

OWASP and Cloud Security

Mike Richter
Cloud Solution Architect

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

Injection

Sensitive Data
Exposure

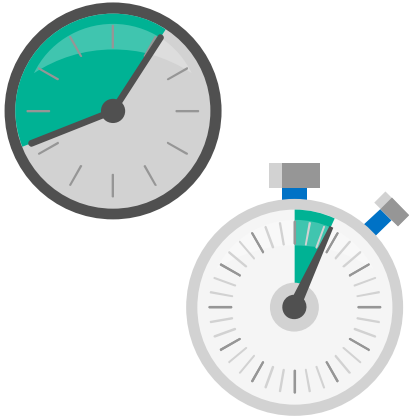
Resources

Cloud

Broken
Authentication

Access Control

Q&A



XSS

CSRF

Direct Object
References

Components

Security
Misconfiguration

Redirects and
Forwards



Threats

The threat landscape today



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

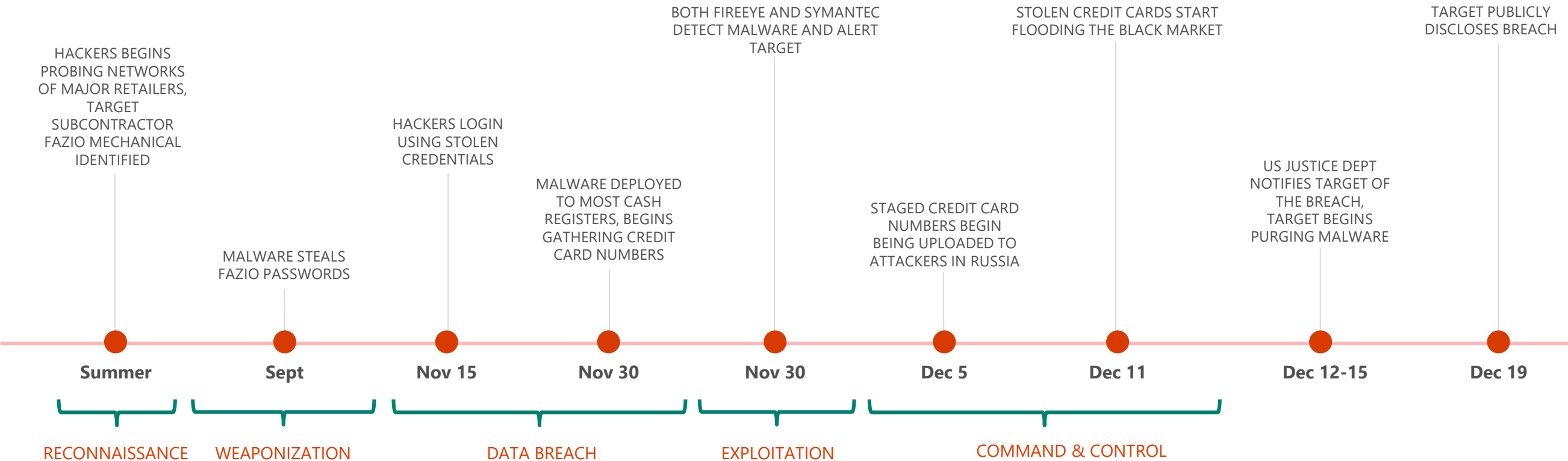
PII records exposed

CEO

of Target resigned



Anatomy of an attack



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

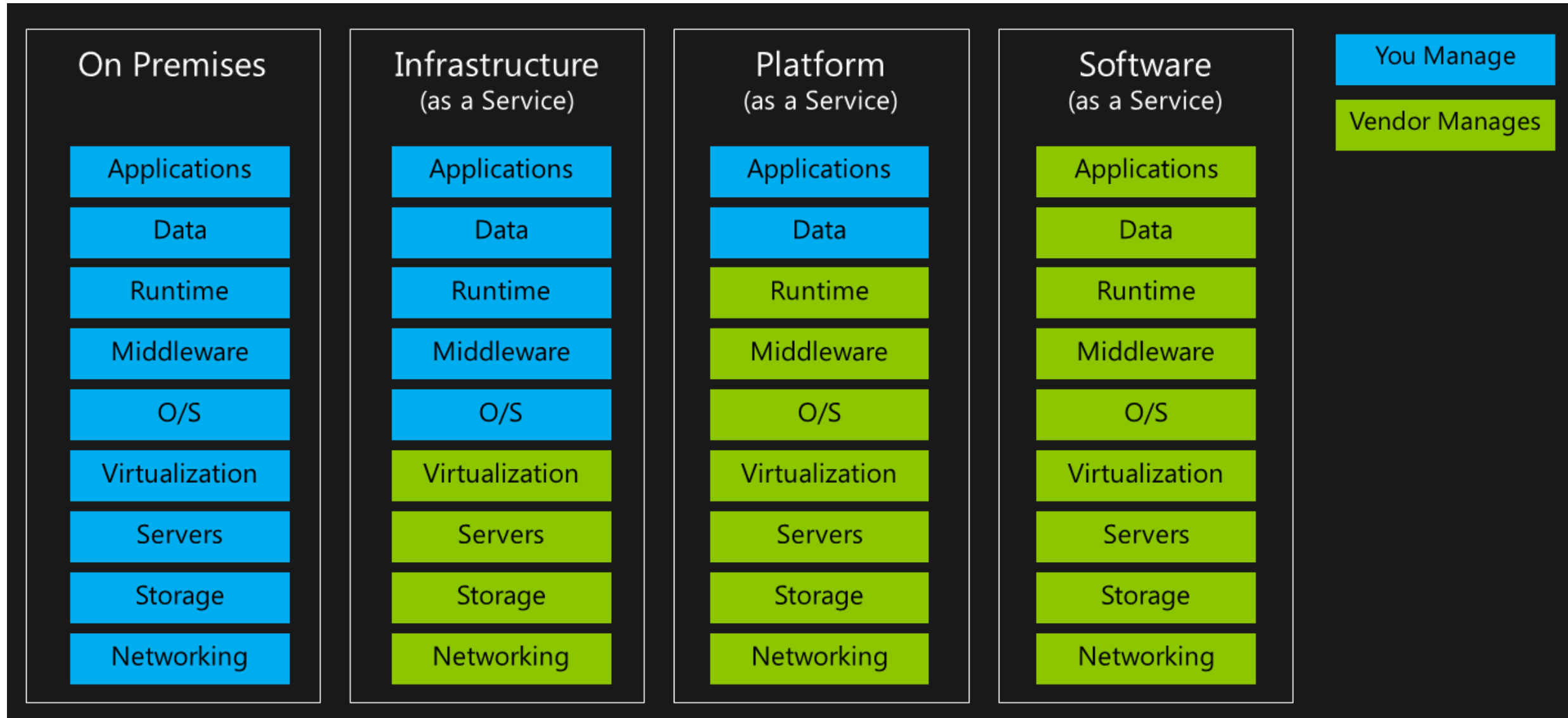
Traditional
approaches are
no longer
effective

Signals create a
lot of noise

On-premises is
not safer than
the cloud

Cloud

Cloud

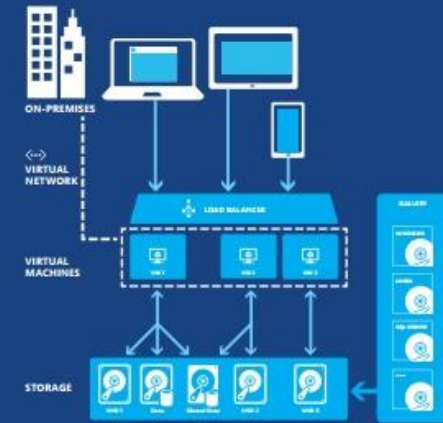


Cloud – Microsoft Azure

What is Microsoft Azure?

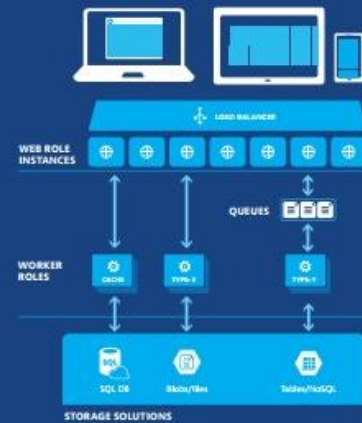
Virtual Machines

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



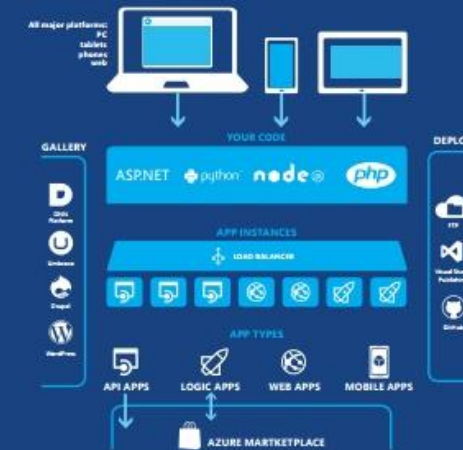
Cloud Services

Easily access and manage three general-purpose VMs, the scalable and update-ready VMs as needed with system monitors. You configure the VMs 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 an 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 statically scale applications in the cloud, and seamlessly integrate them with on-premises resources and back-end 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 clusters and stateful applications composed of microservices.	Batch For running larger-scale parallel and high-performance computing (HPC) applications.	Scheduler Create jobs that run reliably on a single or multiple schedules to create any type of service.	Remote App Access Windows apps from any device and any location that run within RemoteApp VMs.
---	--	--	--	--	--

NETWORKING

Virtual Network Provision and manage VMs in Azure and securely link to your on-premises IT infrastructure.	Express Route Connect on-premises and cloud datacenters directly through dedicated, non-redundant links.	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 Active Directory.	Multi-Factor Authentication Additional layer of security control to protect 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+ edge locations to improve user experience.
---	--

WEB & MOBILE

Web Apps Managed web platform, get started fast and scale as you go using many leading 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/reconfigure business processes by linking your own custom APIs with an API gateway/connector.	API Management Publish and manage APIs to developers, partners and employees securely and at scale.	Notification Hubs Deliver millions of client platform push notifications from any application, backend, or service.
---	---	--	--	---	---

ANALYTICS

HDInsight Big Data (based on Apache Hadoop) analytics that integrate easily with Microsoft Office.	Machine Learning Mine historical data with complete 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 central 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—ideal for dedicated and shared virtual disks for VMs.	Backup Managed service that handles backup/recovery of Windows Server machines/backup agent.	Import / Export For massive data transfer—ship terabyte disks to store data without virtual disks for VMs.	Site Recovery Coordinate replication and recovery of hybrid cloud private cloud.	StorageSimple 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 automatic performance tuning.	DocumentDB Store millions of JSON objects from a highly scalable, fully managed 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 searchable content and ranking models.	Tables Massive scale for semi-structured key/value type data in this column-free, NoSQL, store.
---	---	--	--	---

DEVELOPER SERVICES

Visual Studio Online Store code, plans and track progress, build, deploy and test apps in the cloud collaboration only.	Application Insights Analyze app usage, availability and performance to detect issues and solve problems proactively.
---	---

HYBRID INTEGRATION

Storage Queues Simple message queue for applications for decoupling architecture for scale out.	BizTalk Services Build ESB 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 (publish/subscribe) and on-premises to cloud connectivity solution.
---	---	--	--

MANAGEMENT

Automation Run reusable PowerShell scripts to automate repetitive, 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 on-premises code.
---	---	--	---

COMMERCE

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

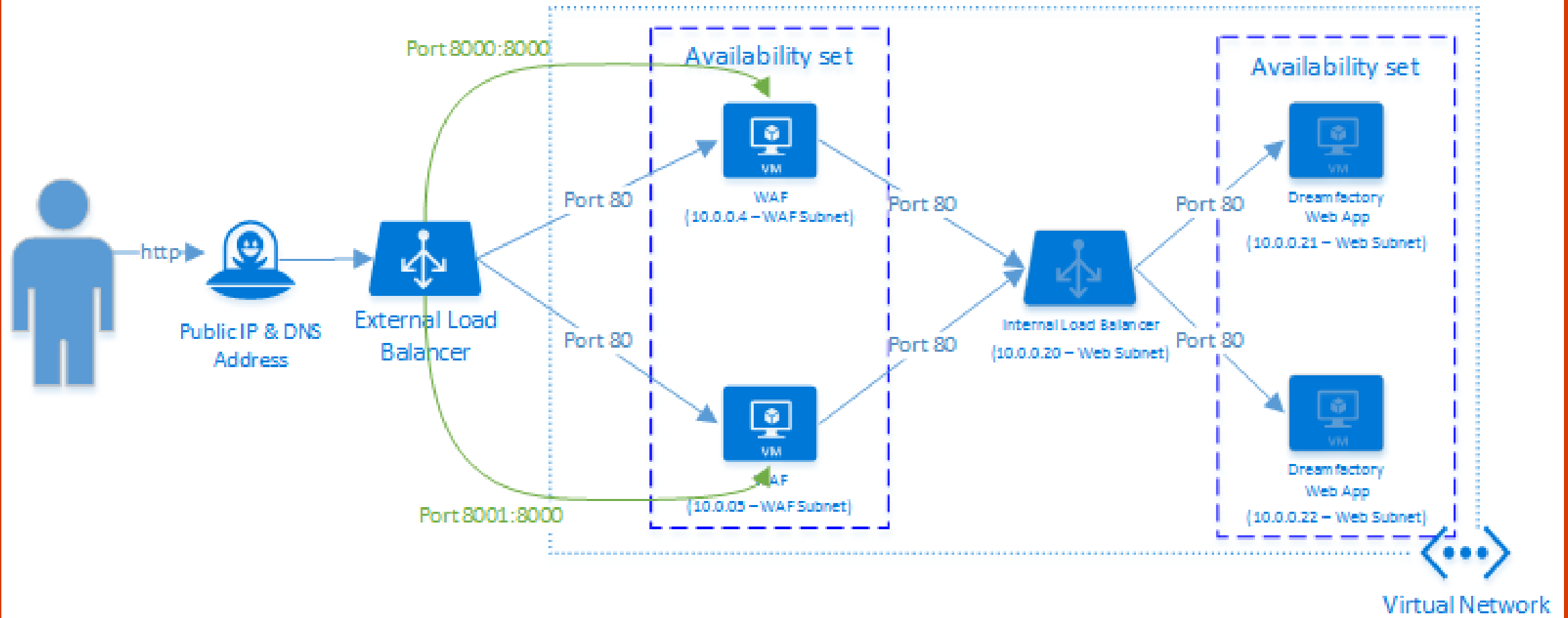
Vulnerability	Impact	Prevention	Cloud Solution
<p>Allowing Untrusted Data</p> <p>Dynamic SQL</p> <pre>String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";</pre>	<ul style="list-style-type: none">• Data Loss or Corruption• Stolen Data• Denial of Access	<ul style="list-style-type: none">• Parameterized Queries• Input Validation	<ul style="list-style-type: none">• Web Application Firewall• PaaS – Web Apps<ul style="list-style-type: none">• Open Source – ModSecurity• IaaS –<ul style="list-style-type: none">• ARM Templates, Immutable Infrastructure• Vendors – Barracuda Networks

Demo: ModSecurity

Demo: Barracuda

WAF for Immutable Infrastructure

WAF Azure Resource Manager Template



OWASP Top 10 | 2. Broken Authentication

Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">• Unprotected Authentication Credentials• Exposed Session IDs• Passwords sent without HTTPS	<ul style="list-style-type: none">• Hacked Accounts• Exposure	<ul style="list-style-type: none">• Use Industry Standard Authentication practices and techniques.	<ul style="list-style-type: none">• 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 | 3. XSS

Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">Echoing unverified, unescaped user data <pre>(String) page += "<input name='creditcard' type='TEXT' value='" + request.getParameter("CC") + "'>";</pre>	<ul style="list-style-type: none">Hacked AccountsExposure	<ul style="list-style-type: none">Use Industry Standard Authentication practices and techniques.	<ul style="list-style-type: none">Identity As a ServiceIndustry Standards – OAuth, Saml, WS FederationMulti-Factor AuthenticationAzure Active DirectoryAzure Active Directory B2C

OWASP Top 10 | 4. Direct Object References

Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">Failing to verify user authorization for requested resources <pre>String query = "SELECT * FROM accts WHERE account = ?"; PreparedStatement pstmt = connection.prepareStatement(query , ...); pstmt.setString(1, request.getParameter("acct")); ResultSet results = pstmt.executeQuery();</pre> <p>http://example.com/app/accountInfo?acct=notmyacct</p>	<ul style="list-style-type: none">Compromised Data	<ul style="list-style-type: none">Check AccessIndirect Object References	<ul style="list-style-type: none">Micro ServicesAPI Management<ul style="list-style-type: none">AuthenticationRate Limiting / ThrottlingQuotasCachingHealth MonitoringAzure Rights ManagementAzure Active Directory Groups (See #7 Access Control)

OWASP Top 10 | 5. Security Misconfiguration

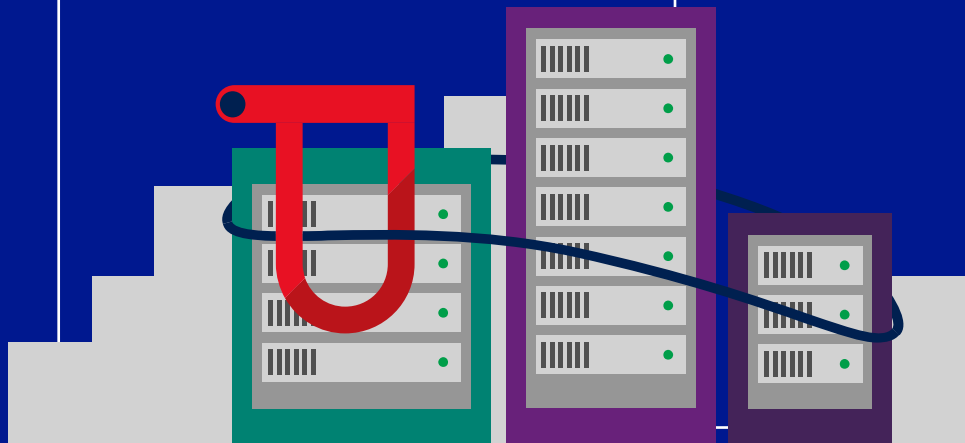
Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">• Access to Default Accounts• Unused Pages• Unpatched Flaws• Unprotected Files	<ul style="list-style-type: none">• Compromised System• Data Loss and Modification	<ul style="list-style-type: none">• Check Access• Indirect Object References	<ul style="list-style-type: none">• Role Based Access Control (RBAC)• DevOps (Staging Slots)• Application Settings



Demo: App Settings and RBAC

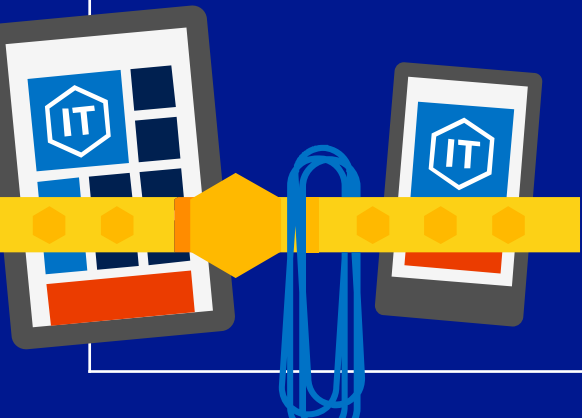
OWASP Top 10 | 6. Sensitive Data Exposure

Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">• Data stored/transmitted in clear text• Weak Cryptography• Weak Key Management	<ul style="list-style-type: none">• Compromised Sensitive Data• Compromised Credentials	<ul style="list-style-type: none">• Encrypt Data in transit and at rest	<ul style="list-style-type: none">• SSL• 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	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">Manipulating URLs grants access to functionality	<ul style="list-style-type: none">Access to unauthorized functionality	<ul style="list-style-type: none">Require Explicit Grants to Specific Roles for Function Access	<ul style="list-style-type: none">Active Directory GroupsClaims based Authentication



Demo: Azure Active Directory Groups

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

Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">Forged HTTP Requests <pre>http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243</pre> <pre></pre>	<ul style="list-style-type: none">Trick VictimsPerform Unintended Operations	<ul style="list-style-type: none">CSRF Unique TokenLibraries that prevent CSRF	<ul style="list-style-type: none">Identity as a ServiceWeb Application FirewallOpen Source –<ul style="list-style-type: none">ModSecurityVendors –<ul style="list-style-type: none">Barracuda Networks

OWASP Top 10 | 9. Vulnerable Components

Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">Use of Vulnerable Components or Framework Libraries	<ul style="list-style-type: none">Impacts from all the OWASP Vulnerabilities	<ul style="list-style-type: none">Don't use componentsUse Component Checker Libraries (ex for .NET and JAVA)	<ul style="list-style-type: none">WAFsMarketplace



OWASP Top 10 | 10. Redirects and Forwards

Vulnerability	Impact	Prevention	Cloud Solution
<ul style="list-style-type: none">Redirects with unvalidated parameters <p><code>http://www.example.com/redirect.jsp?url=evil.com</code></p> <p><code>http://www.example.com/boring.jsp? fwd=admin.jsp</code></p>	<ul style="list-style-type: none">Data Loss or CorruptionStolen DataDenial of Access	<ul style="list-style-type: none">Don't use redirectsUse White list or Mapping	<ul style="list-style-type: none">Don't use redirectsUse White list or Mapping

Resources

Azure Resources

Microsoft Trust Center

Azure Security Center (Public Preview)

Getting Started with Azure Security

<https://azure.microsoft.com/en-us/documentation/articles/azure-security-getting-started/>

Monitoring

Logging

Reporting

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-what-is/>

ModSecurity - <https://azure.microsoft.com/en-us/documentation/articles/active-directory-what-is/>

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

