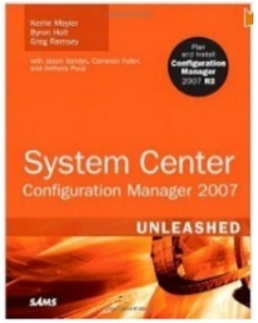
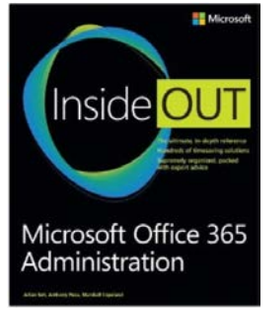
FTL CIO Council
October 18, 2017 Meeting

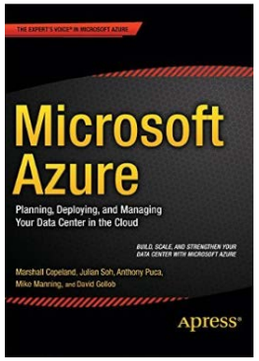
Anthony Puca
Cloud Infrastructure Architect | Federal Government

A little about me…

- Started in technology 28 years ago as a Mainframe Librarian for AMEX
- 7 years @ Microsoft, 7 @ EMC, 7 years @ Avanade and Perot Systems
- Authored books and whitepapers on Microsoft technologies
  - (2001): Original author of the MOF Change Quadrant SMF whitepapers
  - (2008): "*SCCM 2007 R2 Unleashed*" (http://www.amazon.com/System-Center-Configuration-Manager-Unleashed/dp/0672330237)
  - (2013): *Microsoft Office 365 Administration Inside Out* (O'Reilly): (http://www.amazon.com/Microsoft-Office-365-Administration-Inside/dp/0735678235)
  - (2015): *Microsoft Azure: Planning, Deploying, and Managing Your Data Center in the Cloud* (Apress): (http://www.amazon.com/Microsoft-Azure-Planning-Deploying-Managing/dp/1484210441)
- 2004-2010 Recipient of the Microsoft MVP award
- Last 18 years focused on Datacenter and Systems Management







Agenda

1. Microsoft Azure State of the Union
2. Regulations in the Cloud
3. Trends in Cloud Security
4. Changes we're seeing

Momentum

194 billion
External Requests made to Azure App Service

340 billion
Azure SQL query requests processed/day

750 million
Azure Active Directory users

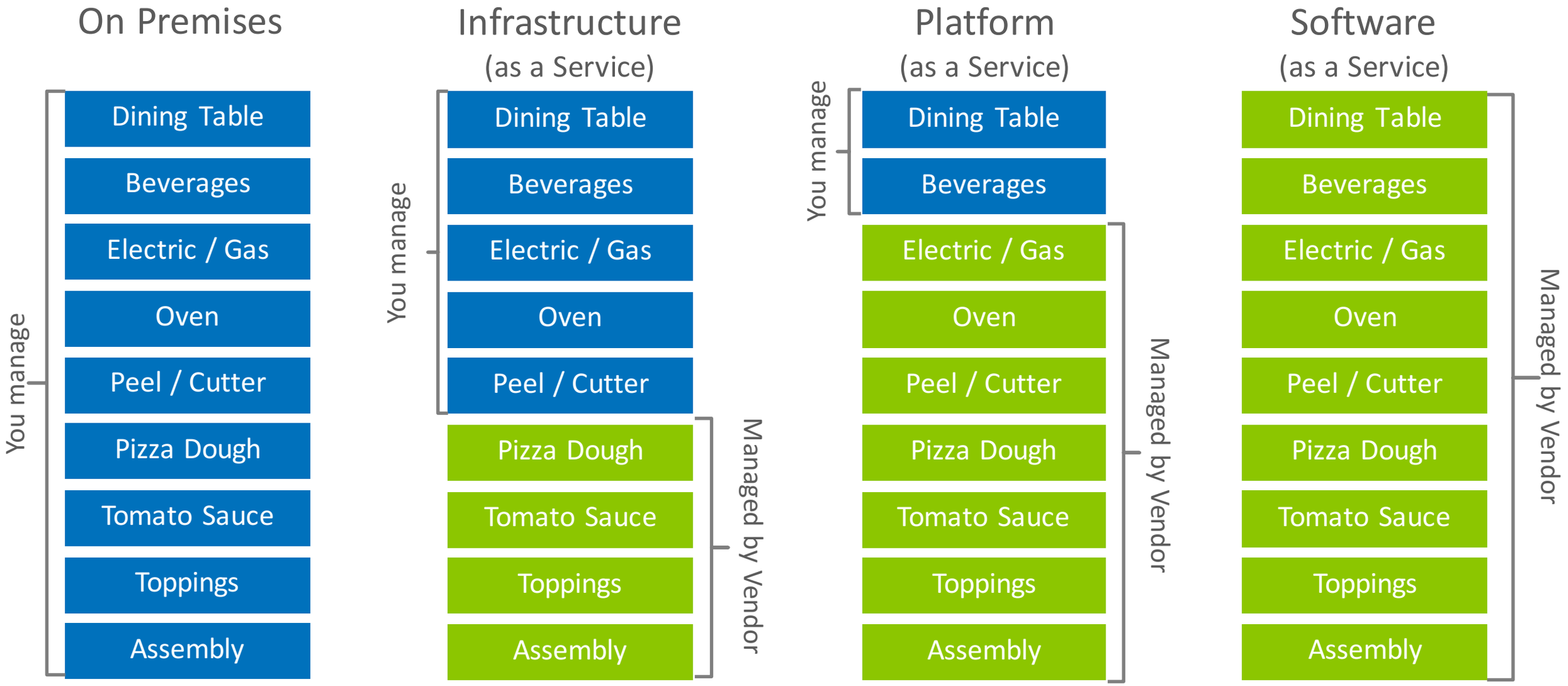
188 billion
Hits to websites run on Azure Web App Service

>90%
of Fortune 500 use Microsoft Cloud

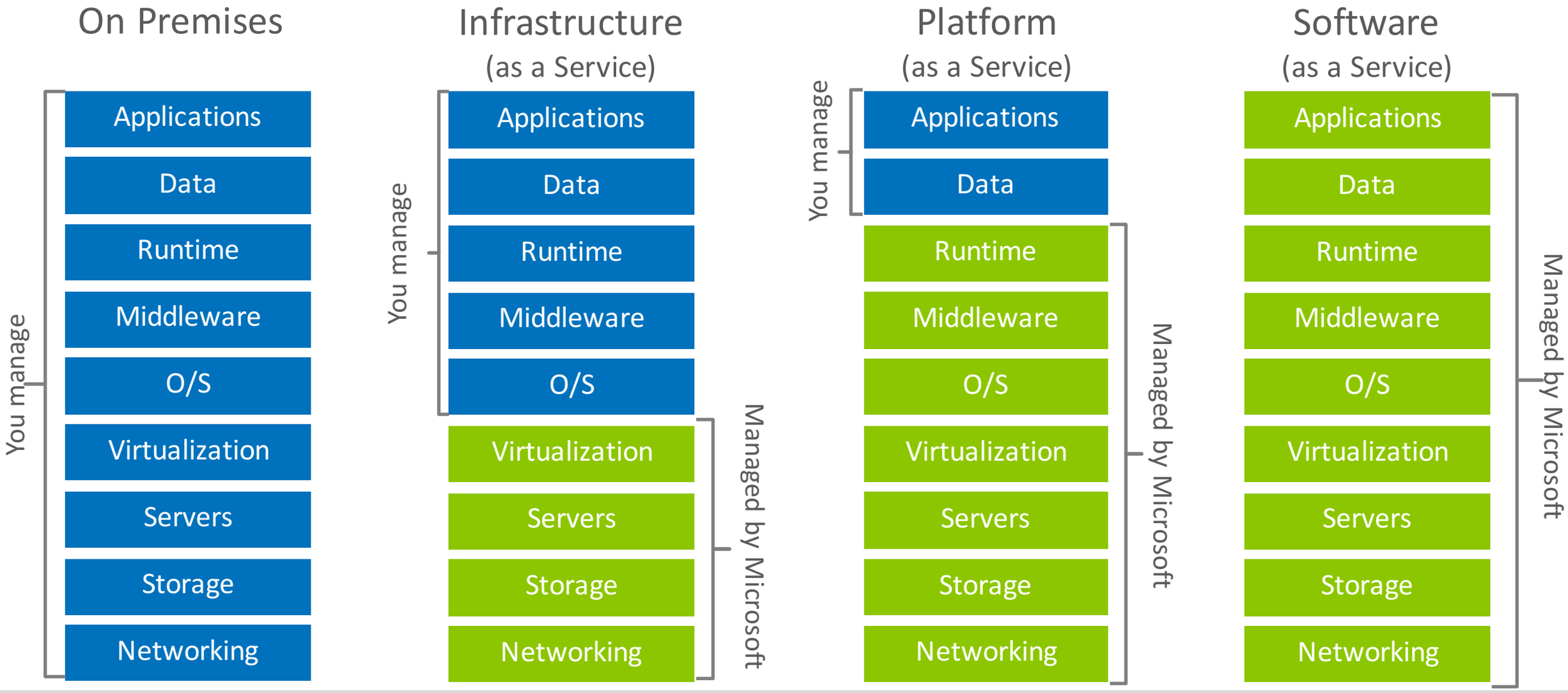
Cloud business value made easy

You Manage

Vendor Manages



Azure business value



Windows Server

Windows Azure Virtual Machines
Windows Server Hyper-V

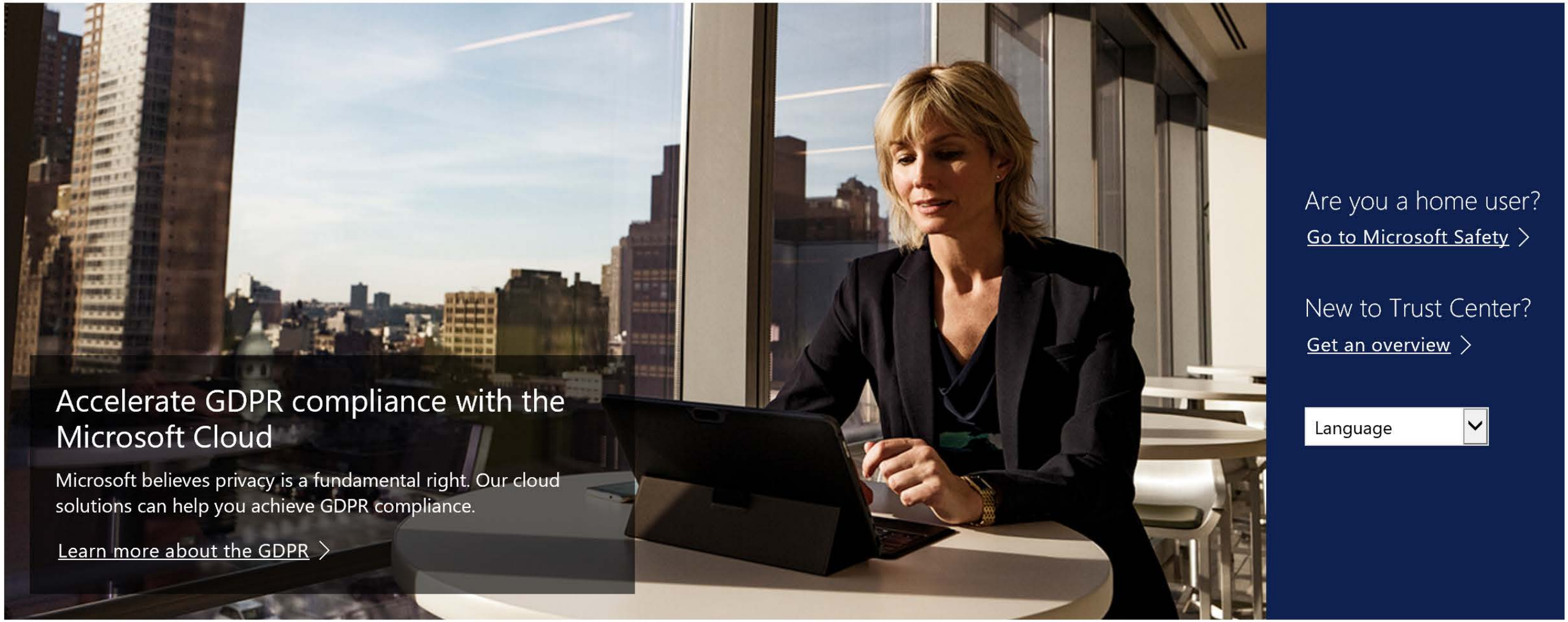
Windows Azure Cloud Services

Office 365
Dynamics CRM

Microsoft

Regulatory Compliance

Trust Center - https://www.microsoft.com/en-us/TrustCenter/default.aspx



Azure covers 54 compliance regimes

Azure has the deepest and most comprehensive compliance coverage in the industry

Trust

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 800-53 & 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

ISO 27001

ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001(aka- ISO 27001) can therefore be formally audited and certified compliant with the standard.

SOC 1 Reports

1. By engaging an independent CPA to examine and report on a service organization's controls, service organizations can respond to meet the needs of their user entities and obtain an objective evaluation of the effectiveness of controls that address operations and compliance, as well as financial reporting at those user entities.
2. To provide the framework for CPAs to examine controls and to help management understand the related risks, the AICPA is establishing three Service Organization Control (SOC) reporting options (SOC 1, SOC 2 and SOC 3 reports).
3. SOC 1 engagements are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization. SOC 1/SSAE 16 reports focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements, typically an auditor to auditor report.

SOC 2 Reports

1. SOC 2 is a report focused on controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy. There are two Types of SOC 2 reports:
    1. Type I accreditation is validation of the design of controls and implementation of controls.
    2. Type 2 accreditation involves an audit period during which evidence is gathered to test the operational effectiveness of the controls. One important thing to note about Type 2 accreditation is that the service must be in operation for a period of time before an organization may obtain this accreditation (typically a minimum period of at least 6 months), as the auditor must have data to test.

FERPA

1. The **Family Educational Rights and Privacy Act** of 1974 (FERPA) is a US law that applies to any educational agency or institution that receives funding from the U.S. Department of Education — i.e., virtually all public K-12 schools and school districts, as well as most private and public postsecondary institutions.
2. The act ensures that parents can access their children's educational records and protects students' privacy rights in those records. Specifically, **FERPA prohibits educational institutions from disclosing "education records" to third parties, unless the parent or student has provided prior written consent or the disclosure falls within a specifically enumerated exception**.
3. For students who are younger than 18 years old, these rights are held by the student's parents. Guidance from the US Department of Education (DOE administers and enforces FERPA) makes it clear that by using a cloud service, an educational institution is disclosing education records to the service provider and therefore the school must either obtain student/parent consent or fit within an exception to the consent requirement.

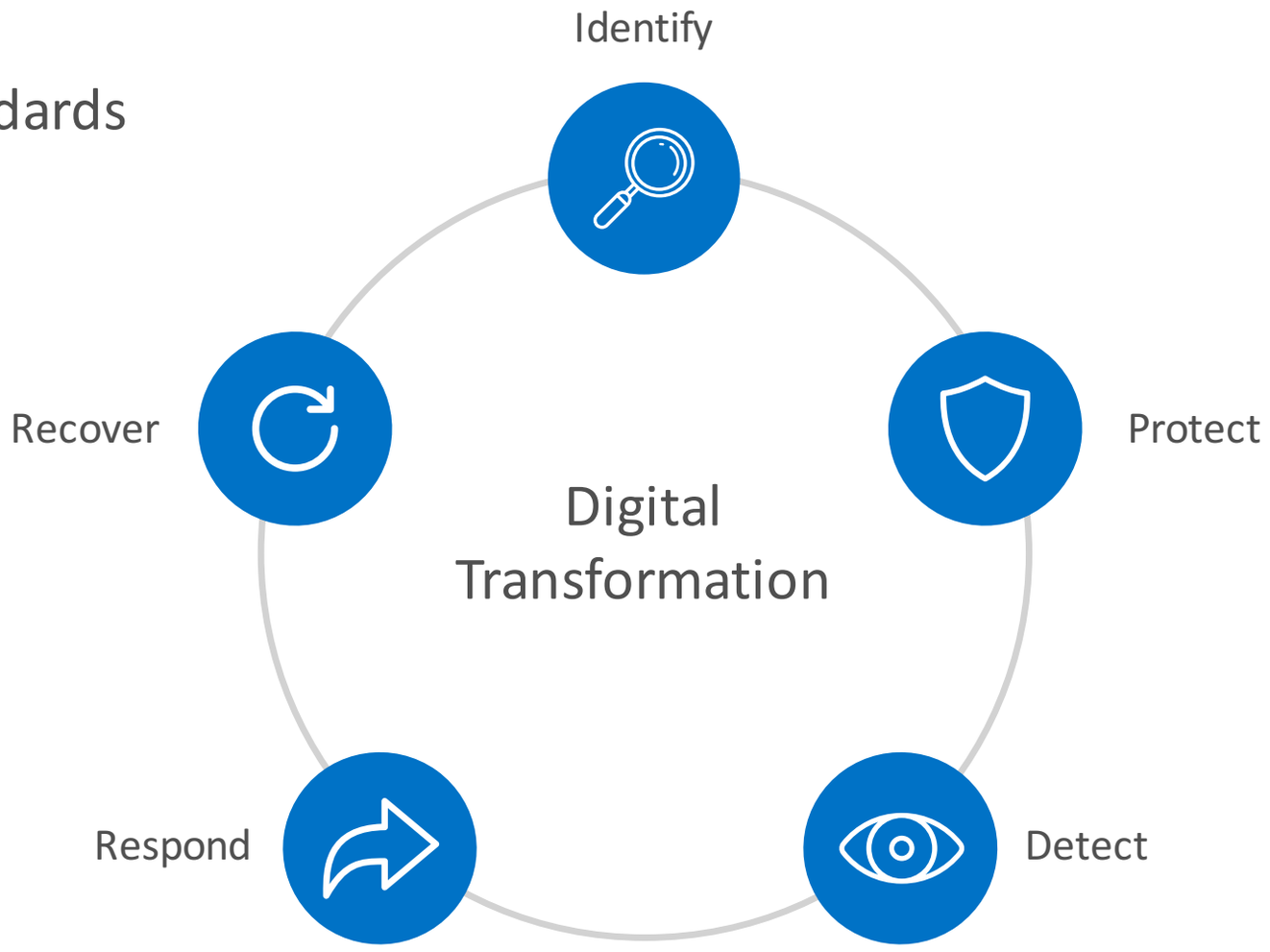
HIPAA/BAA

1. This information is referred to as electronic protected health information (ePHI). HIPAA applies to healthcare providers (e.g. – hospitals and physician offices), health plans, healthcare payors (e.g.- insurance companies) and clearing houses that use ePHI. These organizations are known as "covered entities." under HIPAA. HIPAA establishes standards to ensure the integrity, confidentiality and availability of ePHI, and lays out three types of required and addressable safeguards – physical, technical and administrative – to protect ePHI.
2. A business associate is a service provider whose rendering of services on behalf of the covered entity requires the service provider to create, receive, maintain or transmit the covered entity's ePHI. Pursuant to recent updates to to HIPAA (Final HIPAA Omnibus Rules), business associates are now directly responsible for compliance with HIPAA.
3. For a covered entity to use a service like Microsoft Office 365, Microsoft Dynamics CRM Online, or Windows Azure Core Services where ePHI will be maintained in Microsoft's data centers, Microsoft will be a business associate for HIPAA purposes and is obligated to enter into a required written agreement known as a business associate agreement (BAA), which memorializes Microsoft's HIPAA compliance obligations.

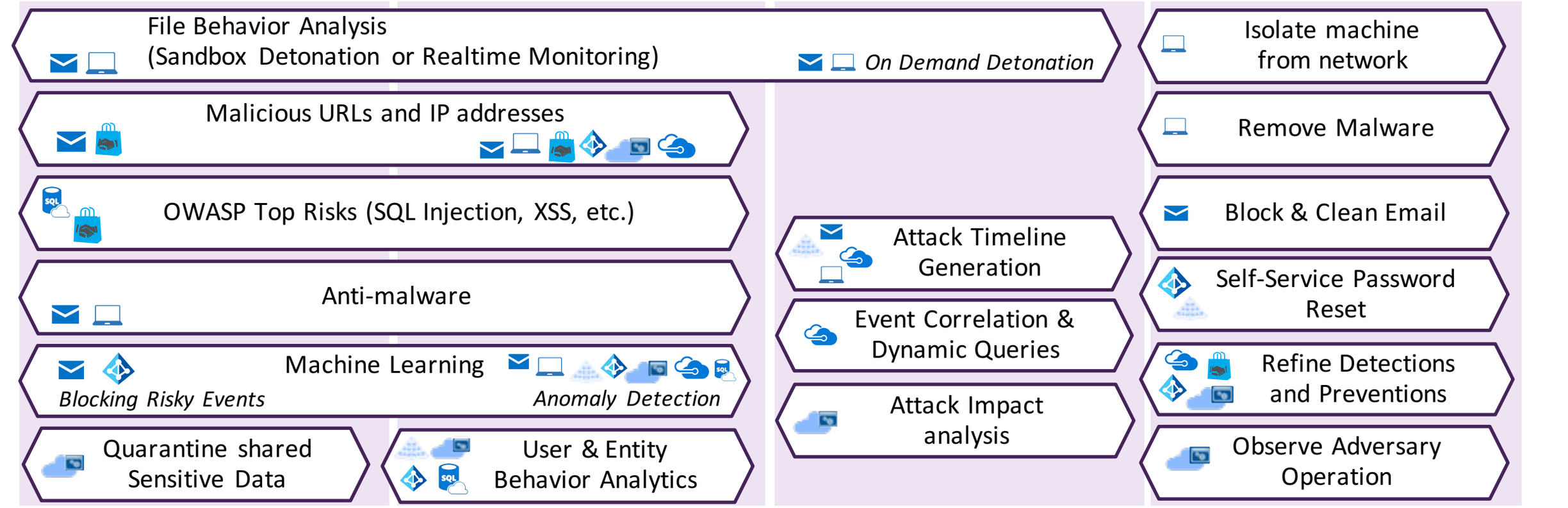
NIST Security Framework & GDPR

NIST: National Institute of Standards and Technology

GDPR: General Data Protection Regulation



NIST Framework Broad Mapping



- Azure AD Identity Protection
- Advanced Threat Analytics / Identity Manager
- Office 365 ATP
- Windows Defender ATP / Defender AV
- Microsoft Cloud App Security
- Azure Security Center
- Azure Web App Firewall / SQL Threat Detection
- Azure Marketplace Partner Capability

Microsoft

Trends in Cloud Security

Core security questions

There is one person in every organization who will click on anything

Central risk: Administrator privileges

Phishing attacks

Stolen admin credentials

Insider attacks

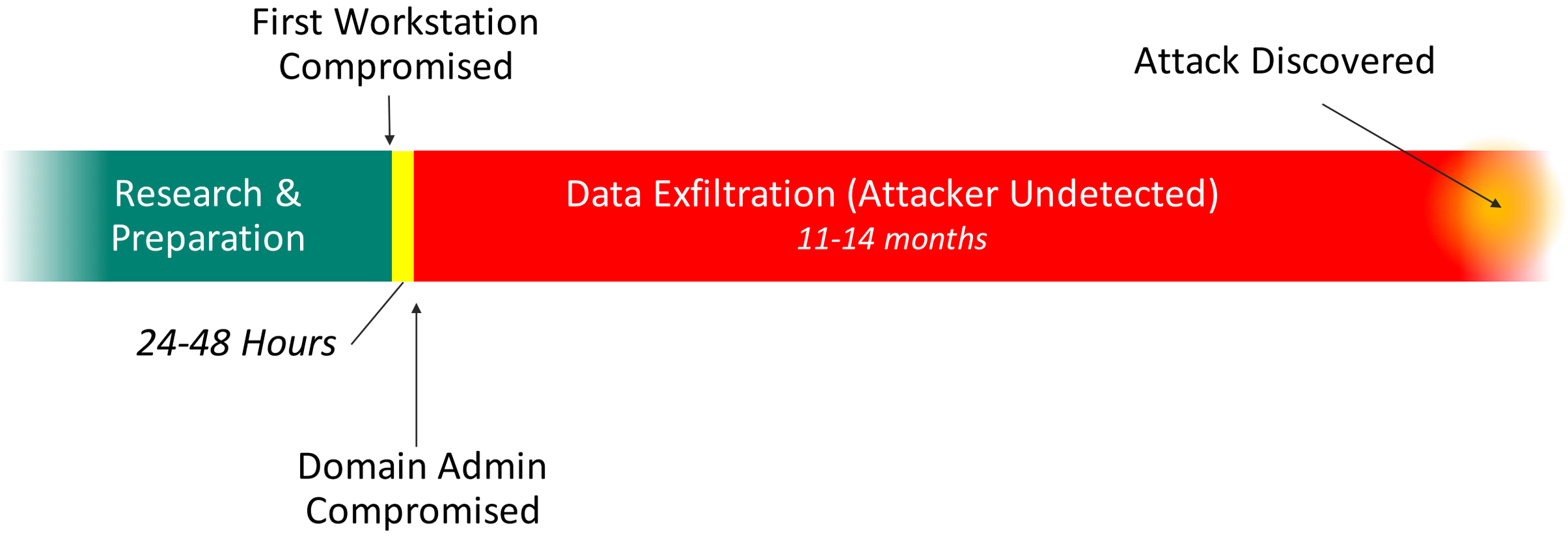
… each of these attacks seeks out & exploits privileged accounts.

---

1. We know that administrators have the keys to the kingdom; we gave them those keys decades ago

2. But those administrators privileges are being compromised through social engineering, bribery, coercion, private initiatives

The anatomy of a typical breach



PLAN

ENTER

TRAVERSE

EXECUTE MISSION

A. Enter and Navigate

Any employee opens attack email

→ **Access to most/all corporate data**

Any

2a Workstation compromised, threat actor gathers credentials

3a Threat Actors use stolen credentials to ***move laterally***

1 Threat Actor targets employee(s) via phishing campaign

Common Attacks

4 Threat Actors exfiltrate PII and other sensitive business data

B. Device Compromise

Targeted employee opens attack email

→ **Access to same data as employee**

2b Employee B opens infected email (Mobile or PC). Attacker disables antivirus

3bc Compromised credentials/ device used to access cloud service / enterprise environment

C. Remote Credential Harvesting

Targeted employee(s) enter credentials in website

→ **Access to same data as employee(s)**

2c Credentials harvested when employee logs into fake website

Conclusion: *change the way we think about security*

We have to "assume breach" – not a position of pessimism, one of security rigor

Problem

A breach will (already did?) happen
Lacking the security-analysis manpower
Can't determine the impact of the breach
Unable to adequately respond to the breach

New approach (in addition to 'prevention')

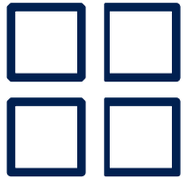
Limit or block the breach from spreading
Detect the breach
Respond to the breach

Modern Security Layers to Mitigate Risk

Network

Operating System

Identity



Application

Information

Communications

Management

Physical

Cybersecurity Reference Architecture

Microsoft

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- Analytics / UEBA
- SIEM
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Windows Security Center
- Azure Security Center
- Office 365
  - Security & Compliance
  - Threat Intelligence

Security Development Lifecycle (SDL)

80% + of employees admit using non-approved SaaS apps for work (Stratecast, December 2013)

Internet of Things

Unmanaged & Mobile Clients

Software as a Service

Office 365
- ASM
- Lockbox

Information Protection
- Cloud App Security

Identity & Access
- Azure Active Directory
- Conditional Access
- Intune MDM/MAM
- Azure AD Identity Protection
- Azure AD PIM
- Multi-Factor Authentication
- Hello for Business
- MIM PAM
- ATA
- Active Directory
- ESAE Admin Forest
- Certification Authority (PKI)

Office 365 DLP

Azure Information Protection (AIP)
- Classify
- Label
- Protect
- Report

Hold Your Own Key (HYOK)

Classification Labels

Azure SQL Threat Detection

SQL Encryption & Data Masking

Endpoint DLP

Windows Info Protection

On Premises Datacenter(s)

- NGFW
- Edge DLP
- SSL Proxy
- IPS
- Office 365 ATP
  - Email Gateway
  - Anti-malware
- Extranet
- Colocation
- Express Route
- Security Appliances
- VPN

Microsoft Azure

SIEM Integration

- Azure Security Center (ASC)
  - Threat Protection
  - Threat Detection
- Azure Key Vault
- Azure App Gateway
- Azure Antimalware
- Network Security Groups
- ...
- SQL Firewall
- Disk & Storage Encryption
- DDoS attack mitigation
- Backup & Site Recovery

Enterprise Servers

- Shielded VMs
- VMs
- VMs
- Domain Controllers

Windows Server 2016 Security
Shielded VMs, Device Guard, Credential Guard, Just Enough Admin, Hyper-V Containers, Nano server, Defender AV, Defender ATP (Roadmap), and more...

VPN

Privileged Access Workstations (PAWs)

Managed Clients

- Sensitive Workloads
- Legacy Windows
- Windows 10
- Mac OS
- IoT
- WEF
- EDR - Windows ATP
- EPP - Windows Defender AV
- System Center Configuration Manager + Intune

Windows 10 Security
- Secure Boot
- Device Guard
- Exploit Guard
- Application Guard
- Credential Guard
- Windows Hello
- Remote Credential Guard
- Device Health Attestation

Nearly all customer breaches that Microsoft's Incident Response team investigates involve credential theft
63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

Last updated July 2017 – latest at http://aka.ms/MCRA

Trends in Global Cybersecurity

Find out about the latest threats to endpoints and the cloud

https://www.microsoft.com/en-us/security/intelligence-report

1. Severity of vulnerabilities
2. Vulnerability complexity
3. New application vulnerabilities
4. Platform-agnostic vulnerabilities
5. Declining Java exploits
6. Extent of exploit kits
7. Most commonly detected objects – Flash/Silverlight (aka ActiveX)
8. Global security concerns
9. Increased Trojan levels
10. Continued complexity of threats

Thank you

- Explore additional resources:
  - Trustworthy Computing Cloud Services: www.microsoft.com/trustedcloud
  - Microsoft Trust Center for Microsoft Azure: http://www.windowsazure.com/en-us/support/trust-center