edgile

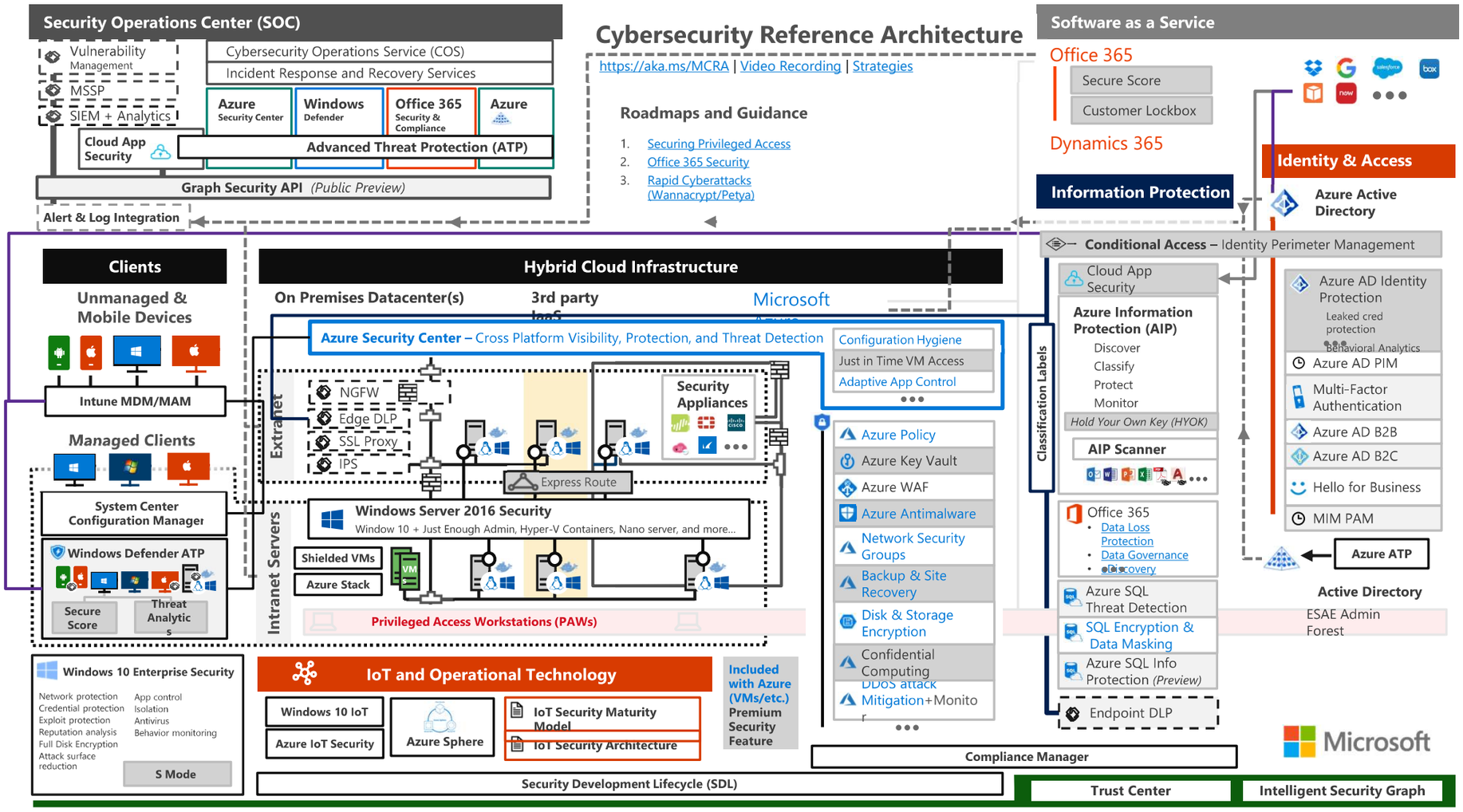
We Secure the Modern Enterprise

Drew Wigodsky

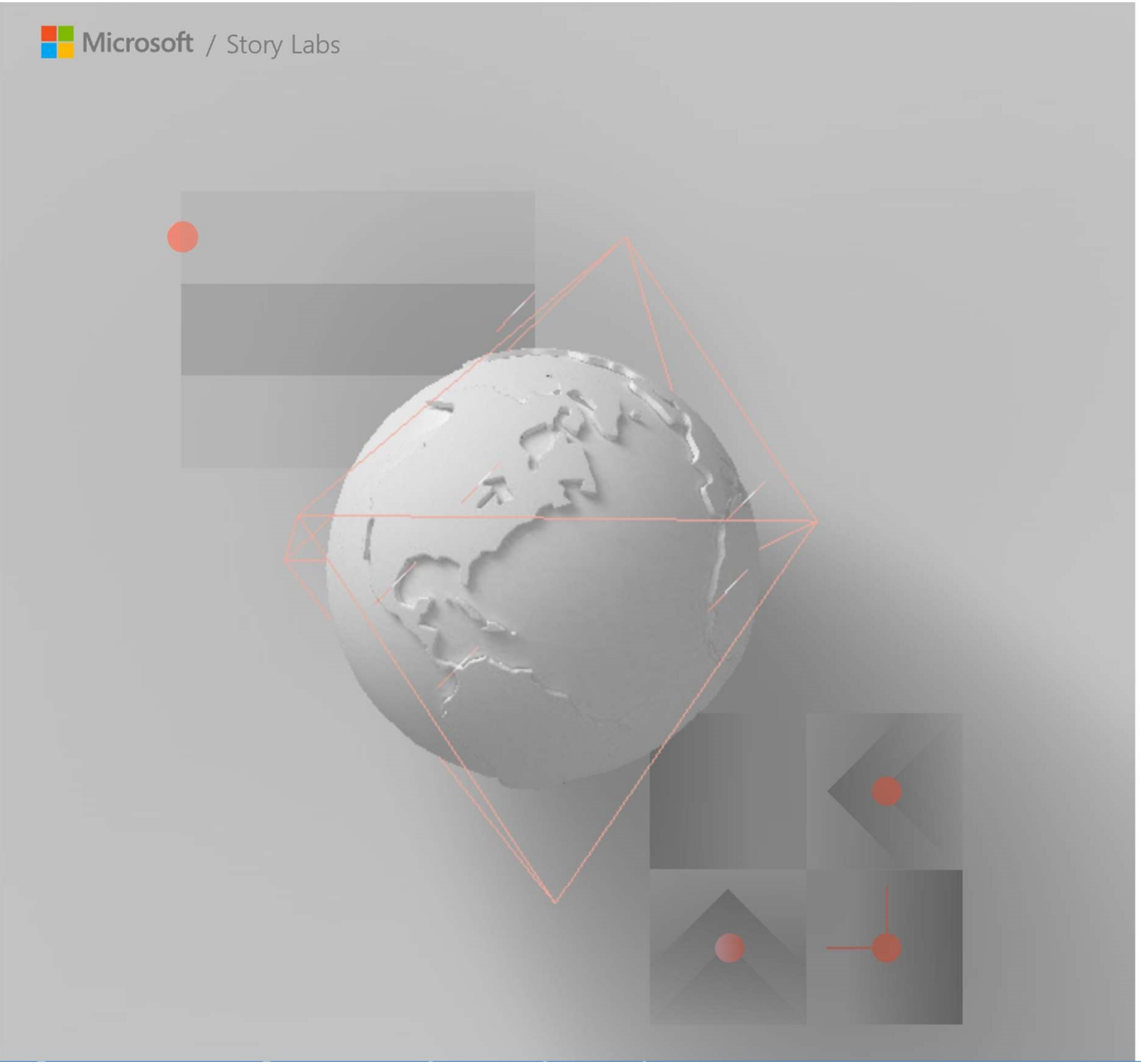
drew@edgile.com

Security is complex...

Cybersecurity Reference Architecture



Microsoft / Story Labs



1 billion

There are more than 1 billion devices running Windows 10.

4 Principles for Modern Security

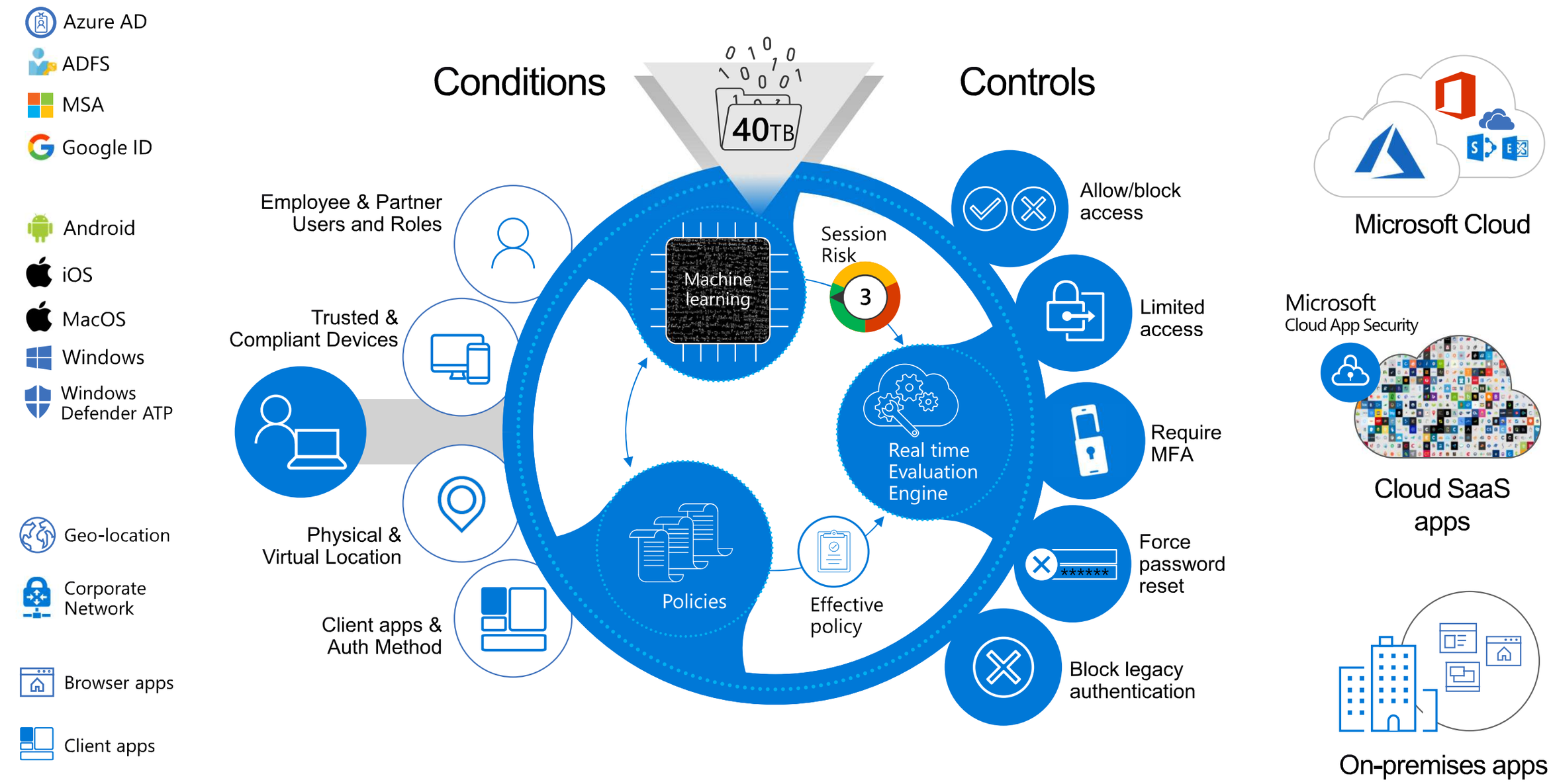
1. **Centralize Access Management in the Cloud**
   Implement zero trust and dynamic access control. Replace passwords with machine intelligence. Enable modern auth for all apps. Minimize investment in legacy identity debt.

2. **Adopt Cloud Security**
   Leverage the investments of cloud platform vendors to enable ML and AI to identify and respond automatically. Reduce alerts and focus staff. Use DevSecOps as a security tool.

3. **Protect Assets**
   Detect, identify and protect sensitive data for regardless of where it's stored, shared or leaked.

4. **Cloud-Enable Integrated Risk Management**
   Update systems and processes using cloud powered solutions for IRM. Integrate risk detection with analysis and response.

Centralize Access Management


Azure AD
ADFS
MSA
Google ID
Android
iOS
MacOS
Windows
Windows Defender ATP
Geo-location
Corporate Network
Browser apps
Client apps
Conditions
Controls
40TB
Employee & Partner Users and Roles
Trusted & Compliant Devices
Physical & Virtual Location
Client apps & Auth Method
Machine learning
Session Risk
3
Real time Evaluation Engine
Policies
Effective policy
Allow/block access
Limited access
Require MFA
Force password reset
******
Block legacy authentication
Microsoft Cloud
Microsoft
Cloud App Security
Cloud SaaS apps
On-premises apps

Secure All User Communities

White Label Consumer experience (B2C)

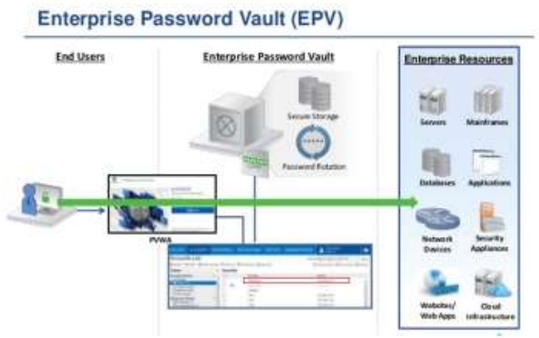
Managed Collaboration with Partners (B2B)

Password-less for Employees (B2E)

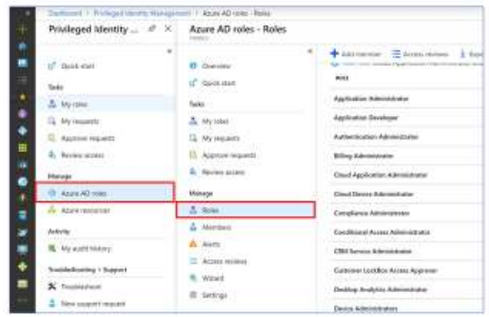
- Outsources IAM to Microsoft
- Leverages $1b/year in security investment and 3,500 security professionals
- Consistent user experience

Secure Privileged Access

On premises

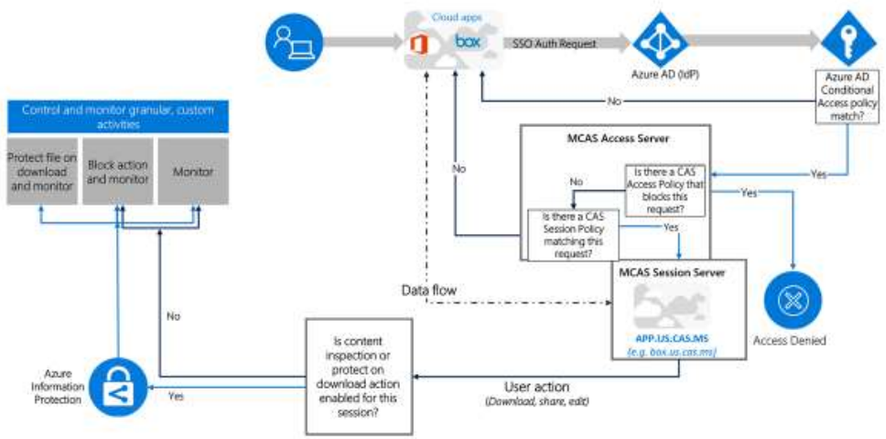


In the cloud

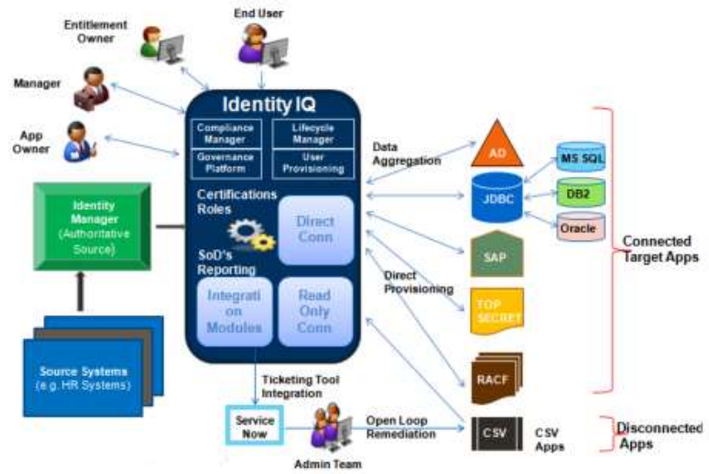


Manage App Access

Conditional Access App Control - Architecture



Address Legacy Identity



Contractor Account Request Overview

Audit DB Last Update Time (US Eastern):

2020-04-23 12:29:20 AM

Contractor Account

Search

ManagerAccountName

Search

Request Status

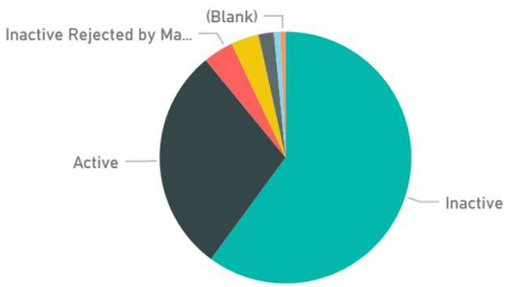
- (Blank)
- Active
- Active Pending Manager Decision
- Active Pending Renewal

When Requested

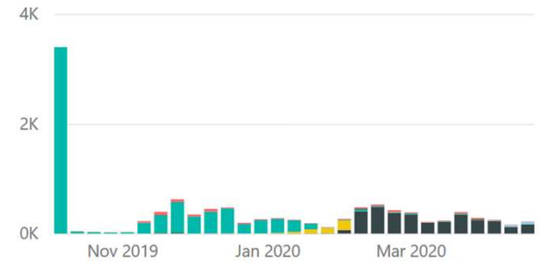
10/10/2019 4/23/2020

contractor_account_name	ContractorDisplayName	ad_account_enabled	request_type	Request Status	when_contract_starts	when_requested	whe
v-guimajs	Guimaraes, Joelcinei (Exactus)	True	System Approved	Inactive		2019-10-10	201
v-genesm	GENEST, Melanie	True	System Approved	Inactive		2019-10-10	201
v-duartas	Duarte, Adriana (ABP)	True	System Approved	Inactive		2019-10-10	201
v-coutus	Couture, Simon (Groupe Perspective)	True	System Approved	Inactive		2019-10-10	201
v-samparm	Sampaio, Reginaldo (Engetherm)	True	System Approved	Inactive		2019-10-10	202
v-savind	Savinda, Dan	True	System Approved	Inactive		2019-10-10	202
v-araujfm	Araujo, Felipe M	True	System Approved	Inactive		2019-10-10	202
v-deshal	DESHAIES-TROTTIER, Lysanne	True	System Approved	Inactive		2019-10-10	202
v-goasdf	Goas Fernandez, Domingo (Honeywell)	True	Extension	Inactive		2019-10-10	202

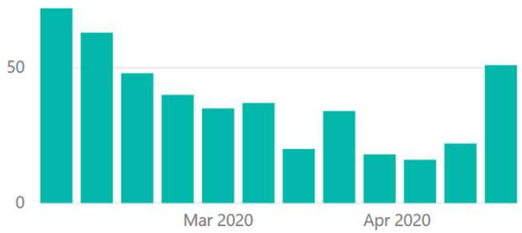
Request Status



When Requested



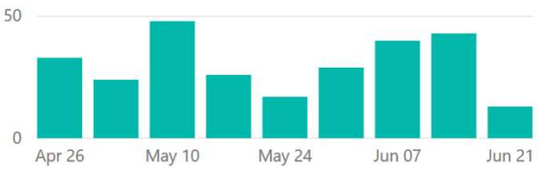
Contractor Accounts Deleted in Last 90 Days



456

Contractor Accounts Deleted in Last 90 Days

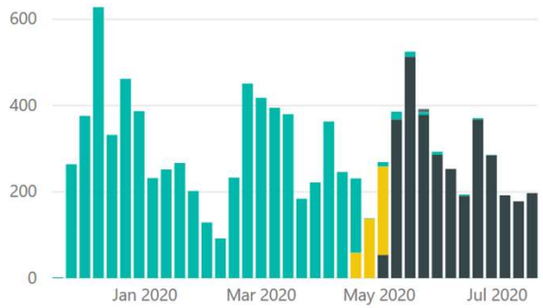
Contractor Accounts Deleted in Next 90 Days



273

Contractor Accounts Deleted in Next 90 days

When Request Expires



Rogue Account Detection

Audit DB Last Update Time (US Eastern): 2020-04-23 12:29:20 AM

Account

Search

extensionAttribute4

- (Blank)
- A
- Contractor
- E

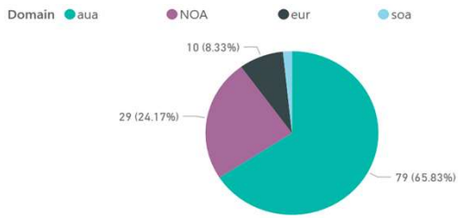
whenCreated

whenCreated: Last 30 Days

3/27/2020 - 4/25/2020

Rogue Accounts Created by Day

Rogue Accounts by Domain



Rogue Accounts

displayName	extensionAttribute14	extensionAttribute4	lastLogonTimestamp	accountDisabled	extensionAttribute5
Agarwal, Subodh - stadmin		A	4/20/2020 6:26:50 AM	False	
Chakraborty, Sangbed - admin		A	4/13/2020 5:03:28 PM	False	
Chakraborty, Sangbed - admin		A		False	
Chakraborty, Sangbed - admin		A	4/23/2020 8:04:22 PM	False	
Chakraborty, Sangbed - tadmin		A	4/23/2020 5:36:56 PM	False	
Chakraborty, Shamik - sadmin		A	4/20/2020 5:26:53 AM	False	
Cmeci, Ildiko		A	4/14/2020 11:23:45 AM	False	
Cmeci, Ildiko - aadmin		A	4/23/2020 4:49:38 PM	False	
Das, Tanima - sadmin		A	4/21/2020 12:29:19 PM	False	
Debroy, Bikash - stadmin		A	4/20/2020 12:27:03 PM	False	

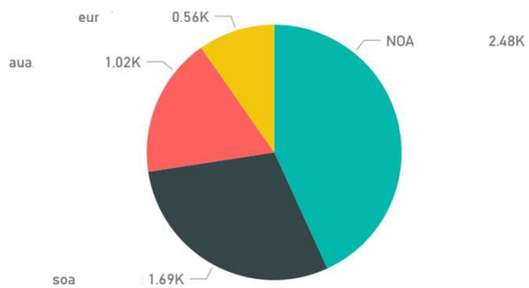
Improperly Owned AD Groups

Audit DB Last Update Time (US Eastern): 2020-04-23 12:29:20 AM

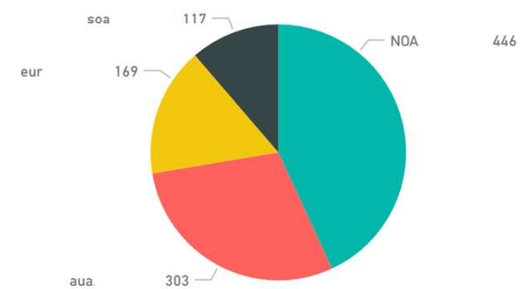
GroupName

Search

Groups with No Managers by Domain



Groups with Disabled Manager Accounts by Domain

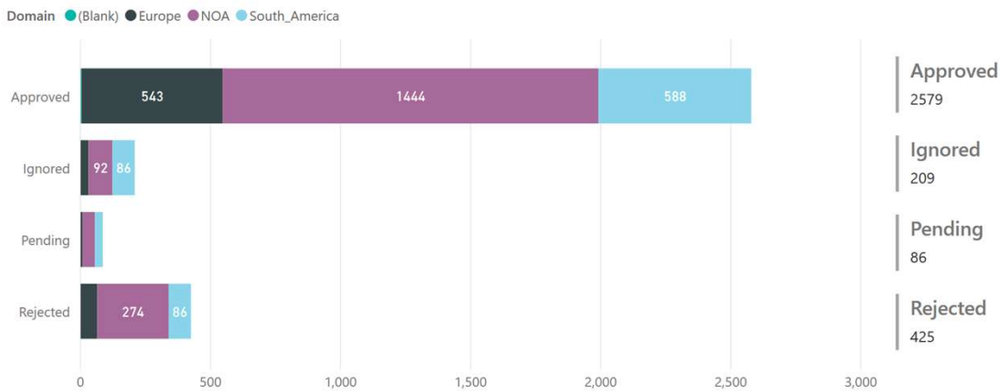


Groups

GroupName	Domain	sAMAccountNameManagedBy	displayNameManagedBy	managerAccountDisabled	DNMana
SOUTH_AMERICA\zCorporate SA Communications DL	soa				

Contractor Account Renewals by Status

Audit DB Last Update Time (US Eastern): 2020-04-23 12:29:20 AM



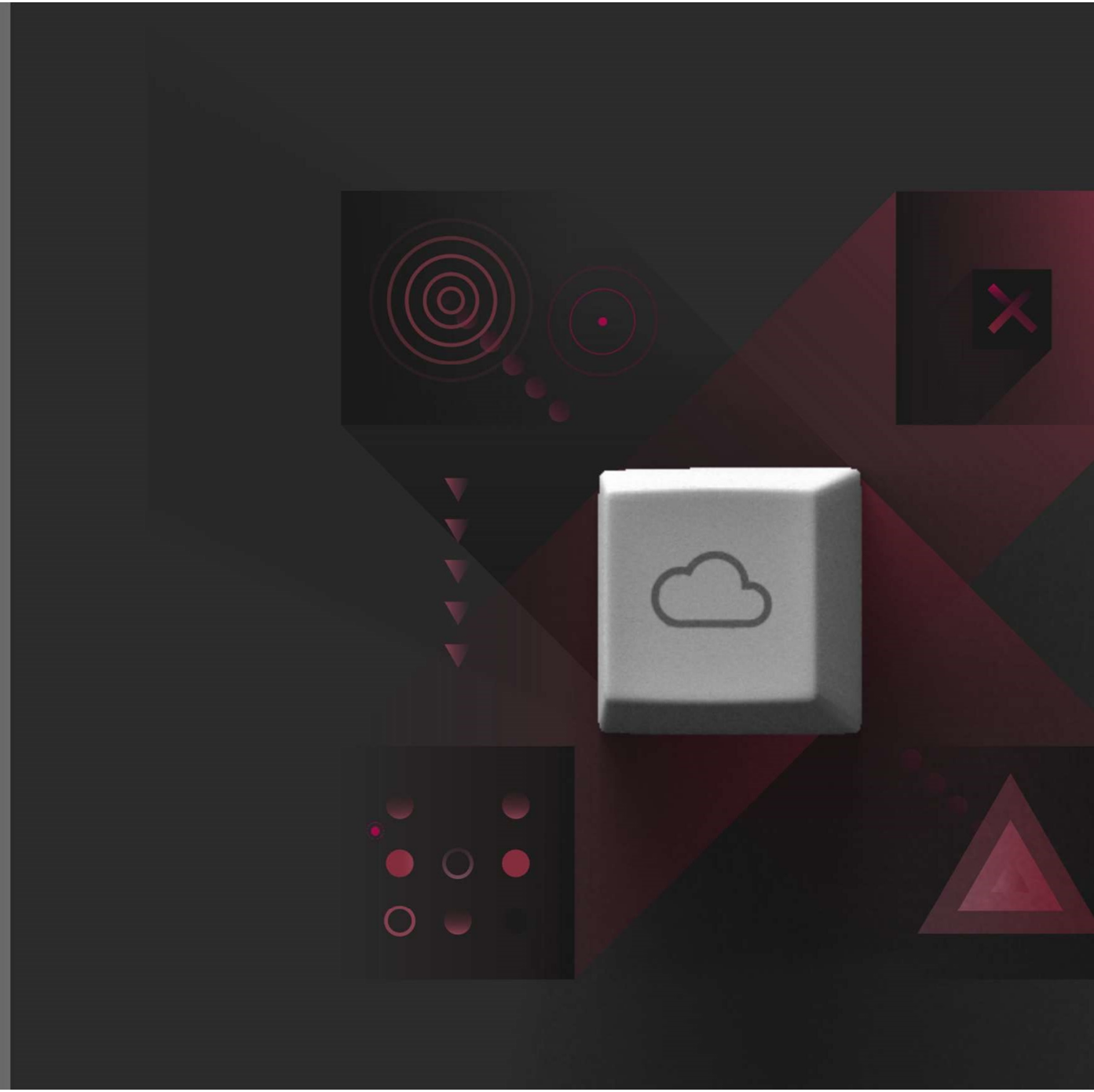
Renewals

status	when_requested	when_expires	_renewal_status	DisplayName	contractor_account_name

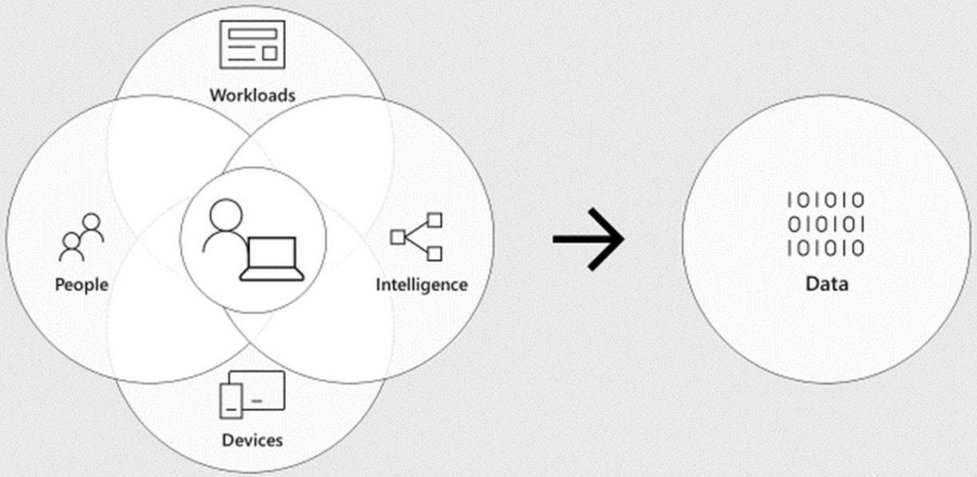
Microsoft / Story Labs

6.5 trillion

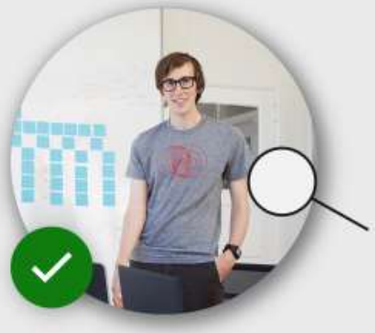
Every day, Microsoft analyzes over 6.5 trillion signals in order to identify emerging threats and protect customers.



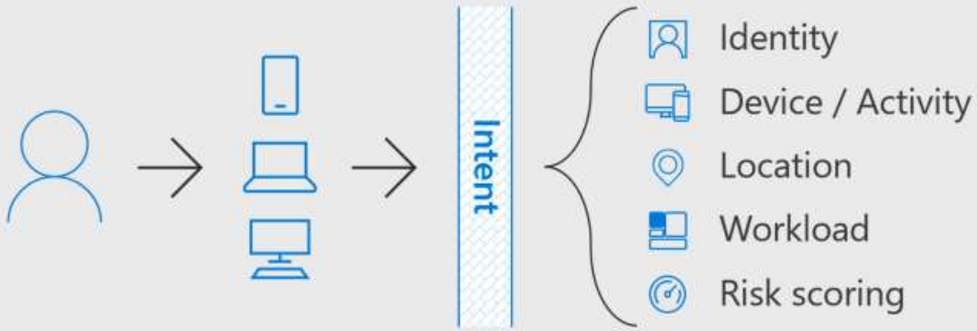
What does Zero Trust mean?



1. Never Trust. Always verify.



2. Assume every resource is on the open internet

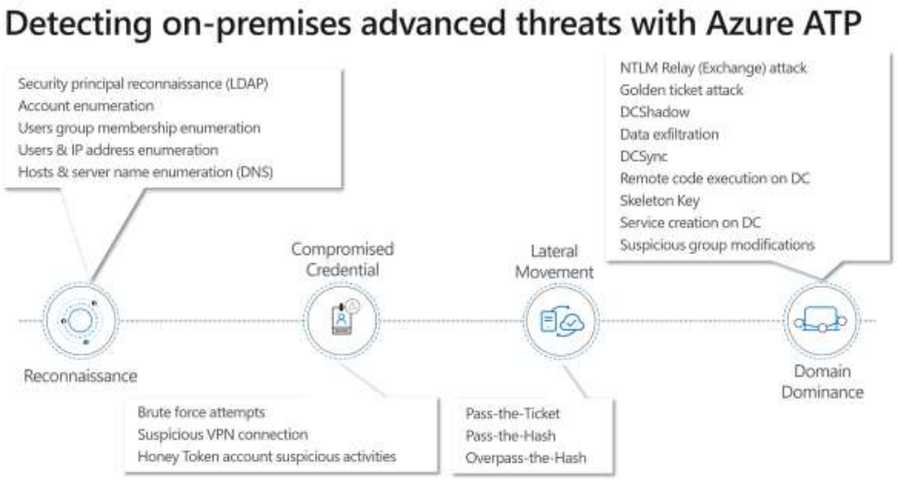


3. Identity is the control plane

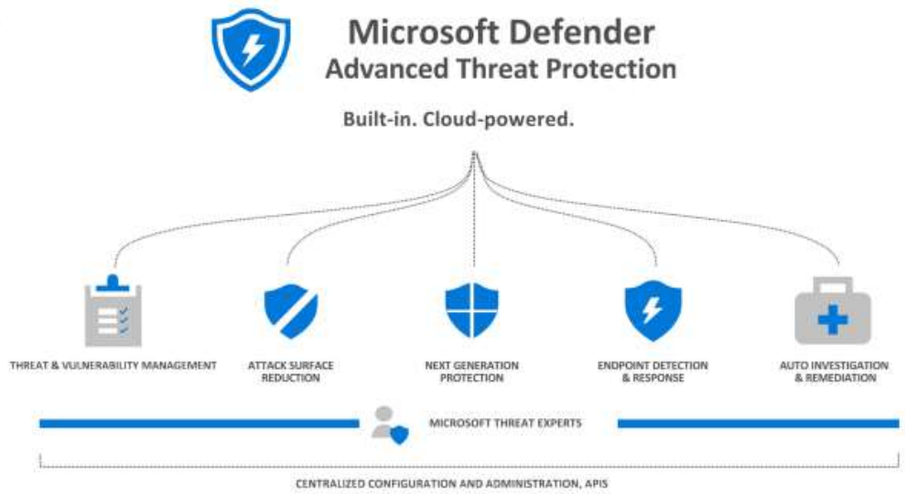
Mapping the Key Elements of Zero Trust

Segmented networks	→	**Logical Micro-segmentation**
Local packet tracking and logs	→	**6.5T correlated signals per day**
Inferred trust	→	**Explicit verification and control**
Reactive response	→	**Automated response**
Walled gardens	→	**Modern mobility**

Detect Unusual Activity - Directory



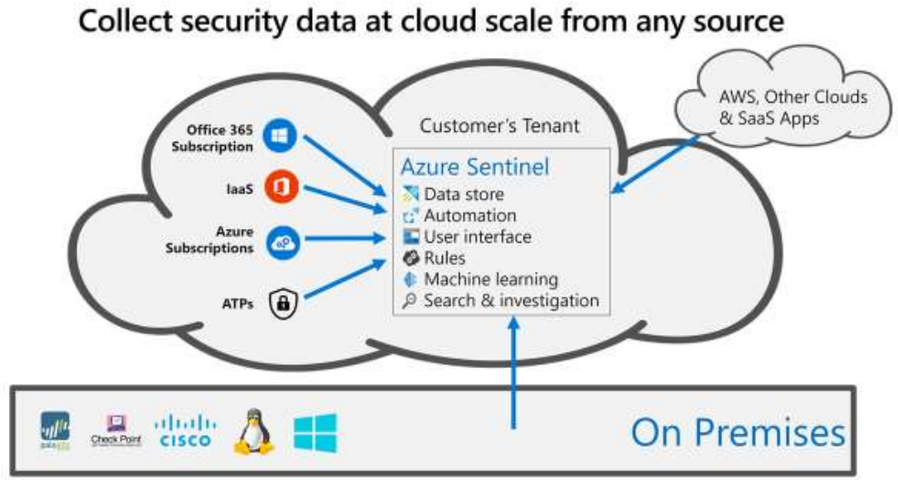
Detect Unusual Activity – Endpoint



Cloud Security and AI

- Persistent Threat Management
  - Intercede in advance
  - Quick identification of threats via continuous close monitoring
  - Automated rapid response
- Software as Security
  - Design security capabilities in code
  - Use desired state configuration to provide persistent enforcement

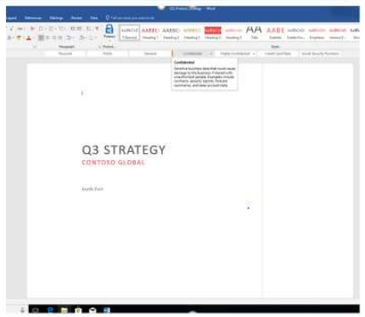
Collect and Assess Signals



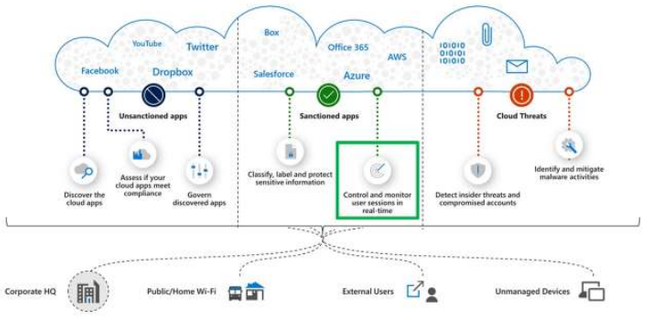
Protect Information Assets

Identify and Protect Data

- Update data governance and data classification programs specific for cloud
- Empower users with technology and corporate approved processes to protect newly created information
- Comb through data stores to identify and address high risk information
- Use systems and devices to monitor and take automated action when sensitive information is leaving trusted zones



Automate Information Control



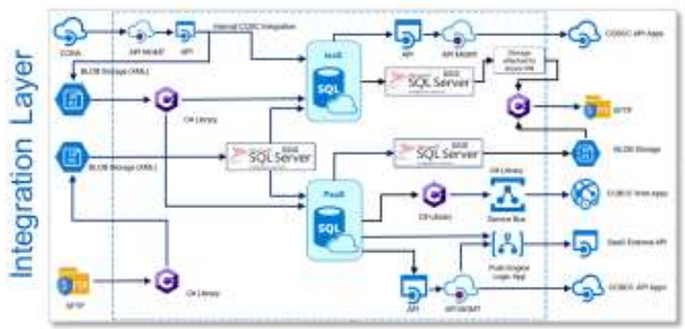
Data Protection Framework

	1 Discovery & Analysis	2 Architecture & Design	3 Deploy & Implement	4 Operationalize
	2 - 4 weeks	3 - 6 weeks	4 – 6 weeks	1 – 2 weeks
INFORMATION PROTECTION FRAMEWORKS • NIST SP 800-53 • ISO 27001 • AICPA Trust Services Principles & Criteria • COBIT	**Key Activities** • Conduct discovery workshops • Assess data repositories (on-premise, cloud, hybrid, partner) • Determine data volume • Assess data lifecycles • Review existing information protection solutions (DLP, SIEM) • Assess data classification scheme • Assess data classification policies • Identify key use cases (PII, PCI, SOX, HIPAA, etc.)	**Key Activities** • Conduct design workshops • Determine data discovery requirements and architecture (AIP, MCAS, DLP) • Create, refine or update classification taxonomy • Determine encryption requirements (as needed) • Develop initial AIP policies • Determine testing requirements • Develop operational processes	**Key Activities** • Build and integrate test tenant • Develop test cases • Develop user communications • Conduct service-desk training • Support execution of test cases • Build and integrate production AIP environment • Conduct AIP Pilot • Refine AIP configuration and policies • Enable AIP within production	**Key Activities** • Optimize operational processes • Finalize reports and dashboards • Prepare run books • Deploying AIP across the organization and work with key teams
• PCI-DSS • SOX • HIPAA • GDPR				
GOVERNMENT & INDUSTRY REGULATIONS	**Key Outputs** • Current state analysis • AIP strategy • AIP roadmap	**Key Outputs** • AIP design • Data classification scheme • Use cases and test plan • Implementation plan	**Key Outputs** • Operational test tenant • Operational AIP production environment • Communications plan • Updated AIP design	**Key Outputs** • Run books • Operationalizing AIP with key teams • Deploying it throughout the organization

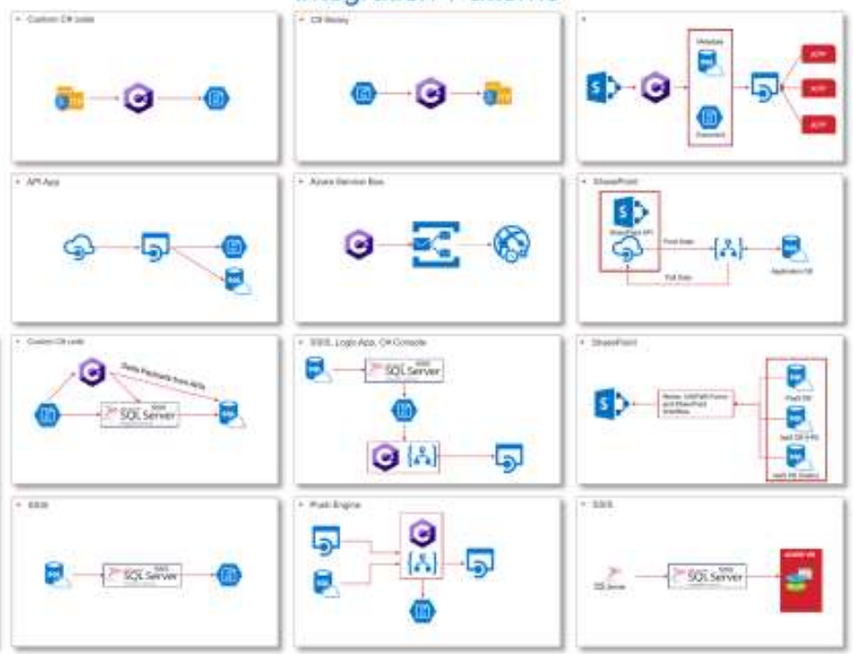
DevSecOps Architecture

Goals:

- Standardize software and infrastructure architectures together
- Integrate security testing early and throughout the development lifecycle
- Know and reuse your integration patterns
- Don't forget encryption guidelines!

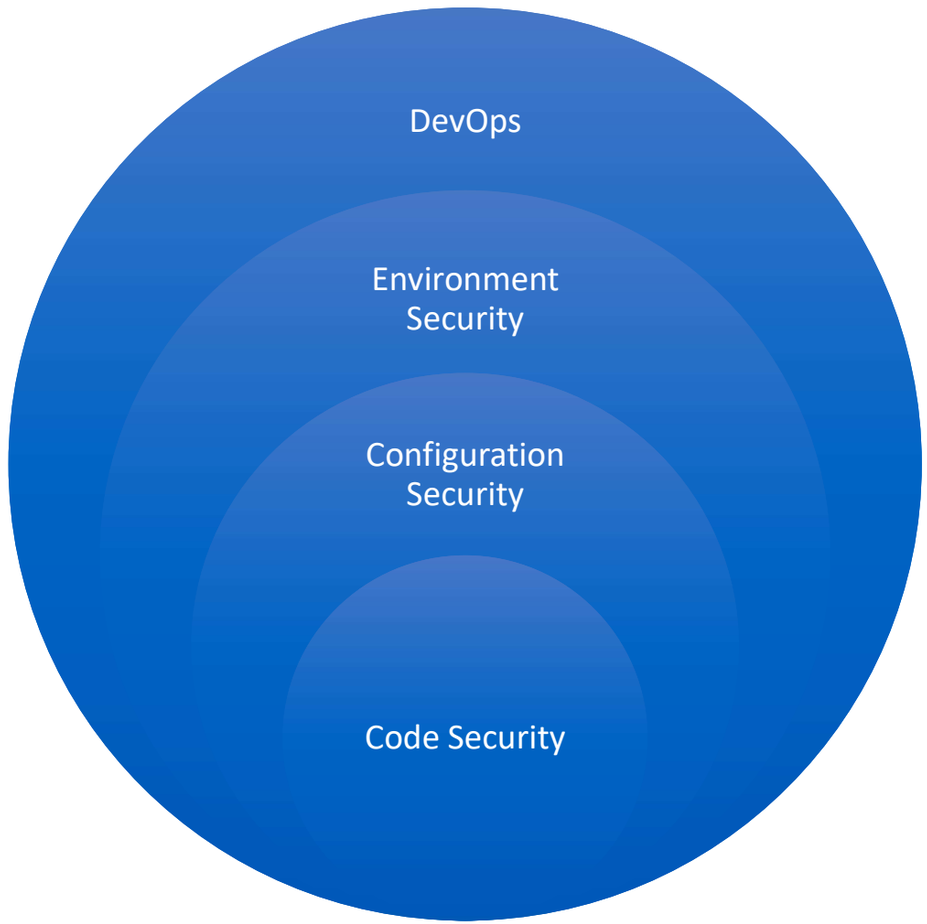


Integration Patterns



Hardwired: Software a Security System

- **Secure** DevOps is a modern approach to cloud development that adds layers to bring all concerns (app, infra, security) into a single process and configuration
- Repeatable processes and patterns
  - Code (standards to secure, test, monitor)
  - Configuration (configuration items, apps with infra)
  - Environment (expected layers, allowed connections)
- Common, clear standards and automated testing reduce time and effort for:
  - Developing new applications
  - Enhancing existing applications
  - Onboarding vendor applications

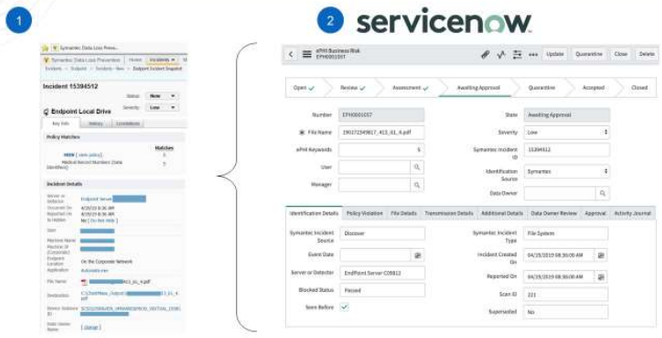


Integrate Risk Management

Use Cloud Systems for IRM

- Streamline compliance processes using modern cloud centric systems with purpose-specific content
- Use systems with workflows for review, approval, activation and record keeping
- Integrate these systems with security layer to automate the detection, review and determination of information
- Demonstrate the return on investment through risk management metrics

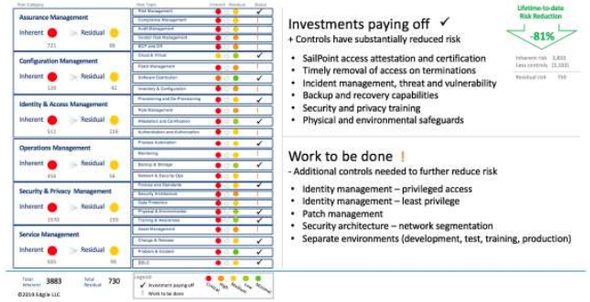
In a System with Integrated Workflow



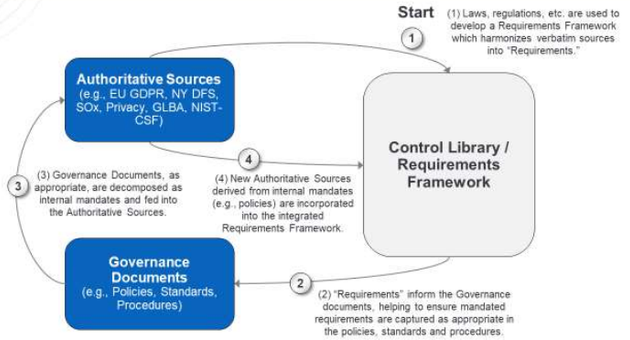
Use Purpose-Specific Content

Deliver Meaningful Metrics

Example of Executive Presentation



Harmonized with Standards and Regs



Remember these

- portal.azure.com
- security.microsoft.com
- portal.cloudappsecurity.com
- securitycenter.windows.com
- protection.office.com
- … and many more!

Edgile & Microsoft

Microsoft Partner
Gold Identity and Security

- An extensive partnership built over the last 16+ years
- Delivering expert implementation services to drive Azure and Microsoft 365
- Deep expertise in 3rd party systems to deliver enterprise implementation

20/20
Microsoft Security System Integrator of the Year

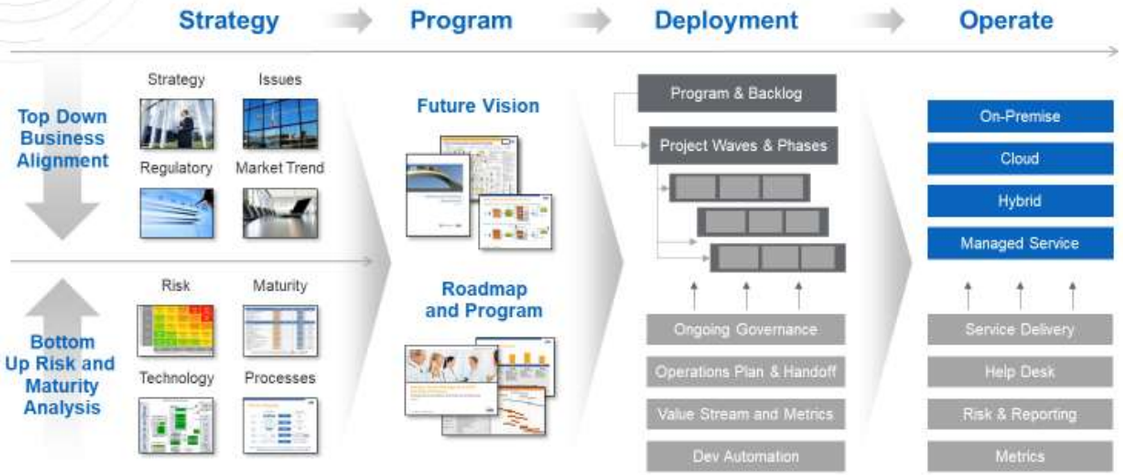
Service	Description
Azure Cyber-Security Strategy	Strategy effort aligning the enterprise around actionable plan for aggressive migration to Microsoft 365
Azure Security Services	Deep security skills applied to drive planning, design, deployment of Azure EMS security technologies
Shadow IT Discovery & Remediation	Provides hard evidence of the extent of an enterprise's cloud environment and introduces appropriate controls using Microsoft 365

Service	Description
Accelerated Transformation	Enables rapid migration of enterprise IT capabilities into the Microsoft 365/Azure platform
B2B / B2C	Allows the enterprise to leverage AzureAD to provide secure B2B and B2C authentication
Azure Managed Security Service	Reduces the complexity of managing the complex and rapidly changing cloud environment off the enterprise's shoulders

Approach

- Founded in 2001 with the mission to Secure the Modern Enterprise
- The Modern Enterprise is transitioning from hybrid to all cloud
- These cloud platforms have security solutions powered by ML and AI
- To Secure the Modern Enterprise – these solutions must be implemented securely and with privacy as the guide post

Strategy



Planning

Coordination is KEY to success- often we find FAILED development and coordination of technology rollout leads to adoption failure

Focus on coordination and delivery so you can go back to work. Define technology owners, creating a sense of ownership and voice for each business unit

Create a list of action items, timelines, and milestones to ensure schedules and deadlines are met

Work as the liaison between interdependent business units, internal vertices, and technology partners to track success of each milestone

Thanks!