Microsoft

Data Security in Azure

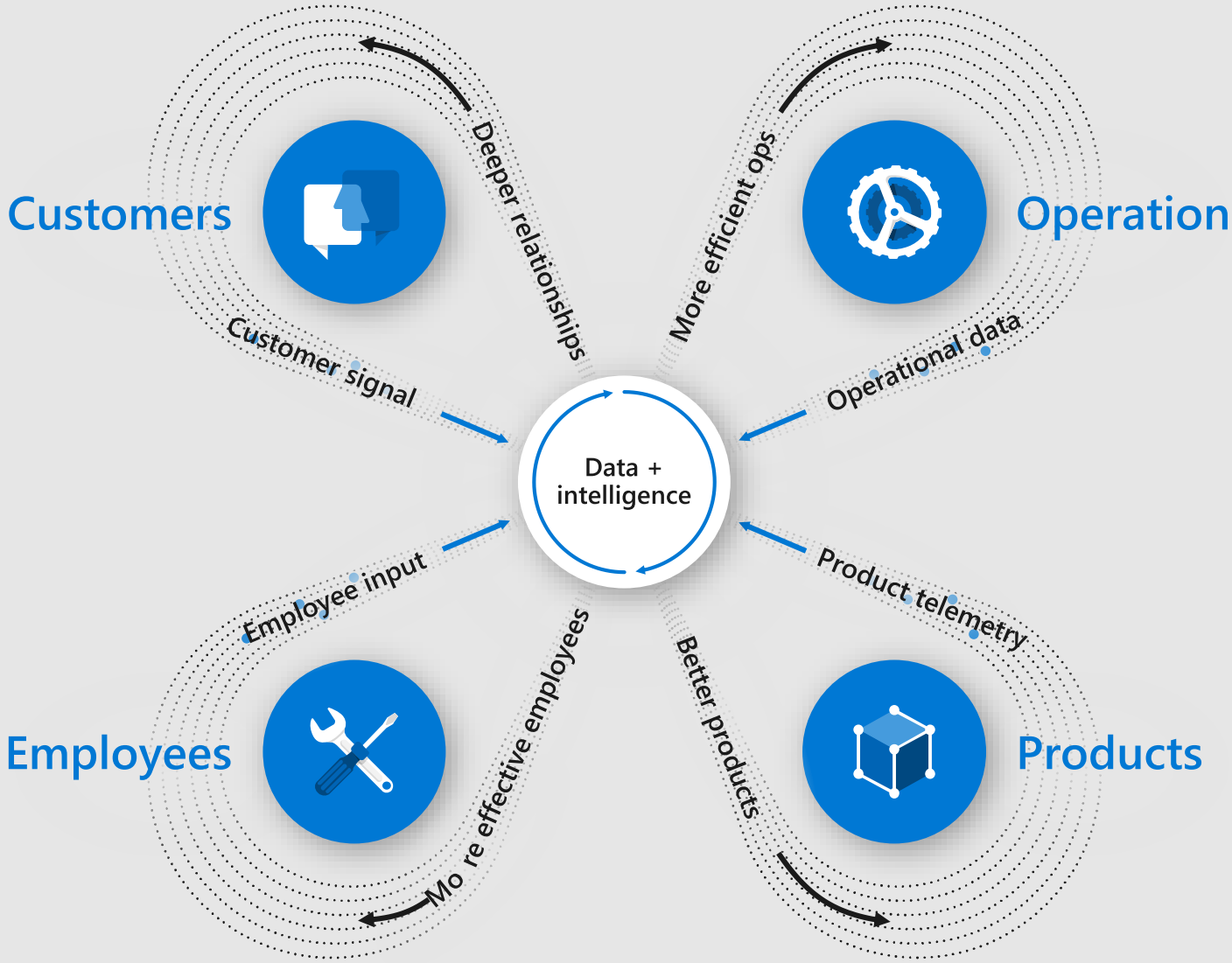
Srini Ambati

Cloud Solution Architect

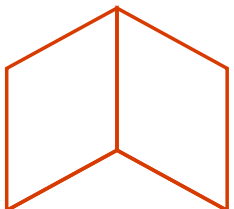
Srini.Ambati@Microsoft.com

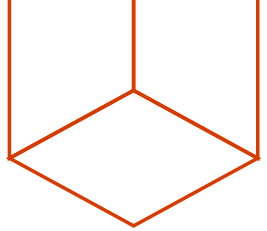
The digital feedback loop

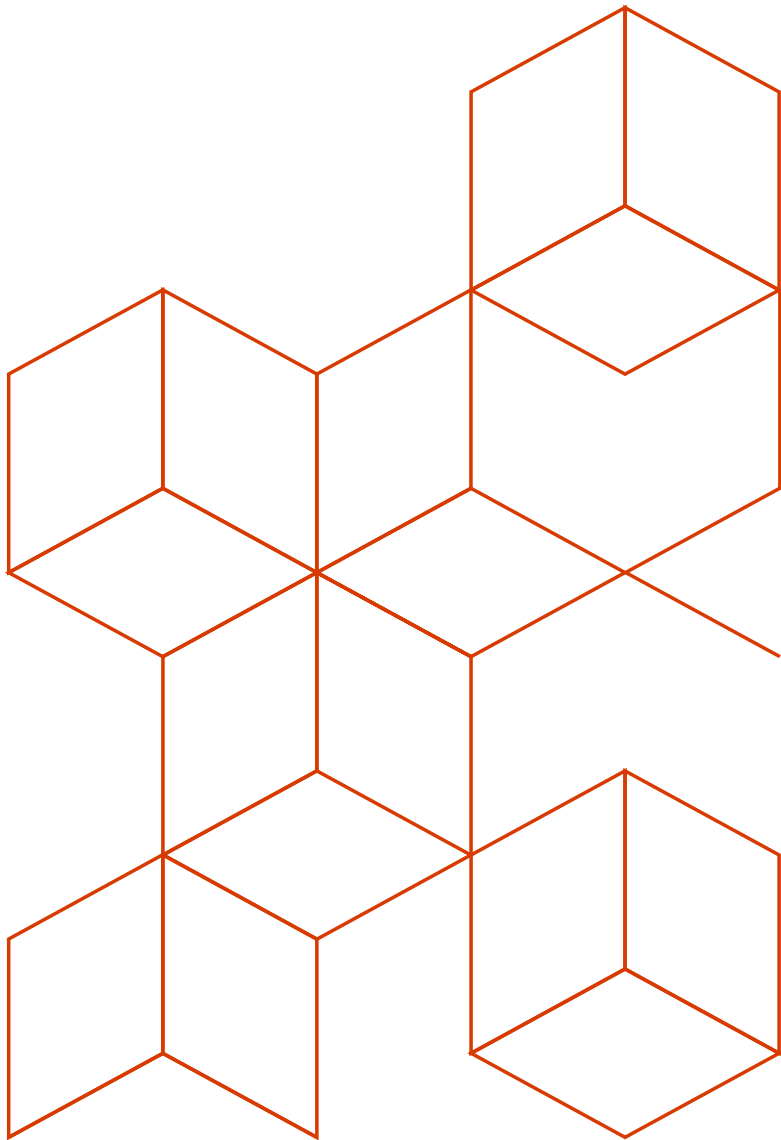
1. Data: Capture digital signal across business
2. Insight: Connect and synthesize data
3. Action: Improve business outcomes



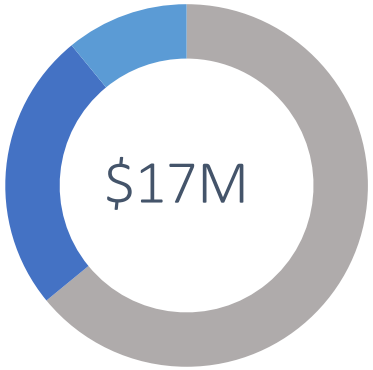
If information is gold, the datastore is a treasure chest.







The security landscape | Business impact



Average cost per business impact per security breach in the US[2]

On average before a cyberattack is detected[3]

$8 trillion

estimated damage costs from cybercrime by 2022[1]

1. Cybercrime & The Internet of Threats 2017 Whitepaper, Juniper Research
2. "Cyber crime: a risk you can manage – information management and governance to protect business innovation", softward.microfocus.com, 2016
3. "M-Trends 2017: A View From the Front Lines", FireEye.com, 2017

Insider Threat: Energy Heist

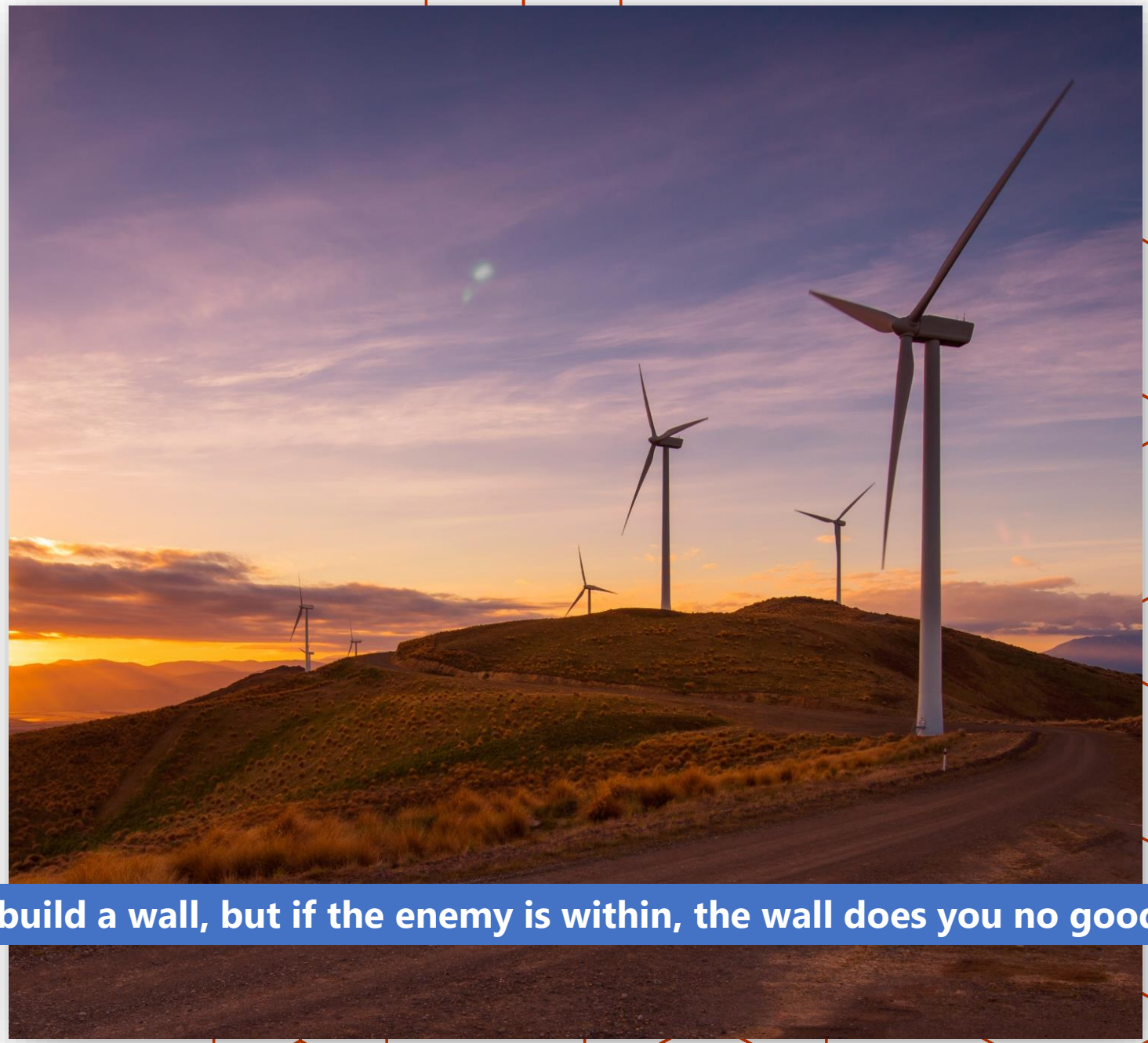
- Employee left clean energy company for foreign customer.
- Prior to leaving, downloaded code to an offsite computer for proprietary wind turbine technology.
- Customer retrofitted its turbines, saving a staggering **$800M**.

Insider Threat: Energy Heist

- Victim corporation lost **$1B+** in shareholder equity and 700 jobs (over half its global workforce).
- The customer nearly destroyed an American company by stealing its IP.

54% of breaches are caused by insiders.[1]

72% of CEOs have taken IP from a past employer.[2]



You can invest in a security perimeter and build a wall, but if the enemy is within, the wall does you no good.

[1] *Information Security Forum*

[2] *Code42 2018 Data Exposure Report*

History-Making Ransomware Heist

- WannaCry made the world sob.
- Used the EternalBlue SMB transport protocol vulnerability to spread at alarming rates around the world.
- Encrypted **176** different files on targets' endpoints; spread to other vulnerable endpoints.
- Also dropped Tor and other fun tech on the endpoints.

History-Making Ransomware Heist

- One of the most aggressive and widespread cyberattacks in history.
- **250,000+** victims across 150 countries
- **50M+ Bitcoin** paid to attackers
  (as of May 25, 2017)

46% of ransomware infections are caused by spam/phishing emails.[3]

#1 Ransomware and APTs are top concerns of IT and security teams.[4]

75% of CISOs agree – data security strategies need to include data recovery as well as prevention.[4]

3 *Raconteur, 2017*

4 *Code42 2018 Data Exposure Report*


WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
WAIT FOR IT
Enter your bank account number.
SCAM.
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.
Dilbert.com DilbertCartoonist@gmail.com
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick

World’s Largest Database Breached

- Tribune News Service reporters paid **500 rupees** for login credentials to a service offered by anonymous sellers over WhatsApp.
- The service allowed reporters to enter any Aadhaar number, a 12-digit unique identifier assigned to **every Indian citizen**.
- Reporters retrieved information – name, address, photo, phone number and email address – on queried citizens stored by UIDAI (Unique Identification Authority of India).

World's Largest Database Breached

- Compromised the personal information of **all 1.1 billion citizens** registered in India.
- Database info can be used to open bank accounts, buy a cellular SIM card, enroll in utilities or receive state aid.

$3.9M The global average cost of a data breach.[5]
(in millions of USD)

$148 The average cost for each lost or stolen record containing sensitive or confidential information in 2018.[6]

When collecting consumer PII data, organizations should enlist endpoint visibility tools to help protect it.

[5, 6] *IBM, Cost of a Data Breach study, conducted by Ponemon Institute 2018*

Starwood Guest Reservation Database Security Incident

Marriott International

Marriott has taken measures to investigate and address a data security incident involving the Starwood guest reservation database. This site has information concerning the incident, answers to guests' questions and steps you can take.

Updated: 4 January 2019

The initial announcement we made on November 30, 2018, about the Starwood guest reservation database security incident stated that there may have been information on up to 500 million guests involved. We also reported that for approximately 327 million of these guests, the information included some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, communication preferences, and encrypted payment card numbers.

When we made this announcement, our work analyzing the data involved was underway. Since that time, we have been working to remove duplicate information and to determine how many records had particular types of data present.

After further data analysis we have identified approximately 383 million records as the upper boundary for the total number of guest records that were involved in the incident. This does not, however, mean that information

starwood Hotels and Resorts

Starwood brands include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels. Starwood branded timeshare properties (Sheraton Vacation Club, Westin Vacation Club, The Luxury Collection Residence Club, St. Regis Residence Club, and Vistana) are also included.

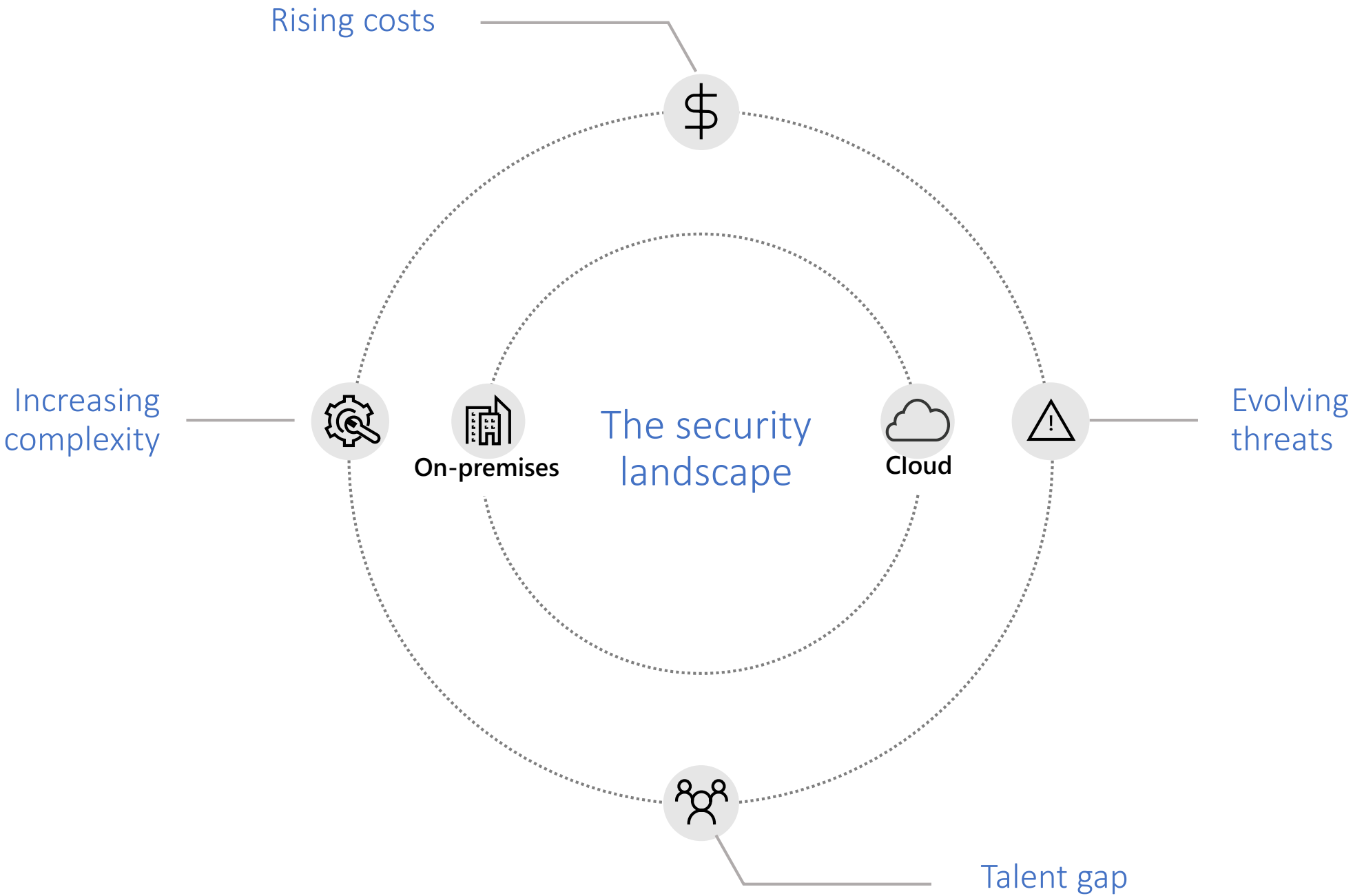
It all adds up…

Ransomware

Insider Threat

File Exfiltration

Your Data


Rising costs
Increasing complexity
On-premises
The security landscape
Cloud
Evolving threats
Talent gap

Key customer trends

Driving new management & security needs

Modernization

Application modernization to improve ROI is in full swing

Scale

Increased cloud adoption is driving the need to better organize and govern

Security

The cloud is now perceived as an asset in fighting evolving threats

Transformation

IT is transforming to play a more strategic role

The Microsoft Cloud -A Cloud You Can Trust

Security

The confidentiality, integrity, and availability of your data is protected.

Privacy & Control

No one can use your data in a way that you do not approve.

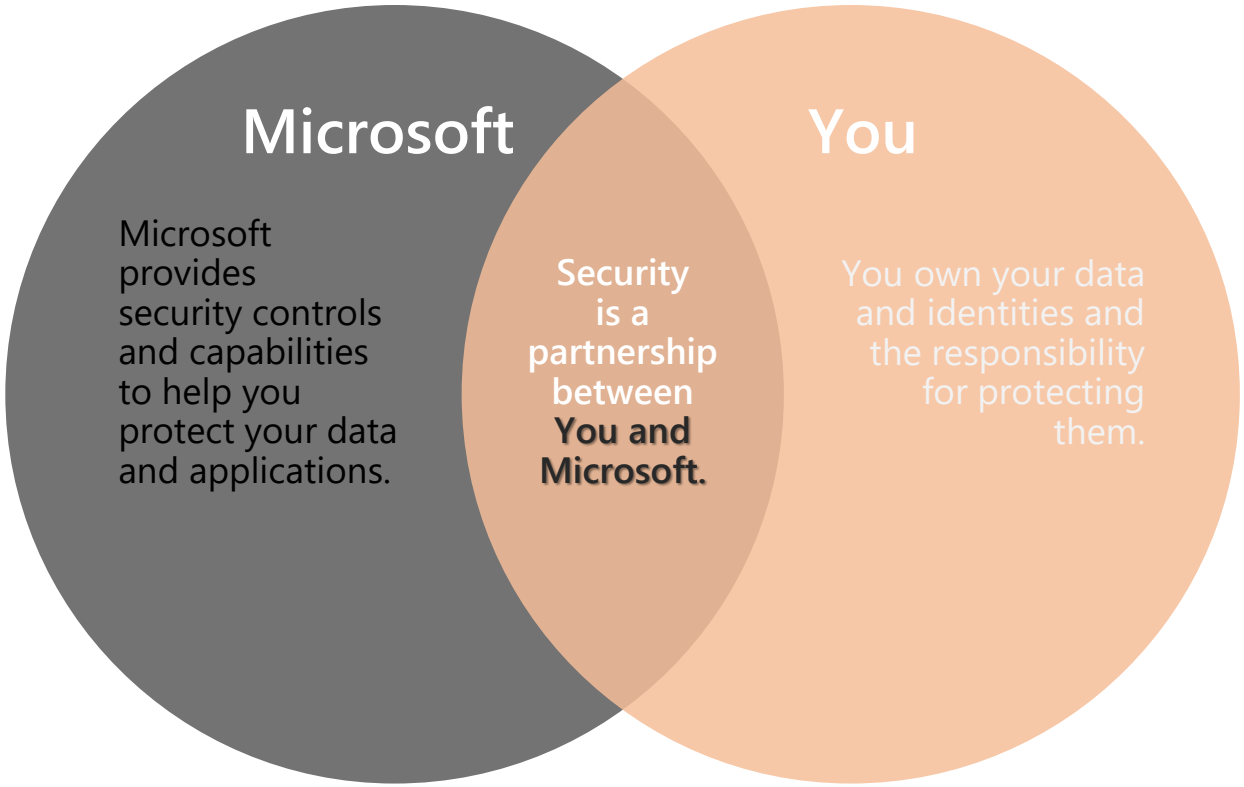
Compliance

Your content is stored and managed in compliance with applicable laws, regulations and standards.

Transparency

You have visibility into how your data is being handled and used.

Let’s partner on security



	Managed by Microsoft / Managed by Customer	On Prem	IaaS	PaaS	SaaS
Administration					
Applications					
Data					
Runtime					
Middleware					
Operating System					
Physical Host					
Physical Network					
Data Center					

95% of Fortune 500 business trust Microsoft Cloud

TEMENOS

"From a security point of view, I think Azure is a demonstrably more secure environment than most banks' datacenters."

— John Schlesinger, Chief Enterprise Architect

Adobe

"Azure complies with multiple international and industry security compliance standards and certifications that our customers demand. This allows us to offer our solutions in Azure with confidence."

— Brandon Pulsipher, Vice President of Technical Operation and Managed Services

---

Smithfield

"Microsoft has a great commitment to the problems of the enterprise. The security built into Azure is huge for us and ensures the safety of our data wherever it is."

— Julia Anderson, Global Chief Information Officer

MERRILL CORPORATION

"Building with the additional layer of Azure security, we feel we have a far better security posture than we could provide ourselves."

— Thomas Fredell, Chief Product Officer

icertis Applied Cloud

"Today, our operations team saves at least 30 percent of its time by using Security Center."

— Monish Darda, Co-founder and CTO

ASSUME BREACH

PROTECT

Security Development Lifecycle
Threat Modeling
Code Review
Security Testing
Network/User/Data/System security

DETECT

Auditing and Certification
Live Site Penetration Testing
Centralized Logging and Monitoring
Fraud and Abuse Detection

LEARN

Post-Breach Assessment

RESPOND

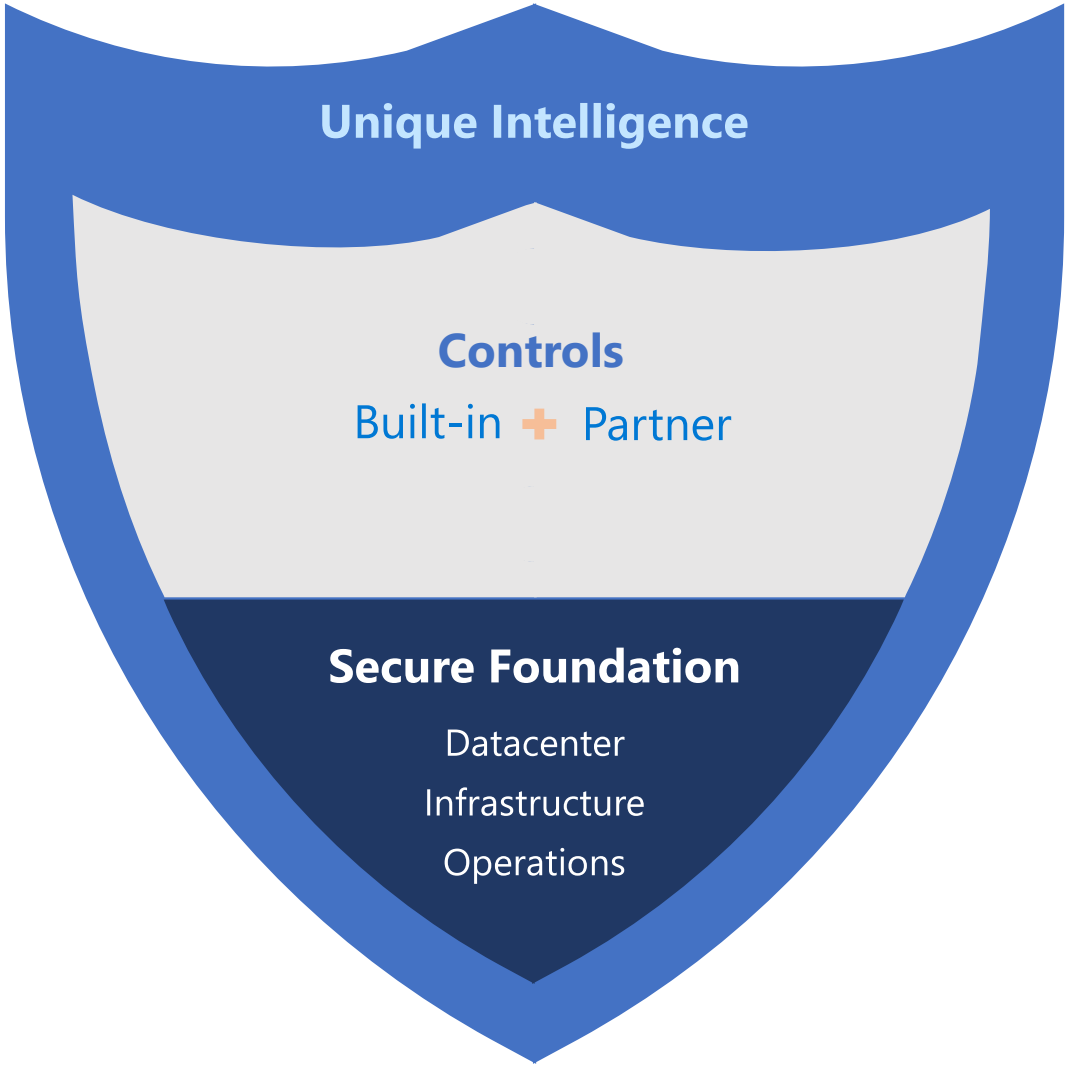
Breach Containment
Coordinated Security Response
Customer Notification

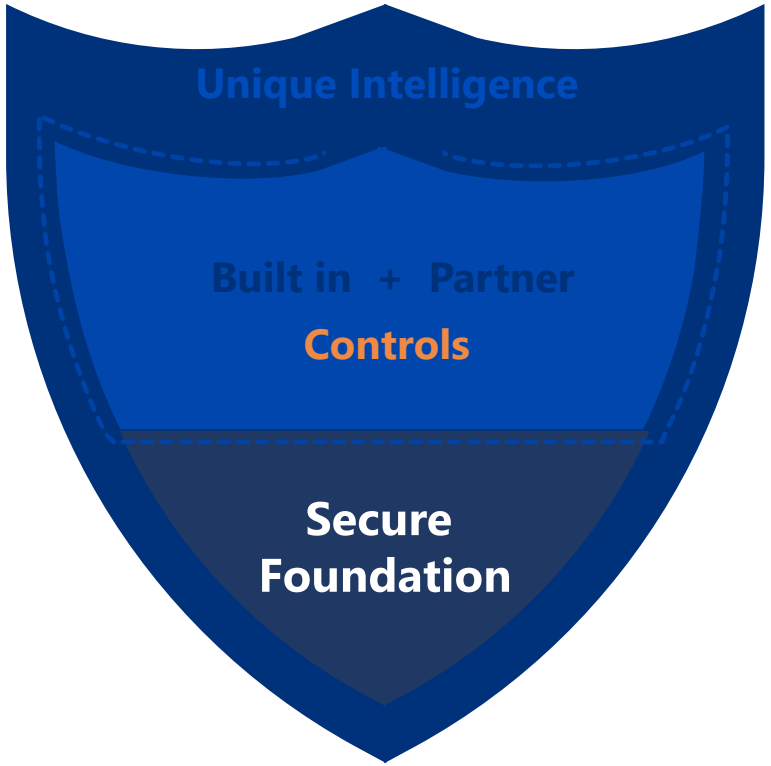
How Azure helps strengthen security

$1B+ annual investments

Over 3500 security experts

Trillions of diverse signals





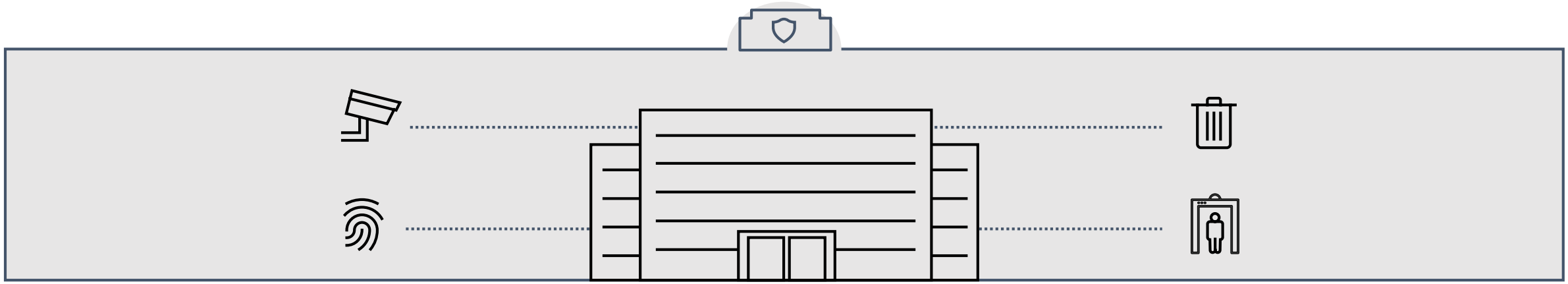
Industry leading security systems across global datacenters

Cloud infrastructure with custom hardware and platform level protections

Collectively secured with cutting edge operational security

Physical datacenter security

Secure foundation



Global datacenters designed and operated by Microsoft

Protected by industry leading security systems

Extensive layers of protection

Helps reduce unauthorized physical access

Extensive layers of protection

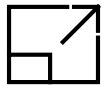
Physical datacenter security

Access approval

Background check

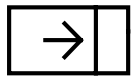
System check

Perimeter



Perimeter fencing

Front entrance gate



1 defined access point

Video coverage

Ongoing roaming patrols

Building

Two-factor authentication with biometrics

No building signage

Ongoing roaming patrols

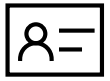
Video coverage

Verified single person entry

24x7x365 security operations

Server environment

Video coverage rack front & back



Employee & contractor vetting

Video coverage

Metal detectors

Inability to identify location of specific customer data

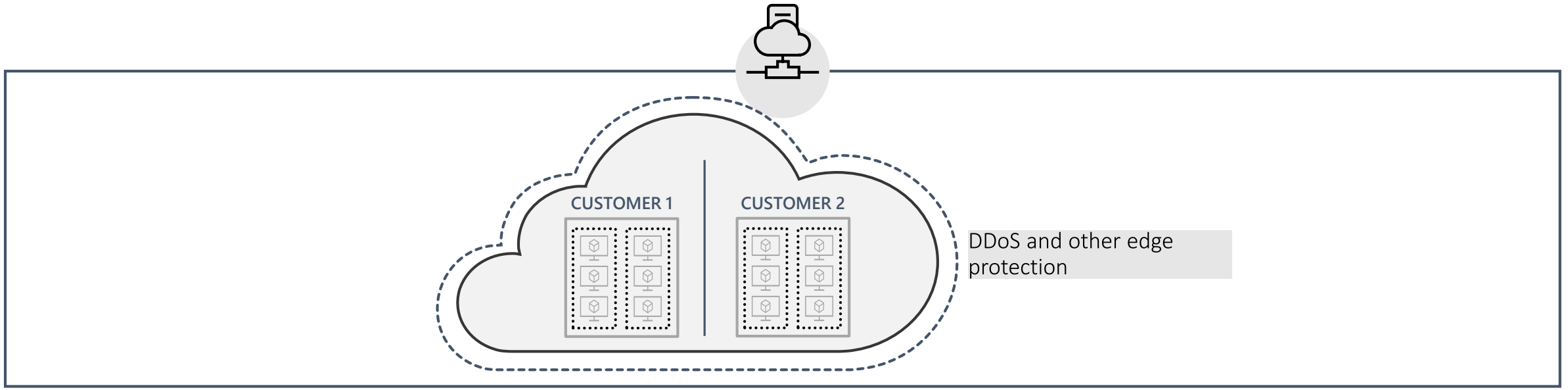
Two-factor authentication with biometrics

Ongoing roaming patrols

Secure destruction bins

Azure infrastructure security

Secure foundation



Protect customer data

Data, network segregation. DDoS protection at the edge. Platform segregation. Confidential computing.

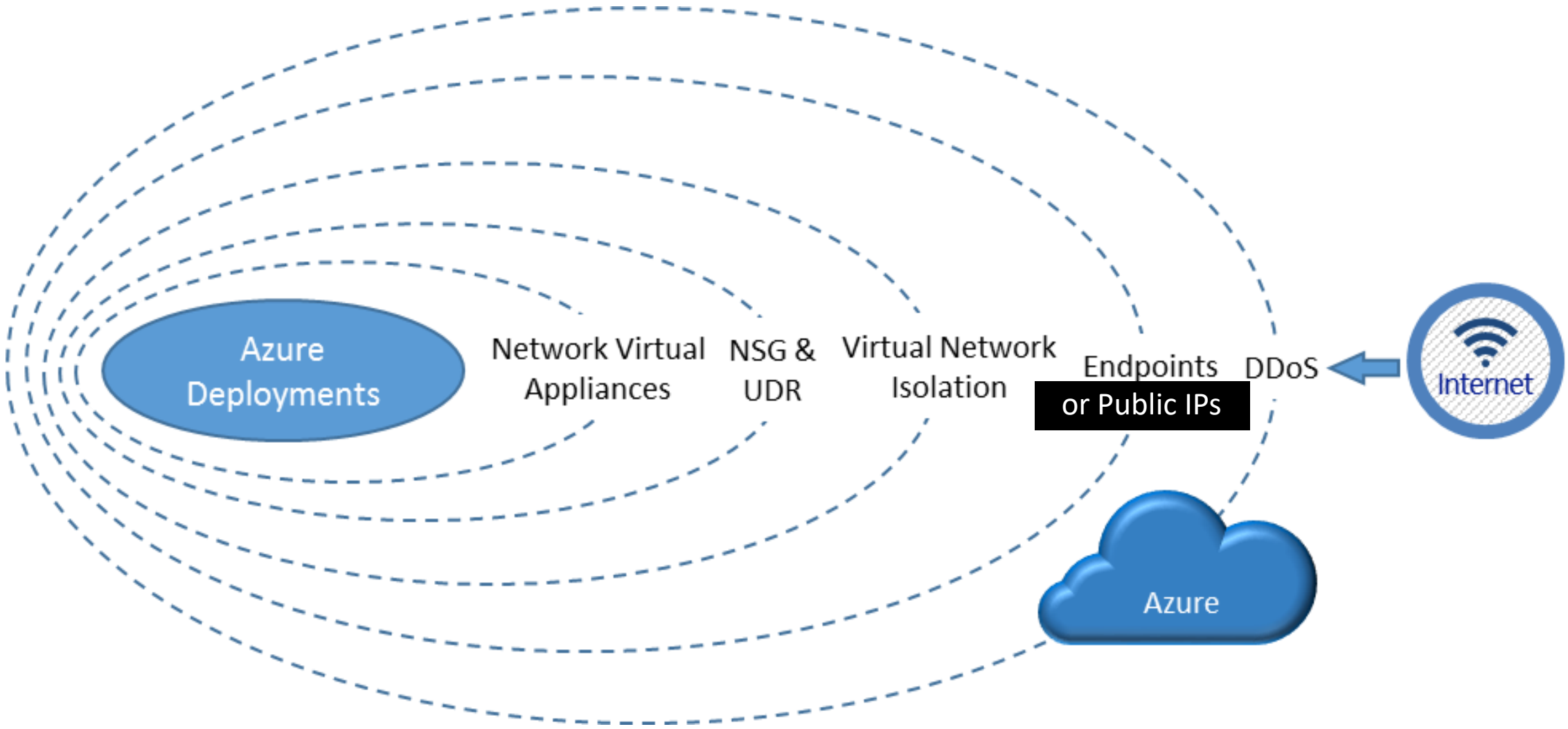
Secure hardware

Custom-built hardware with integrated security and attestation

Continuous testing

War game exercises by Microsoft teams, vulnerability scanning & continuous monitoring

Visualizing the security layers



Restricted access to production

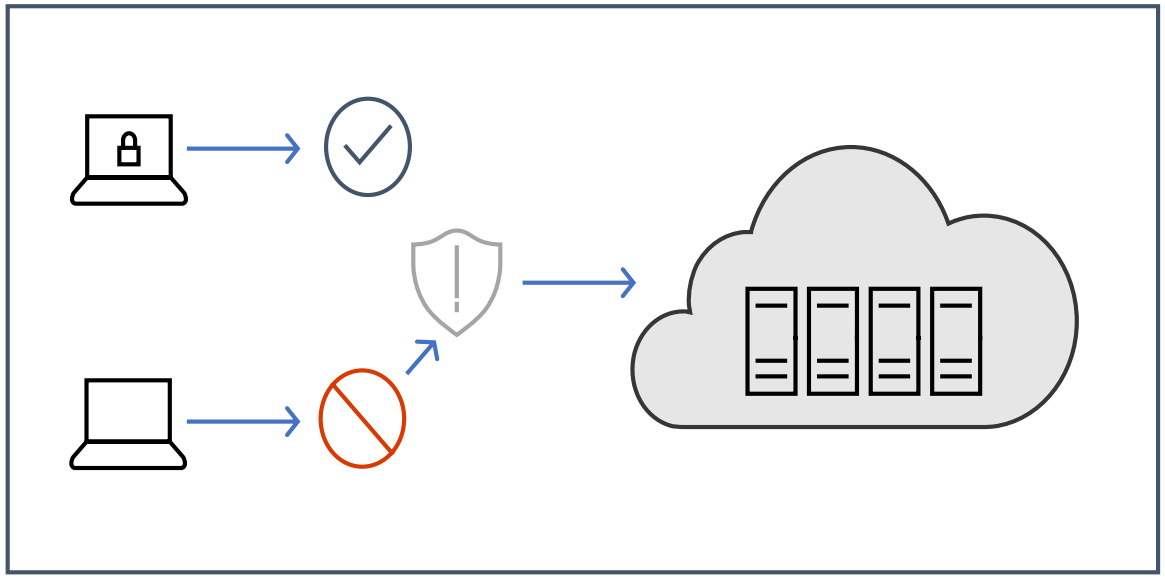
Operational Security

No standing access to production servers and services. Just In Time Elevation required.

Multi-factor authentication required for admin actions

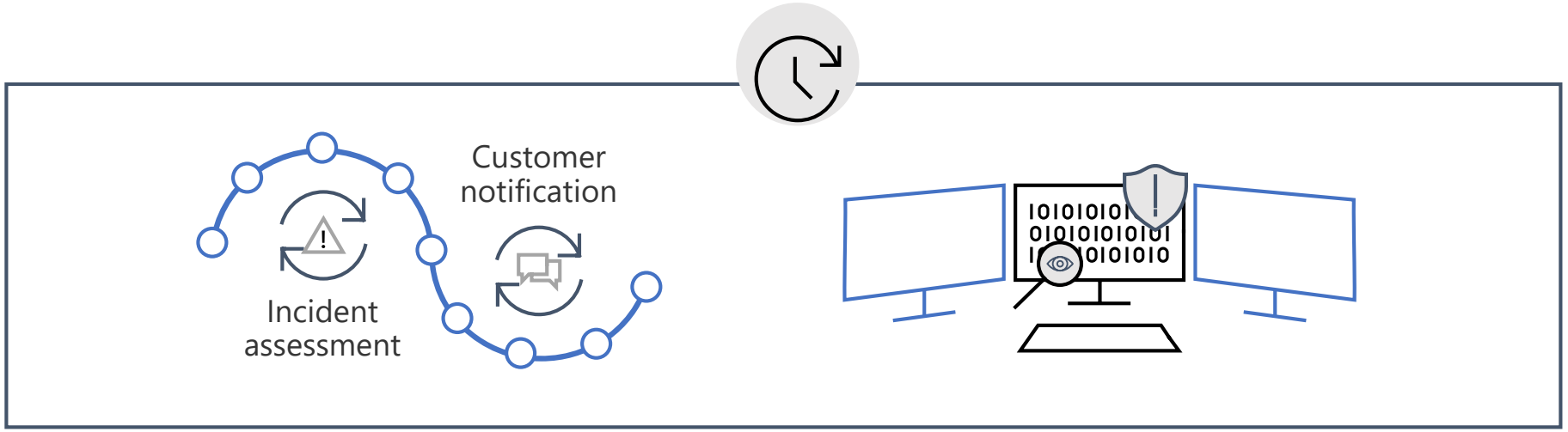
“Secure Workstations” required to access production

Access requests are audited, logged and monitored



Security Response and Monitoring

Secure foundation



Incident response

Multi-step incident response process

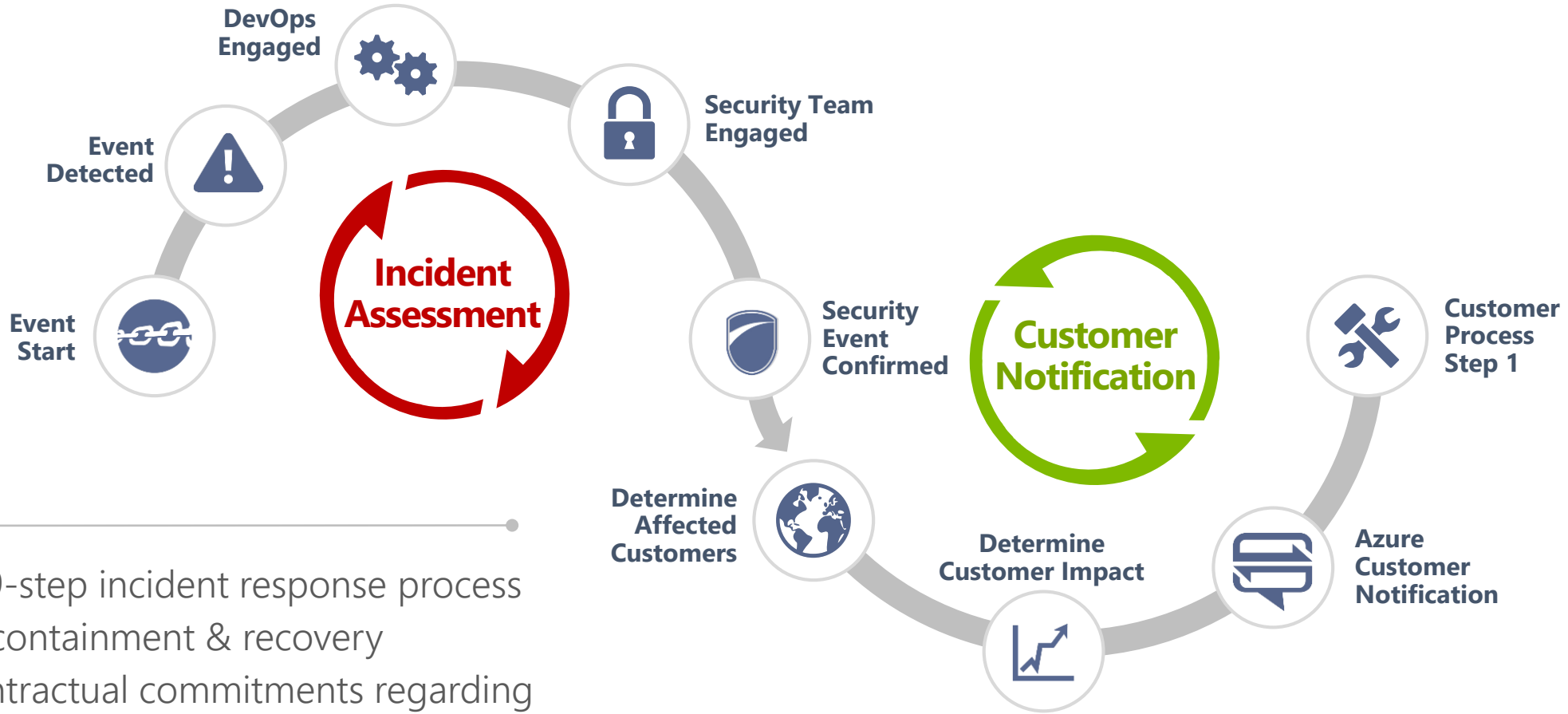
Focus on containment & recovery

3500+ security professionals

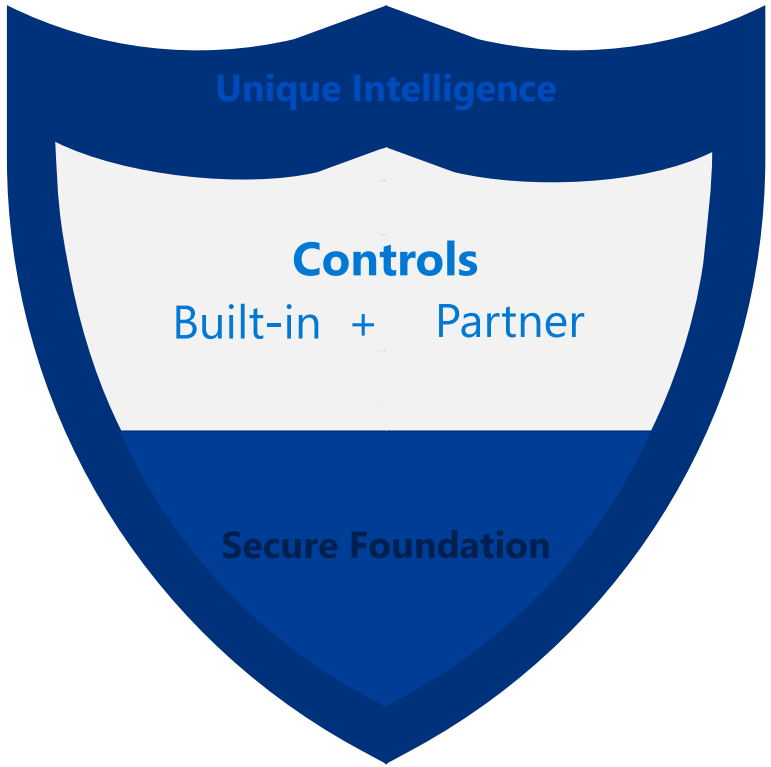
Working to harden, patch and protect the platform

24x7 monitoring for threats; emergency response drills

Incident Response



- ✓ In-depth 9-step incident response process
- ✓ Focus on containment & recovery
- ✓ Makes contractual commitments regarding customer notification + provides forensics



Defense in Depth

Identity & Access	Apps & Data Security	Network Security	Threat Protection	Security Management
Role based access	Encryption	DDoS Protection	Antimalware	Log Management
Multi-Factor Authentication	Confidential Computing	NG Firewall	AI Based Detection and Response	Security Posture Assessment
Central Identity Management	Key Management	Web App Firewall	Cloud Workload Protection	Policy and governance
Identity Protection	Certificate Management	Private Connections	SQL Threat Protection	Regulatory Compliance
Privileged Identity Management	Information Protection	Network Segmentation	IoT Security	SIEM

Microsoft + Partners

A corner of the cyber security landscape

Cybersecurity Reference Architecture

Microsoft

Software as a Service

Office 365
- ASM
- Lockbox

Information Protection
- Cloud App Security

Identity & Access
- Azure Active Directory
- Conditional Access
- Office 365 DLP
- AAD Identity Protection
- AAD PIM
- Multi-Factor Authentication
- Hello for Business
- MIM PAM
- ATA
- Active Directory
- Admin Forest
- Certification Authority (PKI)

Azure Information Protection (AIP)
- Classification Assistance
- Encryption
- Rights Management
- Document Tracking

Classification Labels

Structured Data & 3rd party Apps

Endpoint DLP

Windows Info Protection

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

Unmanaged & Mobile Clients

Intune MDM/MAM

Internet of Things

Vulnerability Management

Security Operations Center (SOC)

Logs & Analytics
- Managed Security Provider
- UEBA
- Analytics
- SIEM
- ATA
- OMS

Incident Response
- Investigation and Recovery

Active Threat Detection
- Hunting Teams
- Enterprise Threat Detection

SIEM Integration

Microsoft Azure

Azure Security Center
- Security Hygiene
- Threat Detection

Azure Key Vault

Azure App Gateway

Azure Antimalware

Network Security Groups

...

SQL Encryption & Firewall

Disk & Storage Encryption

DDoS attack prevention

Backup and Site Recovery

Extranet

On Premises Da...
- NGFW
- DLP
- SSL Proxy
- IPS
- Office 365 ATP
  - Email Gateway
  - Anti-malware

Express Route

Colocation

Security Appliances

VPN

Intranet

Enterprise Servers
- Shielded VMs
- VMs
- VMs
- Domain Controllers

Windows Server 2016 Security
Secure Boot, Nano Server, Just Enough Admin, Hyper-V Containers, Device Guard, Credential Guard, Remote Credential Guard, ...

VPN

Privileged Access Workstations

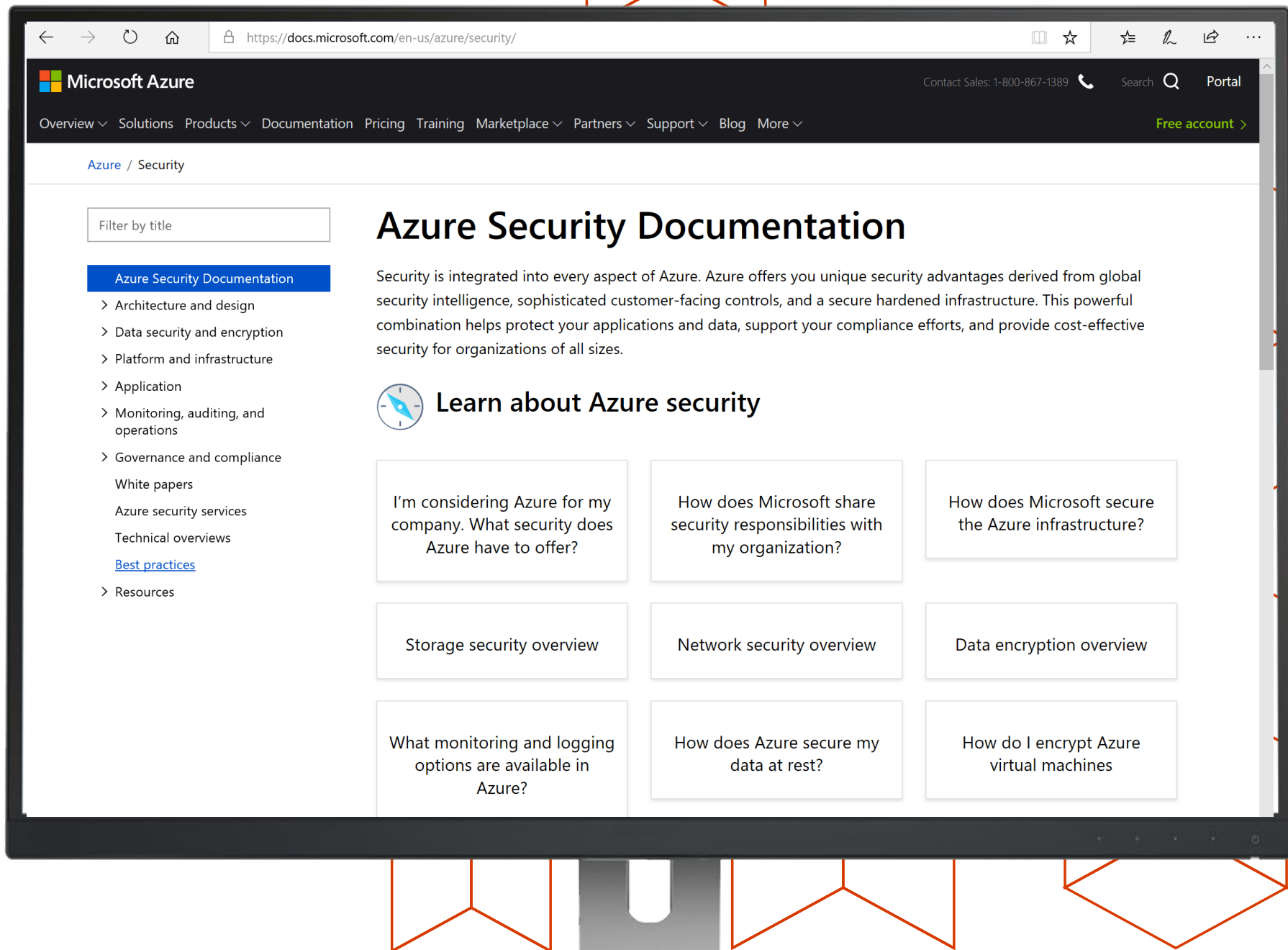
Managed Clients
- Sensitive Workloads
- Legacy Windows
- Windows 10
- Mac OS
- IoT
- EDR - Windows Defender ATP
- EPP - Windows Defender
- System Management + Patching (SCCM + Intune)

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

WEF

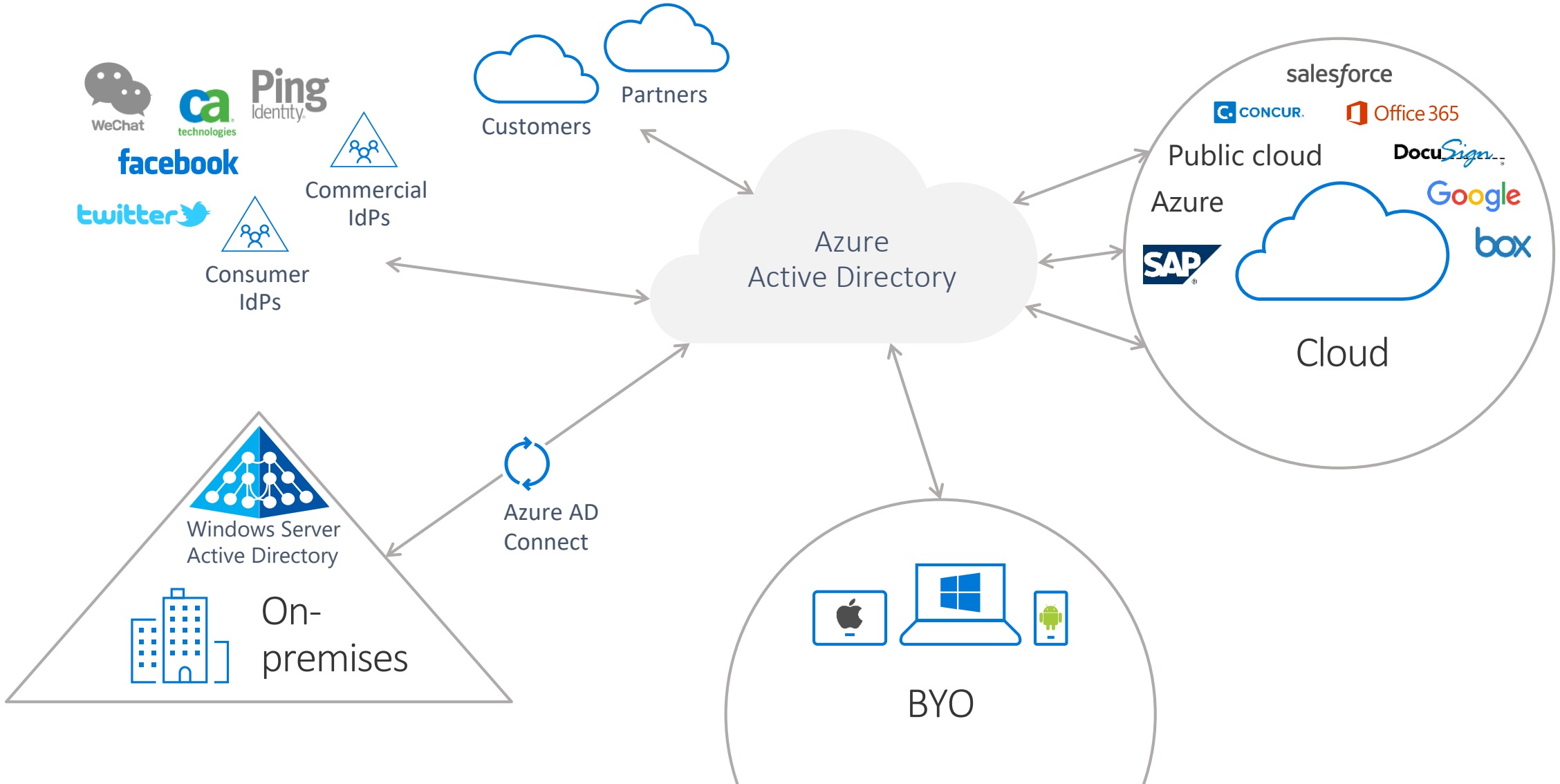
Nearly all customer breaches that Microsoft's Incident Response team investigates involve credential theft
63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

Demo


https://docs.microsoft.com/en-us/azure/security/
Microsoft Azure
Contact Sales: 1-800-867-1389
Search
Portal
Overview
Solutions
Products
Documentation
Pricing
Training
Marketplace
Partners
Support
Blog
More
Free account
Azure / Security
Filter by title
Azure Security Documentation
Architecture and design
Data security and encryption
Platform and infrastructure
Application
Monitoring, auditing, and operations
Governance and compliance
White papers
Azure security services
Technical overviews
Best practices
Resources
Azure Security Documentation
Security is integrated into every aspect of Azure. Azure offers you unique security advantages derived from global security intelligence, sophisticated customer-facing controls, and a secure hardened infrastructure. This powerful combination helps protect your applications and data, support your compliance efforts, and provide cost-effective security for organizations of all sizes.
Learn about Azure security
I'm considering Azure for my company. What security does Azure have to offer?
How does Microsoft share security responsibilities with my organization?
How does Microsoft secure the Azure infrastructure?
Storage security overview
Network security overview
Data encryption overview
What monitoring and logging options are available in Azure?
How does Azure secure my data at rest?
How do I encrypt Azure virtual machines

Identity is a new security control plane

Built-in Controls | Identity



Manage and control user identity and access

Built-in Controls | Identity

Extend on-premises directory to the cloud with single sign-on

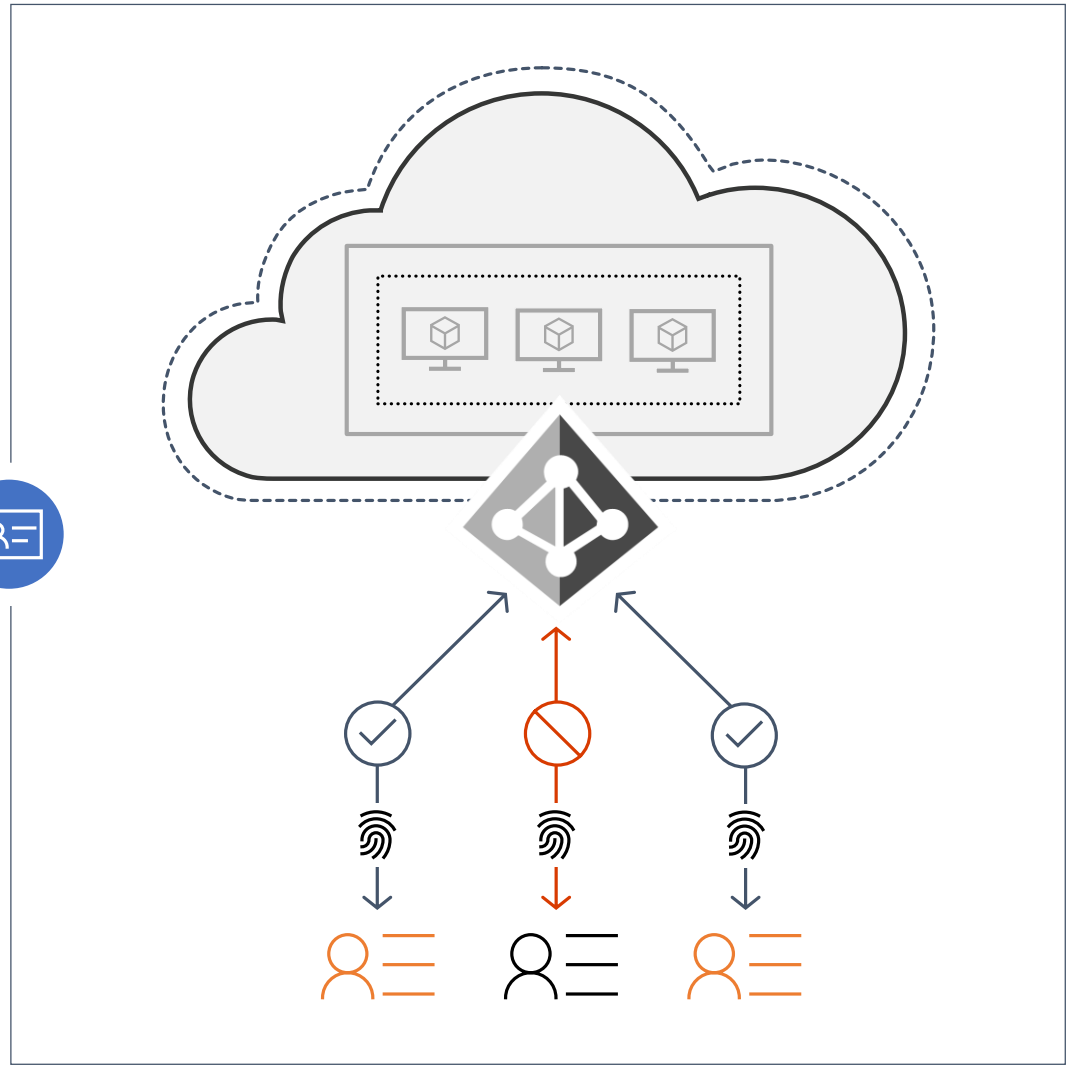
- Azure Active Directory Connect

Use principle of least privilege

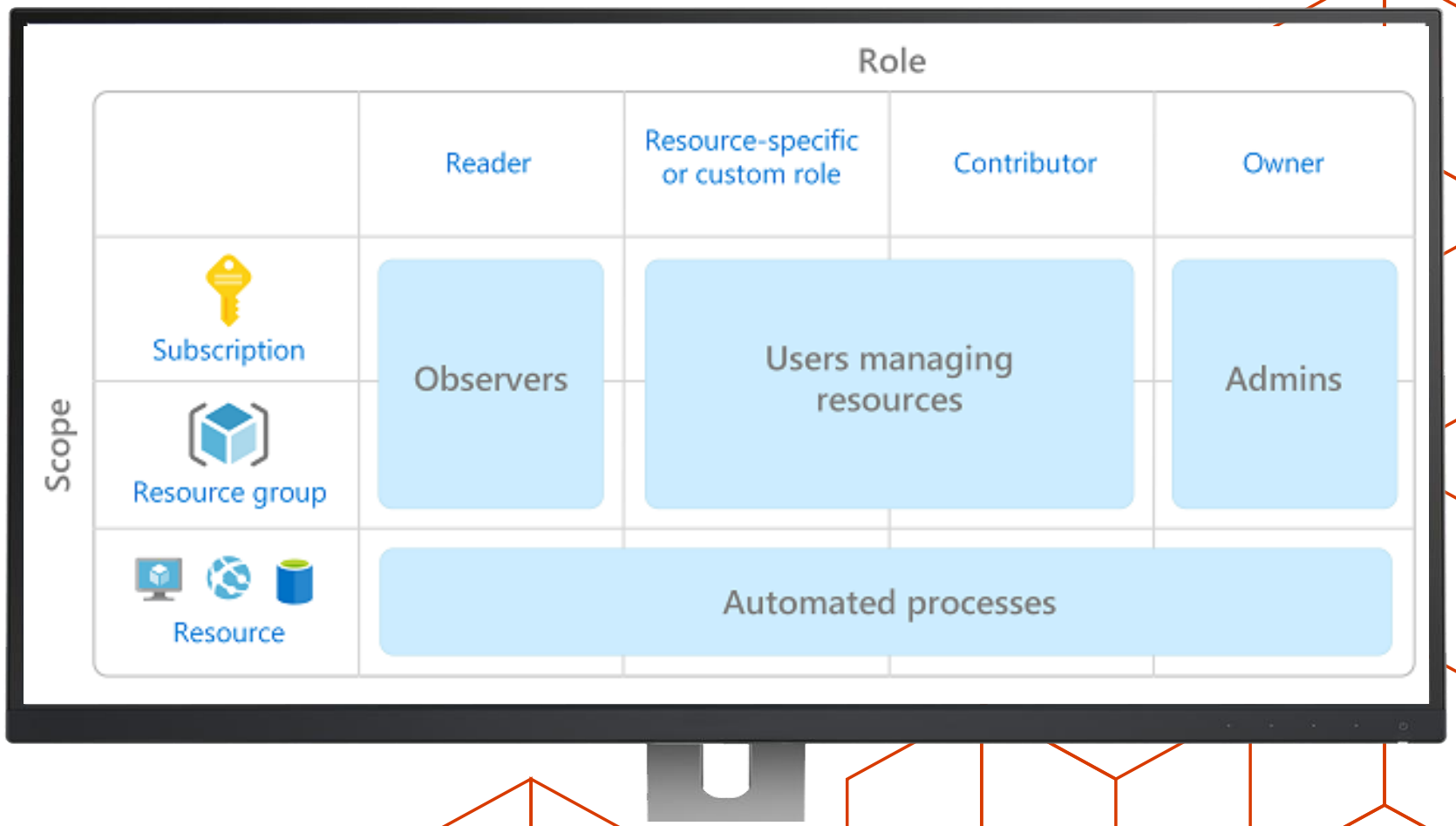
- Azure Role Based Access Control
- AAD Conditional Access policy

Enable additional identity protection

- Configure Multi-factor authentication
- Monitor and control privileged accounts with Azure AD PIM
- Enable additional threat protection with Azure AD Identity Protection



Demo


Role
Reader
Resource-specific or custom role
Contributor
Owner
Scope
Subscription
Resource group
Resource
Observers
Users managing resources
Admins
Automated processes

Data Protection

Data segregation

Logical isolation segregates each customer's data from that of others.

At-rest data protection

Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection

Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Encryption

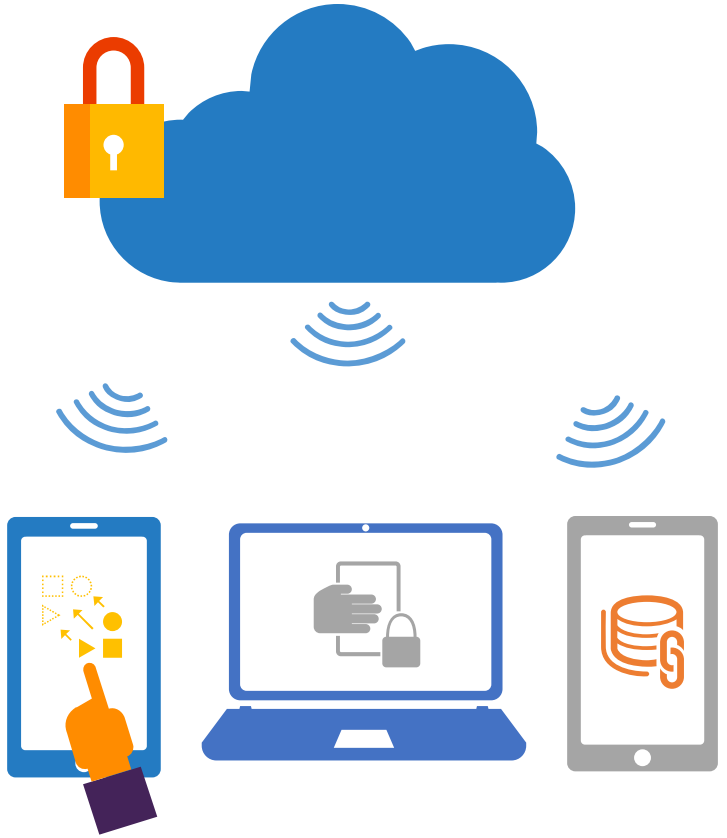
Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data redundancy

Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.

Data destruction

When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer's data inaccessible.



Protect data and communications

Built-in Controls | Data protection

Enable built-in encryption across resources

Azure Storage Service Encryption

Azure Disk Encryption

SQL TDE/Always Encrypted

Encrypt data while in use

Azure confidential computing

Use delegated access to storage objects

Shared Access Signature enables more granular access control

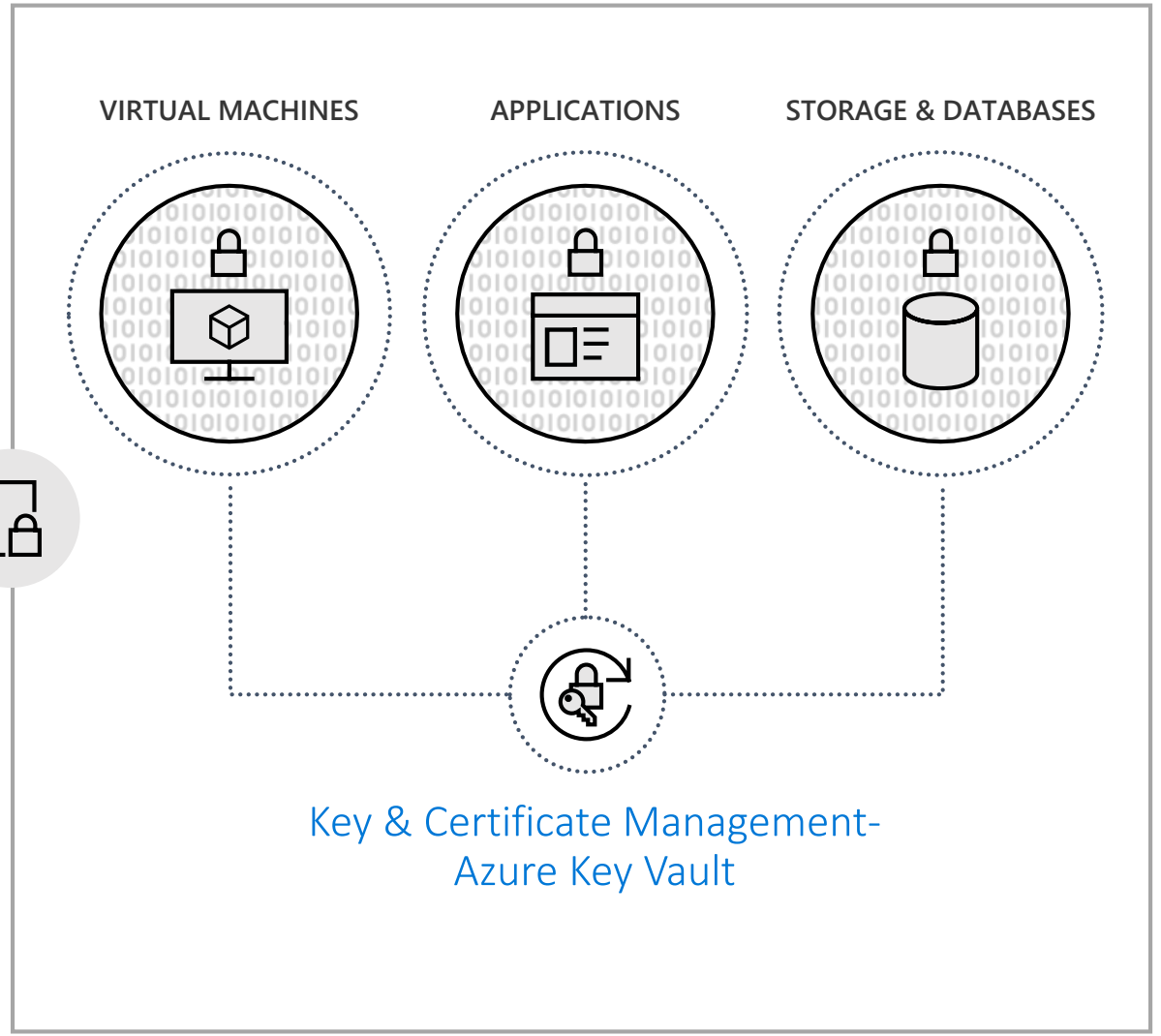
Use a key management system

Keep keys in a hardware HSM/don’t store key in apps/GitHub

Use one Key Vault per security boundary/per app/per region

Monitor/audit key usage-pipe information into SIEM for analysis/threat detection

Use Key Vault to enroll and automatically renew certificates



Network access control

Built-in Controls | Network security

Configure NSG and UDR Controls

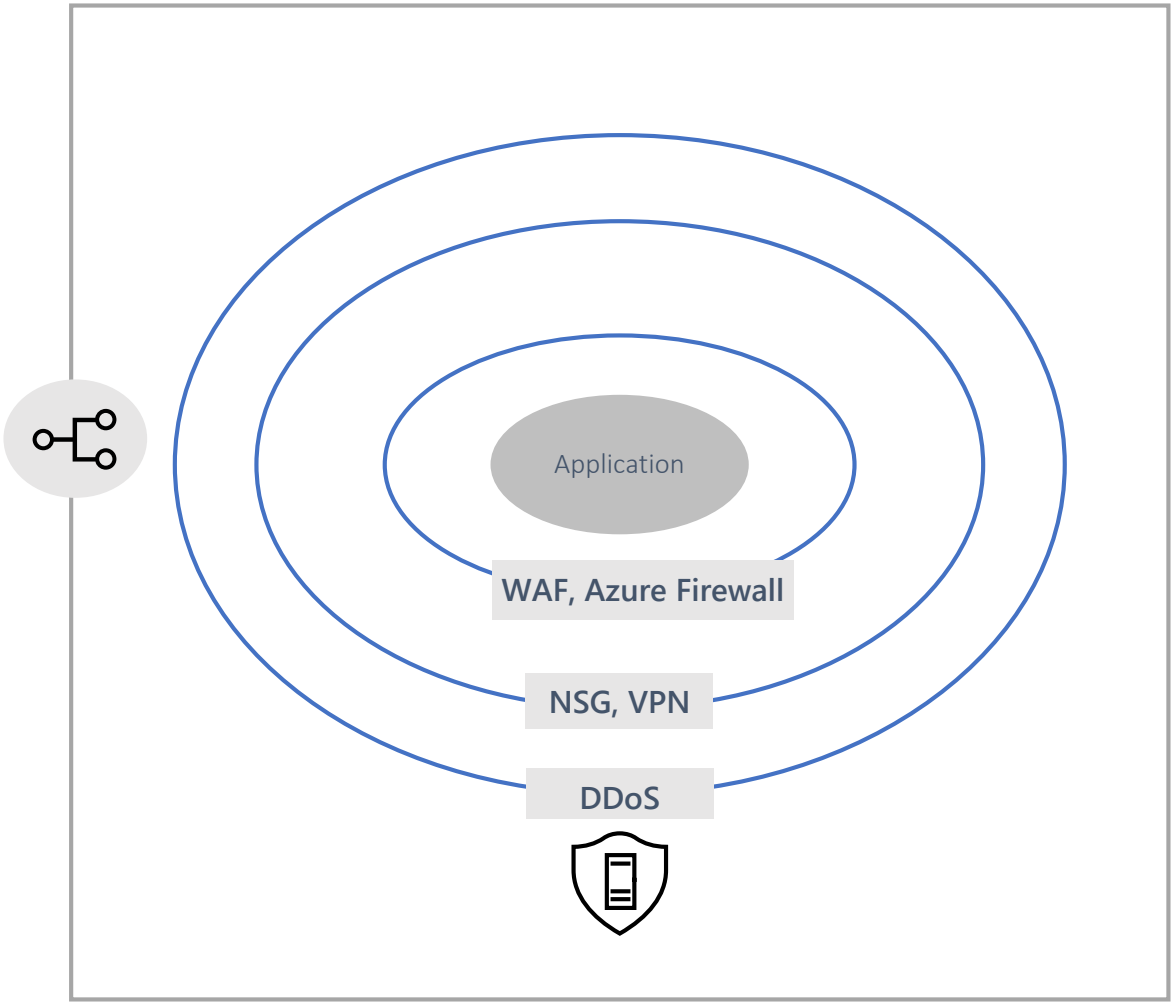
- Configure Network Security Groups for purpose built access
- Apply User Defined Routes to direct traffic
- Implement tiered rule sets

Add Network Virtual Appliances

- Use Virtual Network Appliance to enable additional filtering
- Use Web Application Firewall & network firewall
- Configure DDoS Protection to protect against targeted attacks

Configure Service Specific Rules

- Use application and server firewall rules
- Monitor network security policy per VM with Azure Security Center



Protect workloads against evolving attacks

Built-in Controls | Threat protection

Mitigate potential vulnerabilities proactively

Ensure up to date VMs with relevant security patches

Enable host anti-malware

Reduce surface area of attack

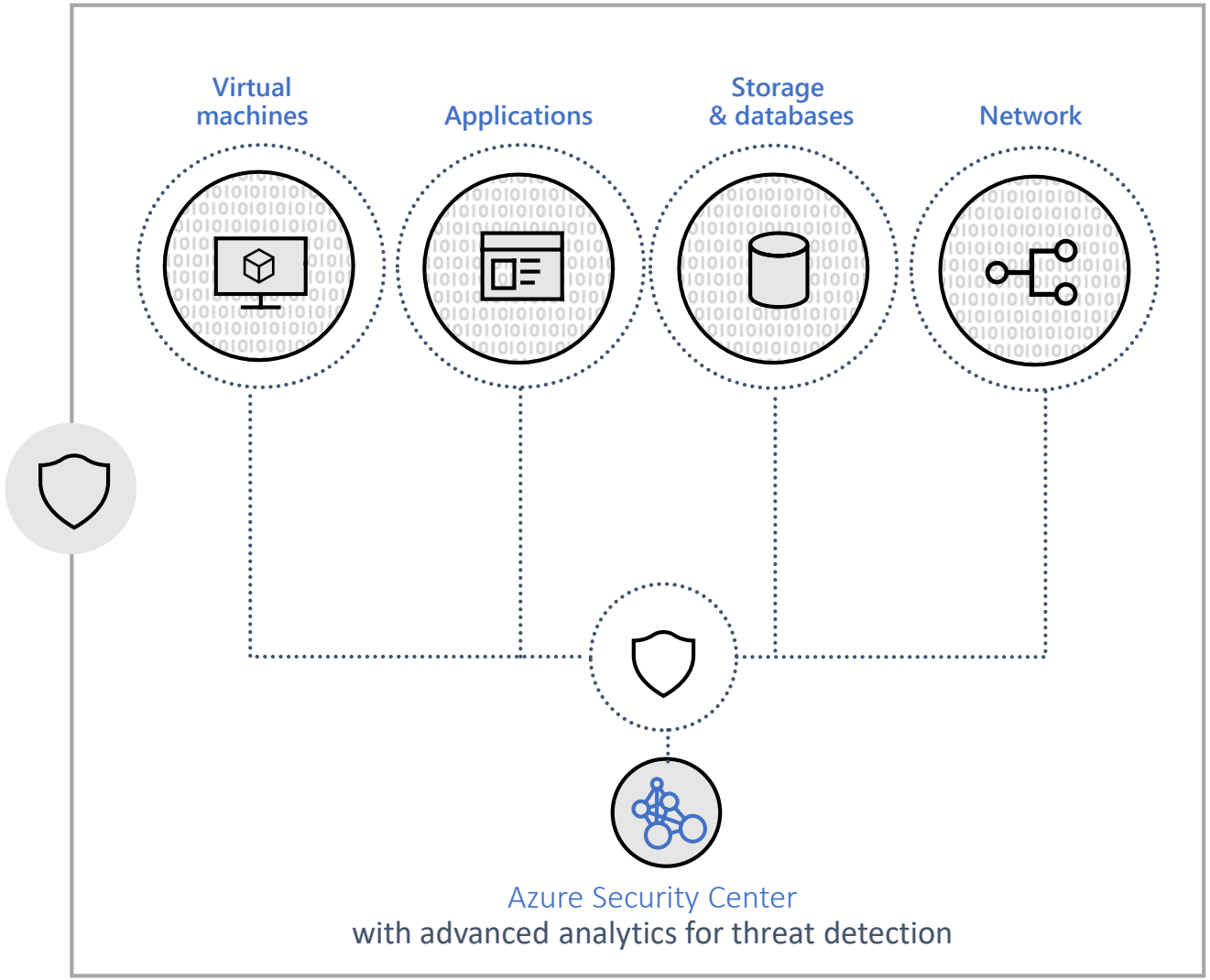
Enable just in time access to management ports

Configure Application Whitelisting to prevent malware execution

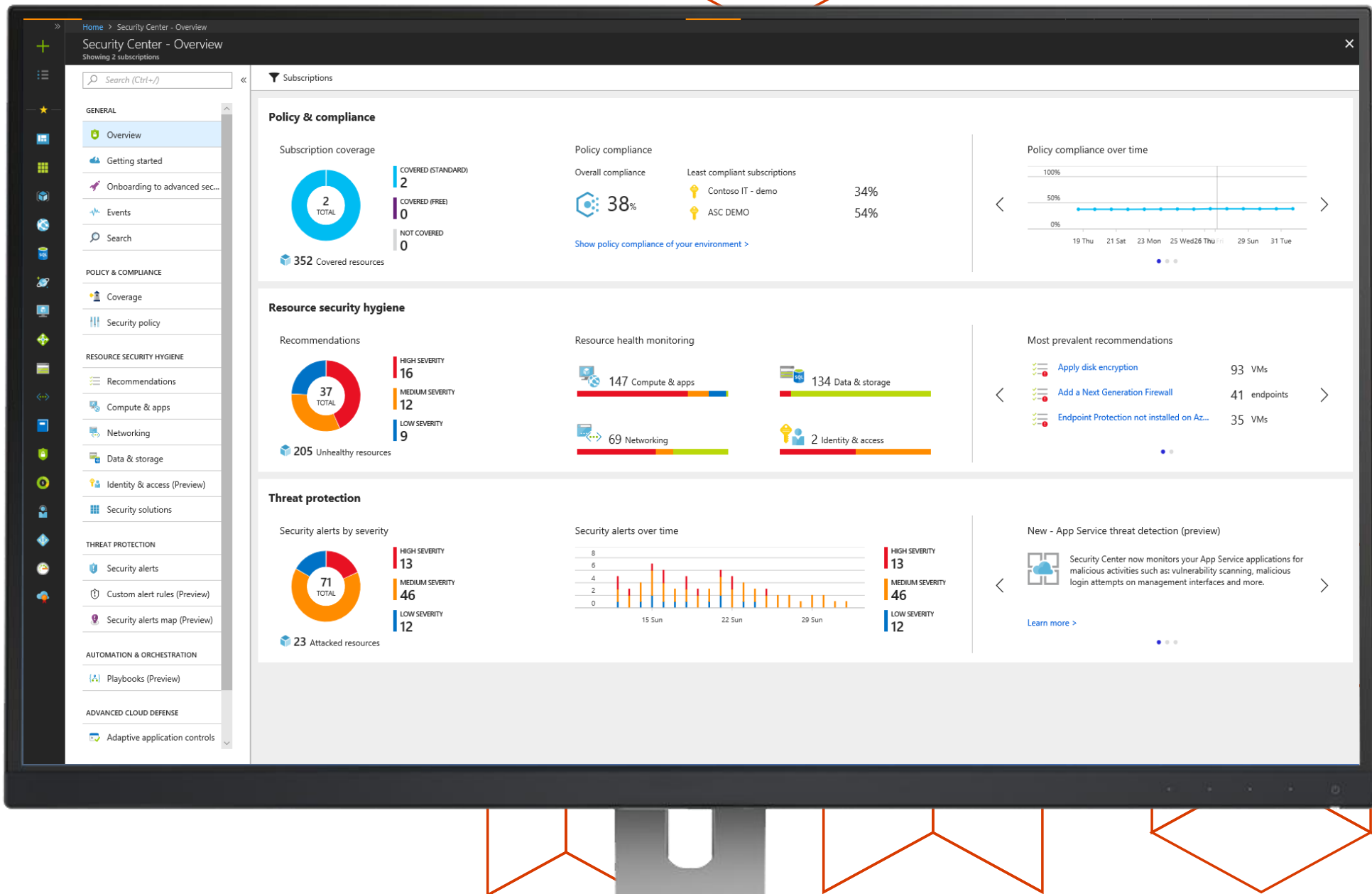
Detect threats early and respond faster

Use actionable alerts and incidents

Interactive investigation tool and playbooks to orchestrate responses



Demo


Home > Security Center - Overview
Security Center - Overview
Showing 2 subscriptions
Search (Ctrl+/)
GENERAL
Overview
Getting started
Onboarding to advanced sec...
Events
Search
POLICY & COMPLIANCE
Coverage
Security policy
RESOURCE SECURITY HYGIENE
Recommendations
Compute & apps
Networking
Data & storage
Identity & access (Preview)
Security solutions
THREAT PROTECTION
Security alerts
Custom alert rules (Preview)
Security alerts map (Preview)
AUTOMATION & ORCHESTRATION
Playbooks (Preview)
ADVANCED CLOUD DEFENSE
Adaptive application controls
Subscriptions
Policy & compliance
Subscription coverage
2 TOTAL
COVERED (STANDARD) 2
COVERED (FREE) 0
NOT COVERED 0
352 Covered resources
Policy compliance
Overall compliance
38%
Least compliant subscriptions
Contoso IT - demo 34%
ASC DEMO 54%
Show policy compliance of your environment >
Policy compliance over time
100%
50%
0%
19 Thu
21 Sat
23 Mon
25 Wed
26 Thu
29 Sun
31 Tue
Resource security hygiene
Recommendations
37 TOTAL
HIGH SEVERITY 16
MEDIUM SEVERITY 12
LOW SEVERITY 9
205 Unhealthy resources
Resource health monitoring
147 Compute & apps
134 Data & storage
69 Networking
2 Identity & access
Most prevalent recommendations
Apply disk encryption 93 VMs
Add a Next Generation Firewall 41 endpoints
Endpoint Protection not installed on Az... 35 VMs
Threat protection
Security alerts by severity
71 TOTAL
HIGH SEVERITY 13
MEDIUM SEVERITY 46
LOW SEVERITY 12
23 Attacked resources
Security alerts over time
8
6
4
2
0
15 Sun
22 Sun
29 Sun
HIGH SEVERITY 13
MEDIUM SEVERITY 46
LOW SEVERITY 12
New - App Service threat detection (preview)
Security Center now monitors your App Service applications for malicious activities such as: vulnerability scanning, malicious login attempts on management interfaces and more.
Learn more >

Enable visibility and control across hybrid workloads

Built-in Controls | Security Management

Enable centralized view of security state across cloud and on-premises workloads

Monitor security across all subscriptions and environments

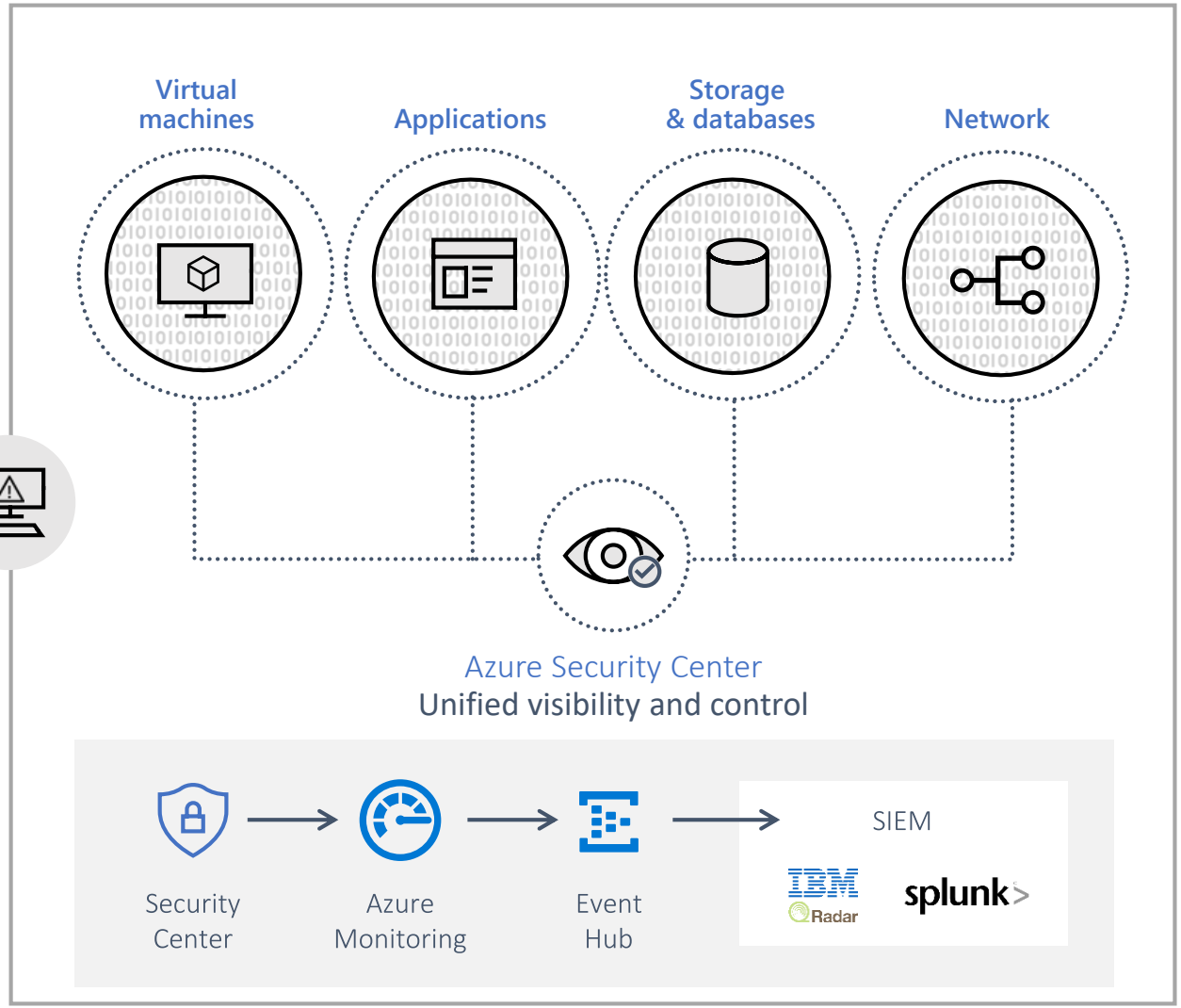
Ensure compliance to your requirements

Configure centralized security policy and view compliance score across different resources in a central dashboard

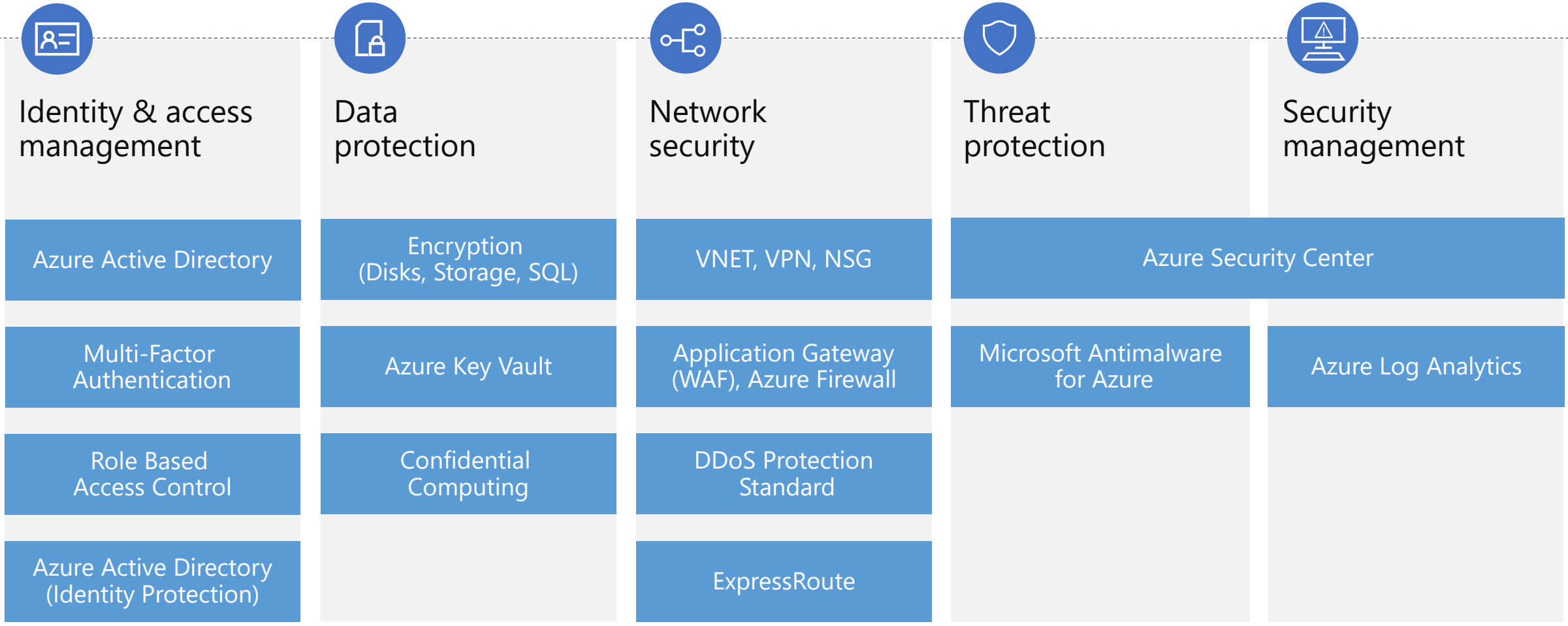
Integrate auditing, logging with existing processes

Configure auditing, logging and use Log Analytics for advanced analysis

Export security data to existing SIEM solutions



Simplify security management with Azure services



Extend your existing security solution to Azure with Marketplace

Partner Solutions

Identity & access management

RSA

Omada

PingIdentity.

DUO

SailPoint

Data protection

gemalto
security to be free

SafeNet
The Foundation of Information Security

THALES

SECURED BY CRYPTERON

Network security

Palo Alto Networks

Check Point
SOFTWARE TECHNOLOGIES LTD.

f5

CISCO

Barracuda

Threat protection

Symantec

McAfee

Qualys Inc

RAPID7

aqua

Security management

HPE ArcSight

Splunk

IBM QRadar

ALERT LOGIC

And **hundreds** more with new partners integrating every month

https://aka.ms/AzureCompliance

Azure covers 91 compliance offerings

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

Global

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 22301:2012
- ISO 9001:2015
- ISO 20000-1:2011
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CIS Benchmark
- CSA STAR Certification
- CSA STAR Attestation
- CSA STAR self-assessment
- WCAG 2.0 (ISO 40500:2012)

US Gov

- FedRAMP high
- FedRAMP moderate
- EAR
- ITAR
- DoD DISA SRG Level 5
- DoD DISA SRG Level 4
- DoD DISA SRG Level 2
- DFARS
- DoE 10 CFR Part 810
- NIST SP 800-171
- NIST CSF
- Section 508 VPATs
- FIPS 140-2
- CJIS
- IRS 1075
- CNSSI 1253

Industry

- PCI DSS Level 1
- GLBA (US)
- FFIEC (US)
- Shared assessments (US)
- SEC 17a-4 (US)
- CFTC 1.31 (US)
- FINRA 4511 (US)
- SOX (US)
- 23 NYCRR 500 (US)
- OSFI (Canada)
- FCA + PRA (UK)
- APRA (Australia)
- FINMA (Switzerland)
- FSA (Denmark)
- RBI + IRDAI (India)
- MAS + ABS (Singapore)
- NBB + FSMA (Belgium)
- AFM + DNB (Netherlands)
- AMF + ACPR (France)
- KNF (Poland)
- European Banking Authority (EBA)
- FISC (Japan)
- HIPAA BAA (US)
- HITRUST certification
- GxP (FDA 21 CFR Part 11)
- MARS-E (US)
- NHS IG Toolkit (UK)
- NEN 7510:2011 (Netherlands)
- FERPA (US)
- CDSA
- MPAA (US)
- FACT (UK)
- DPP (UK)
- TISAX (Germany)

Regional

- Argentina PDPA
- Australia IRAP Unclassified
- Australia IRAP PROTECTED
- Canada Privacy Laws
- China GB 18030:2005
- China DJCP (MLPS) Level 3
- China TRUCS/CCCPPF
- EU EN 301 549
- EU ENISA IAF
- EU model clauses
- EU—US privacy shield
- GDPR
- Germany C5
- Germany IT—Grundschutz workbook
- India MeitY
- Japan CS mark gold
- Japan my number act
- Netherlands BIR 2012
- New Zealand Gov CIO Framework
- Singapore MTCS Level 3
- Spain ENS High
- Spain DPA
- UK cyber essentials plus
- UK G-Cloud
- UK PASF
- Korea K-ISMS
- France HDS

Azure SQL Security

Use Cases for Azure SQL

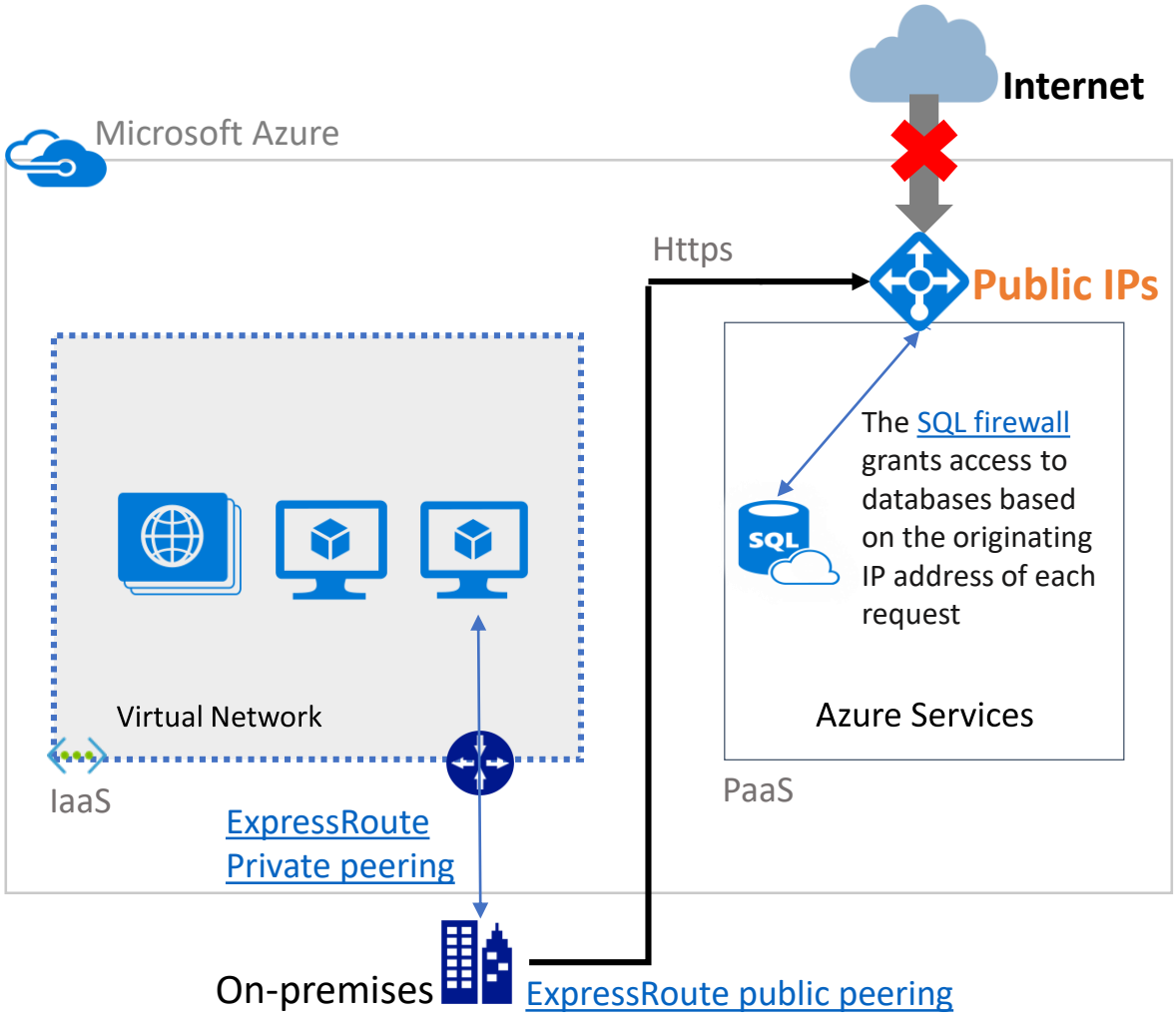
Access Azure SQL from on premise Applications

Access Azure SQL from Azure Applications hosted on IaaS

Access Azure SQL from Azure Applications hosted on PaaS

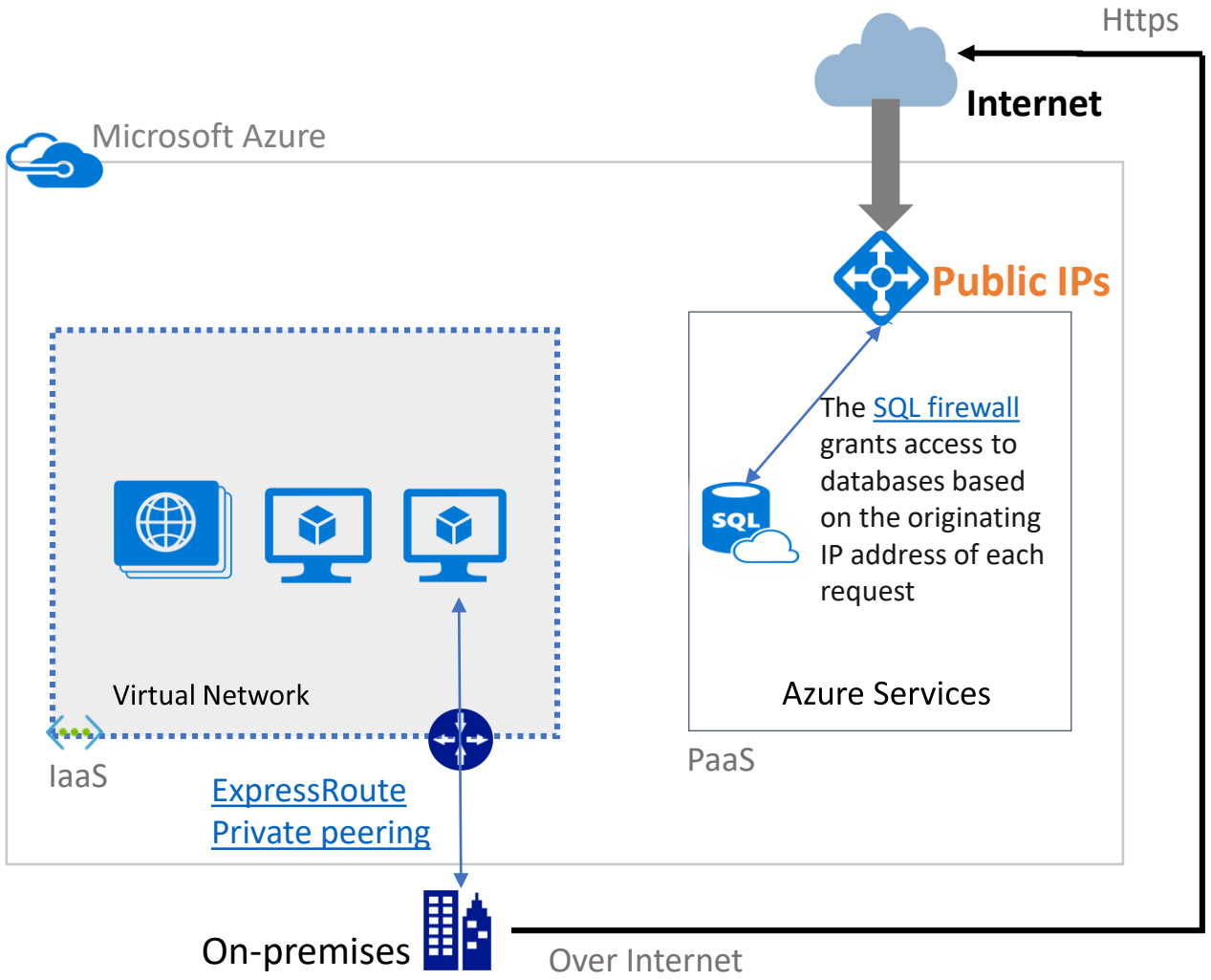
Access Azure SQL from on premise Applications

Option 1



Access Azure SQL from on premise Applications

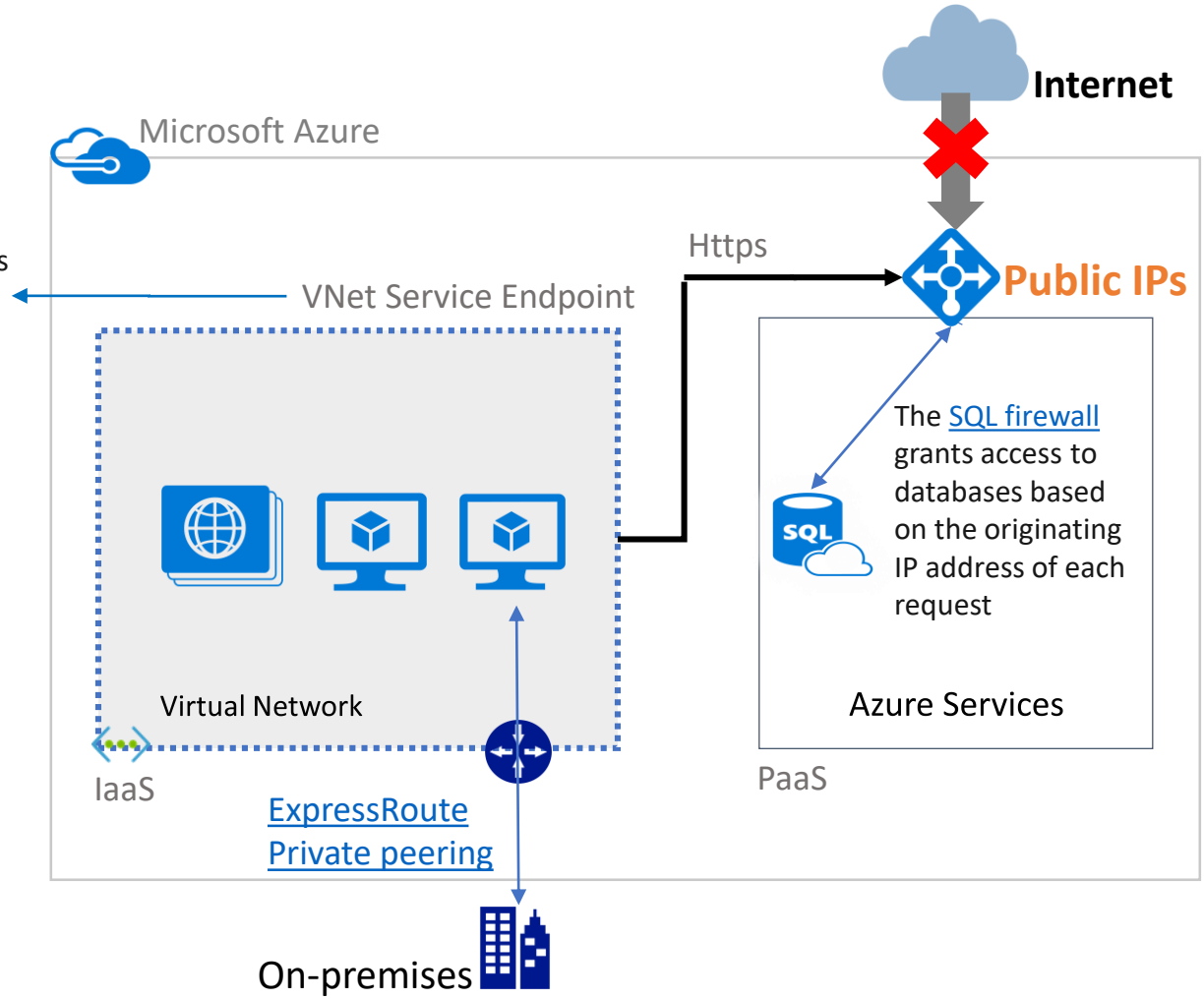
Option 2



Access Azure SQL from Azure Applications hosted on IaaS

Option 1

VNet Service Endpoint allows you to isolate connectivity to your logical server from only a given subnet or set of subnets within your virtual network. The traffic to Azure SQL Database from your VNet will always stay within the Azure backbone network. This direct route will be preferred over any specific routes that take Internet traffic through virtual appliances or on-premises.

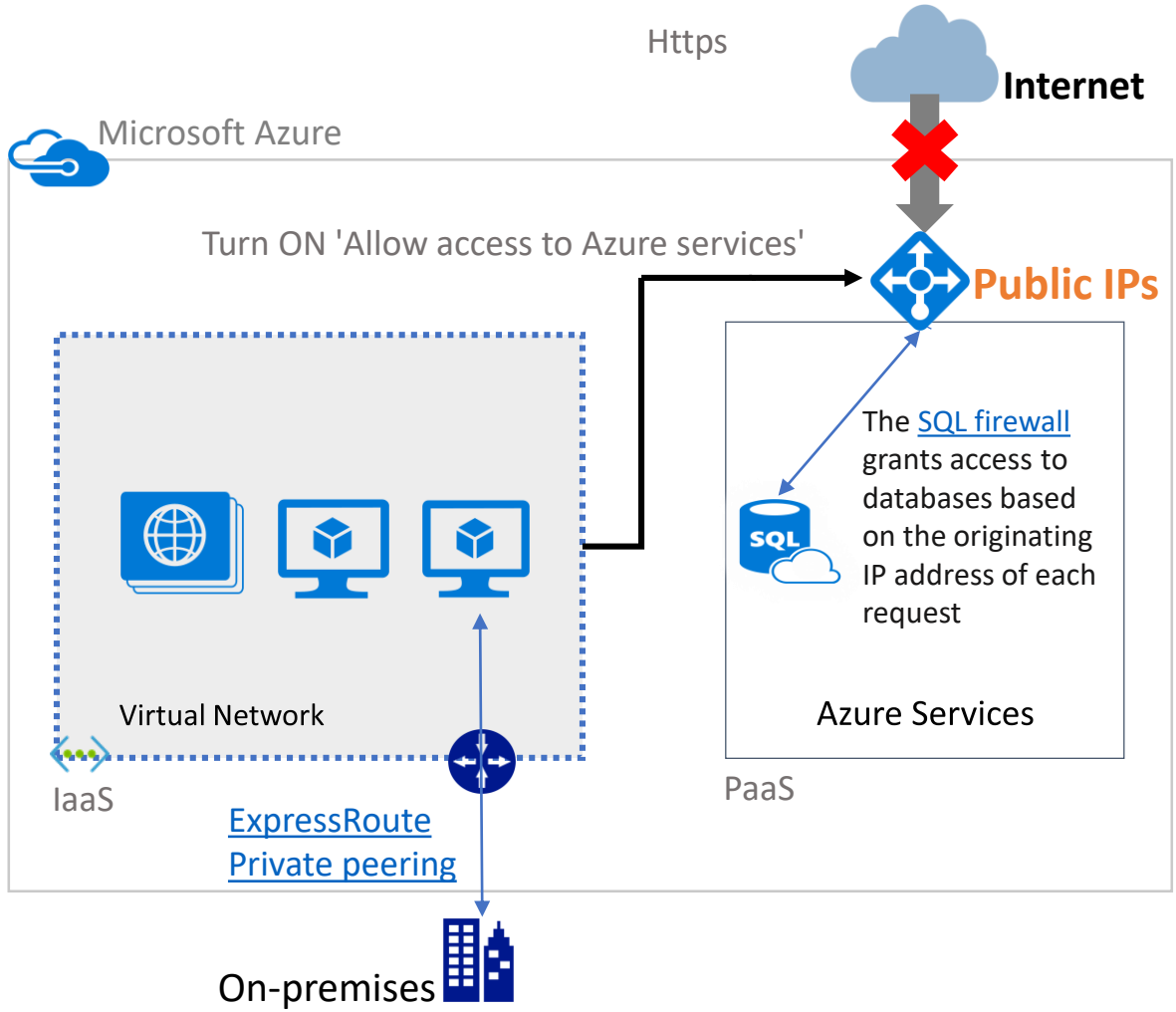


Access Azure SQL from Azure Applications hosted on IaaS

Option 2

The most secure configuration is to set 'Allow access to Azure services' to OFF. If you need to connect to the database from an Azure VM, you should create a Reserved IP and allow only the reserved IP address access through the firewall.

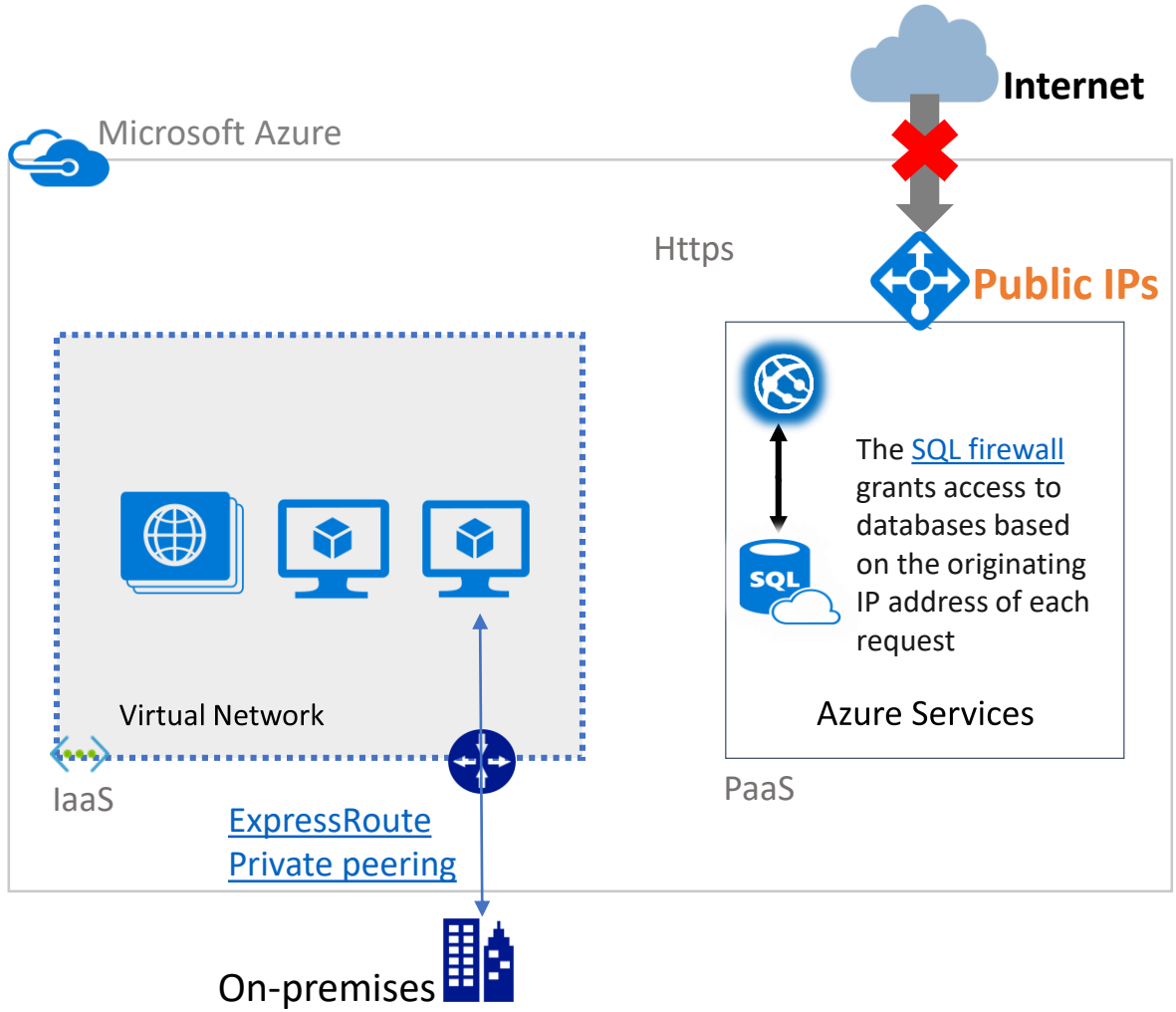
The firewall pane has an ON/OFF button that is labeled Allow access to Azure services. The ON setting allows communications from all Azure IP addresses and all Azure subnets. These Azure IPs or subnets might not be owned by you. This ON setting is probably more open than you want your SQL Database to be. The virtual network rule feature offers much finer granular control



Access Azure SQL from Azure Applications hosted on PaaS

Option 1

The most secure configuration is to set 'Allow access to Azure services' to OFF. If you need to connect to the database from an Azure VM or cloud service, you should create a Reserved IP and allow only the reserved IP address access through the firewall.



Private Endpoints

Connectivity to PaaS services using Virtual Networks

Preview

From on premises

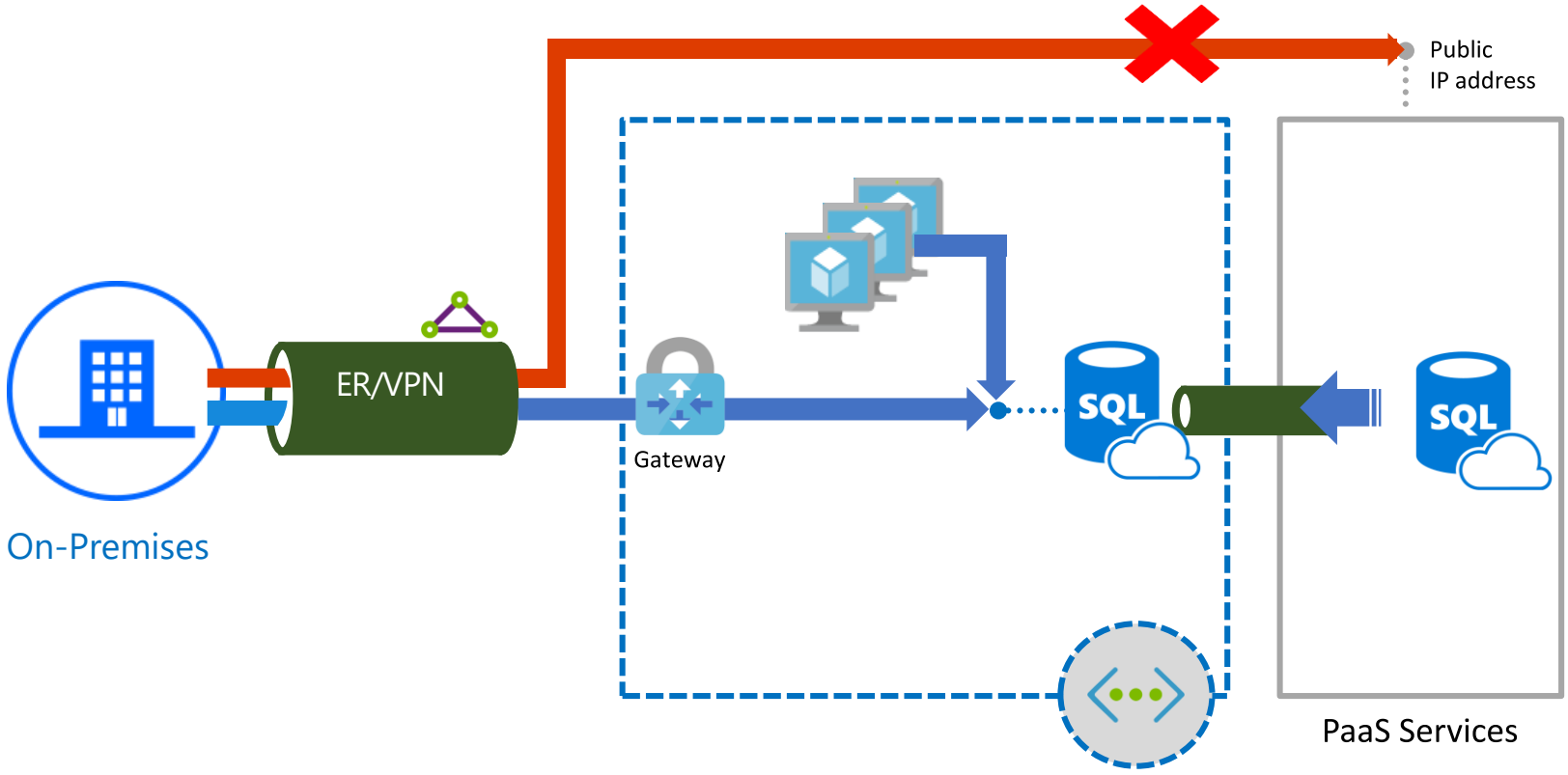
- ✓ Direct connectivity from on premises using ER private peering or VPN tunnels, removing internet traffic.

Within the VNet

- ✓ Connect privately to Azure PaaS resources within your VNet.

Security simplified

- ✓ NSG & Firewall configuration clean within customer address space
- ✓ Predictable IP addresses for PaaS resources

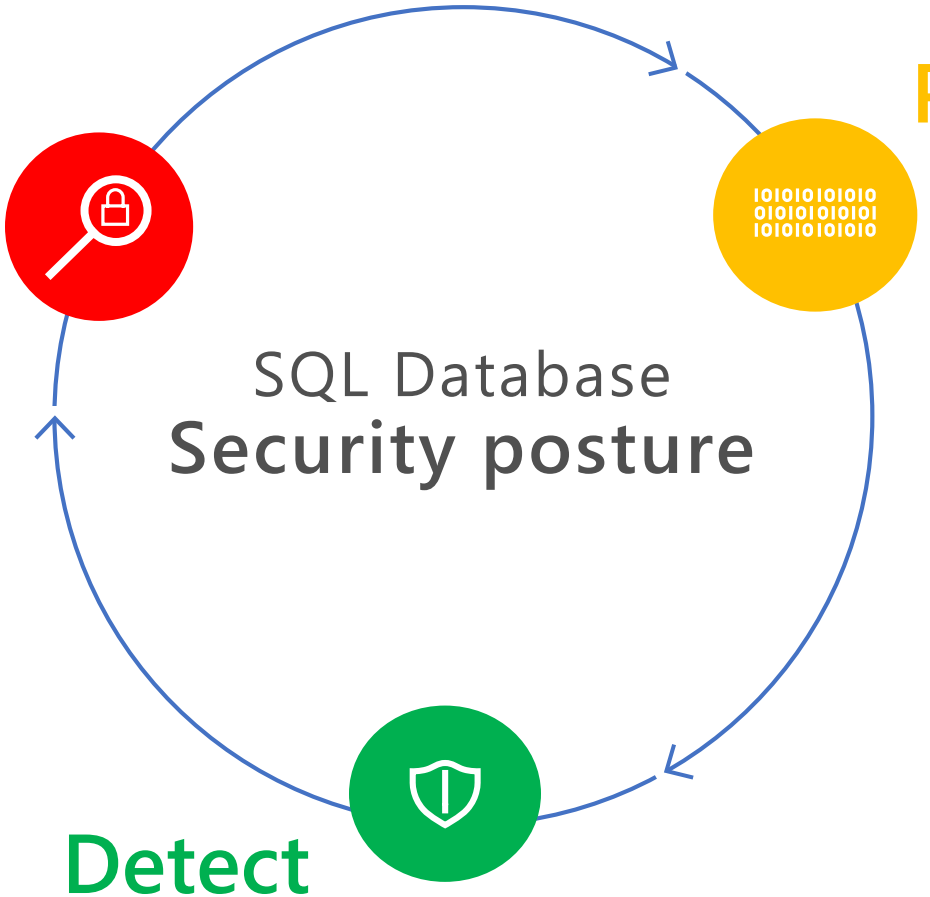


SQL Security Lifecyle

Discover

Security Assessment

- Data Discovery & Classification
- Vulnerability Assessment
- Security recommendations
- Coherent report



Protect

Data Encryption

- Transport Layer Security (transit)
- Transparent Data Encryption (at rest)
- Always Encrypted (in use)

Access Control

- SQL Firewall
- VNET Service Endpoints
- SQL & AAD Authentication
- Multi-factor Authentication
- Row-Level Security
- Dynamic Data Masking
- Static Data Masking (Roadmap)

Detect

Threat Protection

- Auditing log
- Threat Detection alert
- Azure Security Center & Azure Log Analytics

Industry-leading security

Information Protection

- **Encryption in transit** (TLS 1.2 over TDS)
- **Encryption-at-rest** (TDE)
- **Encryption in use** (Always Encrypted)

Access Management

- **SQL Permissions**
- **Native VNET Support for Managed Instance**
- **VNET Service Endpoints**
- **SQL Authentication**
- **Azure Active Directory Authentication - MFA**
- **Dynamic Data Masking**
- **Row-level Security**

Threat Protection

- **SQL Threat Detection**
- **Auditing**
- **SQL Firewall (server & database)**

Security Management

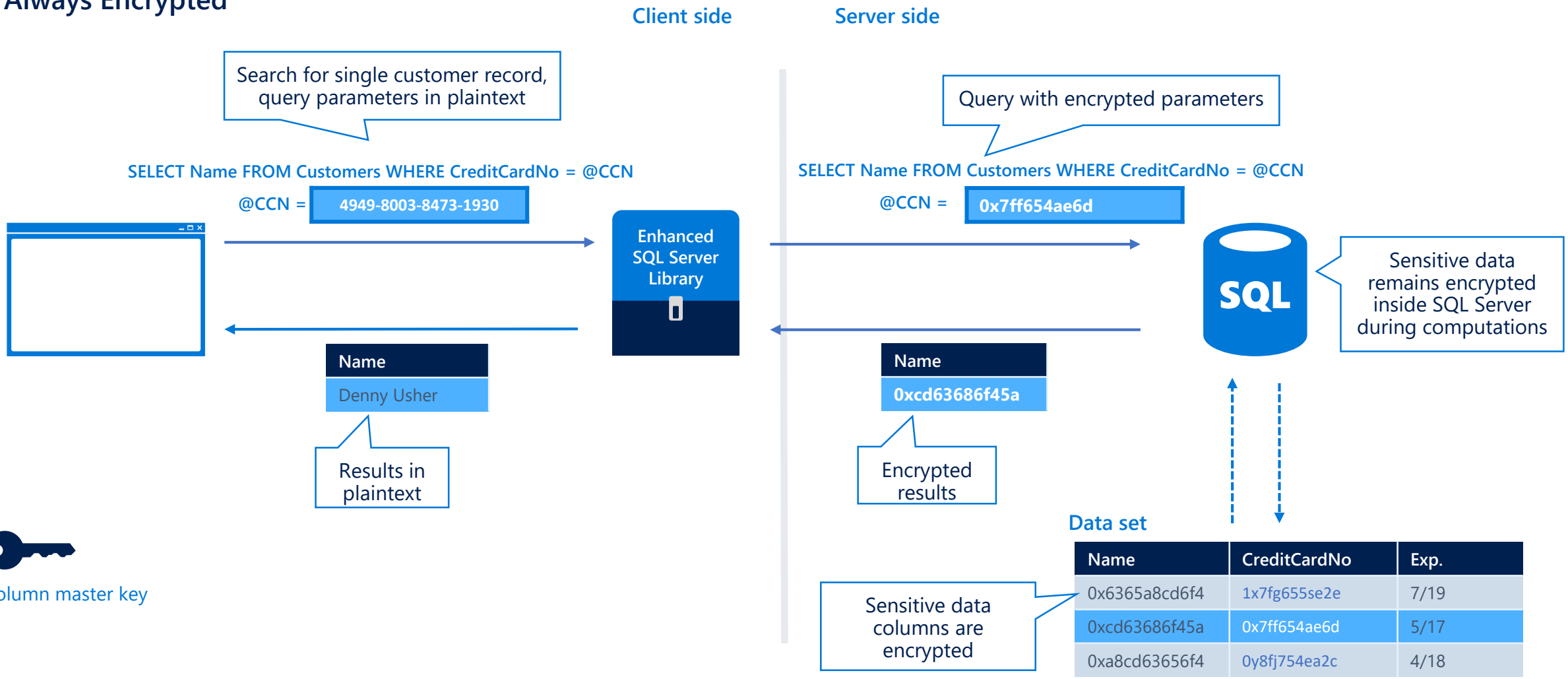
- **Data Discovery & Classification**
- **Vulnerability Assessment**

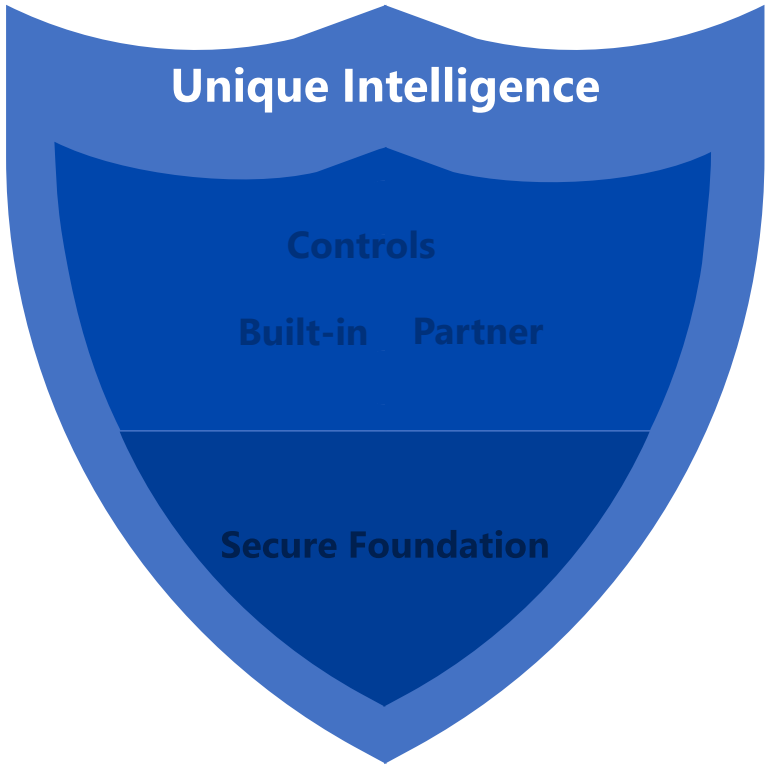
Cloud-only

ENCRYPT DATA IN USE

Protect sensitive data from high-privilege but unauthorized SQL Server users

Always Encrypted





Insights informed by trillions of diverse signals to detect threats faster

1.2B devices scanned each month

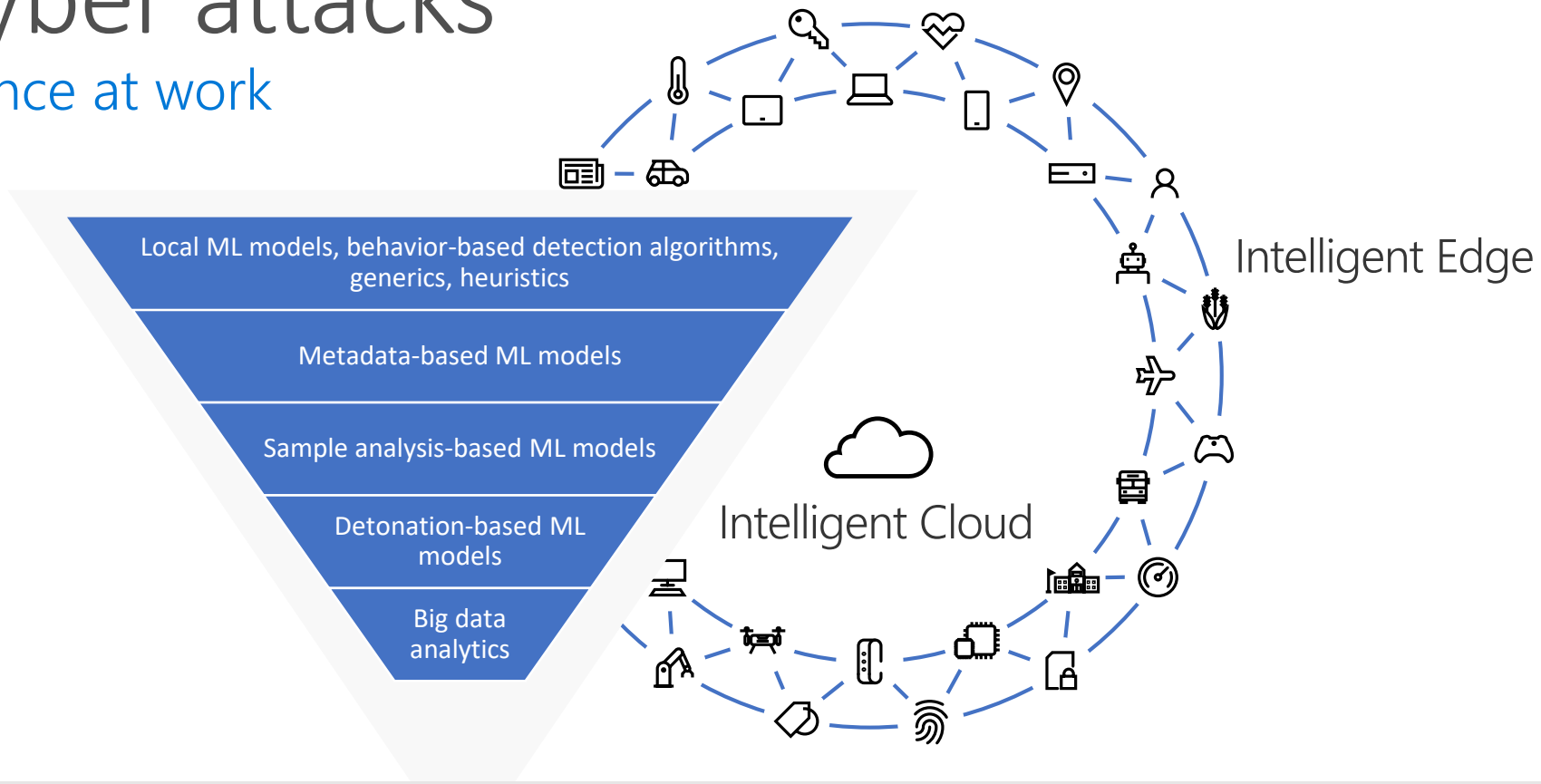
5B threats detected/month

450B monthly authentications

6.5B threat signals analyzed daily

Stopping cyber attacks

Real-world intelligence at work



October 2017 – Cloud-based detonation ML models identified Bad Rabbit, protecting users 14 minutes after the first encounter.

March 6 – Behavior-based detection algorithms blocked more than 400,000 instances of the Dofoil trojan.

2017 — 2018

February 3 – Client machine learning algorithms automatically stopped the malware attack Emotet in real time.

August 2018 – Cloud machine learning algorithms blocked a highly targeted campaign to deliver Ursnif malware to under 200 targets

Unique Intelligence

Integrated with Microsoft services

Threat intelligence

Looks for known malicious actors using Microsoft global threat intelligence

Partners

Integrates alerts from partner solutions, like firewalls and antimalware

Anomaly detection

Uses statistical profiling to build historical baselines

Behavioral analytics

Looks for known patterns and malicious behaviors

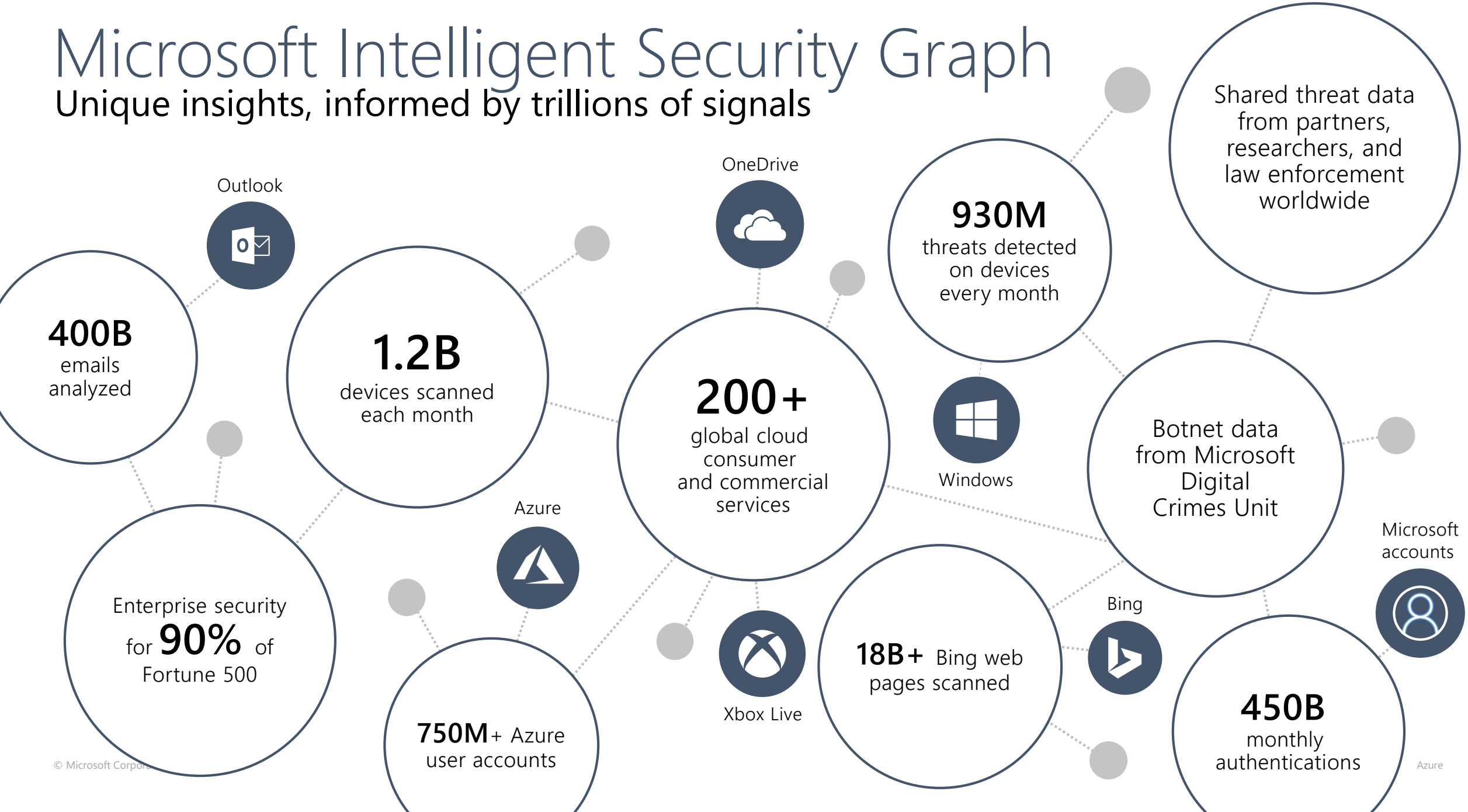
Fusion

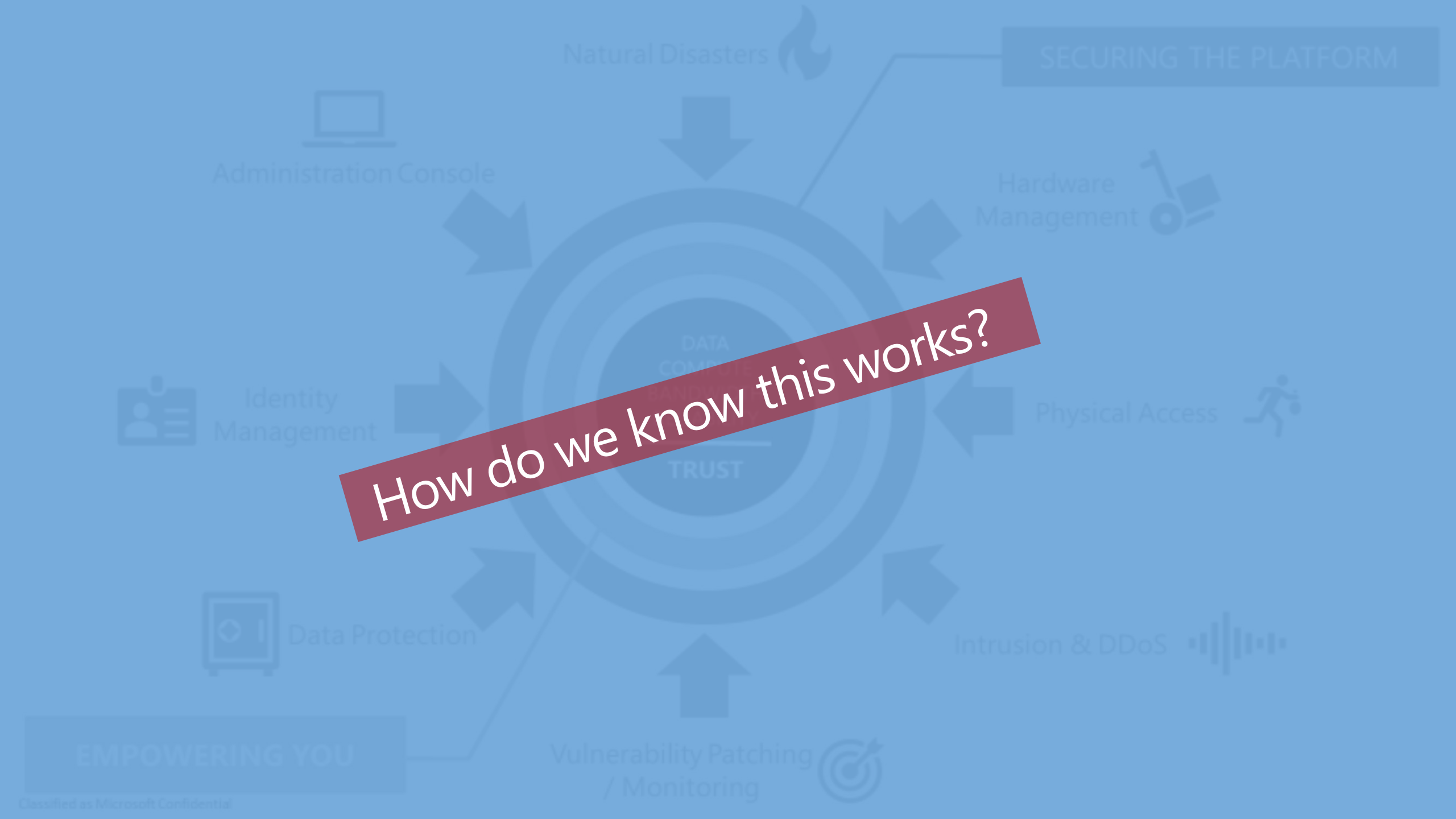
Combines events and alerts from across the kill chain to map the attack timeline

Powered by Microsoft Intelligent Security Graph

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals





How do we know this works?

RED team vs. BLUE team

Red Team

- Dedicated adversary performing targeted and persistent attacks against our Microsoft Online Services.
- Attack and penetrate environments using the same steps adversary's kill chain
- Mean Time to Compromise (MTTC) + Mean Time to Privilege Escalation (MTTP)

Recon → **Delivery** → **Foothold** → **Persist** → **Move** → **Elevate** → **Exfiltrate**

Blue Team

- Dedicated set of security responders or members from across the Security Incident Response, Engineering and Operations organizations.
- Estimated Time to Detection (ETTD) + Estimated Time to Recovery (ETTR)

Gather → Detect → Alert → Triage → Context → Plan → Execute

A Closer Look at How We Use ML

ML Components

We use supervised learning. Our ML model tells us whether observed data is “similar enough” to attack patterns

Generate Labelled Attack Data

- Used as a historical record of attacks
- Regularly re-generated
- Randomization in terms of attack scenario and scope targeted

Train Model on Labelled Data

- Model consumes labelled and unlabelled data
- Applies algorithms to produce a formula
- Offline training

Publish Model to Real Time Data Processing System

- Real time system processes incoming events
- Model formula published regularly to real time system
- All incoming data evaluated by model

Raise Alerts Based on Model

- Model output is a number between 0 and 1
- If above our threshold, we raise an alert

AttackBot: Generating Labelled Data

We need to know what attacks look like. So we built AttackBot!

AttackBot runs against our service regularly, generating a strong set of labelled data

Some sample AttackBot attack scenarios: data exfiltration, command & control, illicit account creation, HBFW modification… and a lot more

Variety of AttackBot runs against our service – we get a regular supply of labelled attack data this way. The ML models consume this data to build knowledge of what attacks look like

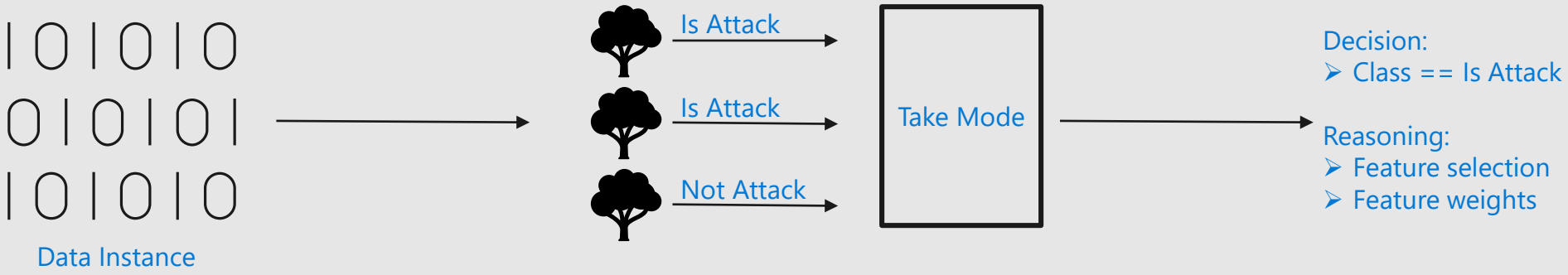
Overview of the model

Model

We use a random forest model and perform cross validation. Random forest algorithms create many decision trees and output the mode of all the decision trees

Advantages

1. **Resistant to overfitting** making it a robust model for our highly diverse security telemetry.
2. **Highly scalable** for large volumes of data.
3. **Not a black box:** Outputs feature selection and associated weights used to make classifications.

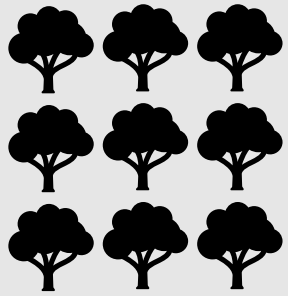


Training the Model

AttackBot generates malicious signals – initial processing logic converts these into model features (detections)

PowershellExploitationMethodNames
RemoteThreadInjection
PowershellEncodedCommand
DataExfilOverLongWindow
ServiceInstalled
C2BasicDetection
… and others

Our random forest model is trained from these true positive detections as well as plenty of benign samples



The model selects and weights features (detections) based on which ones are closely correlated to attacks

Feature	Weight
PowerShellExploitationMethodNames_Max_score	0.315
PowerShellBlacklistEncodedCommand_Max_score	0.1747
PowerShell Encoded Command_Max_score	0.1619
UnusualProcessCreation_Max_probabilityChildProcessGivenParent	0.1379
UnusualProcessCreation_Max_score	0.0582
Audit Currently running process_Max_score	0.0431
UnusualProcessPath_Max_score	0.0381
ServiceInstalled_Max_probabilityServiceInstalledGivenRole	0.024
ServiceInstalled_Max_score	0.0185
MachineAccountWMIPivot_Max_score	0.0114
C2BasicDetectionUdp_Max_score	0.0075

Consuming Model Output + Firing Alerts

The model runs against data from 10-minute time windows, outputting a number in [0,1]

When the output exceeds a threshold, we raise an alert

Each alert will contain the feature variables, weights and total scores that contributed to that decision

Scenario	Signals	IsDetected
Egress-ConnectionToChina	PowerShellExploitationMethodNames C2Stage2Detection locIpDetection C2BasicDetection NewProcessConnection	1
ICEBreakerRandomExfil	PowerShell Encoded Command PowerShellBlacklistEncodedCommand PowershellObfuscatedCommand locIpDetection DataExfilOverLon...	1
Pivot-WithCredentials	IdsWmiSuspiciousActivity MismatchingMachineAccountProcessStart MachineAccountWMIPivot UnusualProcessCreation locDnsRecord...	1
Egress-ConnectionToChina	RemoteThreadInjection C2BasicDetection locIpDetection StableProcessNewConnection NewProcessConnection	1
Suspicious-Process	RemoteThreadInjection UnusualProcessCreation locIpDetection C2BasicDetection	1
Egress-ConnectionToChina	RemoteThreadInjection locIpDetection C2BasicDetection	1
ICEBreakerRandomExfil	PowerShell Encoded Command PowerShellBlacklistEncodedCommand locDnsRecordDetection locCommandDetection locHostNameDet...	1

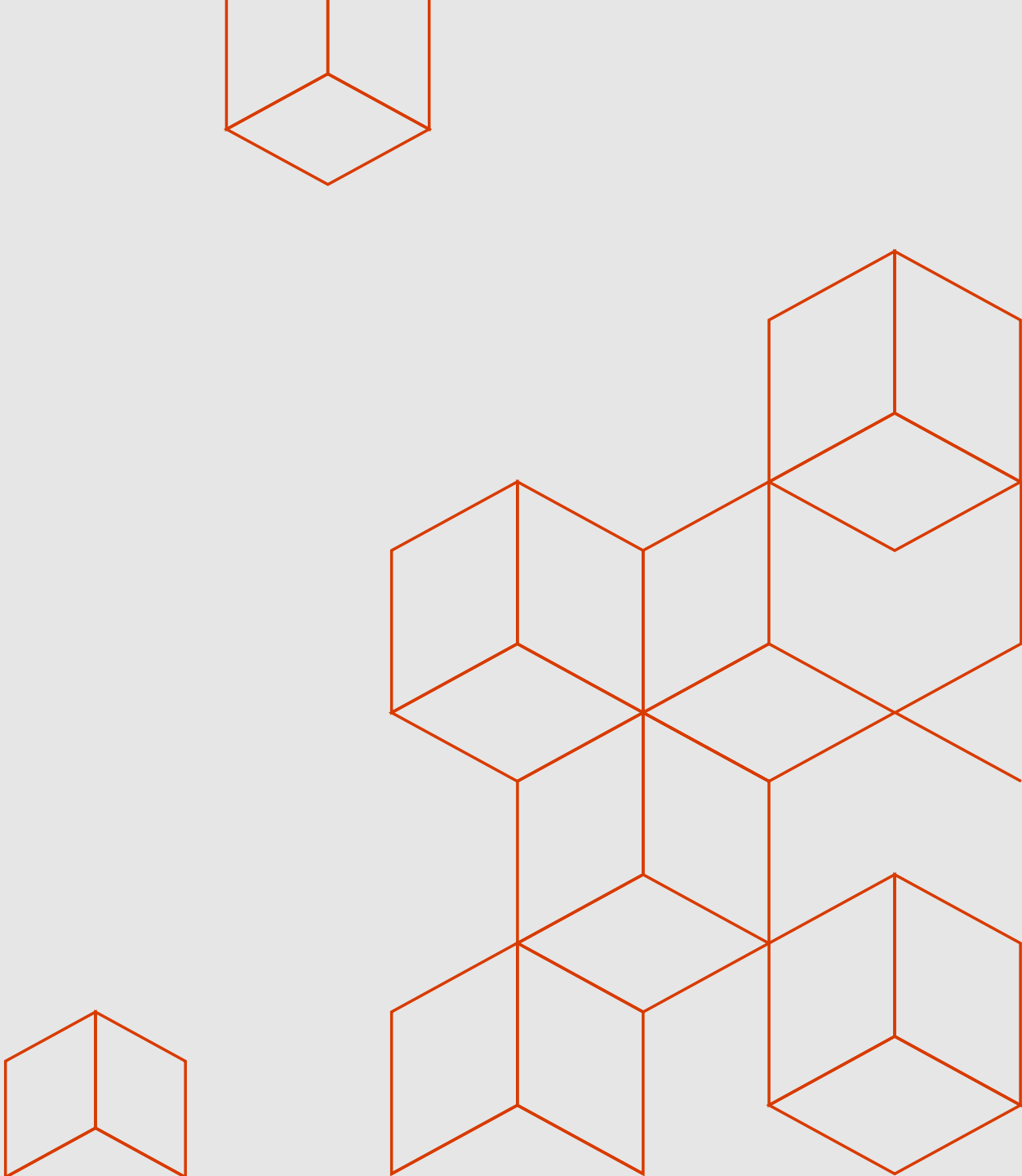
Details

Entity Meta Detection on sinmg01ms104.prdmgt01.prod.exchangelabs.com w/ score 0.92 -
Calculation Time: 2018-09-13T13:24:00.806Z

Scoring Factors:

Feature	Score	Weight	Weighted Score
C2BasicDetection_Max_treeScore1	1.0	0.2457	0.2457
PowerShellExploitationMethodNames_Max_score	0.0	0.1837	0.0
C2Stage2Detection_Max_score	1.0	0.1184	0.1184
PowerShellBlacklistEncodedCommand_Max_score	0.0	0.1174	0.0
C2BasicDetection_Max_treeScore2	0.9954	0.1068	0.1063
PowerShell Encoded Command_Max_score	0.0	0.0621	0.0
C2BasicDetection_Max_score	0.999	0.0505	0.0504
locProcessNameDetection_Max_score	0.0	0.033	0.0
JIT Account Elevated to System_Max_score	0.0	0.013	0.0
locCommandDetection_Max_score	0.0	0.0125	0.0
MismatchingMachineAccountProcessStart_Max_score	0.0	0.0117	0.0
Audit Currently running process_Max_score	0.0	0.0097	0.0
NewProcessConnection_Max_score	1.0	0.0072	0.0072
UnusualProcessCreation_Max_score	0.999	0.0068	0.0068
TsgBypass_Max_score	0.0	0.0048	0.0
ServiceInstalled_Max_score	0.999	0.0027	0.0027

Takeaways



Securing the Platform

Security Development Lifecycle (SDL)

- ✓ Security Embedded in Planning, Design, Development, & Deployment

Infrastructure security controls

- ✓ Datacenter Security
- ✓ Secure Multi-tenancy
- ✓ Network Protection
- ✓ DDoS Defense
- ✓ Data Segregation
- ✓ Data Protection

Operational security controls

- ✓ Prevent & Assume Breach Strategy
- ✓ Incident Response
- ✓ Access Policy & Controls
- ✓ Threat Detection
- ✓ Forensics

Compliance

- ✓ Strategy
- ✓ Certifications

Empowering You

Security Management

- ✓ Identity & Access
- ✓ Data Control
- ✓ Host Protection
- ✓ Operations Management Suite
- ✓ Azure Security Center

Encryption

- ✓ Key Vault
- ✓ Options for Encryption at Rest
- ✓ Options for Encryption in Transit
- ✓ SQL Encryption
- ✓ Disk Encryption

Secure Networking

- ✓ Network Security Groups
- ✓ VPN
- ✓ ExpressRoute

Partner Solutions

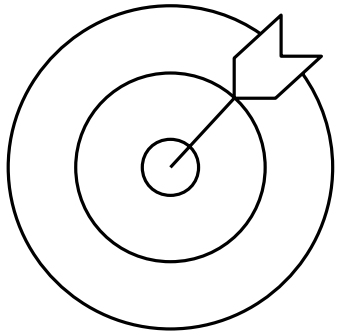
- ✓ Azure Marketplace

Data Control

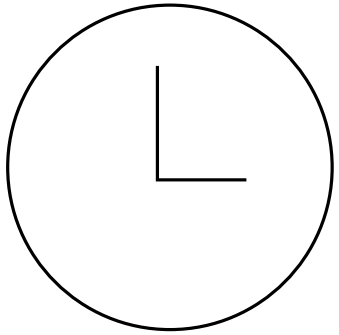
When a customer utilizes Azure, they own their data

Control over data location	Control over access to data	Control over data deletion	Encryption key management
Customers choose data location and replication options.	Strong authentication, carefully logged "just in time" support access, and regular audits (see Data Control section).	When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer's data inaccessible.	Customers have the flexibility to generate and manage their own encryption keys (see Encryption section).

Outcomes We've Achieved



- Alerting accurate enough to page us 24x7 (… yes, this means some alerts at 3am)
- Alerts successfully raised for complex, manual pen tests (not only AttackBot)
- Alerts indicate the specific factors that figured most prominently – enabling remediation



- ML alerts fire within 15 minutes of attack behavior – major improvement over manual investigation
- Model re-trained and published regularly, ensuring that we keep up with environmental changes

We Hope You Remember…

- Microsoft invests heavily in securing the infrastructure that hosts customer data
- In addition to traditional security methods, we use state of the art techniques to make sure we catch and stop attackers at scale
- We never stop innovating and improving: models themselves adapt to the environment, and we are pushing the envelope with new models and techniques

Focus on your most valuable IP.

Let your users be.

90%

Employees involved in an insider threat incident had a history of violating IT security policies prior to the incident [7]

Make your data work harder for you.

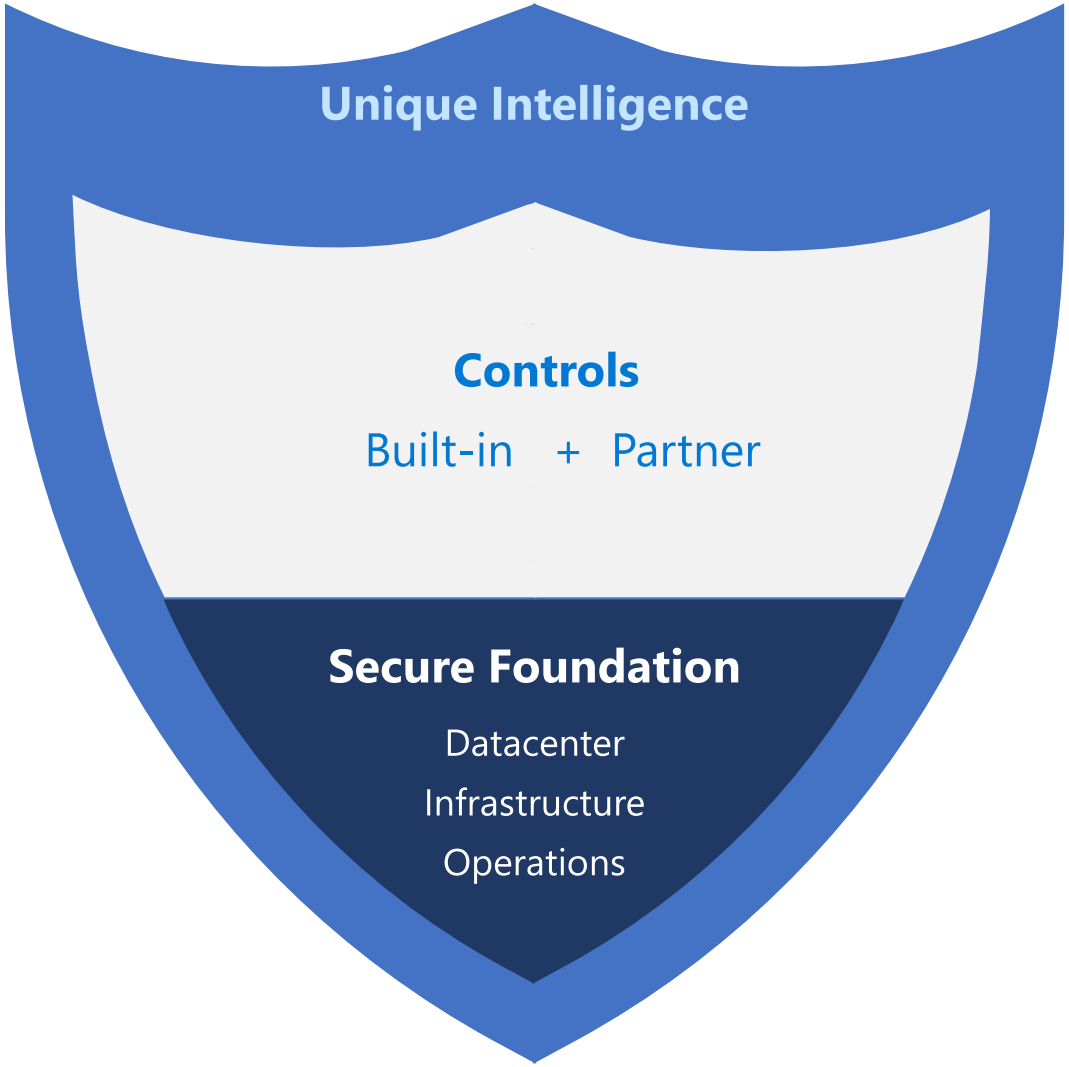
[7] *Code42, "3 Steps to Mitigating Insider Threat Without Slowing Down Users," 2015*

Gain unmatched security

Microsoft managed infrastructure security

Defense in depth with broad set of tools

Faster threat mitigation with insights from trillions of signals



Take the next step today

Learn

Azure security information aka.ms/myASIS

Azure security blog azure.microsoft.com/en-us/blog/topics/security/

Use

Get Started with Azure Security Center aka.ms/AzureSecurityCenterBlade

Deploy Best Practices azure.microsoft.com/en-us/resources/security-best-practices-for-azure-solutions/

Collaborate

Give us feedback on Azure Security feedback.azure.com/forums/216840-security-and-compliance

Azure Security on Facebook facebook.com/groups/azuresec/

References

- https://docs.microsoft.com/en-us/azure/security/
- https://azure.microsoft.com/en-us/blog/topics/security/
- https://azure.microsoft.com/en-us/blog/strengthen-security-with-key-azure-innovations/
- https://www.microsoft.com/en-us/learning/exam-list.aspx
- https://thehackernews.com/
- https://servicetrust.microsoft.com/ViewPage/BlueprintOverview
- https://servicetrust.microsoft.com/ViewPage/PCIBlueprint