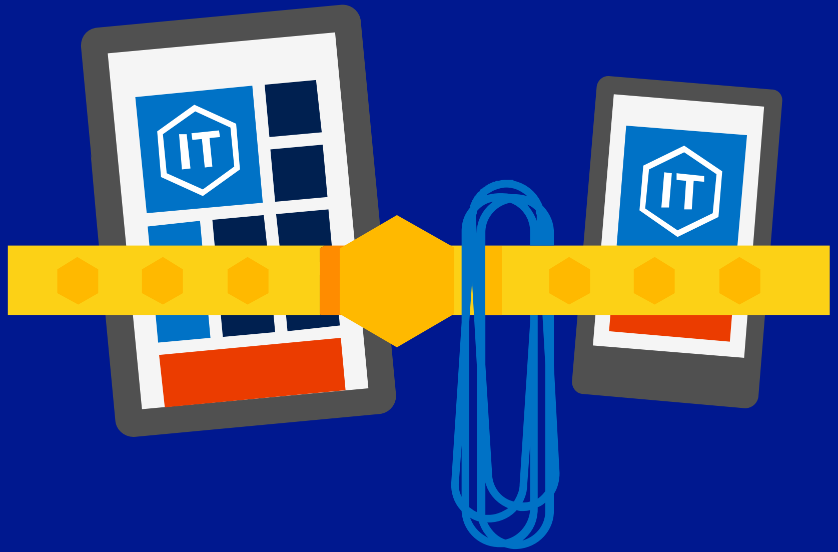
Manipulating URLs grants access to functionality

Impact

Access to unauthorized functionality

Prevention

Require Explicit Grants to Specific Roles for Function Access



Cloud Solution

Active Directory Groups

Claims based Authentication

Demo: Azure Active Directory Groups

OWASP Top 10 8. Cross Site Request Forgery (CSRF)

Vulnerability

Forged HTTP Requests

http://example.com/app/transferFunds?amount=1500&**destinationAccount=4673243243**

<img src="http://example.com/app/transferFunds?amount=1500&**destinationAccount=attackersAcct#**" width="0" height="0" />

Impact

Trick Victims

Perform Unintended Operations

Cloud Solution

Identity as a Service

Web Application Firewall

- Open Source – **ModSecurity**
- Vendors – **Barracuda Networks**

Prevention

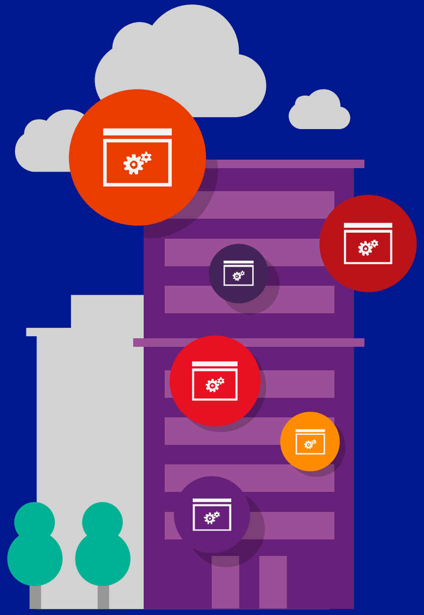
CSRF Unique Token

Libraries that prevent CSRF

OWASP Top 10 9. Vulnerable Components

Vulnerability

Use of Vulnerable Components or Framework Libraries



Impact

Impacts from All the OWASP Vulnerabilities

Prevention

Don’t use components

Use Component Checker Libraries (ex for .NET and JAVA)

Cloud Solution

WAFs

Marketplace

OWASP Top 10 10. Redirects and Forwards

Vulnerability

Redirects with unvalidated parameters

http://www.example.com/redirect.jsp?url=evil.com

http://www.example.com/boring.jsp?fwd=admin.jsp

Impact

Data Loss or Corruption

Stolen Data

Denial of Access

Cloud Solution

API Managemtent

Web Application Firewall

- Open Source – **ModSecurity**
- Vendors – **Barracuda Networks**

Prevention

Don’t use redirects

Use White list or Mapping

More Info

Azure Trust Center - https://azure.microsoft.com/en-us/support/trust-center/

Azure Active Directory - https://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/

ModSecurity - https://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/

Barracuda - https://azure.microsoft.com/en-us/blog/configuring-barracuda-web-application-firewall-for-azure-app-service-environment/

Azure Marketplace - https://azure.microsoft.com/en-us/marketplace/

Azure Storage Security - https://azure.microsoft.com/en-us/documentation/articles/storage-manage-access-to-resources/

Azure SQL DB Security - https://azure.microsoft.com/en-us/documentation/articles/sql-database-security-guidelines/

Azure Web App Security - https://azure.microsoft.com/en-us/documentation/articles/web-sites-security/

Azure API Management - https://azure.microsoft.com/en-us/services/api-management/

Role Based Access Control (RBAC) - https://azure.microsoft.com/en-us/documentation/articles/role-based-access-control-configure/

Azure Rights Management https://products.office.com/en-us/business/microsoft-azure-rights-management

Q&A

Microsoft