Microsoft

Microsoft Empowerment Session for Telstra

Abbas Kudrati
Chief Cybersecurity Advisor (Asia)
Abbas.Kudrati@Microsoft.Com
https://aka.ms/abbas

Current role:

- **Chief Cyber Security Advisor** – Microsoft Asia
- **Professor of Practice in Cyber Security** – LaTrobe University
- **Executive Advisory Board Member – Cyber Security** – Deakin University and LaTrobe University
- **Global Threat Advisory Board Member** – EC-Council ASPAC

Previous roles (last 6):

- KPMG Australia : **CISO**
- Public Transport Victoria : **CISO**
- National Bank of Kuwait : Dy **CISO**
- eGovernment Authority – Bahrain: **CISO**
- Ernst & Young – Bahrain : **Manager IT Advisory**
- KPMG Kuwait, Bahrain Qatar : **Assistant Manager IRM**

Awards and Accolades:

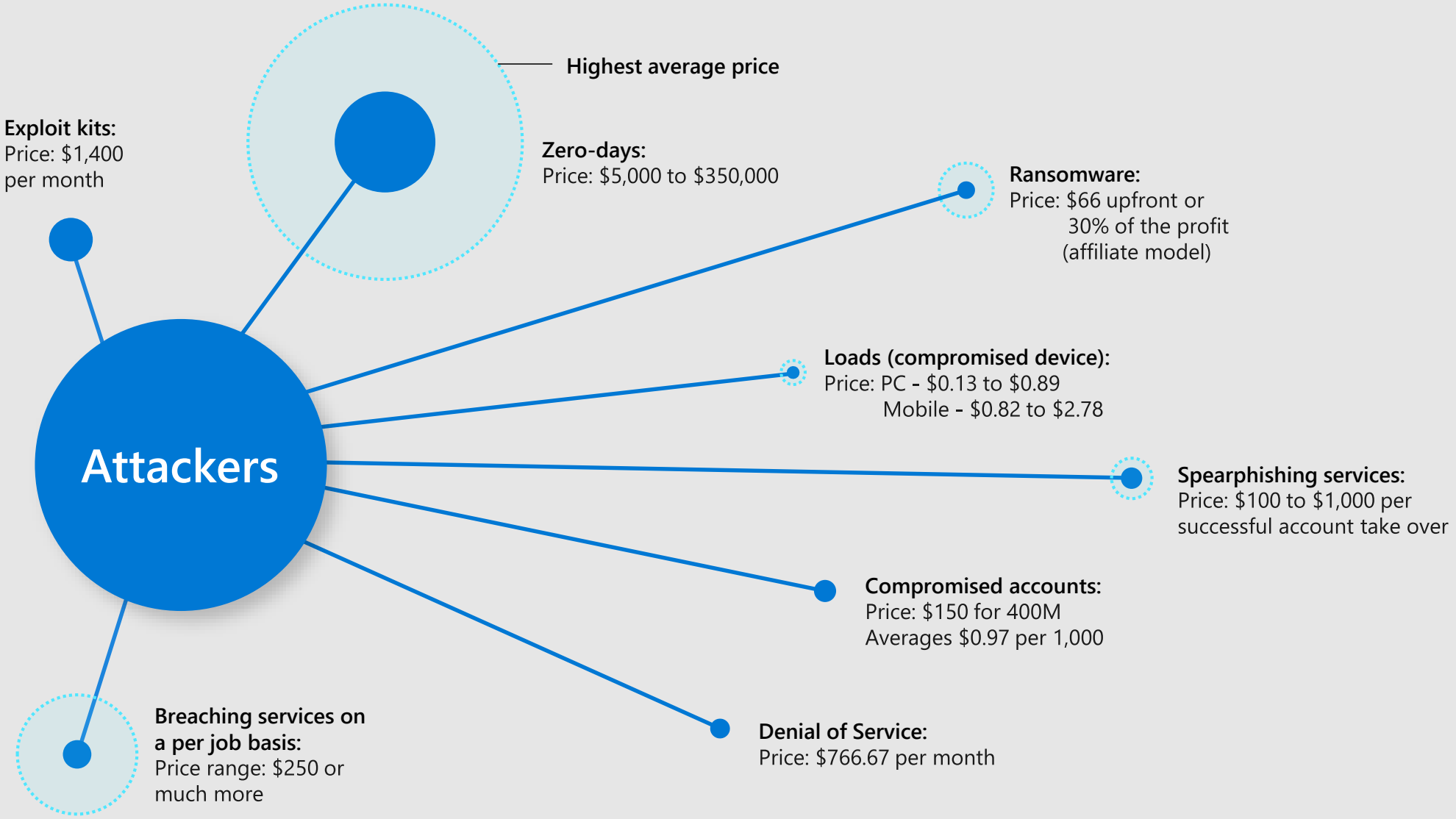
- 2019 **"Top Cybersecurity Advisor for APJ" Microsoft**
- 2018 **"Best Security Professional"** ISACA Oceanic CACS
- 2018 **"CISO 100 Award"** by CISO Council, UAE
- 2017 SPLUNK **"Boss of the SOC "BOTS"** Winner for Melbourne region
- 2015 Australian **"CISO of the year"** finalist
- 2014 Middle East **"IT Governance Professional of year"**
- 2011 Middle East **"Security Strategist of year"**

Certifications and Qualifications:

- Certified Chief Information Security Officer **(C|CISO)**
- Certified Information Security Manager **(CISM)**
- Certified in Cloud Security Knowledge **(CCSK)**
- Certified Information System Auditor **(CISA)**
- Certified in Governance of Information Technology **(CGEIT)**
- Certified Block Chain Expert **(CBE)**
- Certified Ethical Hacker **(C|CEH)**
- Certified Computer Forensic Hacking Investigator **(C|HFI)**
- TOGAF 8 Certified Enterprise Architect **(TOGAF CEA)**
- **COBIT 5** Foundation Certified
- **ISO 27001: 2005** Lead Auditor
- **PRINCE 2** Practitioner and Foundation Certified
- ITIL Foundation Certified **(ITIL)**
- EC Council Disaster Recovery Professional **(E|DRP)**
- SABSA Foundation Certified
- **MCSE+** Security
- Microsoft Certified Azure Foundation
- Microsoft Certified M365 Foundation
- **CCNA**
- Bachelor of Commerce – Accounting and Auditing

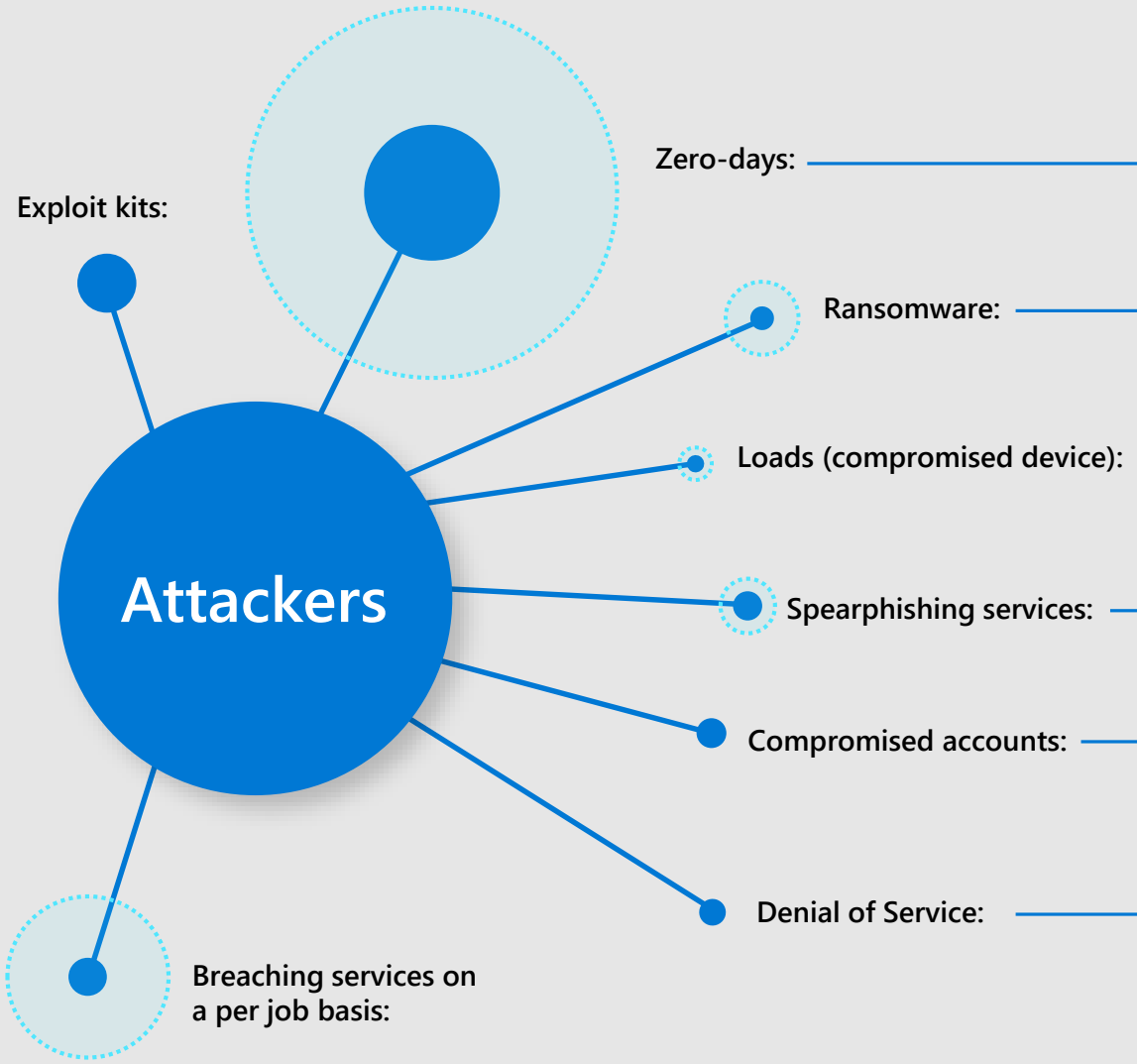
Attack services are cheap

More details at https://aka.ms/CISOWorkshop



Attack services are cheap

More details at https://aka.ms/CISOWorkshop



FOCUS ON HYGIENE (NOT ZERO DAYS)

Zero day vulnerabilities are expensive and impractical for many attacks. https://aka.ms/CyberHygiene has guidance from Microsoft + NIST, the Center for Internet Security (CIS), and US DHS NCCIC (formerly US-CERT)

FOCUS ON MFA/PASSWORDLESS & ZERO TRUST

Attackers have moved to Identity attacks like phishing and cred theft (which easily evade traditional network defenses)

Increase cost of these attacks starting with administrative privileges and other business critical assets

ENABLE DDoS PROTECTION FOR CRITICAL SERVICES

Ensure that your business-critical services have DDoS protection from Azure platform or a capable 3rd parties

How We Secure Azure

Azure Security Services and Capabilities*

Network Security

- Virtual Network Service Endpoints
- DDoS protection
- Network Security Groups
- NSG service tags
- NSG Application Security Groups
- NSG Augmented Rules
- Global Virtual Network Peering
- Azure DNS Private Zones
- Site-to-site VPN
- Point-to-site VPN
- ExpressRoute
- Azure Virtual Networks
- Virtual Network Appliances
- Azure Load Balancers
- Azure Load Balancer HA Ports
- Azure Application Gateway
- Azure Web Application Firewalls

Compliance Program

- Microsoft Trust Center
- Service Trust Platform
- Compliance Manager

DDoS Mitigation

- Azure DDoS Protection
- Azure Traffic Manager
- Autoscaling
- Azure CDN
- Azure Load Balancers
- Fabric level edge protection

Pen Testing

- Per AUP
- Per TOS
- No contact required

Encryption

- Azure Key Vault (no dedicated option, though)
- Azure client-side encryption library
- Azure Storage Service Encryption
- SQL Transparent Data Encryption
- SQL Always Encrypted
- SQL Cell/Column Level Encryption
- Azure Cosmo DB encrypt by default
- Azure Data Lake encrypt by default
- VPN protocol encryption (ssl/ipsec)
- SMB 3.0 wire encryption

Identity and Access Management

- Azure Active Directory
- Azure Active Directory for Devs
- Azure Active Directory B2C
- Active Directory Domain Services
- Azure Active Directory MFA
- Conditional Access
- Azure Active Directory Identity Protection
- Azure Active Directory Privileged Identity Management
- Azure Active Directory App Proxy
- Azure Active Directory Connect
- Azure RBAC
- Azure Active Directory Access Reviews

Security Docs Site

- Azure Security Information site on Azure.com

Infrastructure Security

- Comes with Azure Data Centers

Config & Management

- Azure Security Center
- Azure Resource Manager
- Azure Automation
- Azure Advisor

Data Loss Prevention

- Cloud App Discovery
- Azure Information Protection

Monitoring and Logging

- Azure Log Analytics
- Azure Monitor
- Azure Application Insights

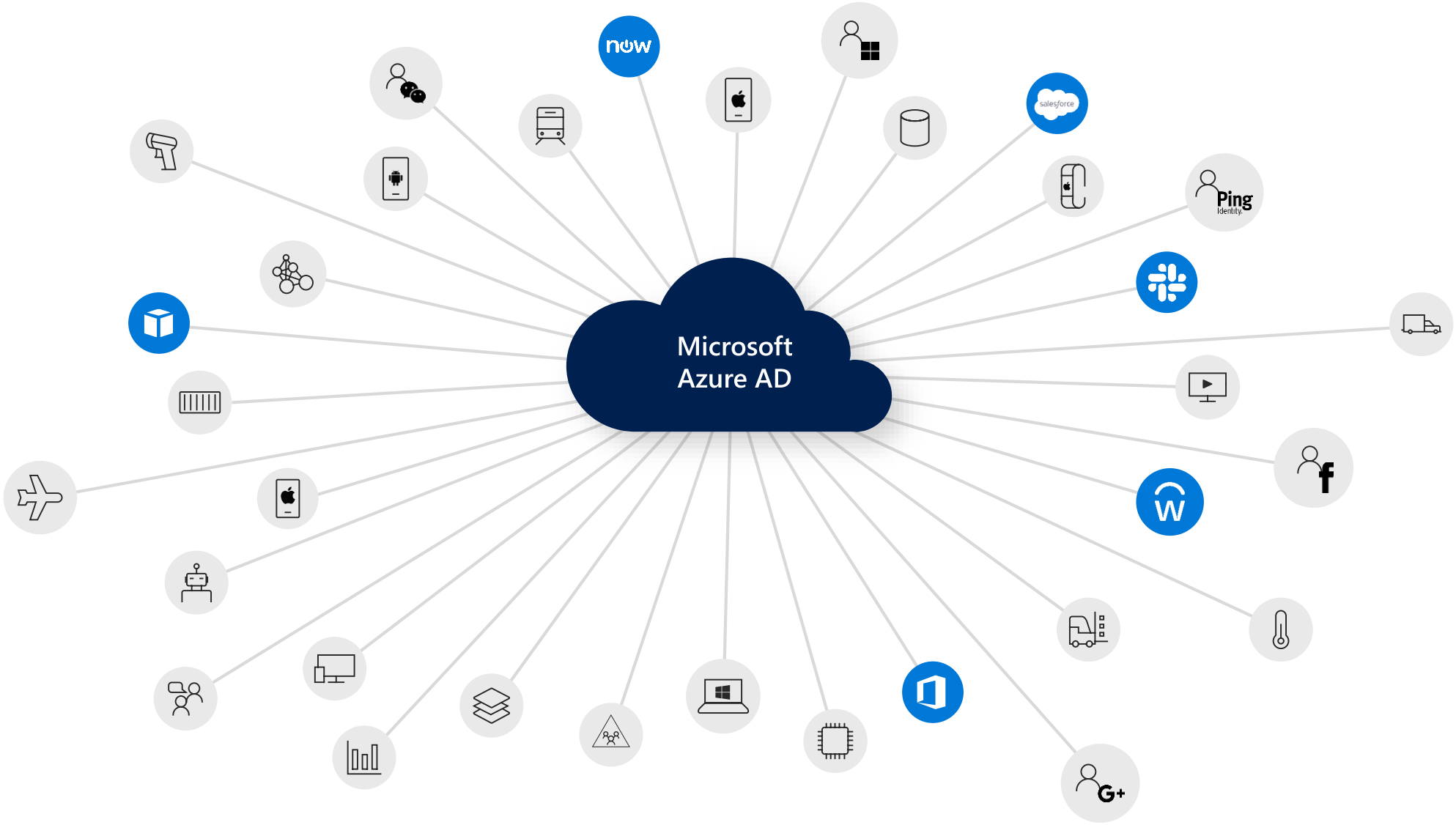
*Level2-moderate depth analysis

Microsoft

Azure Active Directory

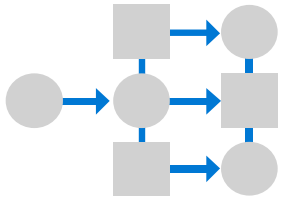
Your universal platform to manage and secure identities

Identity is the control plane for digital transformation



Microsoft Azure Active Directory

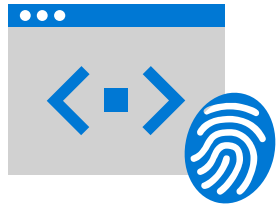
Your universal platform to manage and secure identities



Connect your workforce to any app

Protect and govern access

Engage with customers and partners



Accelerate adoption of your apps

Azure Active Directory—the world's largest cloud identity service

Thousands of organizations, millions of active users, billions of daily requests

100K+

Enterprise customers
Using Azure AD

250M+

Azure AD
Monthly active users

30B+

Azure AD
Daily authentication requests

Engineered for availability and security

Cloud-native, hyper-scale, multi-tenant architecture

Each **physical datacenter** protected with world-class, multi-layered protection, and engineered for maximum availability

Global cloud infrastructure with secure hardware and data segregation

Secured with cutting-edge **operational security**

- Restricted access
- 24x7 monitoring
- Global security experts

Customer success stories across every industry

Financial Services

"We are able to take an influx of customers in stride. The Azure cloud can be scaled according to our needs. Secondly, we pay only for the identities that actually want to access the system."

– Debeka

Türkiye'nin Finansı Türkiye Finans · Debeka · SİGORTA CİNİ

Government

"That's the power of the solution for us. It supports the integration of legacy applications, in whatever state they are in, to talk to the new identity management component."

– New Zealand Ministry of Education

U.S. Securities and Exchange Commission · Ministry of Education Te Tāhuhu o te Mātauranga · Shropshire Council

Healthcare

"For physicians, every second counts. If they need to get into an application right away to view an x-ray, for example, they can do that quickly and securely with [Azure] Multi-Factor Authentication."

– Presence Health

St Luke's · Presence Health · Canadian Cancer Society

Manufacturing

Azure AD "Conditional Access right now has finally gotten to a point where it has surpassed any reason for me to keep a firewall."

– Walsh

QANTAS · WALSH · MAERSK

Media & TelCo

"Azure AD is the backbone of everything I do, from eliminating multistep processes around provisioning… to connecting to countless applications."

– LA Clippers

Realmadrid · CLIPPERS · COMCAST

Retail

"Microsoft's commitment to improving security and the cloud is clear. It is the relationship that has allowed us to securely implement Azure AD at our scale."

– Walmart

asos · SUBWAY · Walmart

Robust ecosystem to integrate with your existing tools

Microsoft integrates with a wide variety of partners to extend the value of your existing tools, apps, and services with Azure AD

Business Applications

zendesk
cisco Webex
SAP
Adobe
ATLASSIAN
now

HR Management

successfactors An SAP Company
workday.
cornerstone

Secure Hybrid Access

f5
zscaler
Akamai
CITRIX

Passwordless Authentication

yubico
ENSURITY TECHNOLOGIES
FEITIAN WE BUILD SECURITY
HID
AUTHENTREND

Custom Authentication Factors

SECUREAUTH
DUO
Symantec. VIP
PingIdentity.
Entrust Datacard
TRUSONA

Identity Governance

SAVIYNT
Omada
imprivata

Built on open standards

The most compliant platform

- More certifications than any other cloud provider
- Industry leader for customer advocacy and privacy protection
- Unique data residency guarantees
- Microsoft is committed to GDPR compliance


Azure Active Directory,
your universal platform

Why choose Azure Active Directory as your universal platform

Industry-leading security

Complete IAM solution

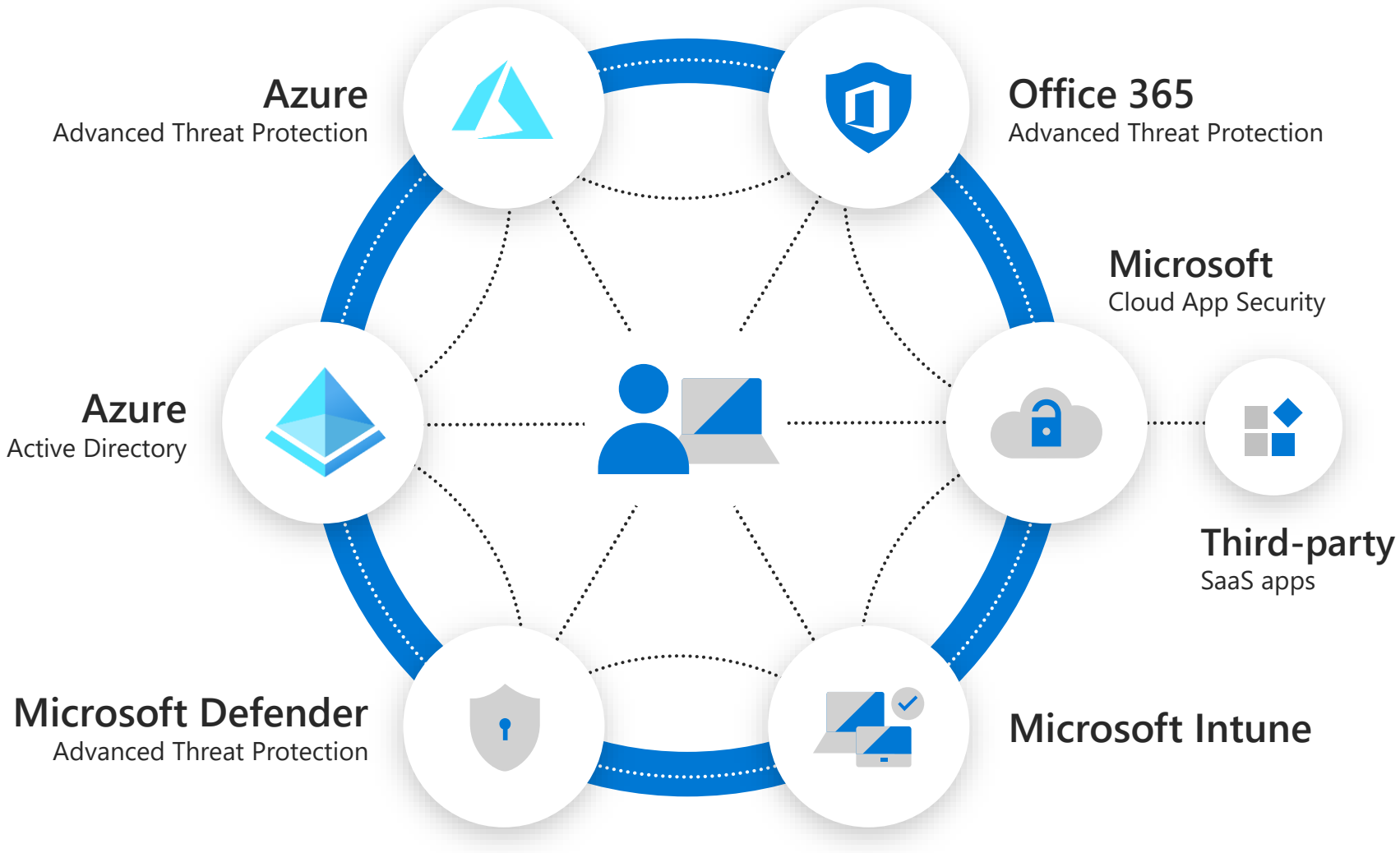
Seamless user experience

Access lifecycle management

Implementation support

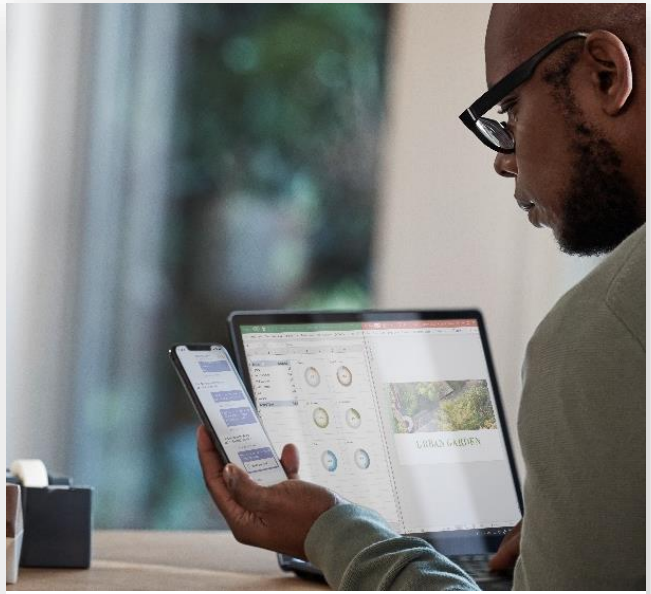
Industry-leading security

Industry-leading security



Protect and govern access

Verify user identities with strong authentication to establish trust



We support a broad range of multi-factor authentication options

Including password-less technology

- Microsoft Authenticator
- Windows Hello
- FIDO2 Security key
- Biometrics

- Push notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

Multi-factor authentication prevents 99.9% of identity attacks

Azure AD Password Protection

Dynamic banning of passwords based on known bad patterns and those you define

Global banned password list

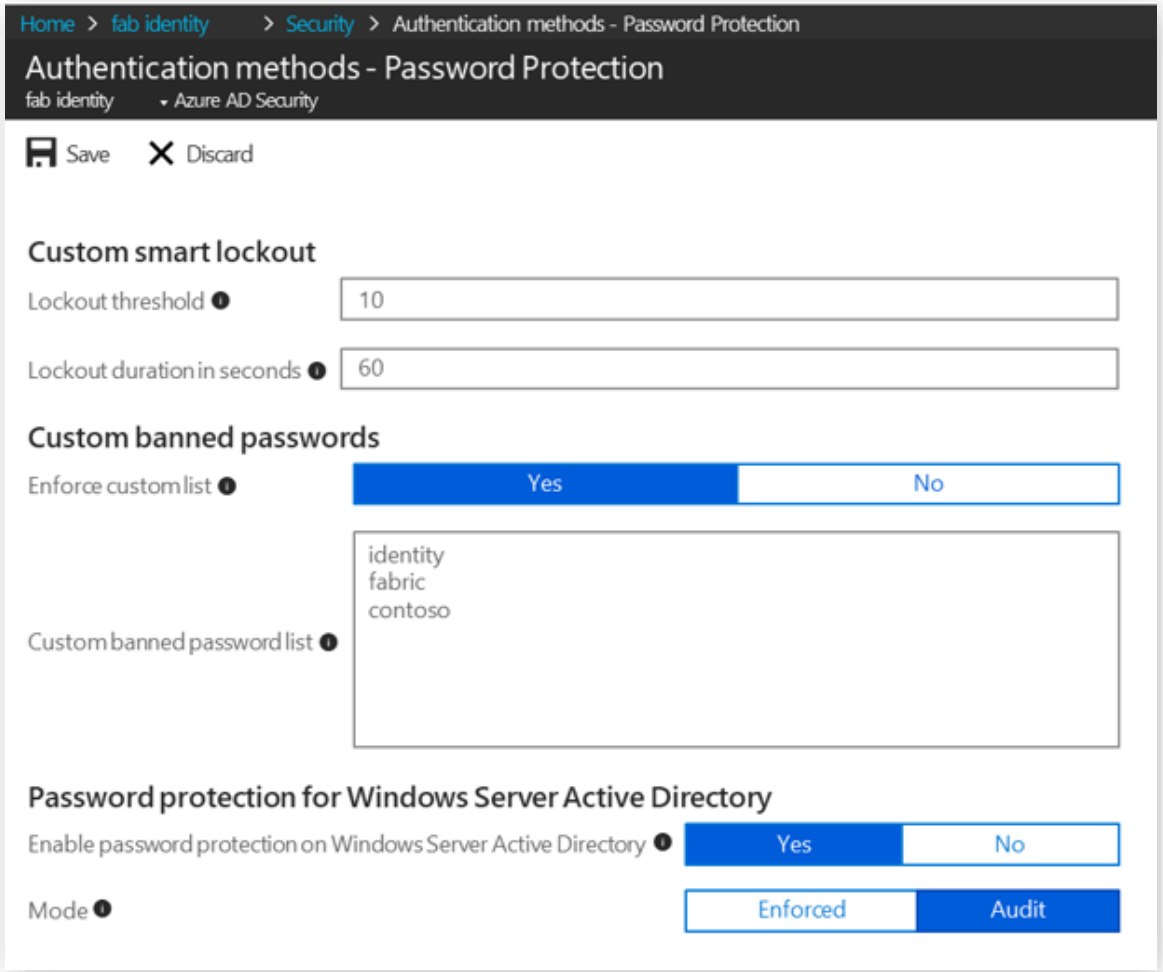
Microsoft defines a global list with almost 2,000 words, phrases, patterns

Custom banned password list

1,000 words and phrases unique to your organization

Banned password algorithm

Finds all weak password variations



Conditional Access

Azure AD
ADFS
MSA
Google ID

Android
iOS
MacOS
Windows
Windows Defender ATP
jamf
Lookout

Geo-location
Corporate Network

Browser apps
Client apps

Conditions

Employee and partner users and roles
Trusted and compliant devices
Physical and virtual location
Client app and auth method
Target application

171TB

Machine learning
Session risk
3
Real-time evaluation engine
Policies
Effective policy

Controls

Allow/block access
Limited access
Require MFA
Force password reset
Block legacy authentication
Require approved application

Microsoft Cloud
Microsoft Cloud App Security
Cloud SaaS apps
On-premises and web apps

Identity protection

Intelligently detect and respond to compromised accounts

300%

increase in identity attacks over the past year

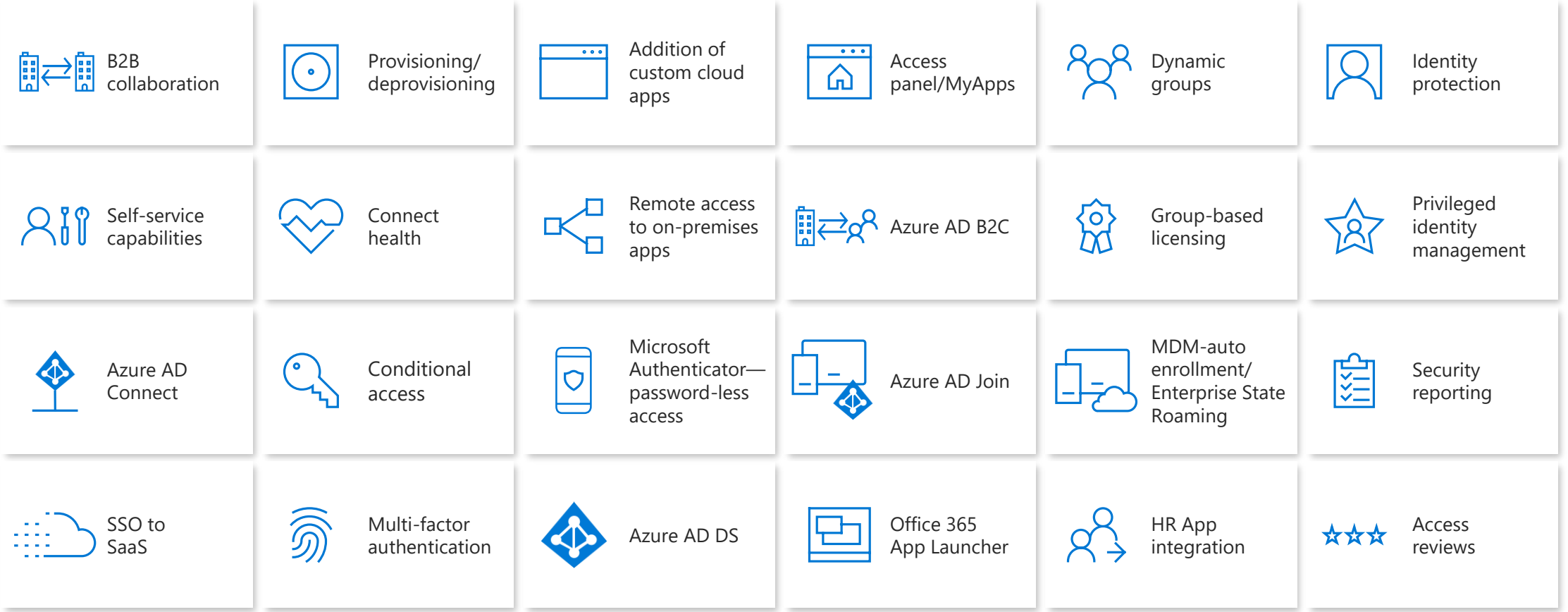
Real-time detection

Automated remediation

Connected intelligence

Azure AD offers depth and breadth

Identity and access management for employees, partners, and customers



Why Azure AD?

Industry-leading security

Simple, integrated, complete identity solution

Open and interoperable ecosystem

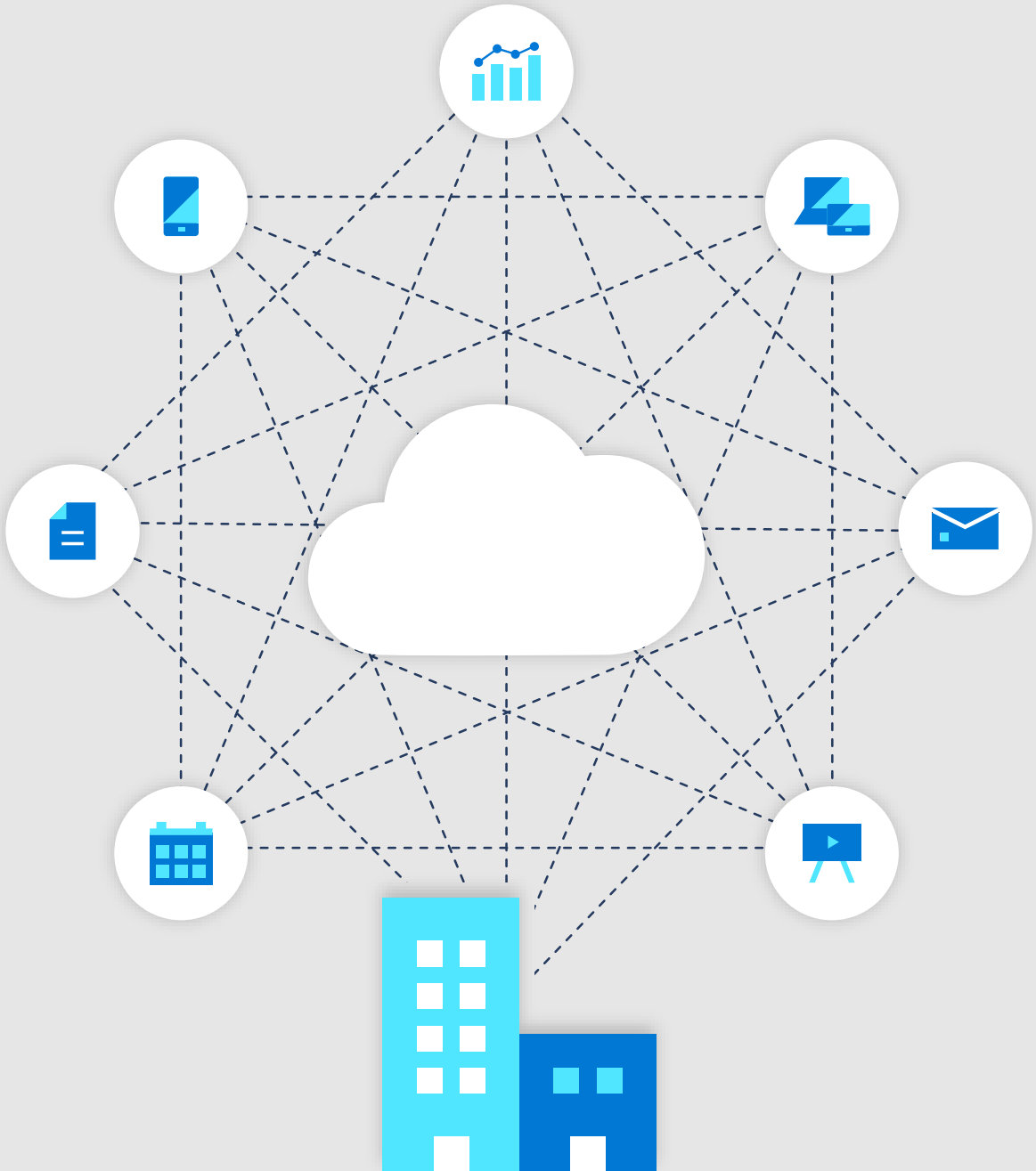
Microsoft

Securing your cloud perimeter with Azure Network Security

- Azure DDOS Protection
- Application Gateway – Azure WAF

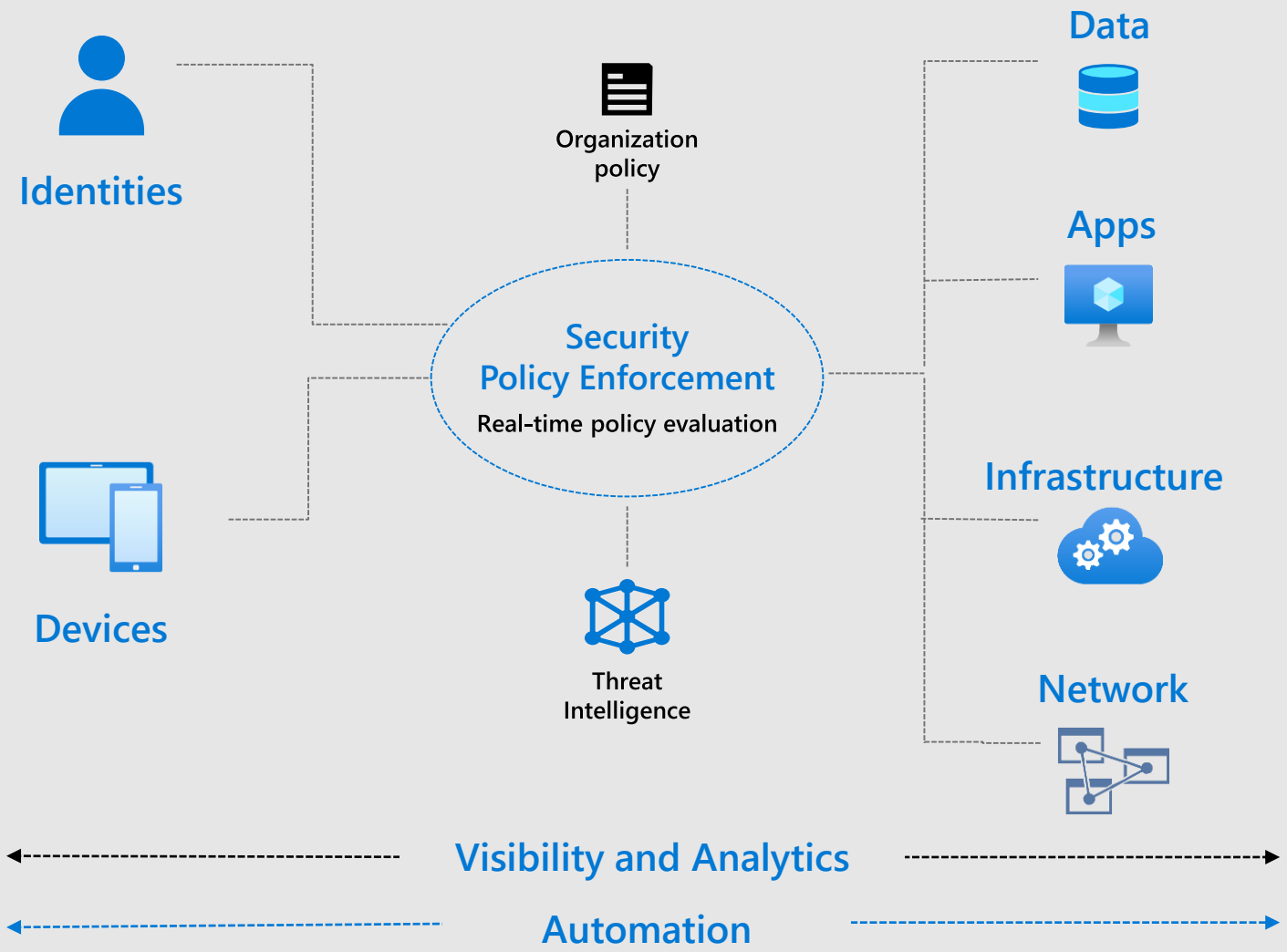
Traffic to the cloud is at a tipping point

- Applications moving to cloud
- SaaS apps usage is increasing
- Modern apps are growing



Network security approach requires foundational change

Zero Trust Architecture

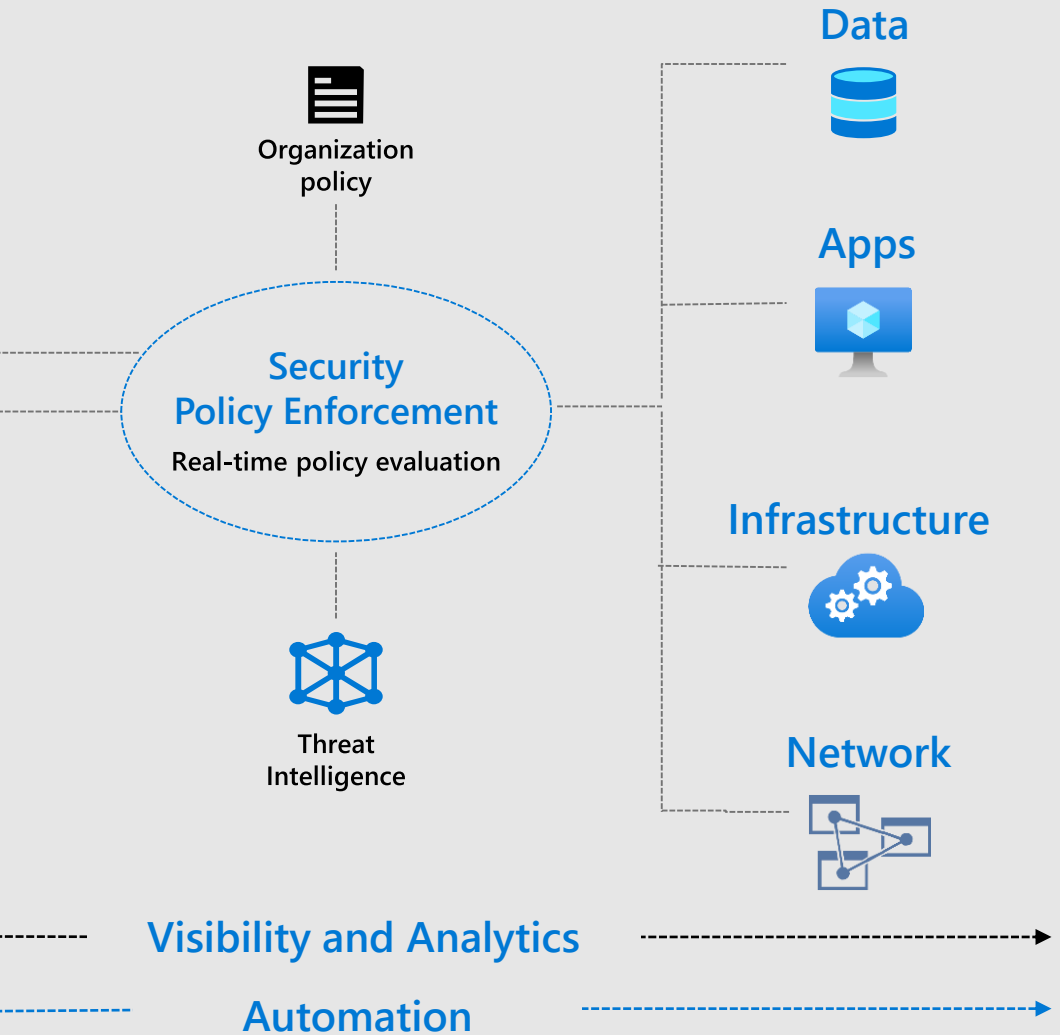


Guiding Principles of Zero Trust :

1. Verify explicitly
2. Use least privilege access
3. Assume breach

https://www.Microsoft.com/en-us/security/

Zero Trust Networking Maturity Model

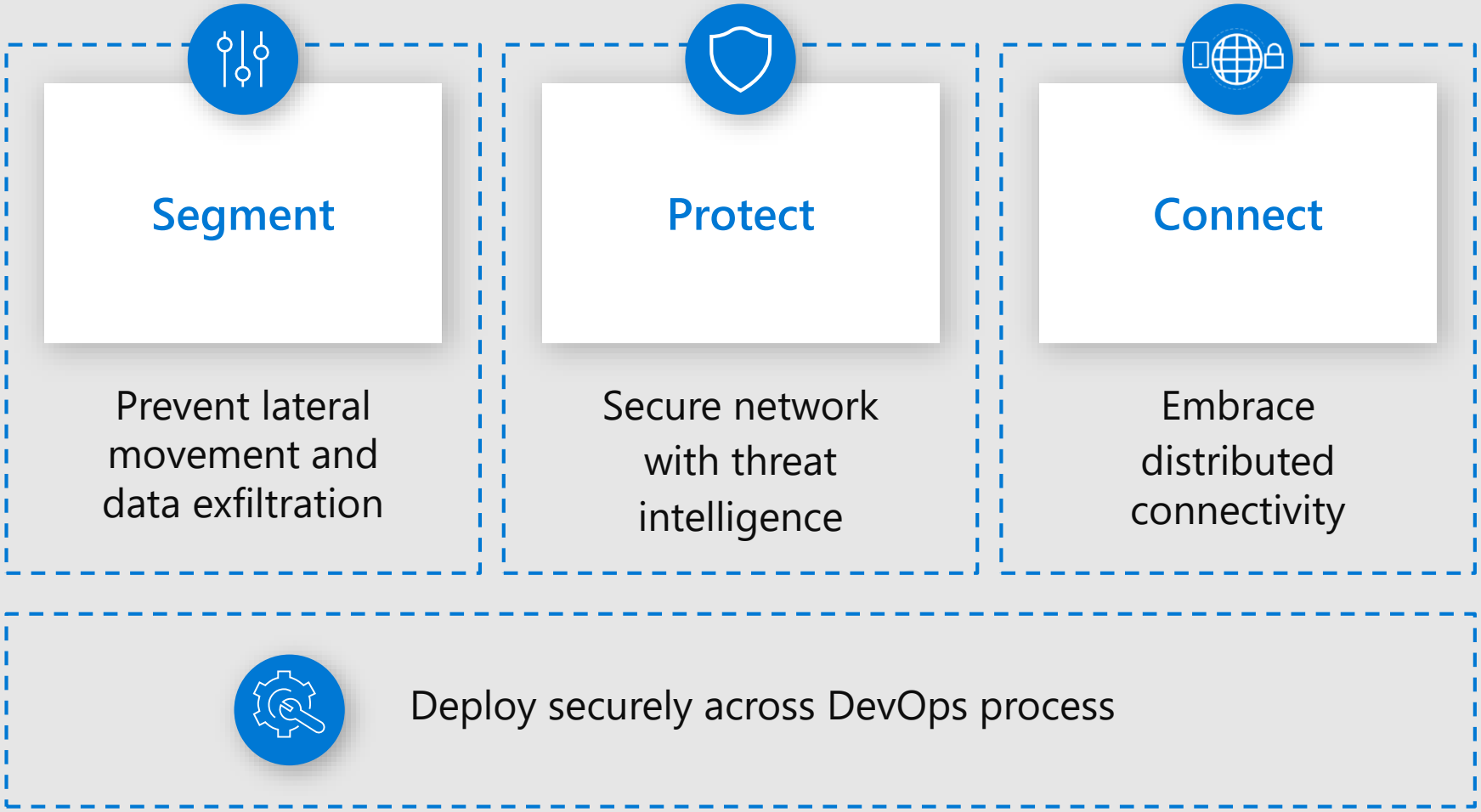


Network

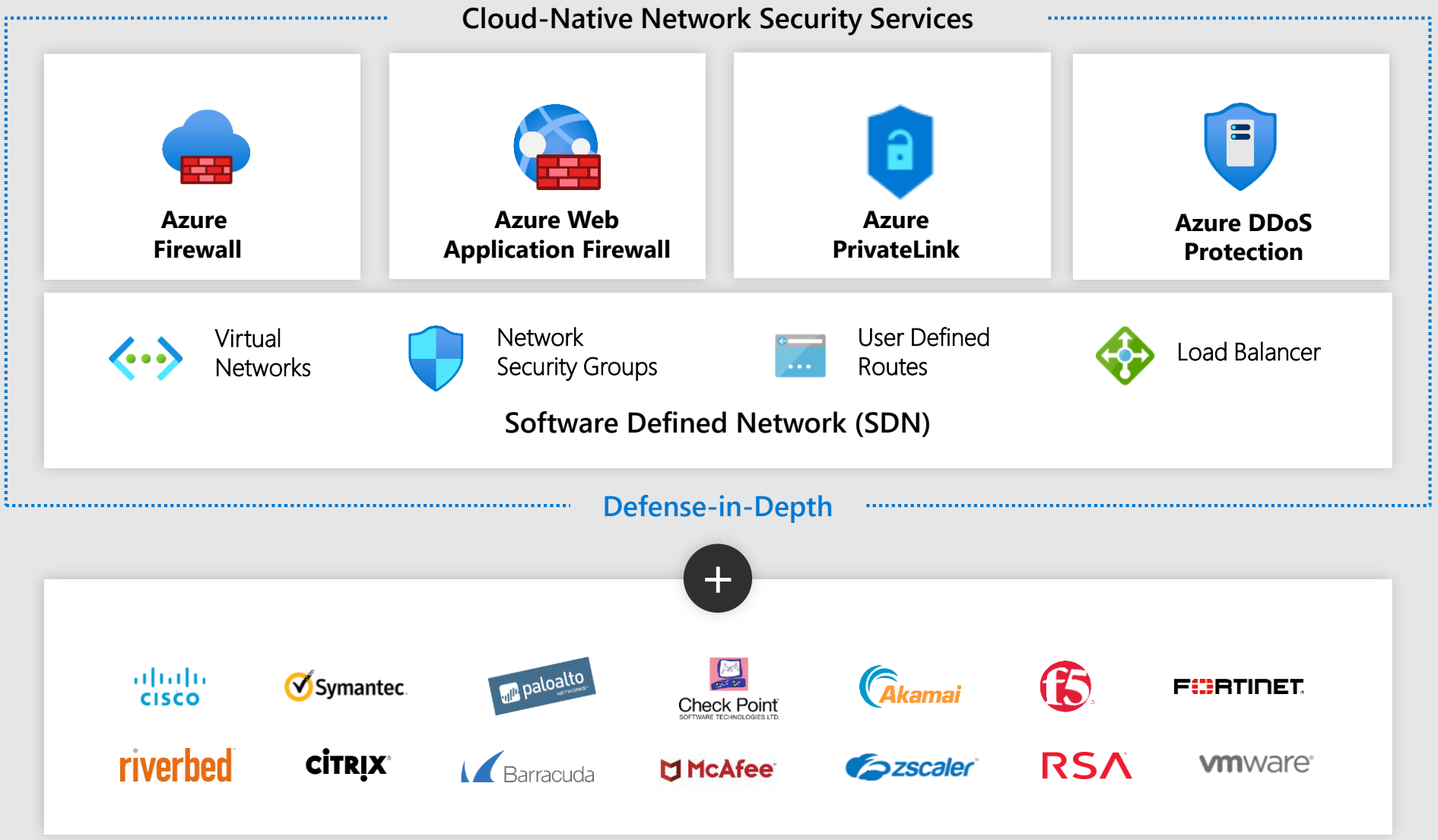
Traditional	Advanced	Optimal
Few network security perimeters and flat open network	Many ingress/egress cloud micro-perimeters with some micro-segmentation	Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation
Minimal threat protection and static traffic filtering	Cloud native filtering and protection for known threats	ML-based threat protection and filtering with context-based signals
Internal traffic is not encrypted	User to ap internal traffic is encrypted	All traffic is encrypted

Azure Network Security

Cloud native services to help secure cloud perimeter



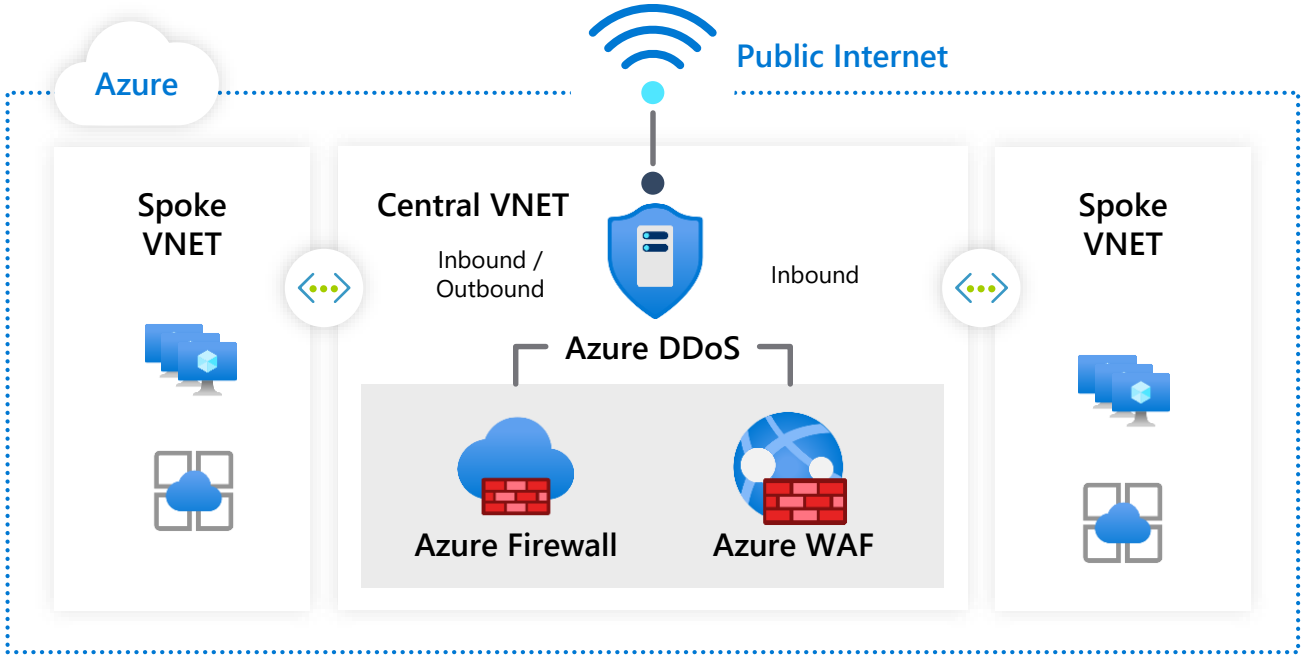
Achieving Zero Trust with Azure Networking

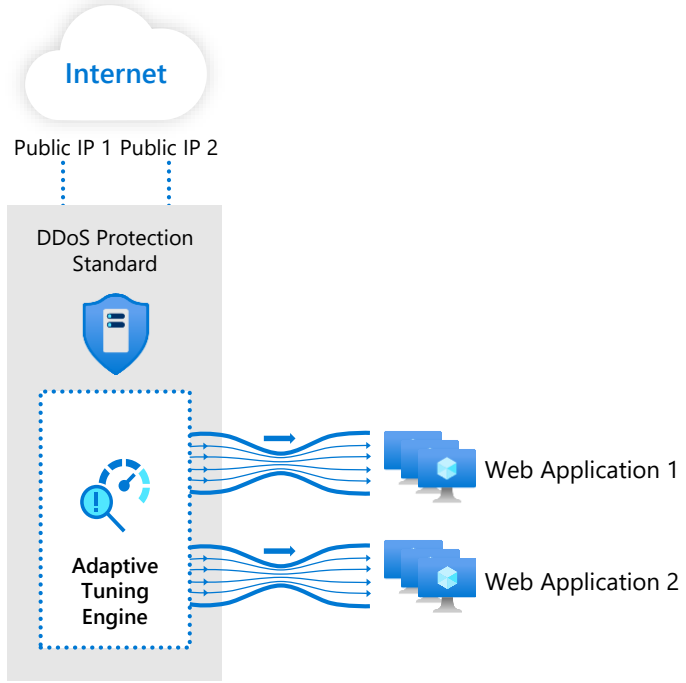


Azure DDoS Protection Standard

Cloud scale DDoS protection for Azure

1. Azure global network
2. Adaptive tuning
3. Attack analytics and metrics
4. DDoS Rapid Response (DRR)
5. SLA guarantee and cost protection





Azure DDOS Protection

Standard

Tuned to your apps

Logging, alerting and telemetry via Azure Monitor

L7 Protection via Web App Firewall (WAF)

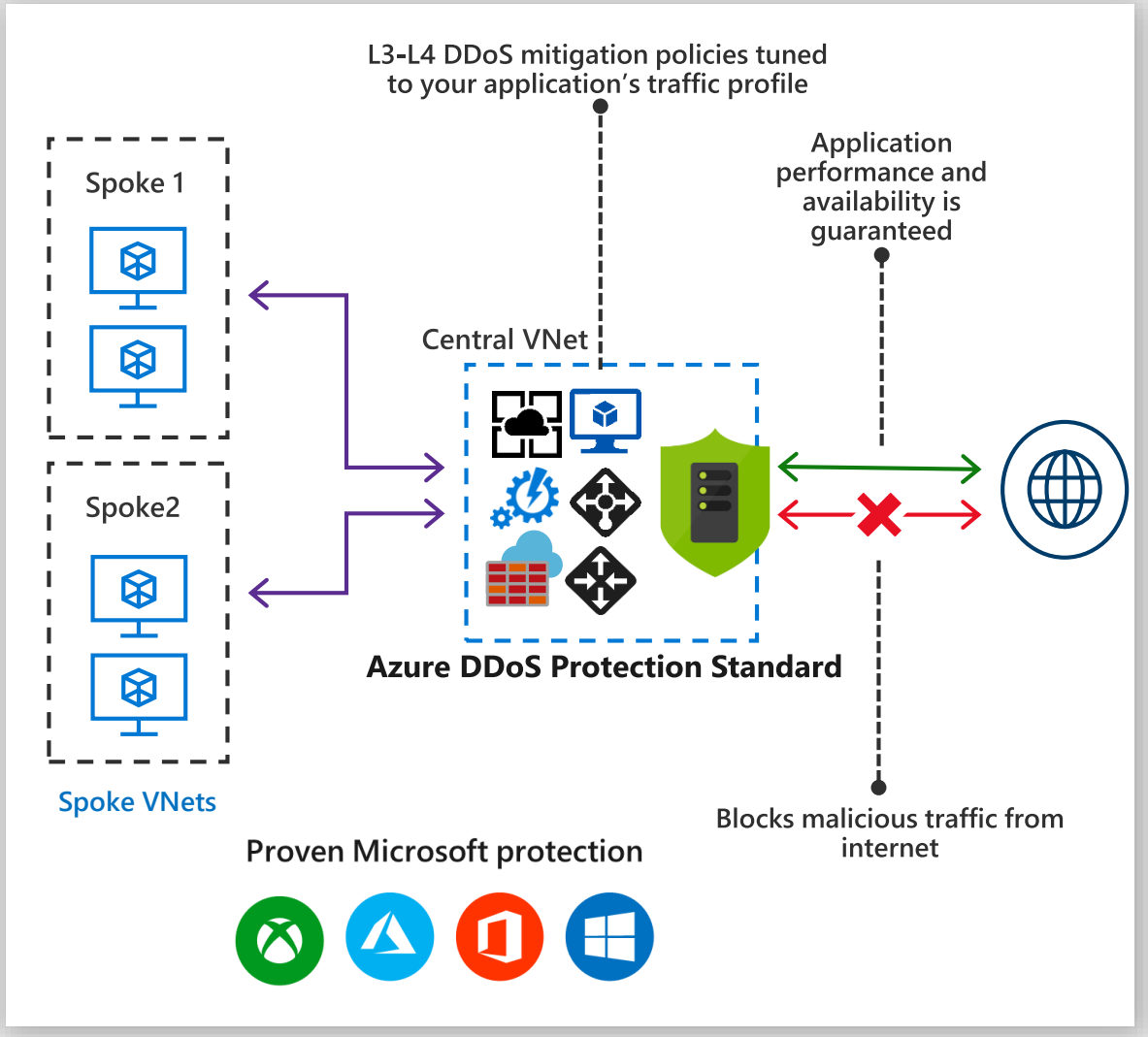
Availability Guarantee and Rapid Response Support

Basic

Always on L3/L4 attack protection

Deployed today in all Azure regions

No additional charge and available to all Azure Customers



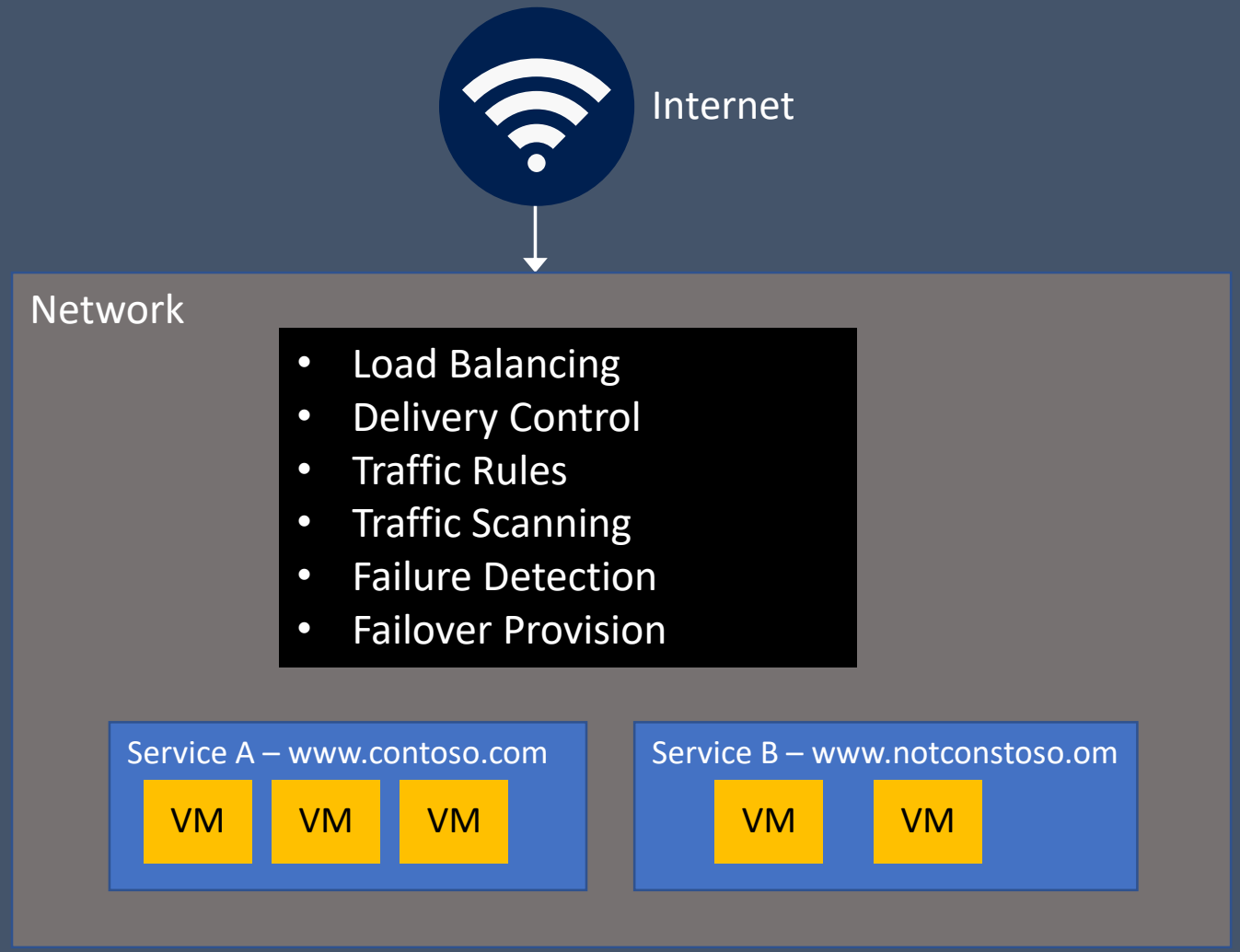
Application Gateway

- Dedicated network “virtual” appliance which virtualizes network functions at layer 7 – Application Level

Or

- A device which peeks into application-level data before customer’s service and performs certain functions before forwarding:
- Like
  - Delivery controller
  - Load balancing
  - Security - Web application firewall

User Story: Application Gateway



We know Network "**Can't Do Without**"s: Router, Switches, Hubs, DHCP Server, Proxy, DNS, etc

What are additional services **Customer** look for in a smart and safe network ?

Network Functions Virtualized!

Features	OSI Model Layer 4 - Transport	OSI Model Layer 7 - Application

Load Balancer	• Server IP/Port
	• Server Affinity -Source IP/Port
		• HTTP/HTTPS
		  ○ Hostname – Mutli-tenant backend
		  ○ Server Affinity using cookie data

Content Delivery	• IP Headers: Server IP & Port	• HTTP/HTTPS - based URL/Header/Body
Server Probes (Failure Detection)	• TCP Probing (<backend_ip>:80)	• HTTP Probing (http://<backend_ip>/probe)
Failover	• Region level – using Dynamic DNS • Network level	• Network level

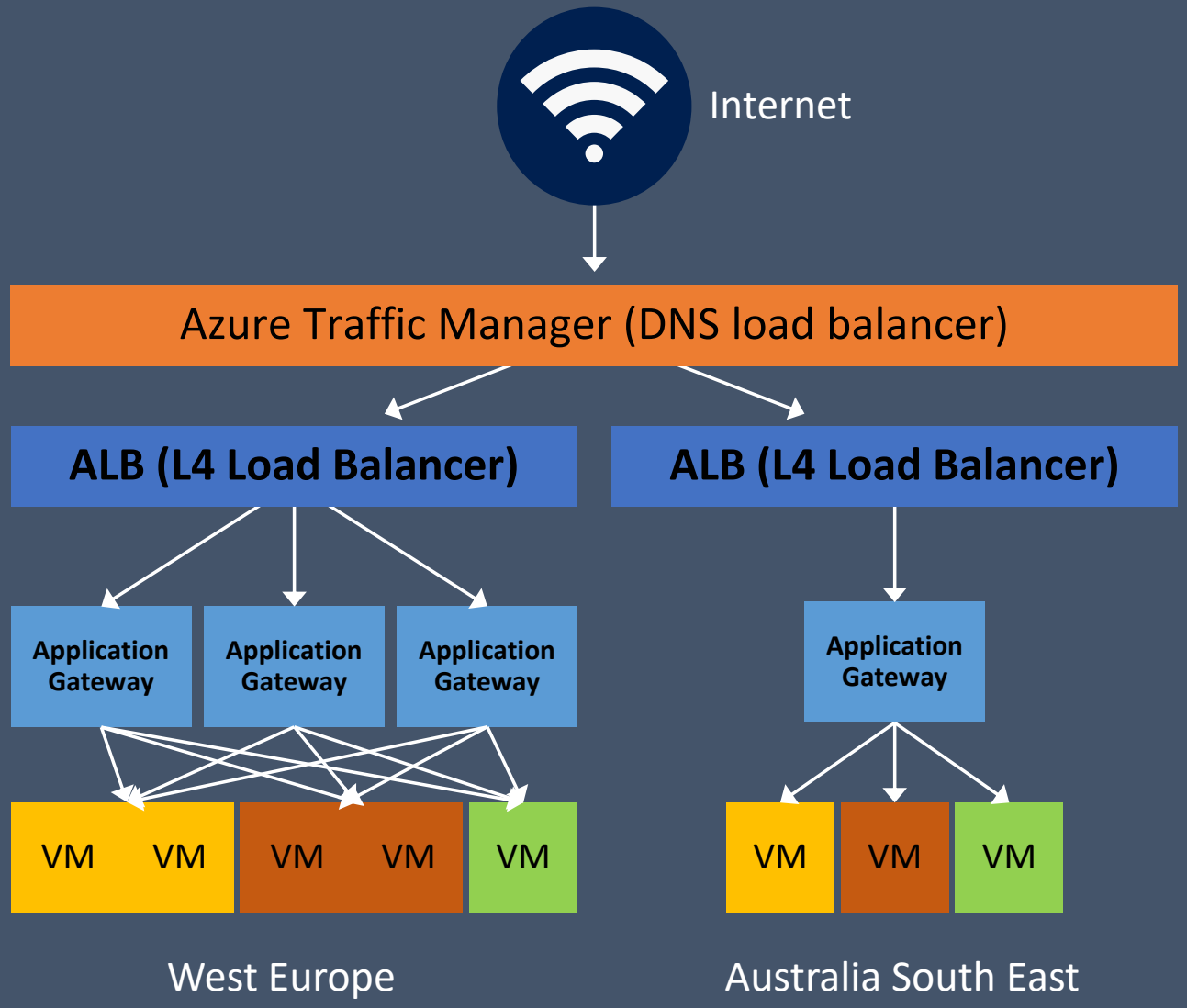
Security	• IP Blacklist
	• DDoS Attack
	• Allow/Deny Traffic Rules
		• Web Application Firewall(WAF)
		  ○ SQL Injection
		  ○ Cross-Site Scripting
		• Encryption/Decryption – TLS/SSL
		• Redirection – (HTTP to HTTPS)
		• SSL Offload + Central Certificate management - for all fronted services

Testing	• A/B Testing – Client IP	• A/B testing – using request filtering
Network Diagnostics (Backend health)	• IP packet – location/demographic	• HTTP packet – deeper logging with http payload

Application Gateway Use-Case Stories

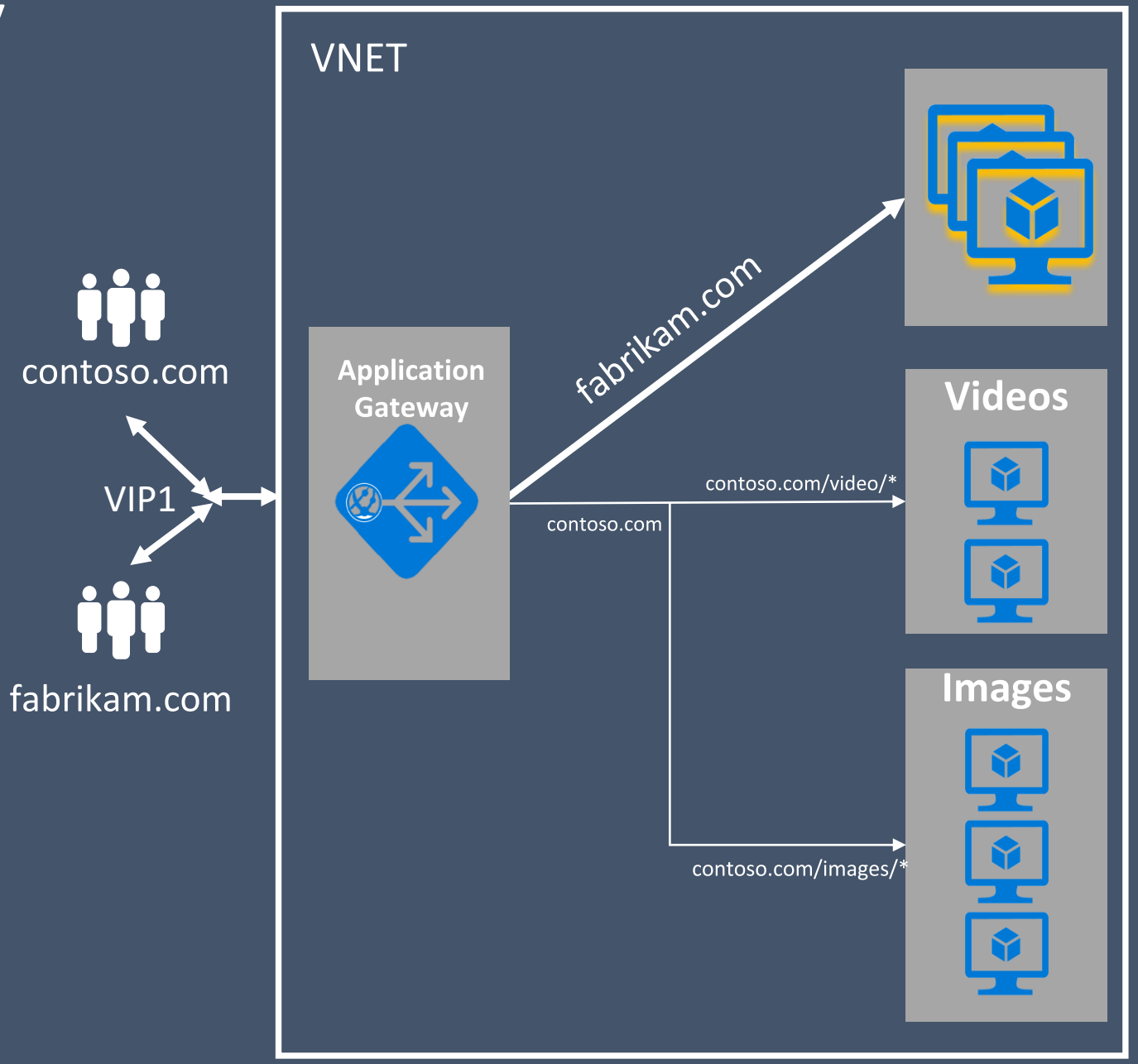
Load Balancer Story

AZURE SERVICE	WHAT	EXAMPLE
Traffic Manager (TM)	Cross-region redirection and availability	http://news.com ➔ apac.news.com ➔ emea.news.com ➔ us.news.com
Azure Load Balancer (SLB, ILB)	In-region scalability and availability	emea.news.com ➔ AppGw1 ➔ AppGw2 ➔ AppGw2
Azure Application Gateway (AppGW)	URL/content-based routing and Load Balancing	news.com/top news news.com/sports news.com/images
VMs	Web servers	IIS, Apache, Tomcat



Content Delivery Story

- Multi site support
  - Each domain to its own backend pool
  - SSL offload via Server Name Indication (SNI)
- URL based routing
  - Backend pool selection based on request path



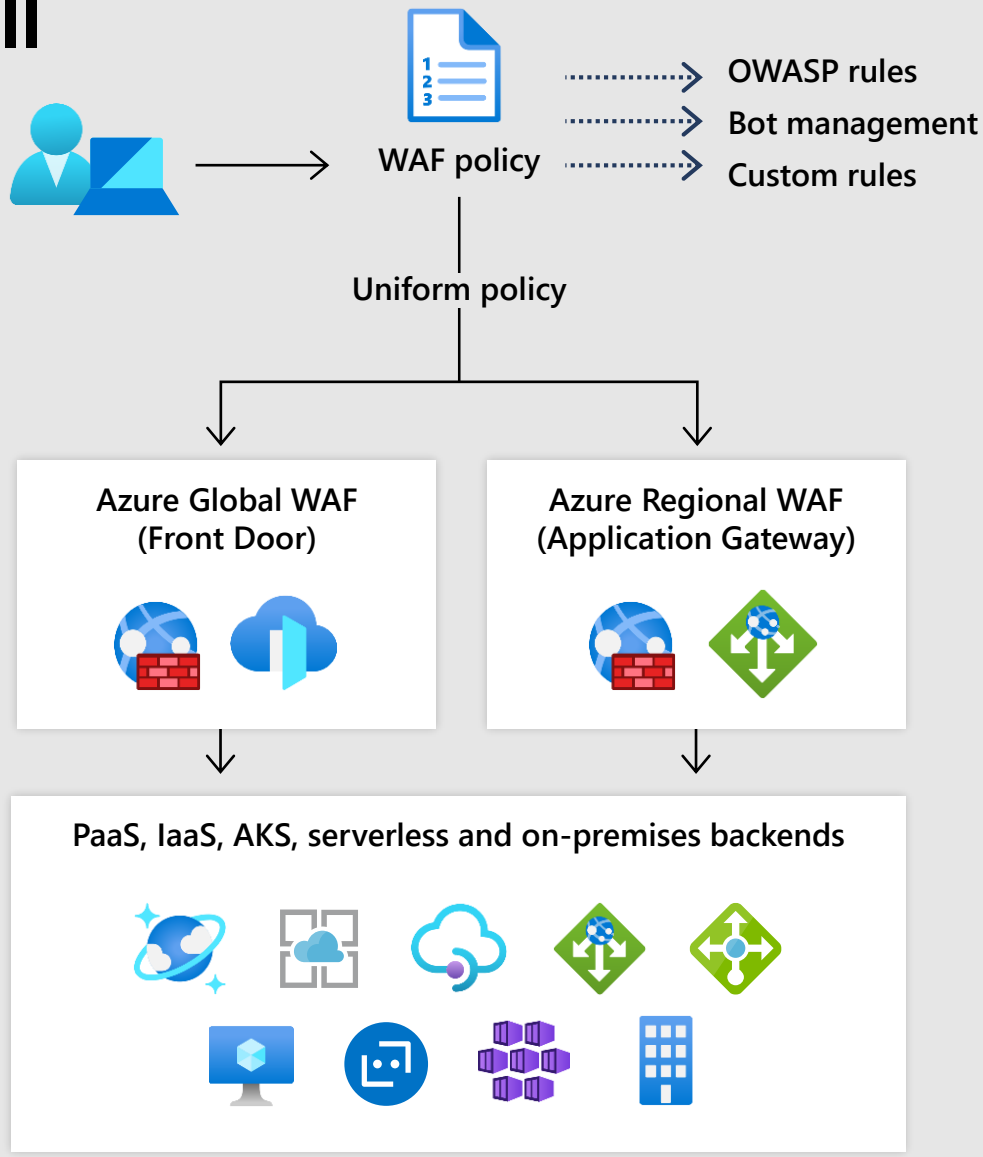
Security Story

Features	Examples
SQL injection protection	statement = "**SELECT** * **FROM** users **WHERE** name = '" + userName + "';" **SELECT** * **FROM** users **WHERE** name = '' **OR** '1'='1';
Cross site scripting protection	*$user_name = $_GET['name']; echo "Welcome $user_name ";* *http://www.yoursite.com/index.html?name=<script>alert('XSS vulnerability')</script>*
Protection against HTTP protocol violations	Content-Length: null
Prevention against bots, crawlers, and scanners	Causes unnecessary amount of hits

Azure Web Application Firewall

Protect your apps at network edge or in Azure regions using a Unified WAF policy

PREVIEW



Microsoft threat intelligence

- Protect apps against automated attacks
- Manage good/bad bots with Azure BotManager RuleSet

Site and URI path specific WAF policies

- Customize WAF policies at regional WAF for finer grained protection at each host/listener or URI path level

Geo filtering on regional WAF

- Enhanced custom rule matching criterion includes filtering by country

Microsoft

Protect your cloud workload from threats using Azure Security Center

Azure Security Center helps unify security management and protects hybrid cloud workloads

Gain visibility and control

Centrally manage security of hybrid workloads

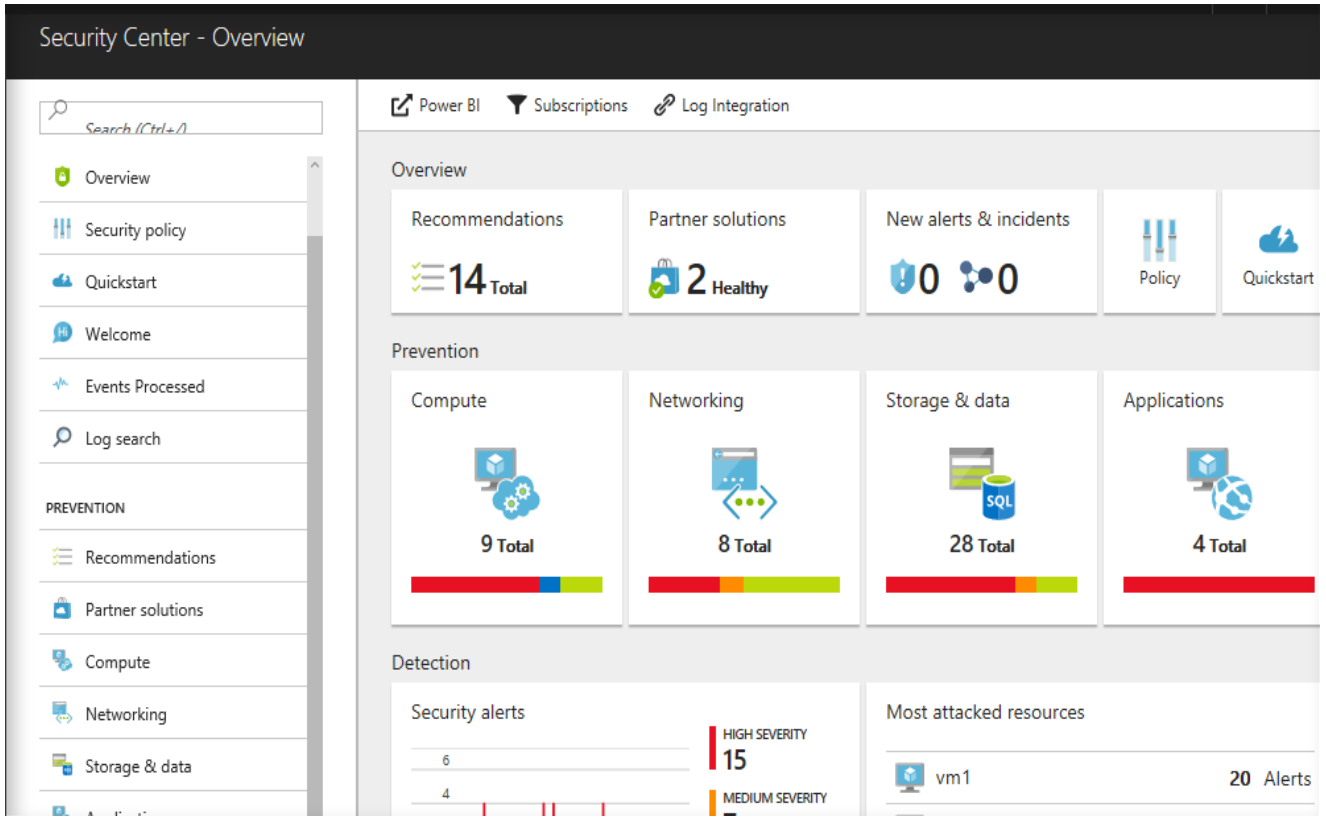
Prevent threats with adaptive controls

Harden OS, VNet, storage, and SQL configurations and apply preventive controls

Enable intelligent detection and response

Monitor VM events and network traffic to identify threats and react quickly

Azure Security Center
Gain Visibility and Control



Automatically discover and monitor security of Azure resources across compute, networking, storage and apps

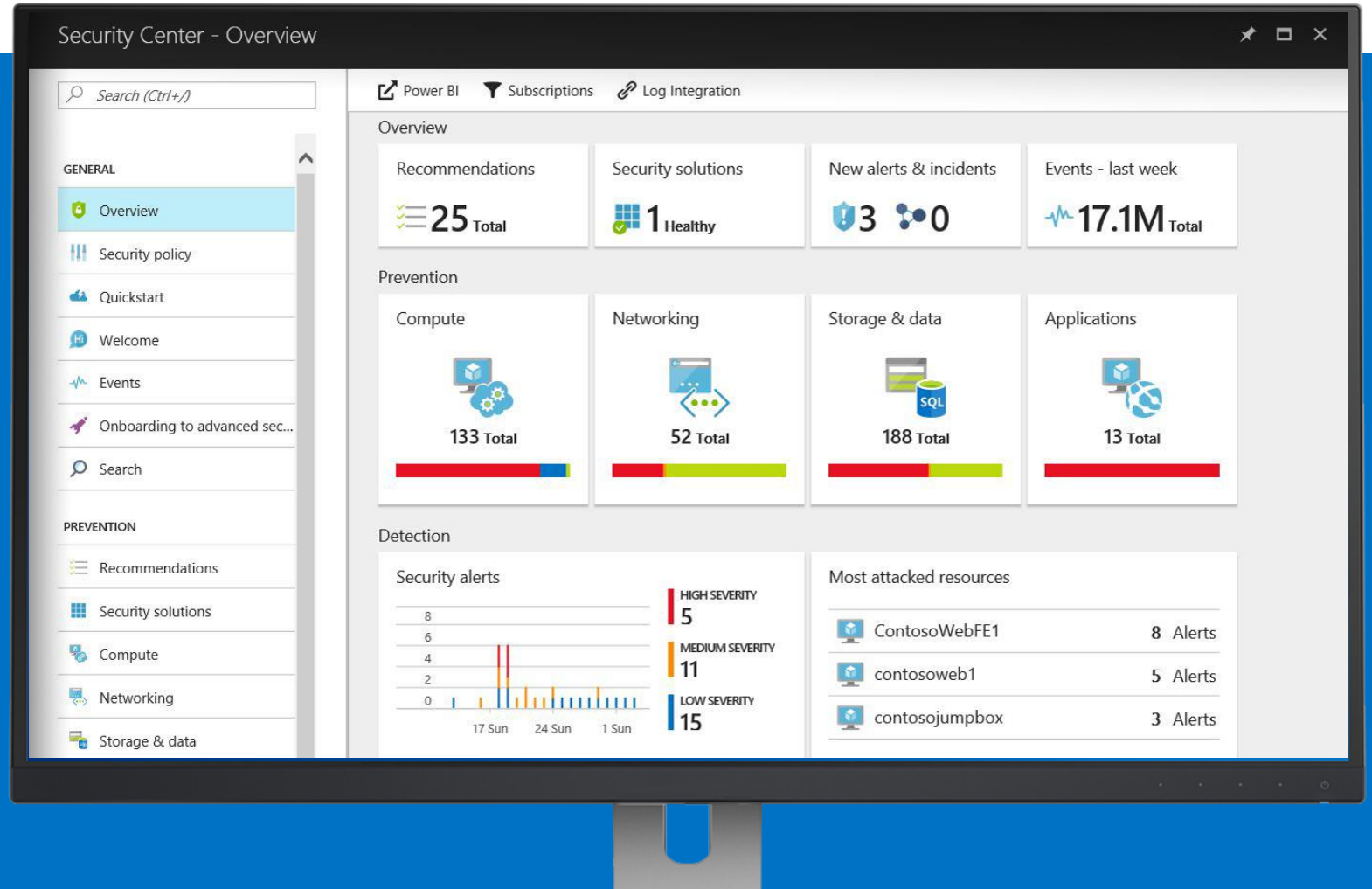
Central policy management – create and apply policies across multiple subscriptions

Simplify security operations with visual, interactive investigations

Azure Security Center

Unified Visibility and Advanced Threat Protection, Detection, and Response

- **Identify security events that require your attention**
- **Run built-in or customer security assessments**
- **Resolve prioritized, actionable security recommendations**
- **Limit exposure to brute-force attacks with port lock-down and just-in-time access**
- **Block malware with adaptive whitelisting**



Azure Security Center

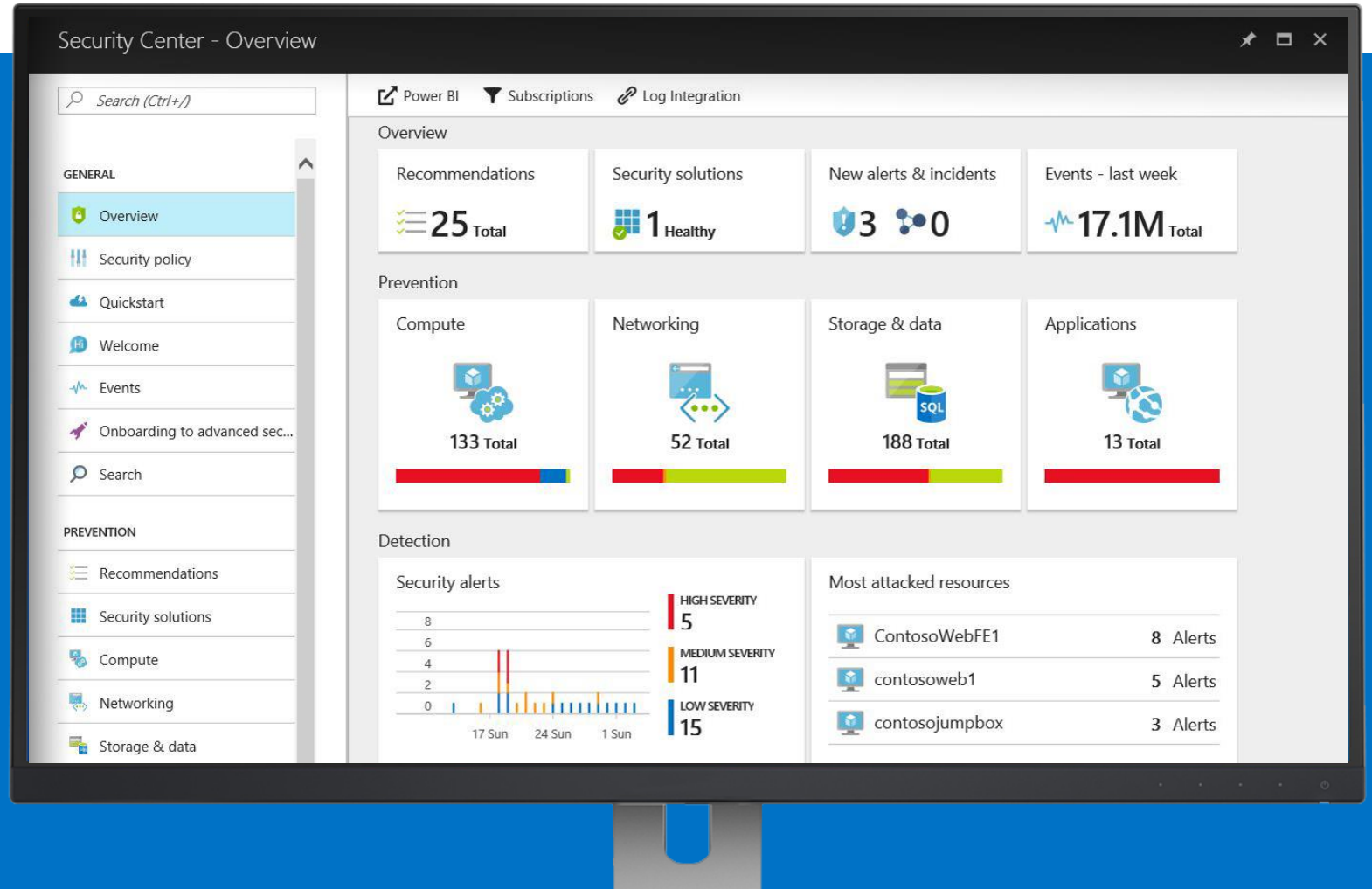
Security State Across Hybrid Workloads

Built-in Azure; No Setup Required

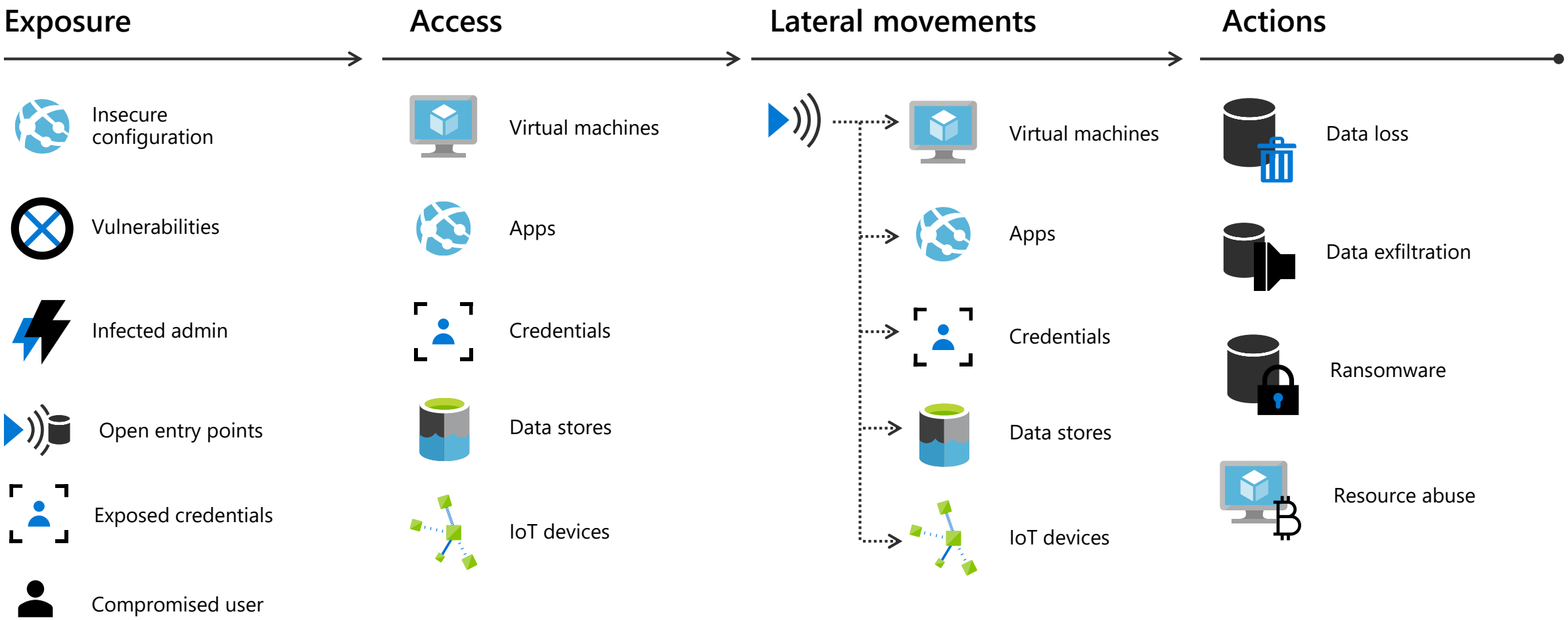
- Automatically discover and monitor security of Azure resources

Gain Insights for Hybrid Resources

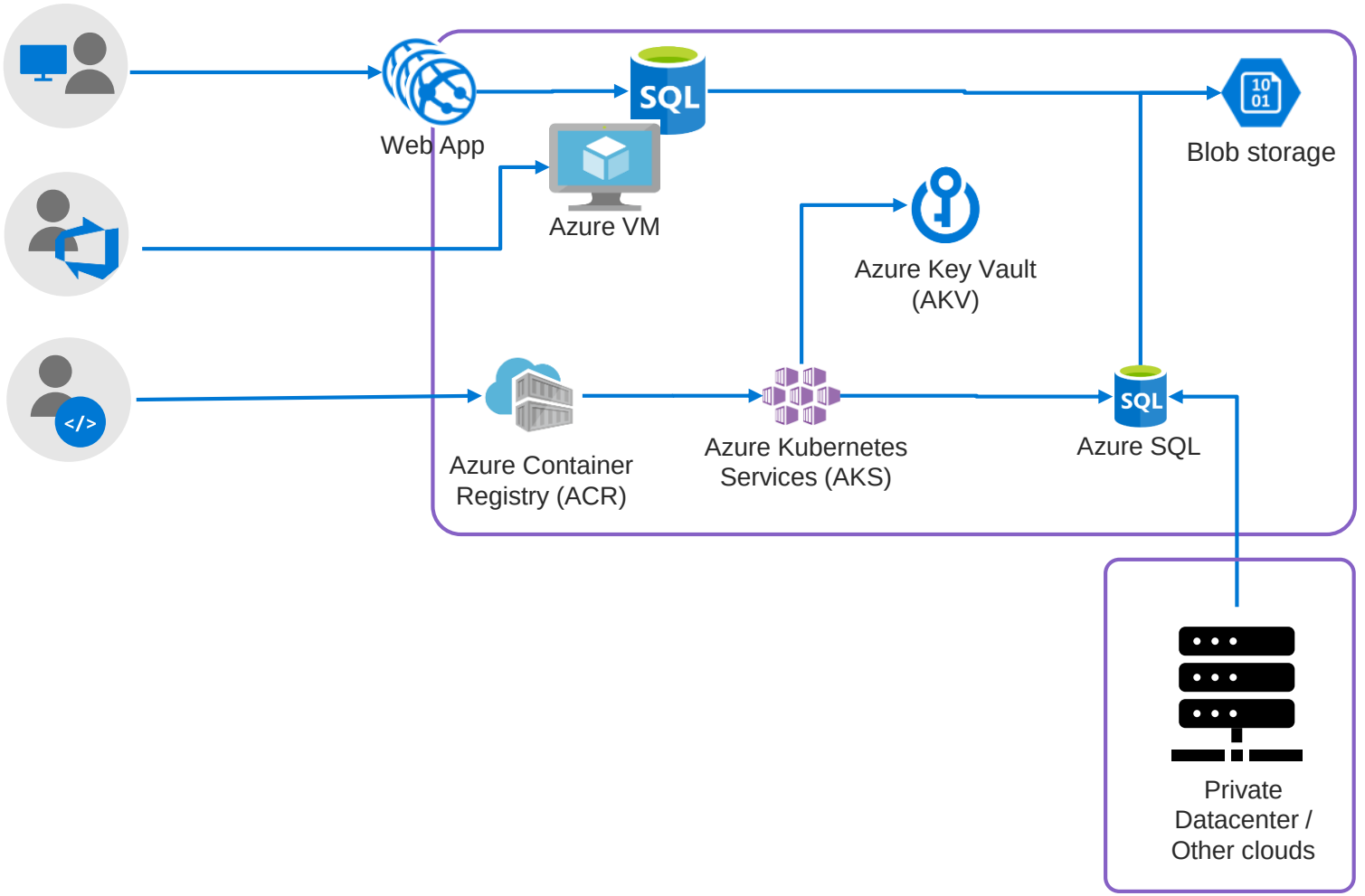
- Easily onboard resources running in other clouds and on-premises



Threat actors leverage a variety of exposures to breach



Workloads become heterogenous and hybrid



Common threats we see in the wild

VMs

- Brute force of open management ports
- Exploit through an unpatched vulnerability
- Run bitcoin mining on a compromised VM

Containers

- Exposed Kubernetes dashboards
- RBAC not configured in the cluster
- Insecure container/host configuration

App services

- Web shell deployment
- server-side request forgery (SSRF)
- Reconnaissance attempts

SQL Database

- SQL injection vulnerabilities and attacks
- Access by a remote threat actor
- Brute-force against SQL credentials

Storage account

- Use to propagate malware or load malicious images/packages
- Access by a remote threat actor
- Public access to storage accounts
- Harvest for reconnaissance or exfiltration of data

Key Vault

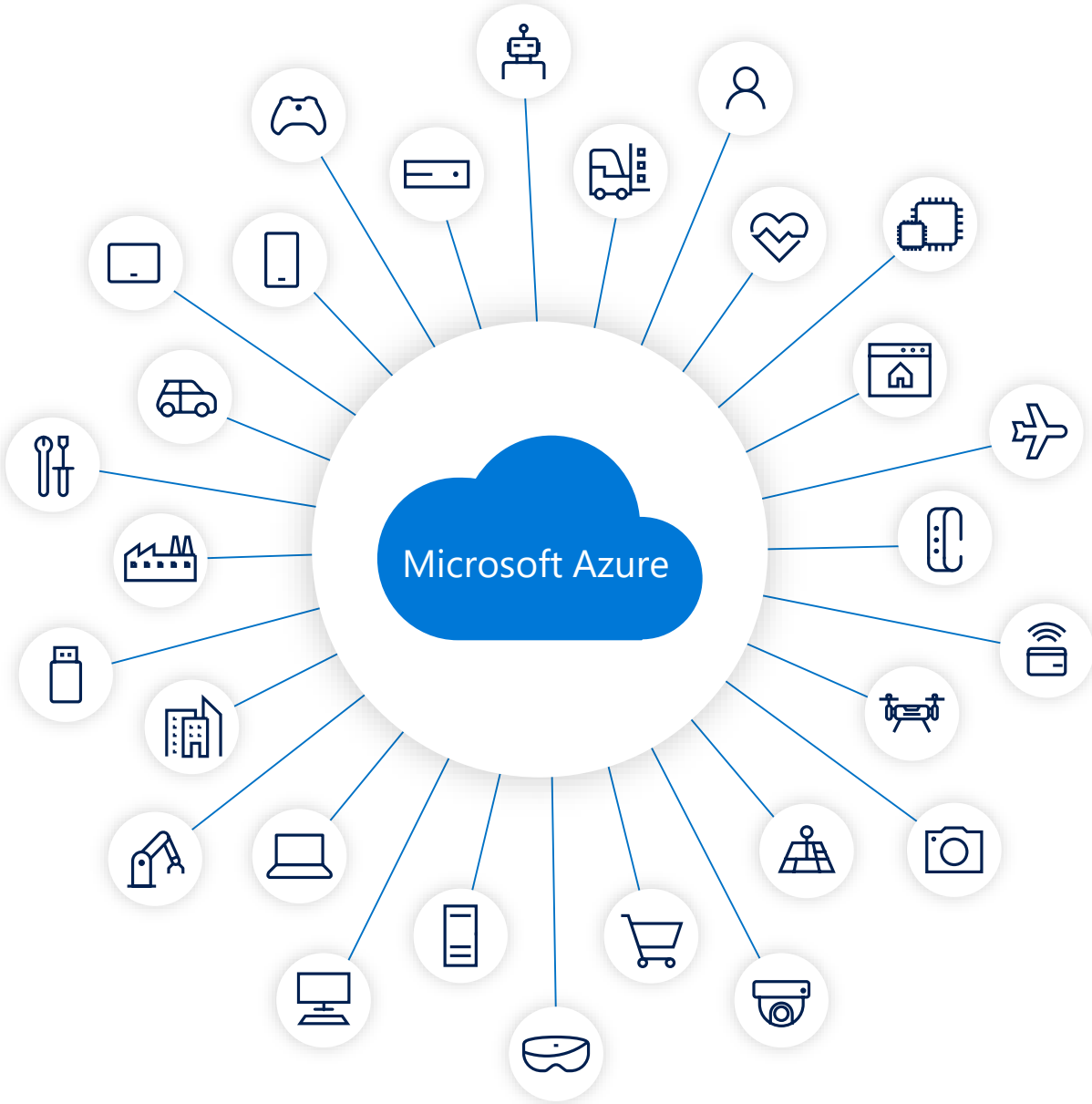
- Permissive policies grant access to unneeded resources
- Harvest for secrets

Gain unmatched security with Azure

$1B annual investment in cybersecurity

3500+ global security experts

Trillions of diverse signals for unique intelligence



Azure security center

Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Protect against threats

For servers

For cloud native workloads

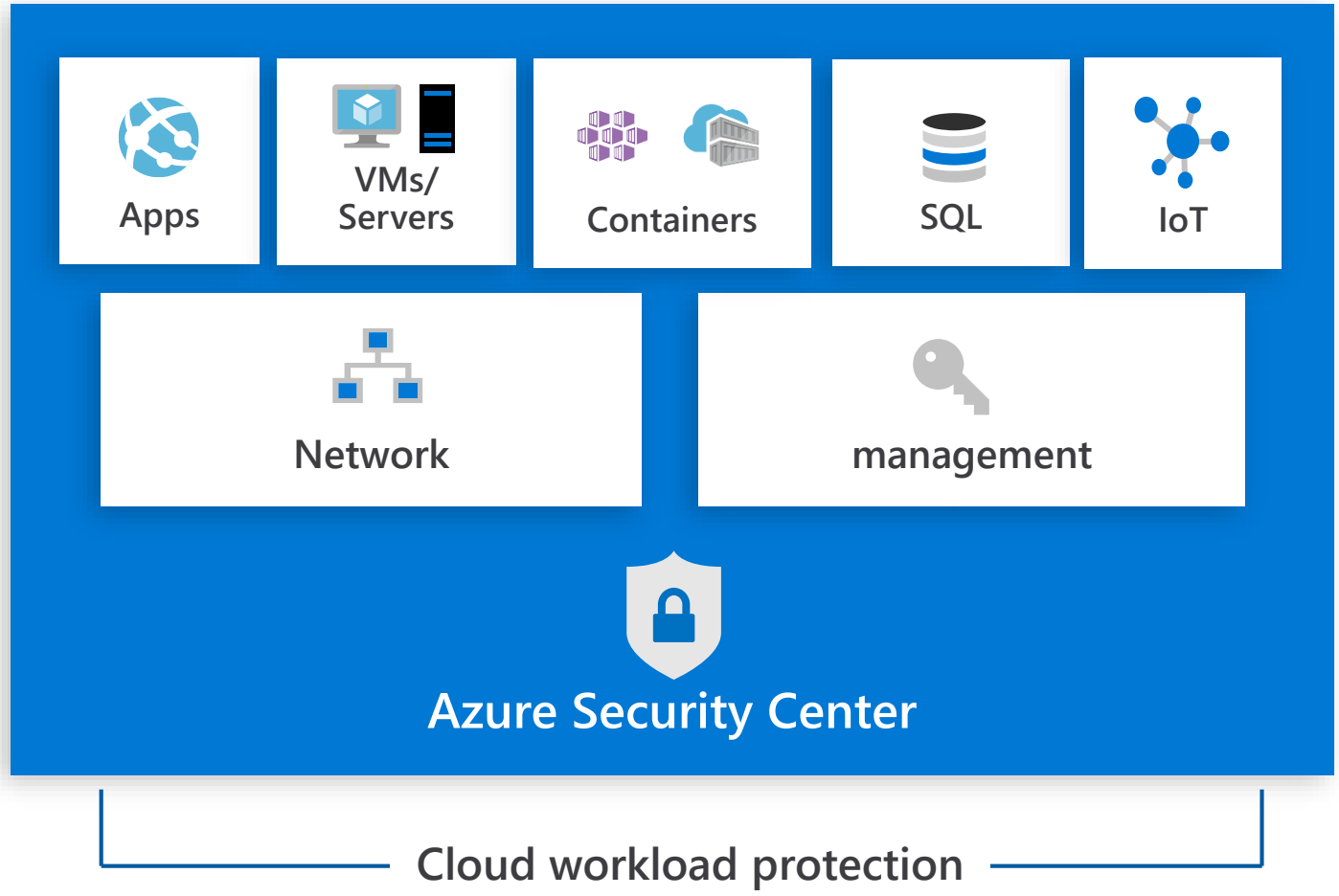
For databases and storage

Get secure faster

Protect your workloads from threats

Use industry's most extensive threat intelligence to gain deep insights

- Detect & block advanced malware and threats for Linux and Windows Servers on any cloud
- Protect cloud-native services from threats
- Protect data services against malicious attacks
- Protect your Azure IoT solutions with near real time monitoring
- Service layer detections: Azure network layer and Azure management layer (ARM)



Settings - Pricing tier

ASC DEMO

Search (Ctrl+/)

Settings

- Pricing tier
- Data Collection
- Email notifications
- Threat detection
- Workflow automation (Preview)
- Continuous export (Preview)

Save

The Standard tier provides enhanced security. Learn more >

Free (for Azure resources only)	Standard
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Azure Secure Score	✓ Azure Secure Score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

Pricing will apply to: 126 resources in this subscription

Select pricing tier by resource type

Resource Type	Resource Quantity	Pricing	Plan
Virtual machines	45 VMs and VMSS instances	$15/Server/Month	Enabled Disabled
App Service	5 instances	$15/Instance/Month	Enabled Disabled
PaaS SQL servers	6 resources	$15/Server/Month	Enabled Disabled

By clicking Save, the standard tier will be enabled on selected resource types. The first 30 days are free.
Virtual machines, SQL servers, App Service instances and Kubernetes Service instances are billed hourly, only for running resources.
For more information on Security Center pricing, visit the pricing page.

Ignite 2018

Ignite 2019

Get secure fast, just turn it ON

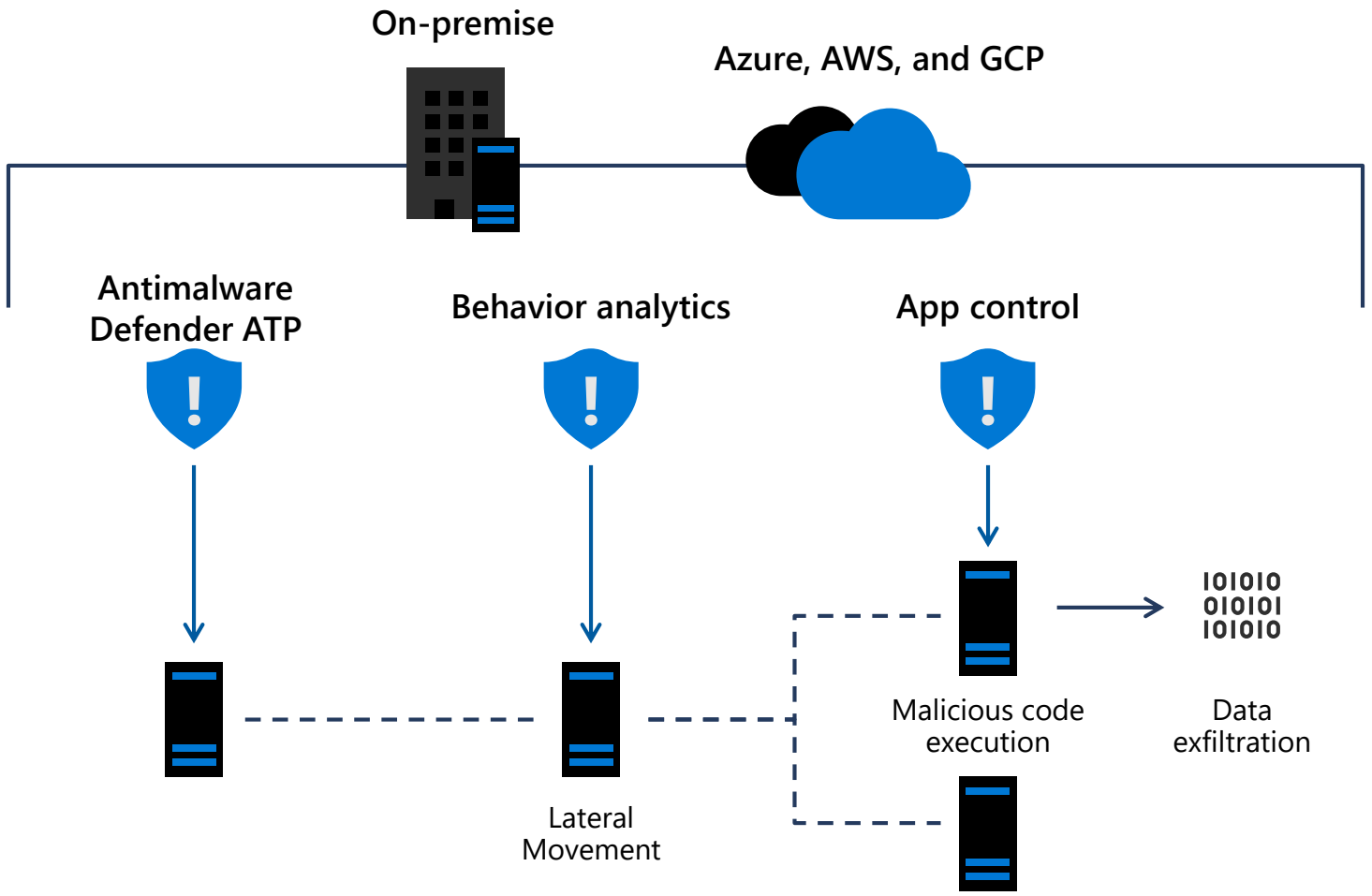
Protect Linux and Windows VMs from threats

Reduce open network ports:

- Use Just-in-Time to avoid exposure of management ports
- Limit open ports with adaptive network hardening

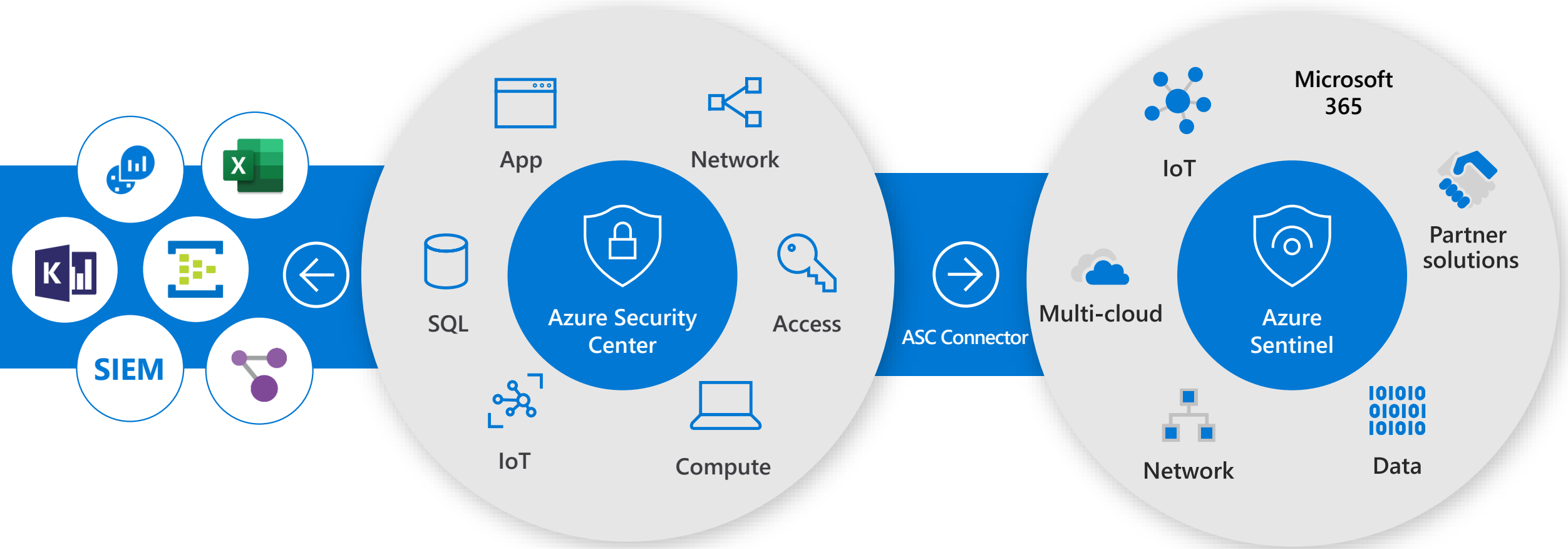
Protect against malware:

- Block malware with adaptive application controls
- Built-in Microsoft Defender ATP EDR
- Crash dump analysis and fileless attack detections



Threat protection for cloud at scale:
Export assessments and alerts for security roles

NEW



Azure Security Center
Cloud Workload Protection

Azure Sentinel
Cloud Native SIEM

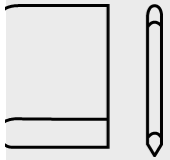
Best support for your enterprise need

Kubernetes 101 Docs
aka.ms/LearnAKS

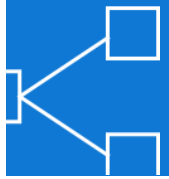
Best practices
aka.ms/aks/bestpractices

Hear from experts
aka.ms/k8s/lightboard

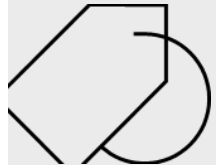
Case studies
aka.ms/aks/casestudy



Microservices architecture
aka.ms/aks/microservices



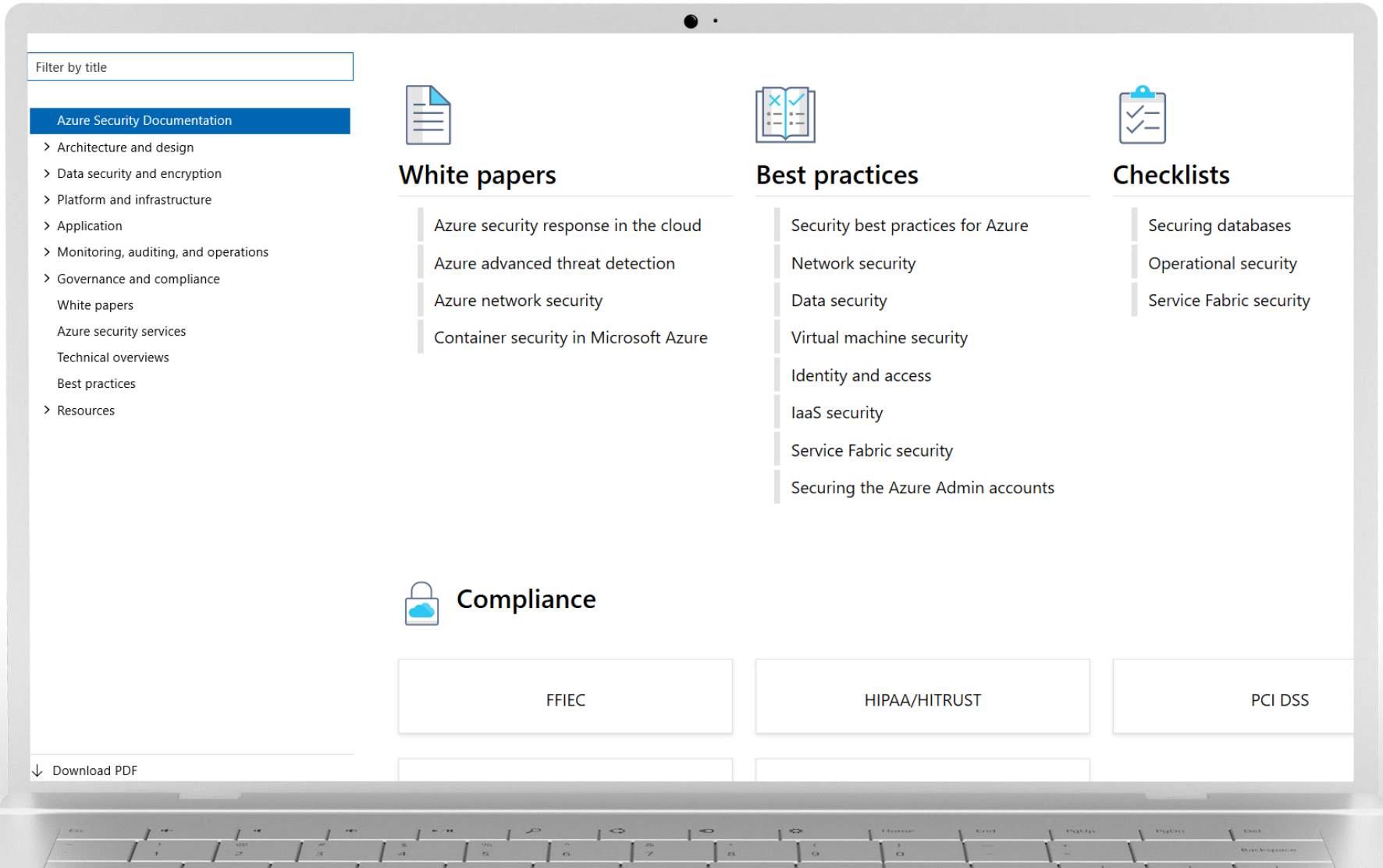
Try for free
aka.ms/aks/trial



Feedback on the roadmap? Tell us at https://aka.ms/aks/feedback

Azure Security Documentation

https://aka.ms/MyASIS



Azure Security Documentation Site has extensive information on security topics

Microsoft

Questions !

The cloud you can trust, with the numbers to prove it

90+

compliance offerings—the largest portfolio in the industry

95%

of Fortune 500 companies trust their business on Azure

$1 billion

investment (US dollars) per year in security to protect customers' data from cyberthreats