OWASP and Cloud Security

Mike Richter
Cloud Solution Architect

Objectives

Threats

Landscape

What is the Cloud

Services

Shared Controls

OWASP TOP 10

Vulnerabilities

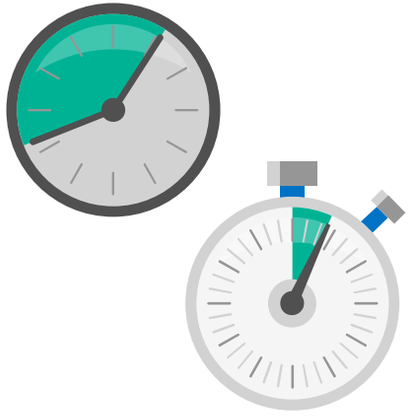
The Cloud Can Protect You!

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

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Documents, SSNs, email, passwords, unpublished scripts, marketing plans, financial and legal information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

The Target breach

Targeted corporate network

Total "kill chain" failure

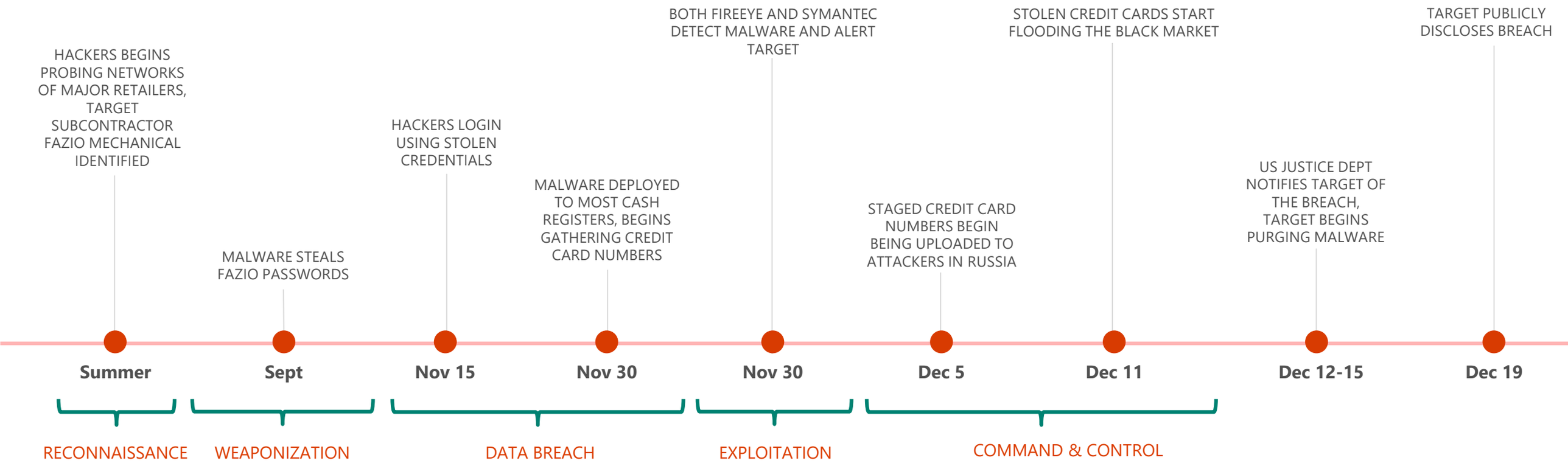
Multiple alerts ignored

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

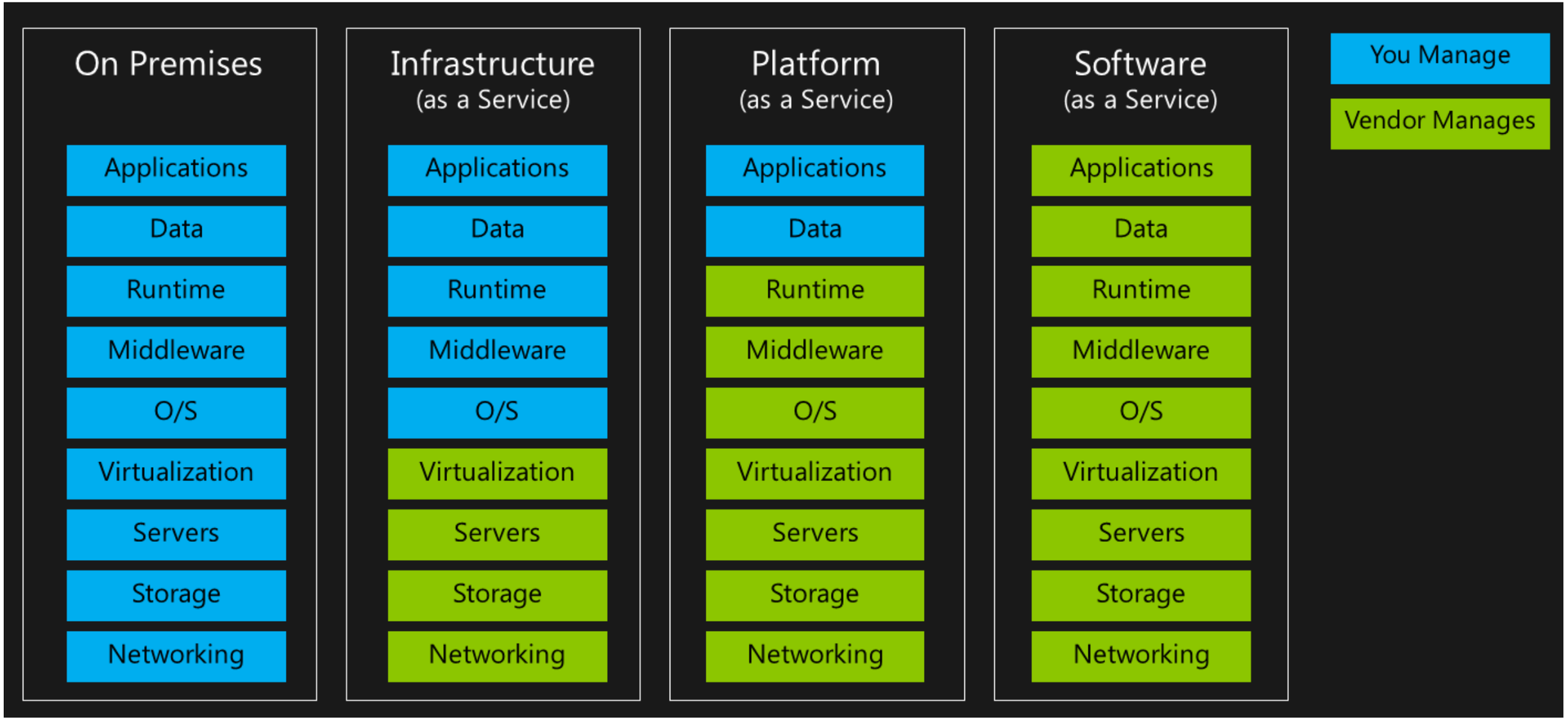
Traditional approaches are no longer effective

Signals create a lot of noise

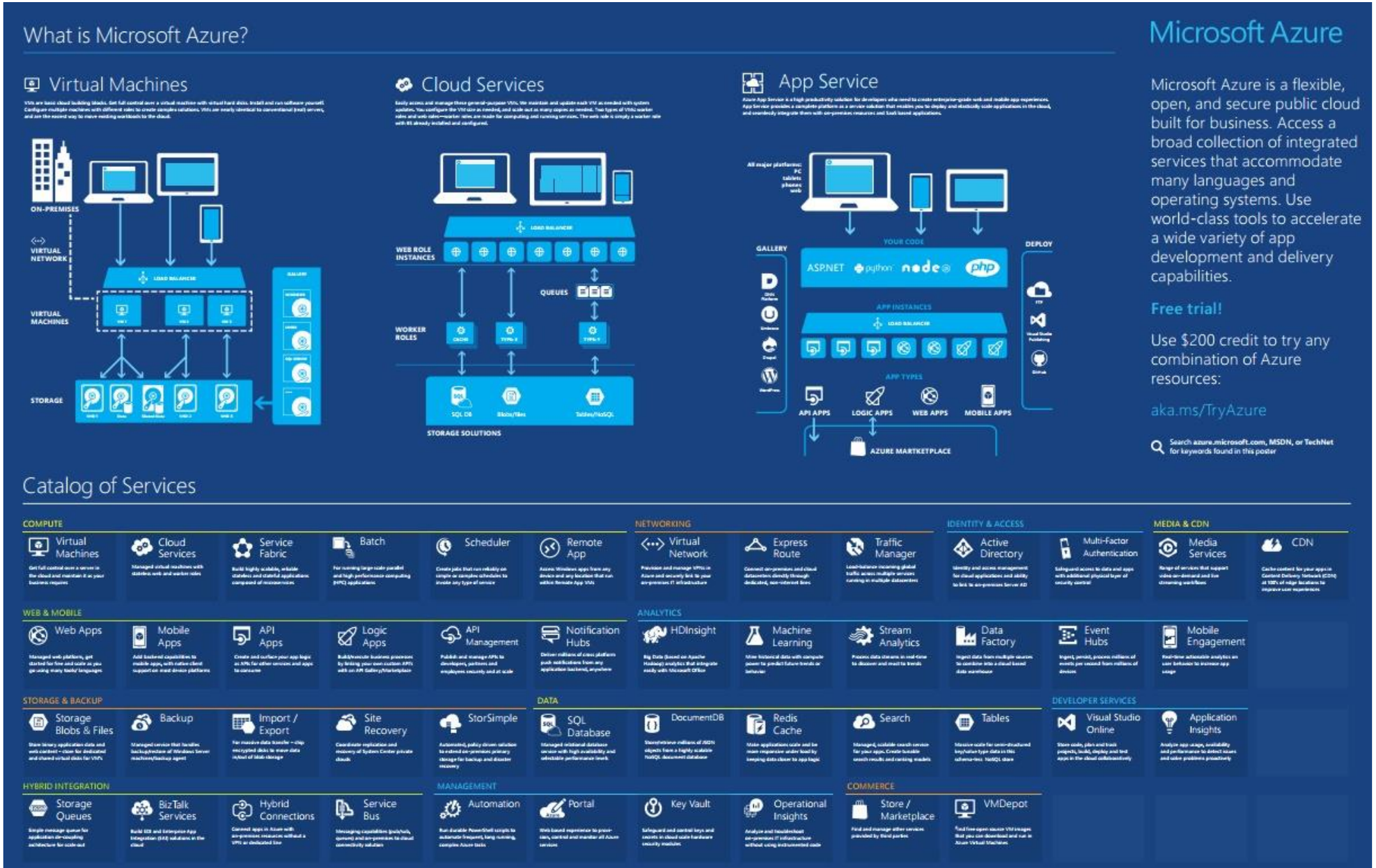
On-premises is not safer than the cloud

Cloud

Cloud


On Premises
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Infrastructure
(as a Service)
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Platform
(as a Service)
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
Software
(as a Service)
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
You Manage
Vendor Manages

Cloud – Microsoft Azure



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

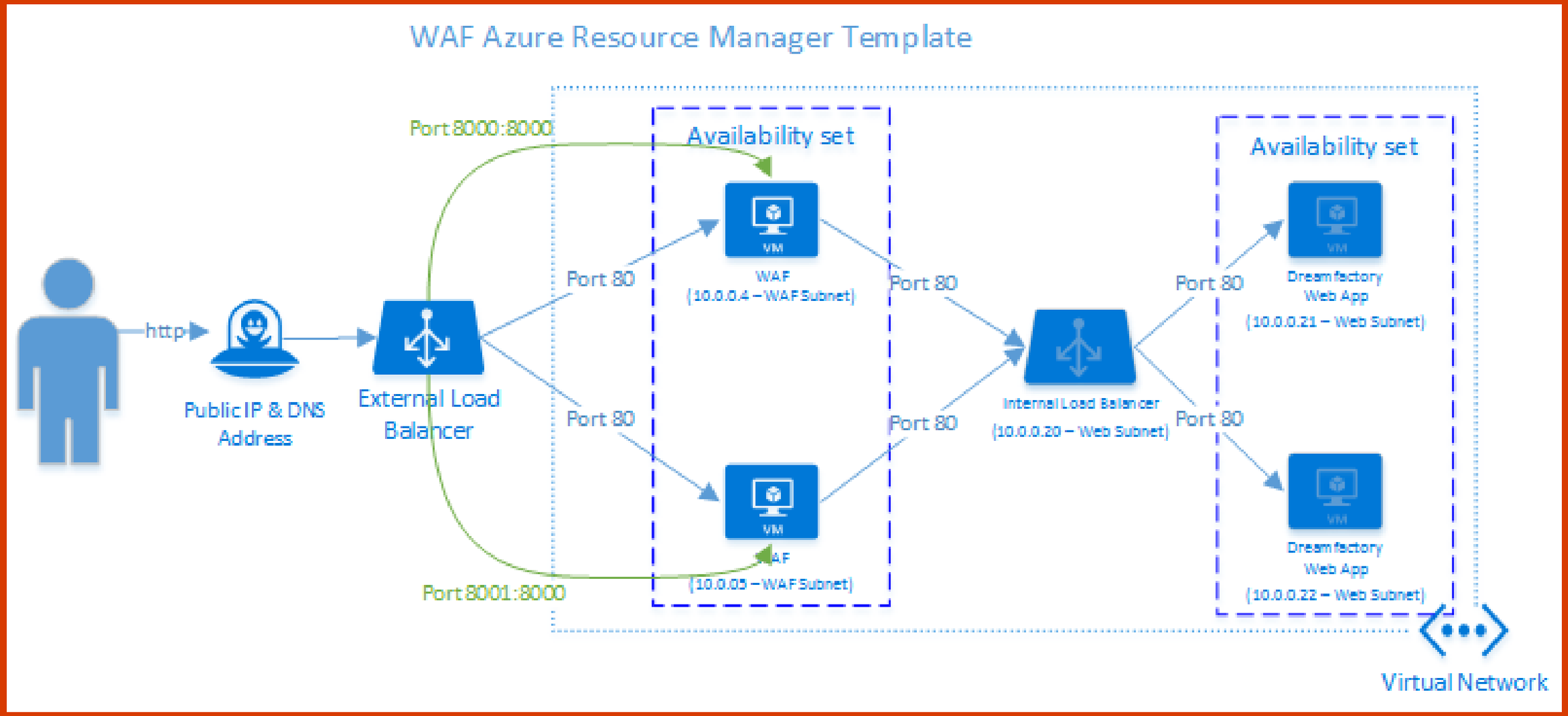
Vulnerability	Impact	Prevention	Cloud Solution

Allowing Untrusted Data
Dynamic SQL
 	
`String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";`
	• Data Loss or Corruption
	• Stolen Data
	• Denial of Access
		• Parameterized Queries
		• Input Validation
			• 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 | 2. Broken Authentication

Vulnerability	Impact	Prevention	Cloud Solution
• Unprotected Authentication Credentials • Exposed Session IDs • Passwords sent without HTTPS	• Hacked Accounts • Exposure	• Use Industry Standard Authentication practices and techniques.	• 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
• Echoing unverified, unescaped user data `(String) page += "<input name='creditcard' type='TEXT' value='" + request.getParameter("CC") + "'>";`	• Hacked Accounts • Exposure	• Use Industry Standard Authentication practices and techniques.	• Identity As a Service • Industry Standards – OAuth, Saml, WS Federation • Multi-Factor Authentication • Azure Active Directory • Azure Active Directory B2C

OWASP Top 10 | 4. Direct Object References

Vulnerability	Impact	Prevention	Cloud Solution

• 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=notmyacct`
	• Compromised Data	• Check Access
		• Indirect Object References
			• Micro Services
			• API Management
			  • Authentication
			  • Rate Limiting / Throttling
			  • Quotas
			  • Caching
			  • Health Monitoring
			• Azure Rights Management
			• Azure Active Directory Groups (See #7 Access Control)

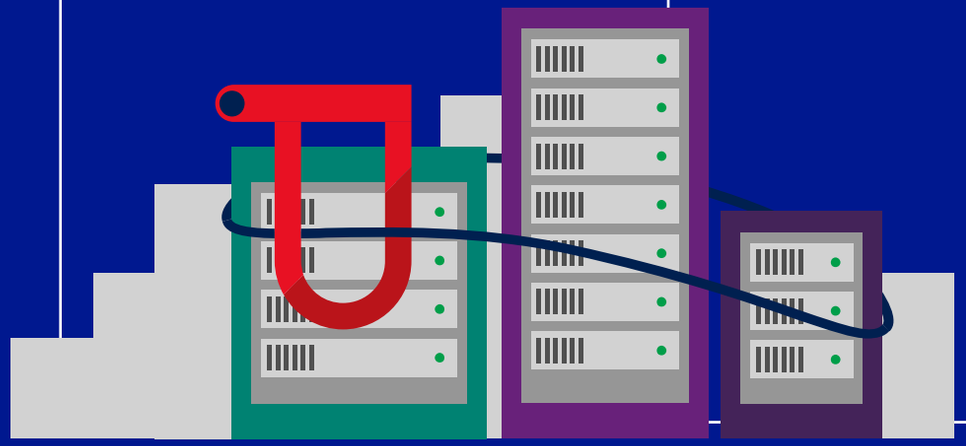
OWASP Top 10 | 5. Security Misconfiguration

Vulnerability	Impact	Prevention	Cloud Solution
• Access to Default Accounts • Unused Pages • Unpatched Flaws • Unprotected Files	• Compromised System • Data Loss and Modification	• Check Access • Indirect Object References	• 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
• Data stored/transmitted in clear text • Weak Cryptography • Weak Key Management	• Compromised Sensitive Data • Compromised Credentials	• Encrypt Data in transit and at rest	• 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
• Manipulating URLs grants access to functionality	• Access to unauthorized functionality	• Require Explicit Grants to Specific Roles for Function Access	• Active Directory Groups • Claims based Authentication

Demo: Azure Active Directory Groups

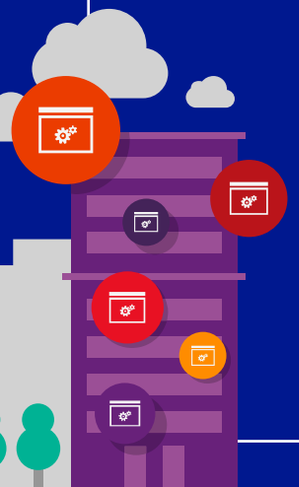
OWASP Top 10 | 8. Cross Site Request Forgery (CSRF)

Vulnerability	Impact	Prevention	Cloud Solution

• 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" />`
	• Trick Victims
	• Perform Unintended Operations
		• CSRF Unique Token
		• Libraries that prevent CSRF
			• Identity as a Service
			• Web Application Firewall
			• Open Source –
			  • ModSecurity
			• Vendors –
			  • Barracuda Networks

OWASP Top 10 | 9. Vulnerable Components

Vulnerability	Impact	Prevention	Cloud Solution
• Use of Vulnerable Components or Framework Libraries	• Impacts from all the OWASP Vulnerabilities	• Don't use components • Use Component Checker Libraries (ex for .NET and JAVA)	• WAFs • Marketplace



OWASP Top 10 | 10. Redirects and Forwards

Vulnerability	Impact	Prevention	Cloud Solution
• Redirects with unvalidated parameters http://www.example.com/redirect.jsp?url=evil.com http://www.example.com/boring.jsp?fwd=admin.jsp	• Data Loss or Corruption • Stolen Data • Denial of Access	• Don't use redirects • Use White list or Mapping	• Don't use redirects • Use 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-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