

Yes, You Can Have Security & Trust in the Cloud – Here's How

Diana Kelley
Cybersecurity Field CTO
@dianakelley14

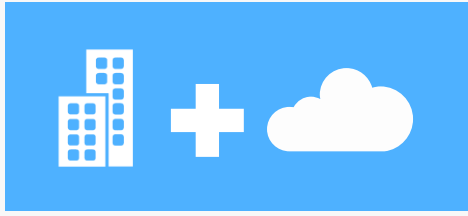


PA TechCon, May 1, 2018
10:15a-11a

Agenda

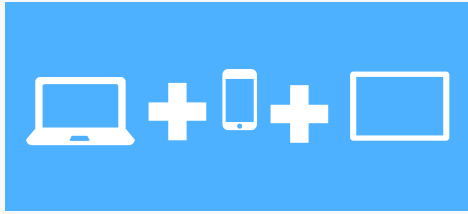
- Something old, something new
- Cloud as a security opportunity
- Hybrid Cloud and an Integrated Experience
- Shared Responsibility
- Security Built in Cloud

Information Security is in Transformation



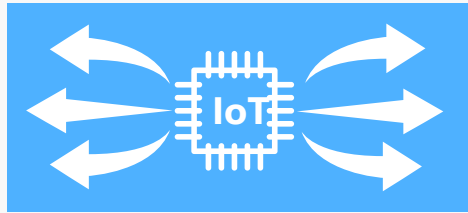
Enterprise IT is Cloud Hybrid

- Cloud adoption is inevitable (Digital Transformation + industry momentum)
- Legacy systems will take years to migrate or retire



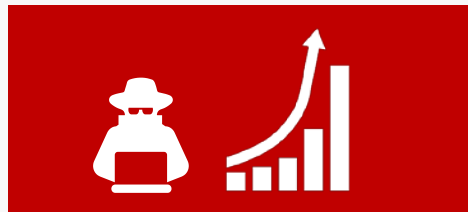
Technology Mobility and Volume is Exploding

- Increasing demand for first class experience on mobile devices
- Variance in trustworthiness of mobile devices



Pervasive Digital Transformation and IoT

- IoT adoption driving a wave of app development and cloud usage
- Enterprise PC Security strategies applying poorly to IoT devices



Increasingly Hostile Environment

- Increased attack surface with new technologies creates new blind spots
 - Attacks rising in volume and sophistication to capture illicit opportunities
- Note:** Attackers generally invest in [technical sophistication](#) only as needed

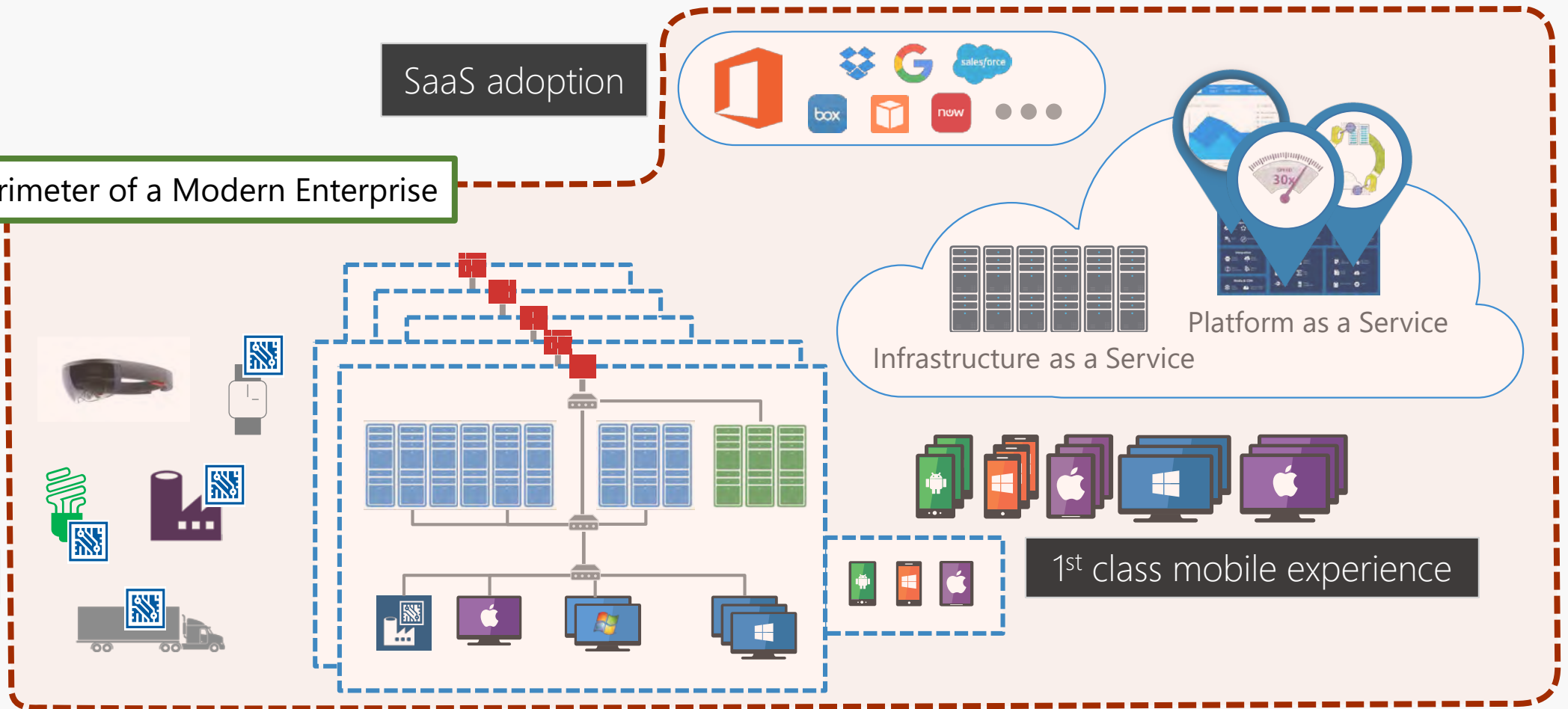
Enterprise in Transformation

Cloud Technology

SaaS adoption

Perimeter of a Modern Enterprise

Internet of Things



ENGAGE
YOUR CUSTOMERS



EMPOWER
YOUR EMPLOYEES



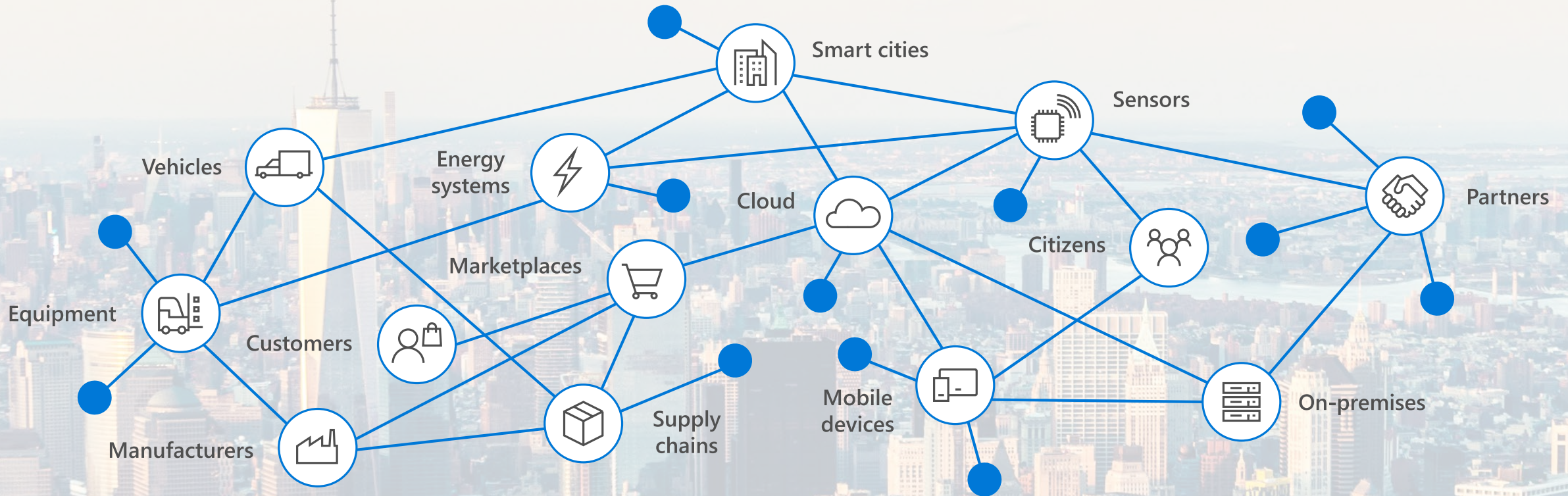
OPTIMIZE
YOUR OPERATIONS



TRANSFORM
YOUR PRODUCTS



The digital estate



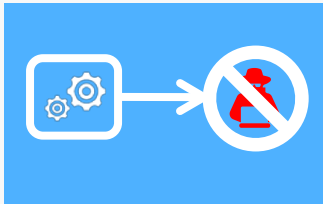
Imperatives and opportunity to reimagine security

Monitor and manage your hybrid cloud estate:



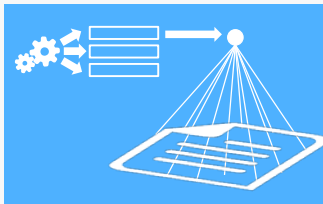
Visibility and Control over Blind spots

Identity security perimeter to protect cloud, mobile, and IoT assets
Automated policy monitoring and enforcement for modern estate



Agile and Efficient Threat Protection

Automated and integrated toolsets for response efficiency and effectiveness
Integrated telemetry to reduce noise and increase accuracy



Find and Protect Intellectual Property & Regulated data

Automate classification as documents are created
Persist data protection throughout its lifecycle

Securing the Modern Enterprise

Integrated Security Experience

Integrate trillions of diverse threat signals, TPM hardware isolation, machine learning, and human analysis into platform and tools

We Run on Cloud

7+ Years of Azure and Office 365

We Run Cloud Services

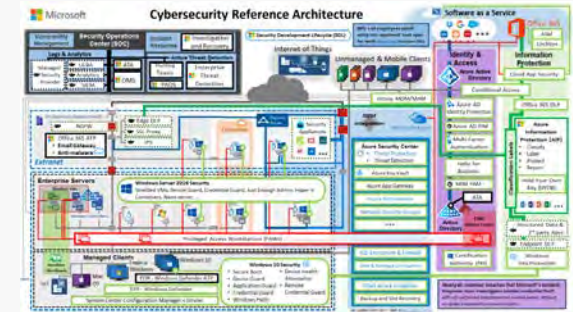
22 years of Online Experience

Security is in our DNA

- 15 years of investment into trustworthy and secure computing
- More than \$1 billion per year in security research and development

We manage attacks 24x7

- Continuous attacks on Microsoft environments
- Attacks on enterprise customers

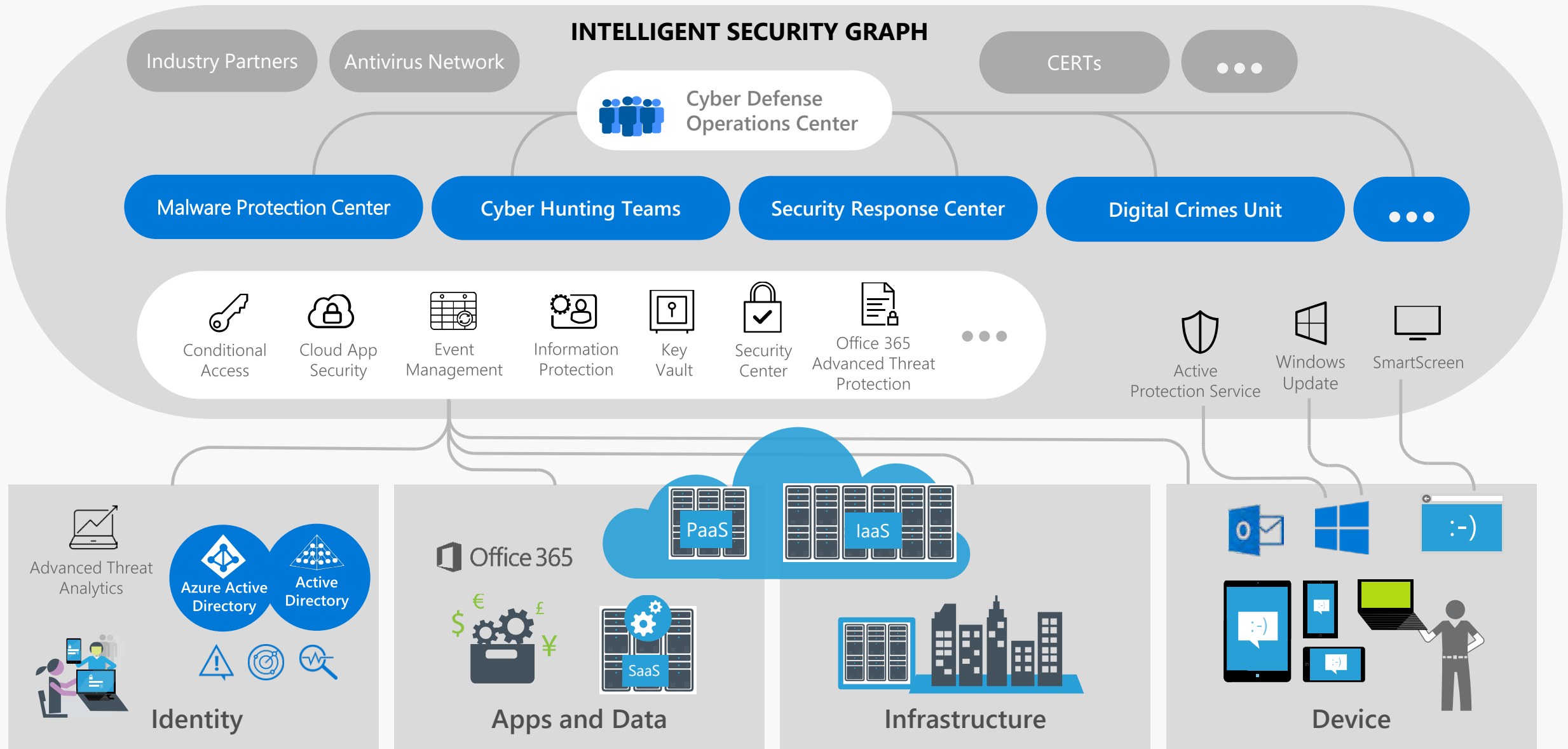


Cybersecurity Reference Architecture

Recommended Strategies & capabilities

- Security Management
- Threat Protection
- Information Protection
- Identity & Access Management
- ...and more

Building an Integrated Security Experience

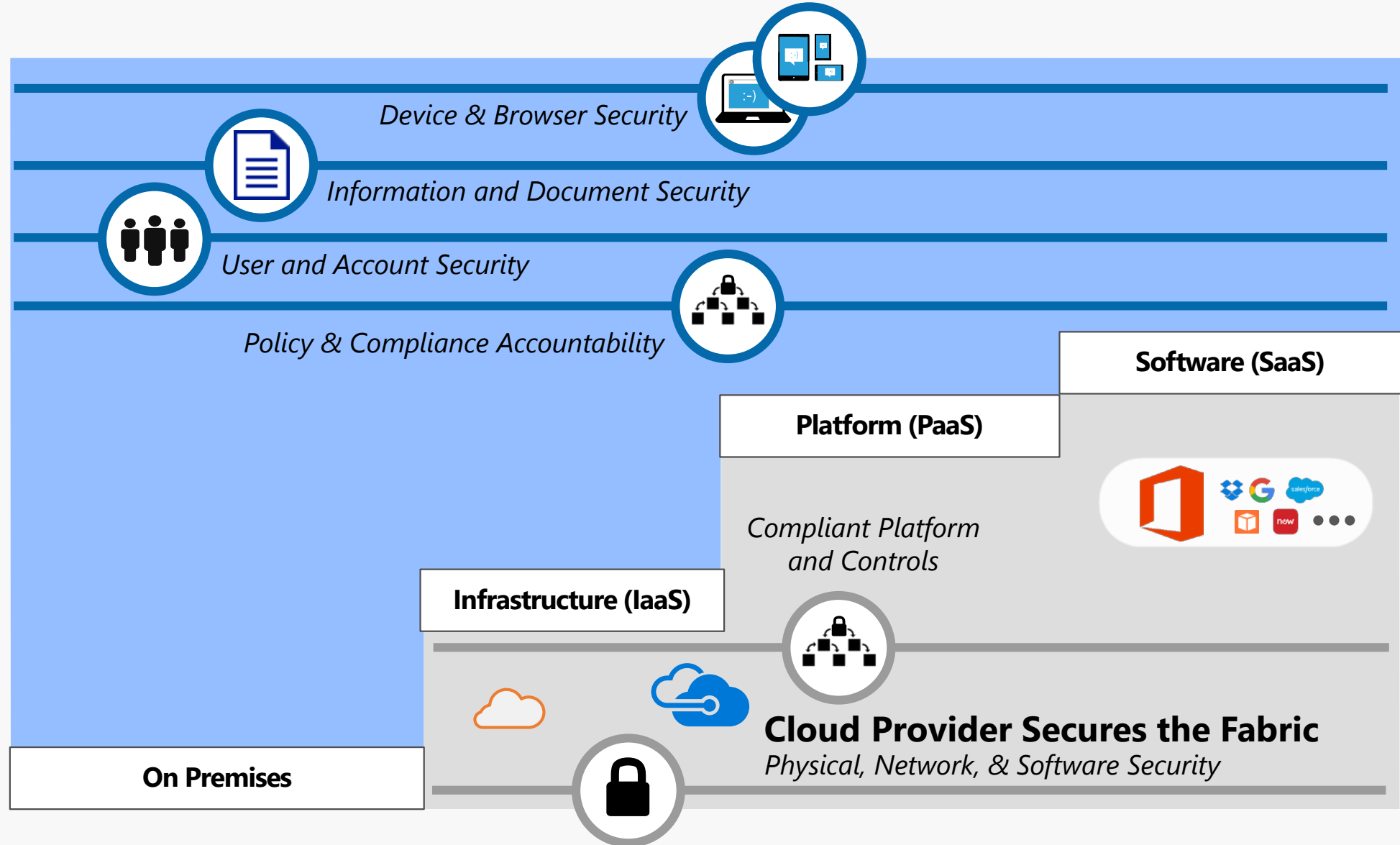


Cloud Security is a partnership

Sharing security, privacy, and compliance responsibility with cloud provider(s)

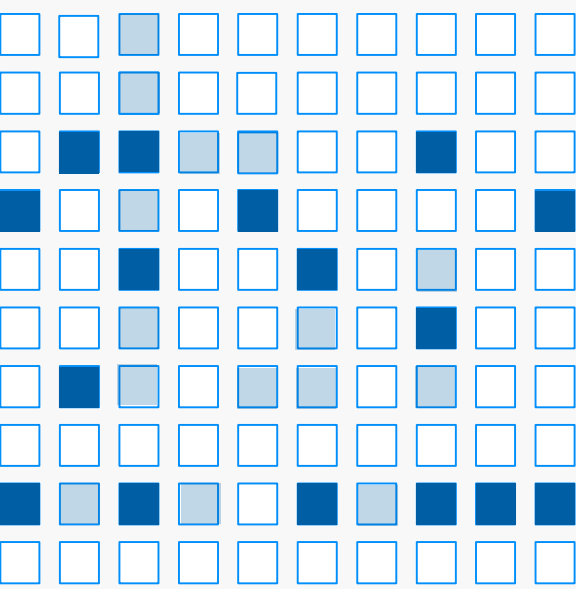
Access & Usage

Always your responsibility

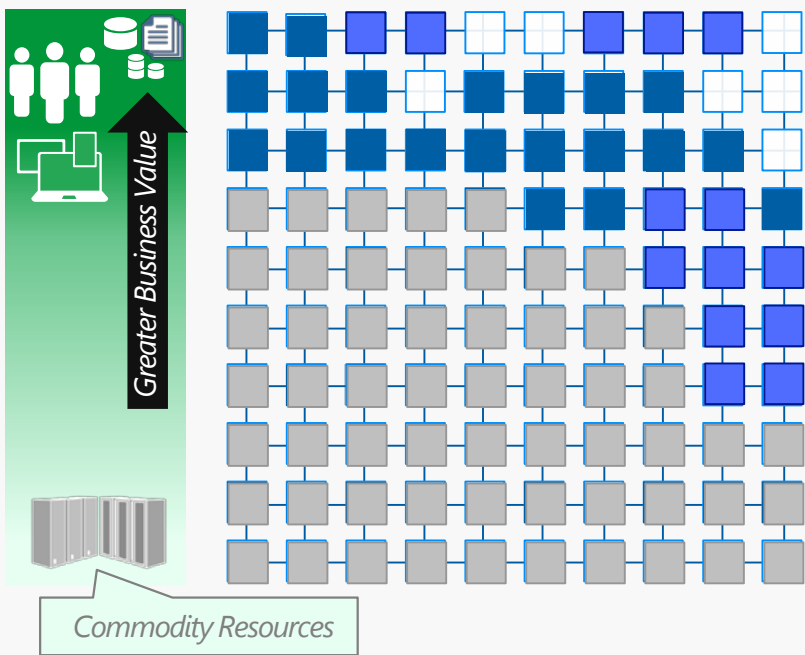


Security Advantages of Cloud Era

TRADITIONAL APPROACH



CLOUD-ENABLED SECURITY



Cloud Technology enables security to:

- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use Cloud intelligence improve detection/response/time

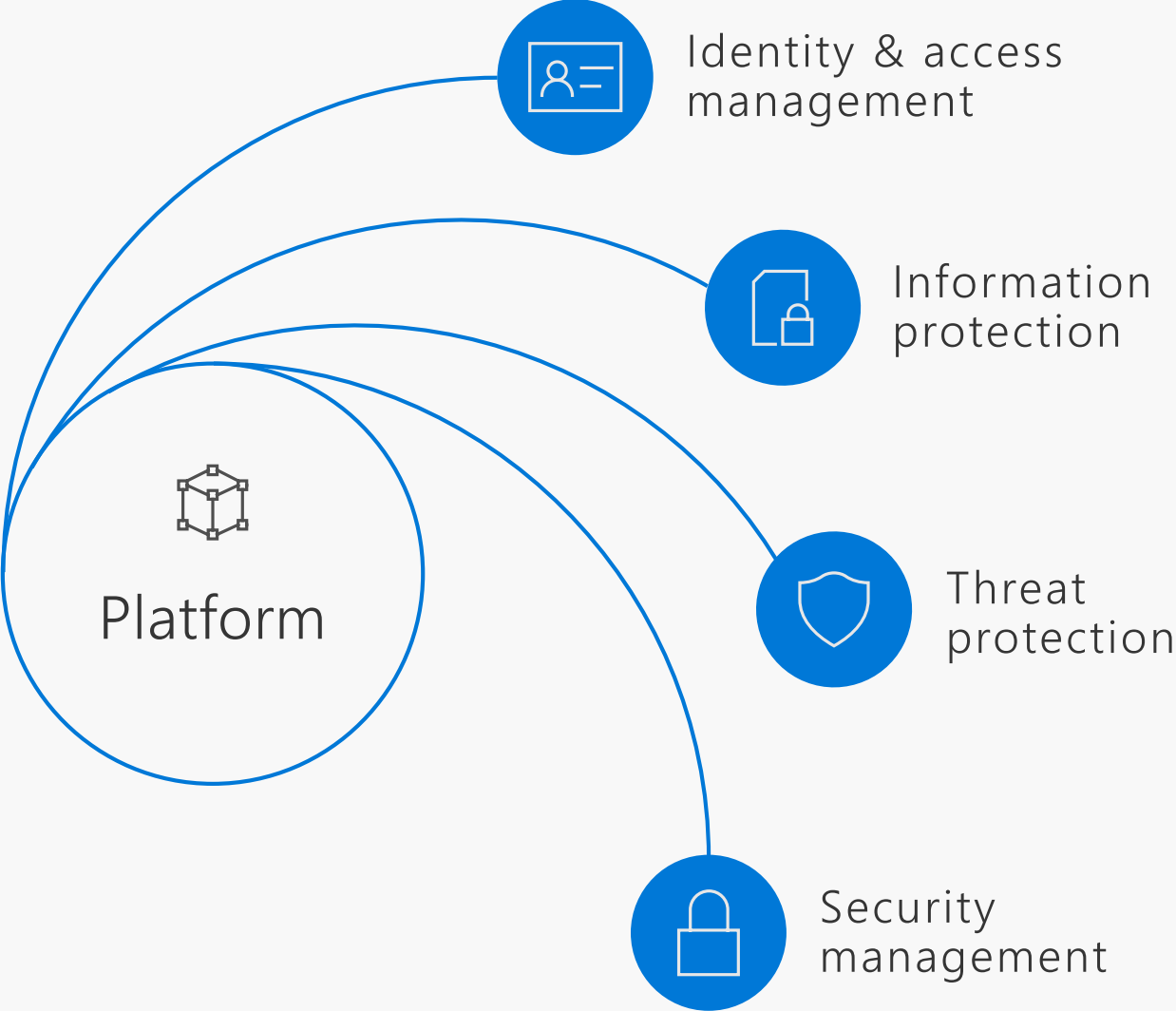
Security is a challenging and under-resourced function

- | | |
|--------------------------------|--|
| ■ Satisfied responsibility | □ Unmet responsibility |
| ■ Partially met responsibility | ■ Cloud Provider responsibility (Trust but verify) |

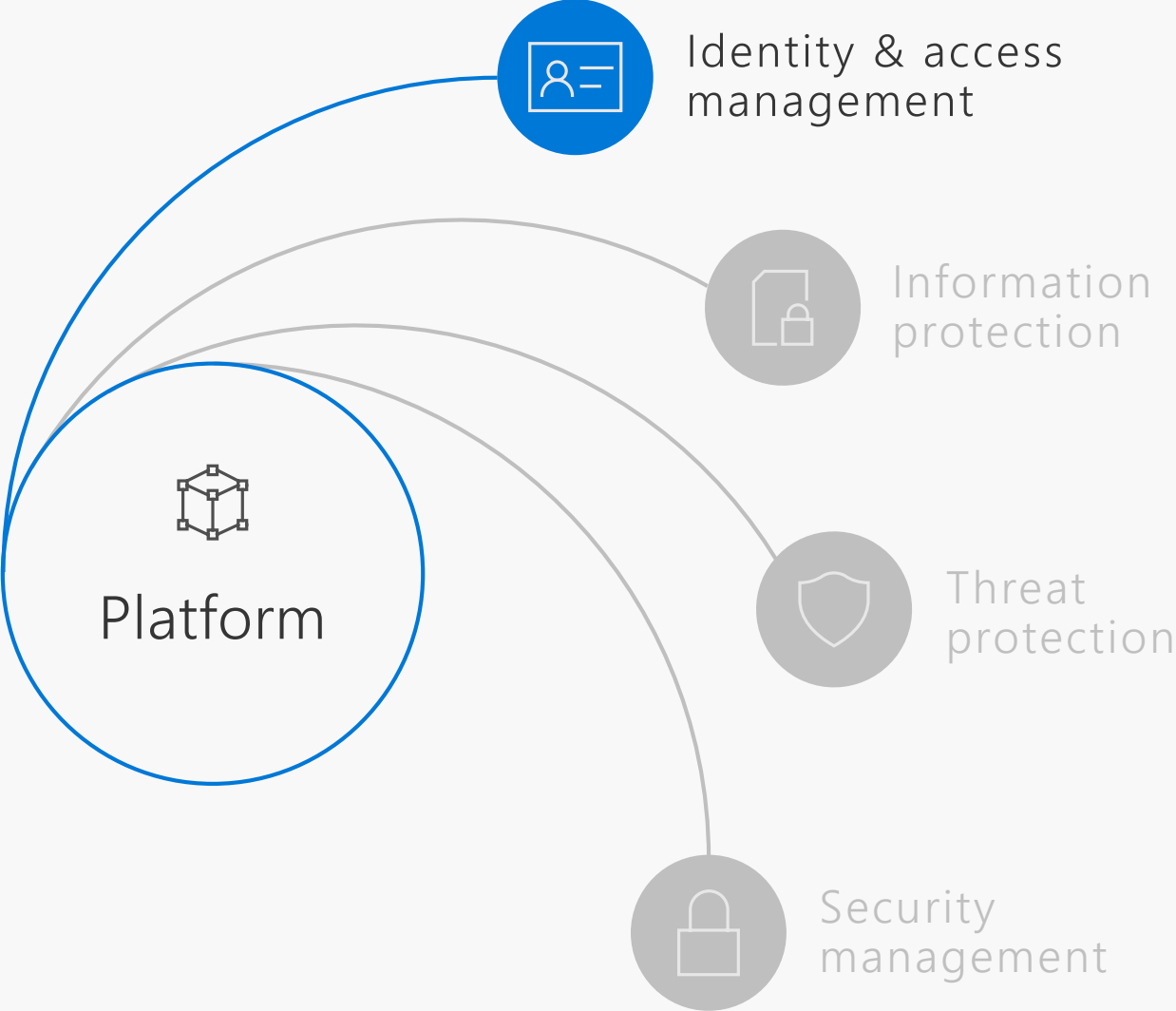
Responsibility Zones

Responsibility	SaaS	PaaS	IaaS	On-prem	
Data governance & rights management	Customer	Customer	Customer	Customer	Always retained by customer
Client endpoints	Customer	Customer	Customer	Customer	
Account & access management	Customer	Customer	Customer	Customer	
Identity & directory infrastructure	Customer	Customer	Customer	Customer	
Application	Microsoft	Customer	Customer	Customer	Varies by Service Type
Network controls	Microsoft	Customer	Customer	Customer	
Operating system	Microsoft	Microsoft	Customer	Customer	
Physical hosts	Microsoft	Microsoft	Microsoft	Customer	
Physical network	Microsoft	Microsoft	Microsoft	Customer	Transfers to Cloud Provider
Physical data center	Microsoft	Microsoft	Microsoft	Customer	
	Microsoft	Microsoft	Microsoft	Customer	

Built in
security



Built in
security



How much control do you have over access?

Can your access control policies
adapt to changing conditions?

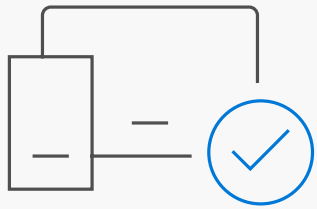
Can you improve user experience
and strengthen access protection?

How do you protect user credentials?



Identity and access management

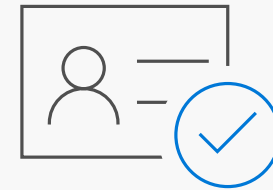
Prove users are authorized and secure before granting access to apps, data, and devices



Protect at the
front door

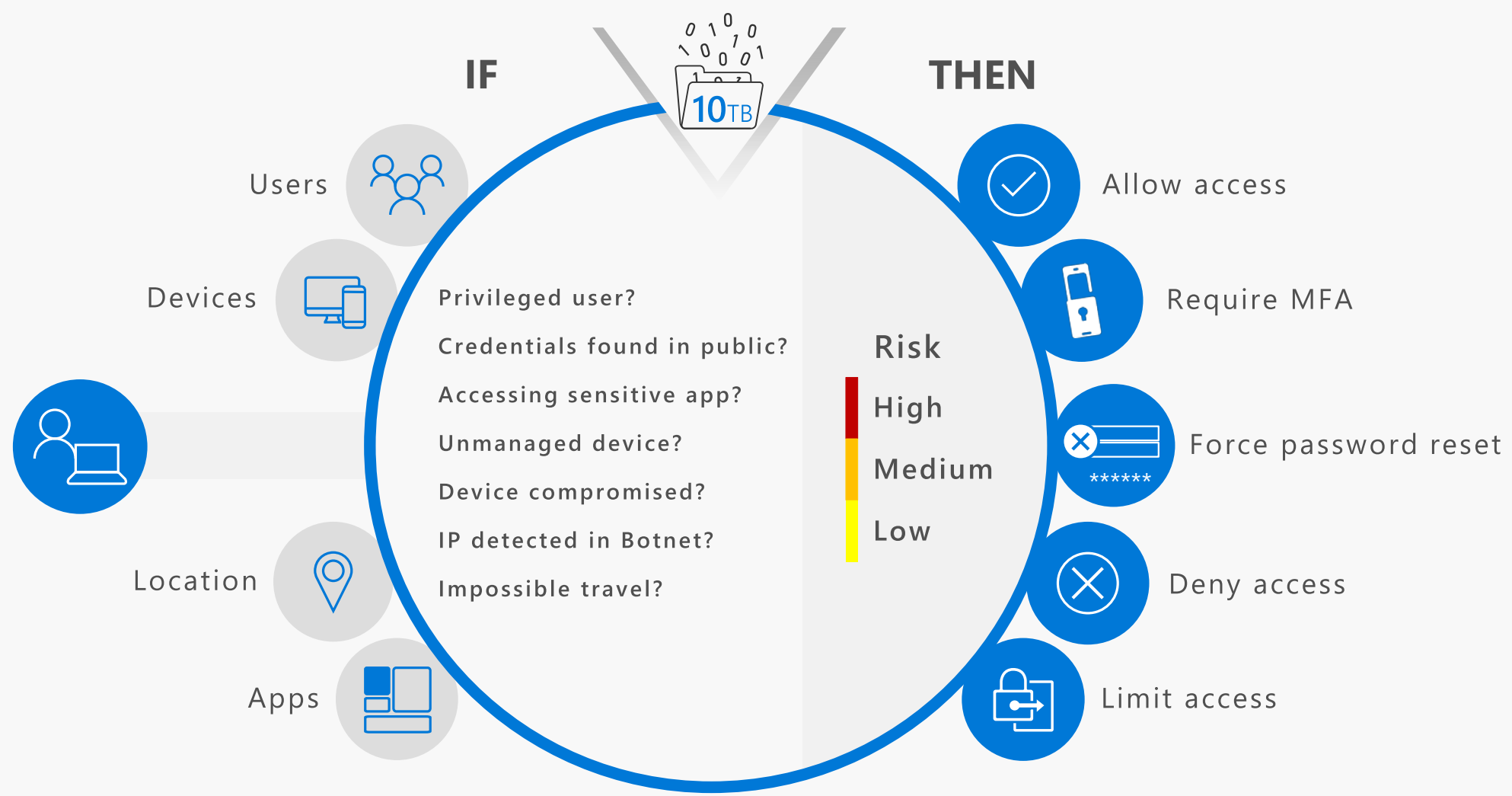


Improve user
experience while
maintaining security

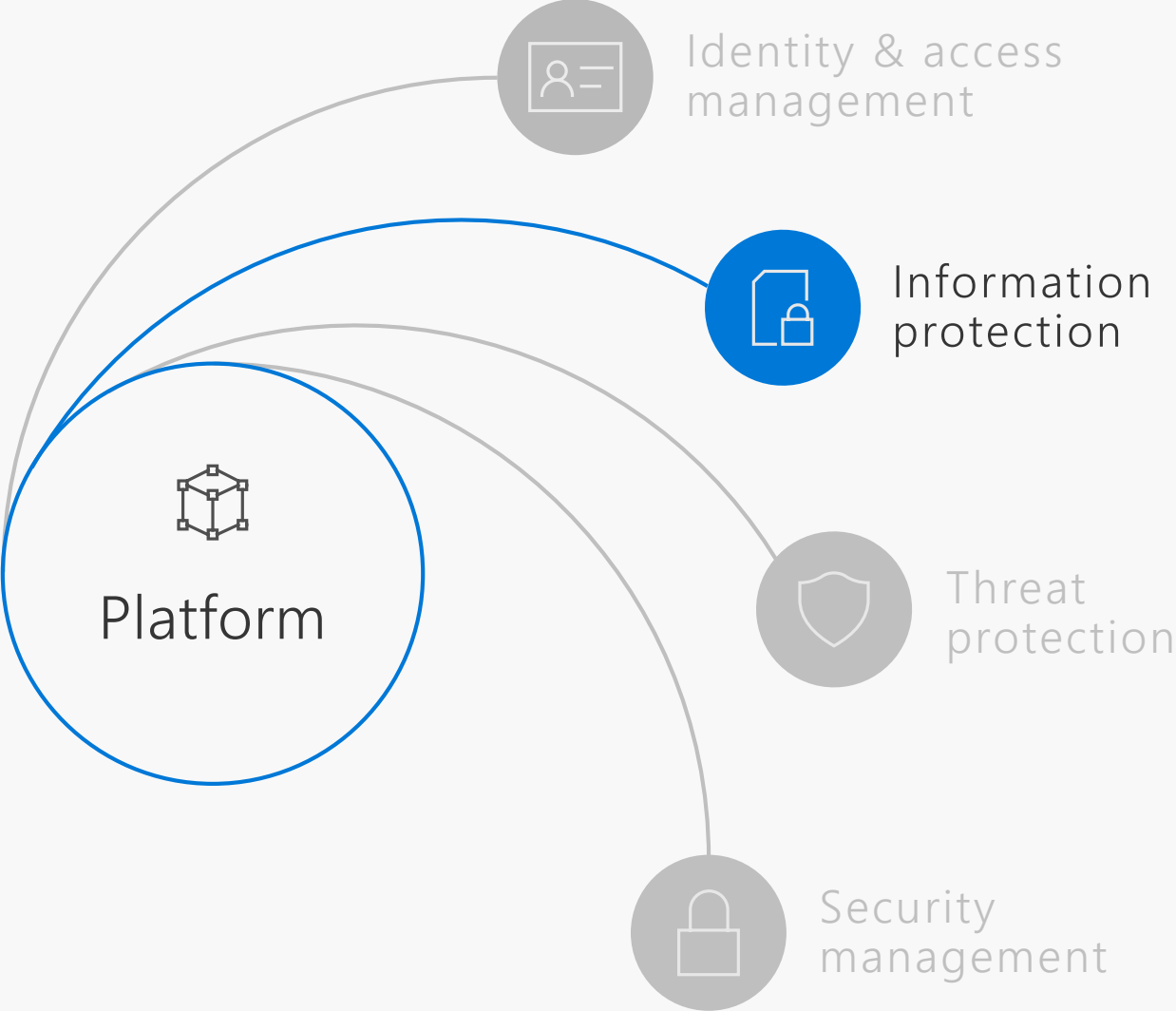


Safeguard your
credentials

Protect at the front door with Conditional Access



Built in
security



Do you have a strategy for protecting and managing sensitive information?

Do you know where your sensitive data resides?

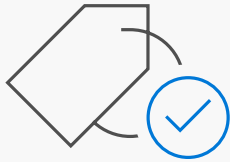
Do you have control of your data as it travels inside and outside of your organization?

Are you using multiple solutions to classify, label, and protect sensitive data?



Information protection

Comprehensive protection of sensitive data throughout the lifecycle—across devices, apps, cloud services, and on-premises



Detect & classify
sensitive information

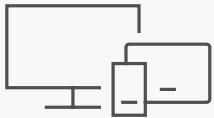


Apply protection
based on policy



Monitor &
remediate

Across



Devices



Apps

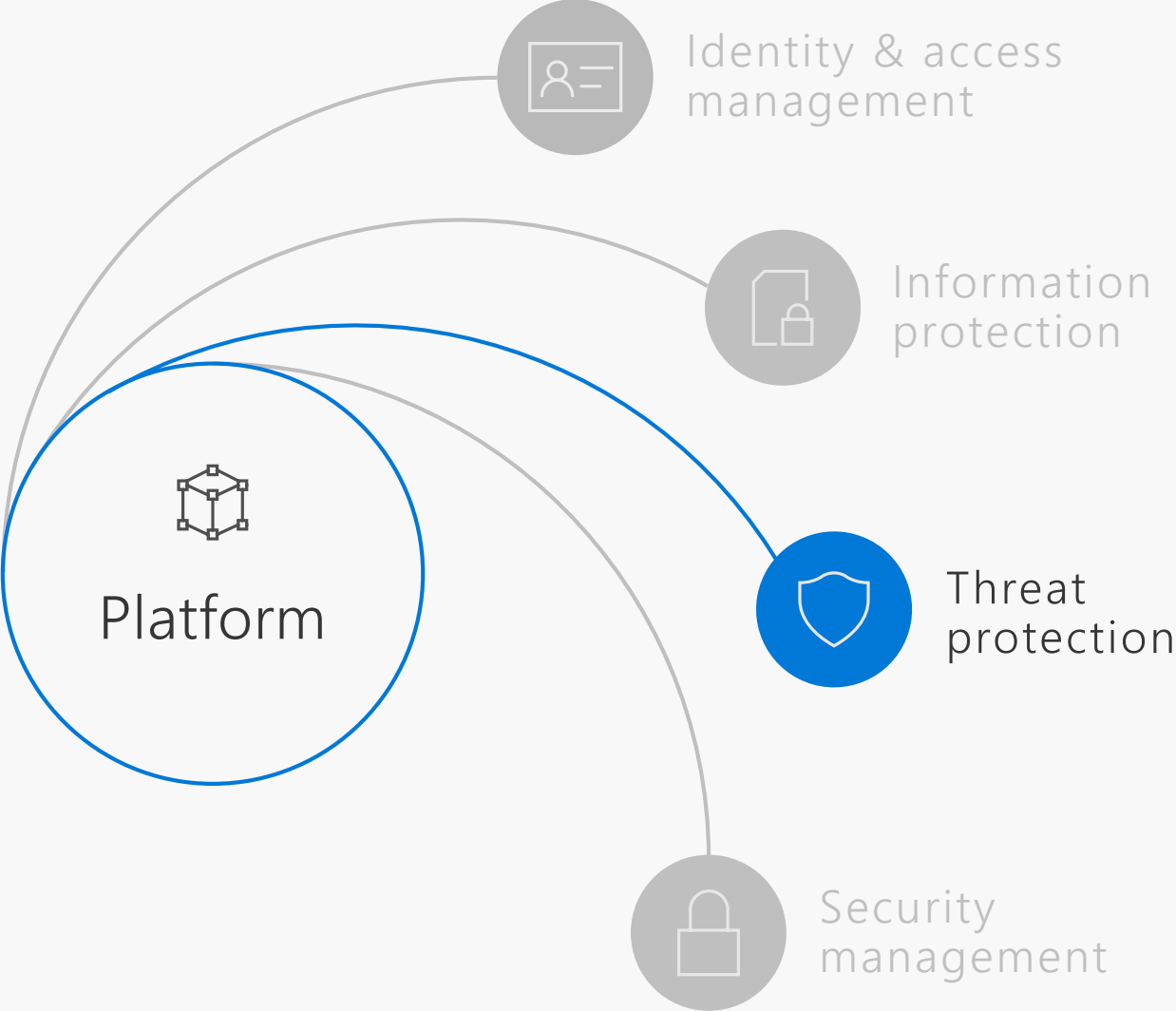


Cloud services



On-premises

Built in
security



How do you protect your organization from advanced threats?

How quickly can you detect suspicious activities on your network?

How do you know if credentials have been compromised?

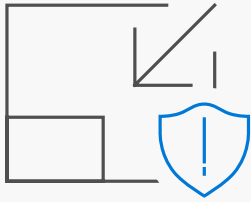
How quickly can you remediate advanced threats?

How do you protect your users from email threats?

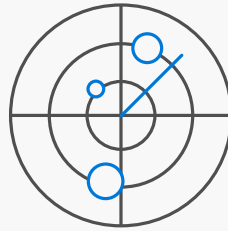


Threat protection

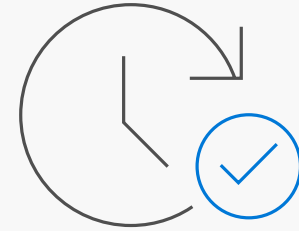
Built in, cloud driven, automatic protection



Reduce attack
surface

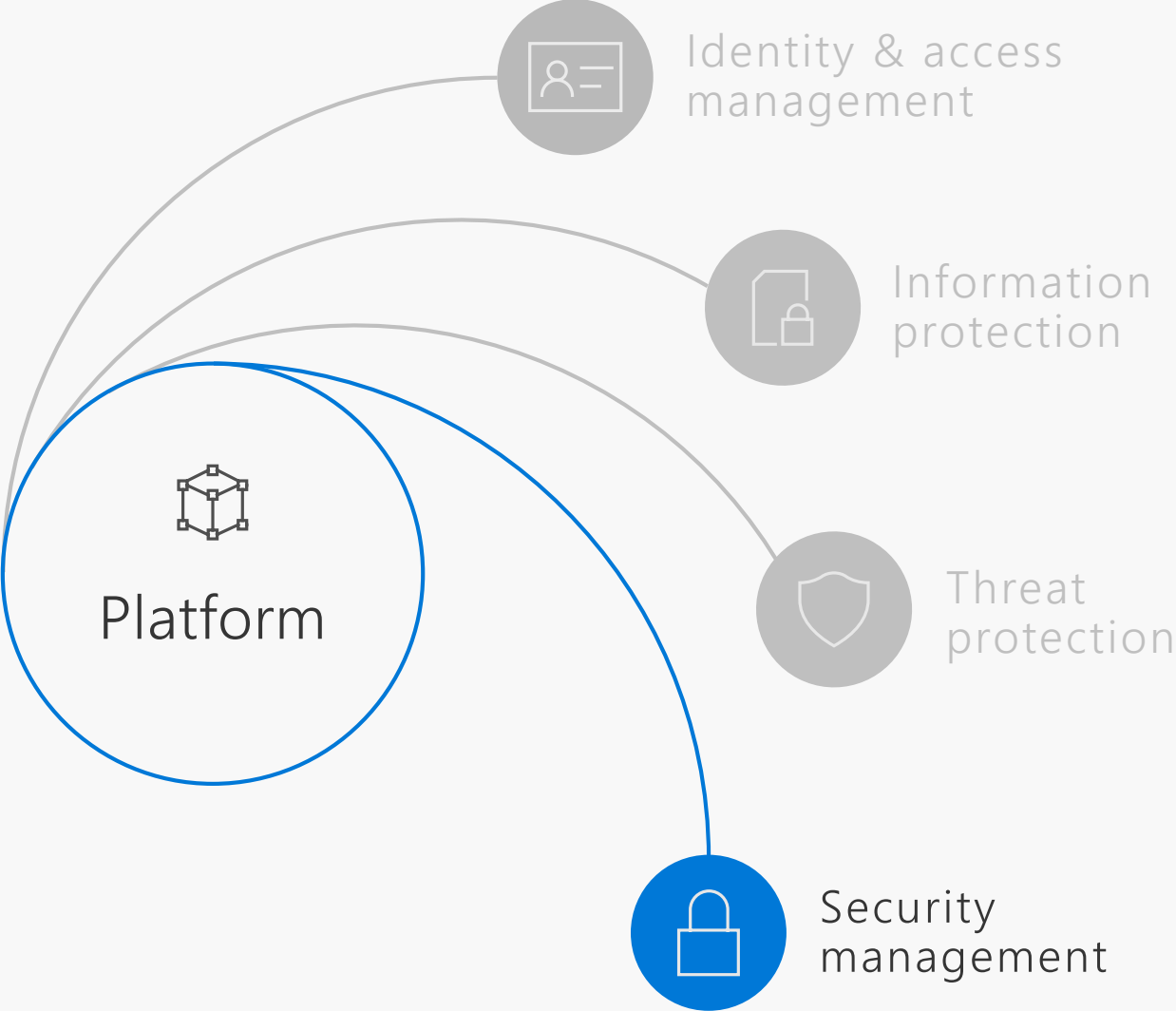


Detect attacks faster
and block them



Respond automatically
to breaches where
appropriate

Built in
security

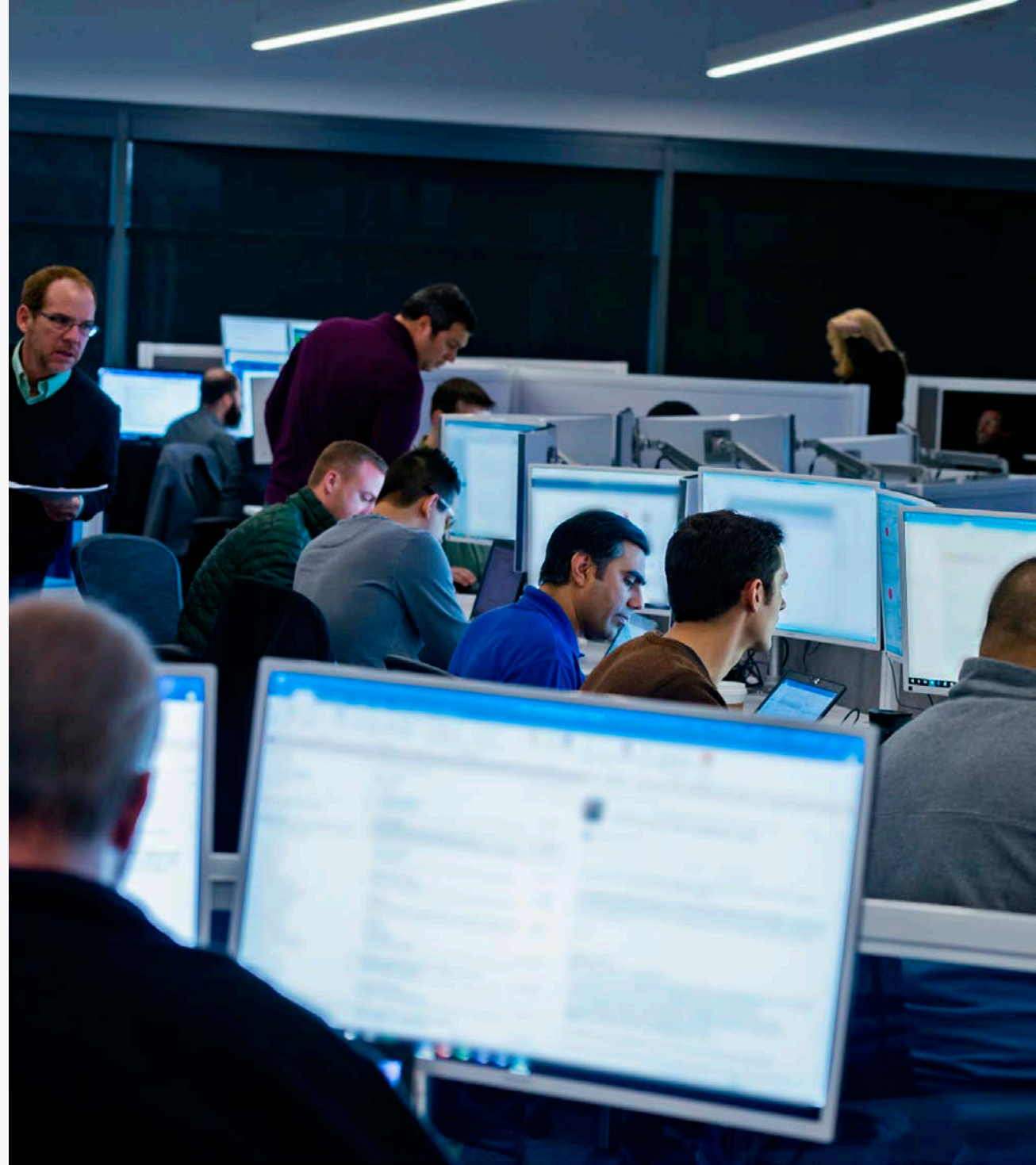


How do you manage security?

Do you know the security state
of your full estate in real time?

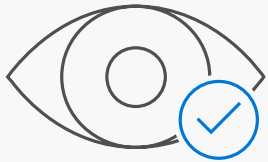
How easily can you configure and
manage the security posture across
your estate?

How do you proactively improve your
security practices over time?

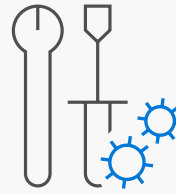


Security management

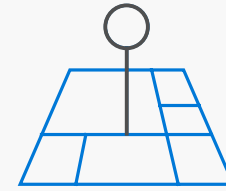
Provide visibility, control, and guidance, with shared intelligence across the digital estate



Visibility

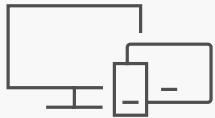


Control



Guidance

Across



Devices



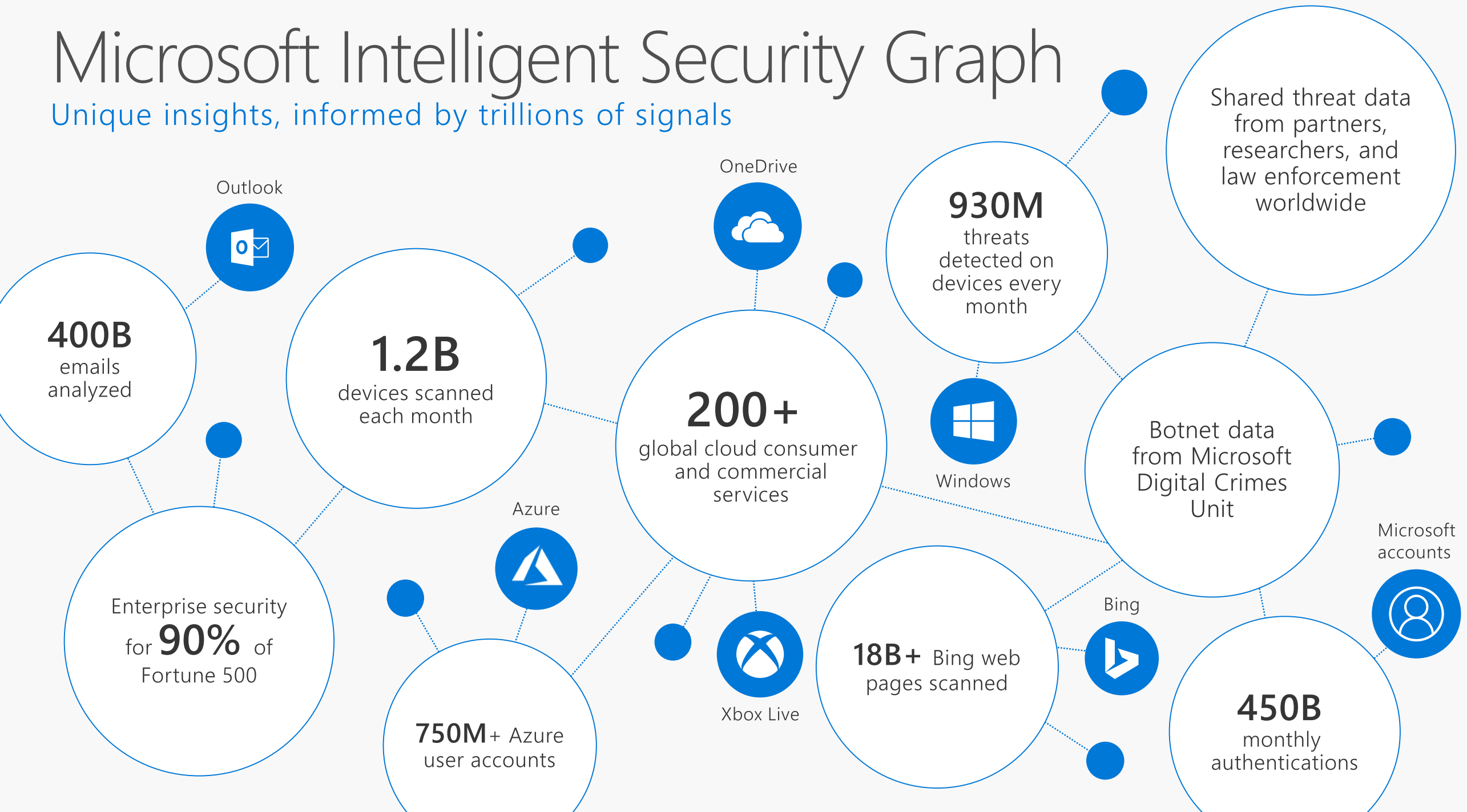
Apps & data



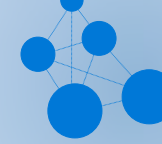
Infrastructure

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Integrating with your SIEM

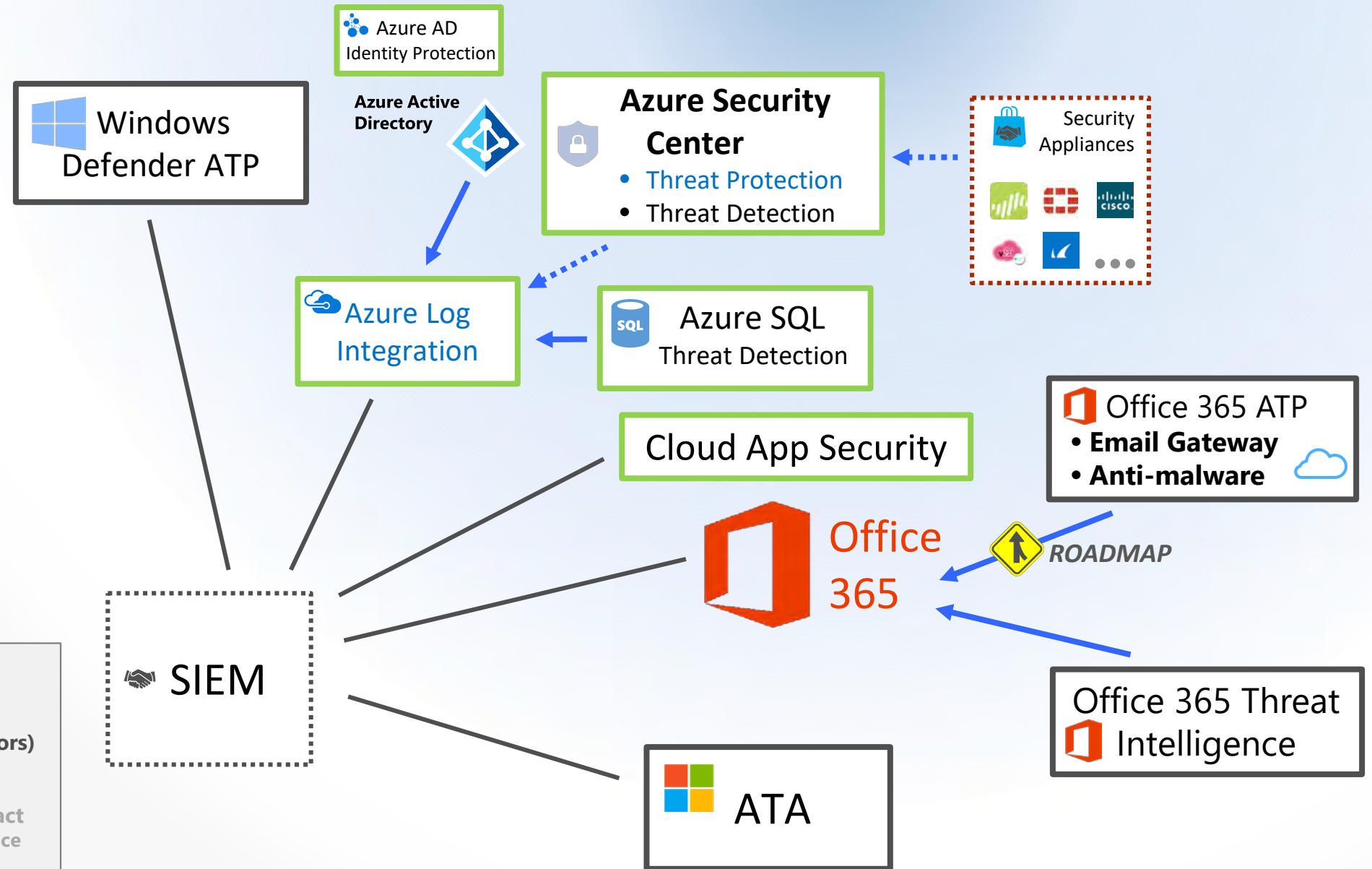


Powered by the
Intelligent Security Graph

*Connect to
your existing
SIEM tool and
processes*

— Log Integration
← Audit Logs
← Alerts

1. Maximize Visibility
 - a. Internal
 - b. External
2. Reduce manual steps (and errors)
 - a. Automate
 - b. Integrate (with SIEM)
3. Maximize human analyst impact
 - a. Deep expertise and intelligence
 - b. Continuous Learning



Microsoft Cloud Services infrastructure

Global, hyper-scale, enterprise-grade infrastructure offering data residency and business continuity in 14 worldwide geos

Enterprise reliability

via 100+ data centers and Microsoft's global network edge

Compliance leadership

with standards and commitments including ISO 27001, FISMA, and EU Model Clauses

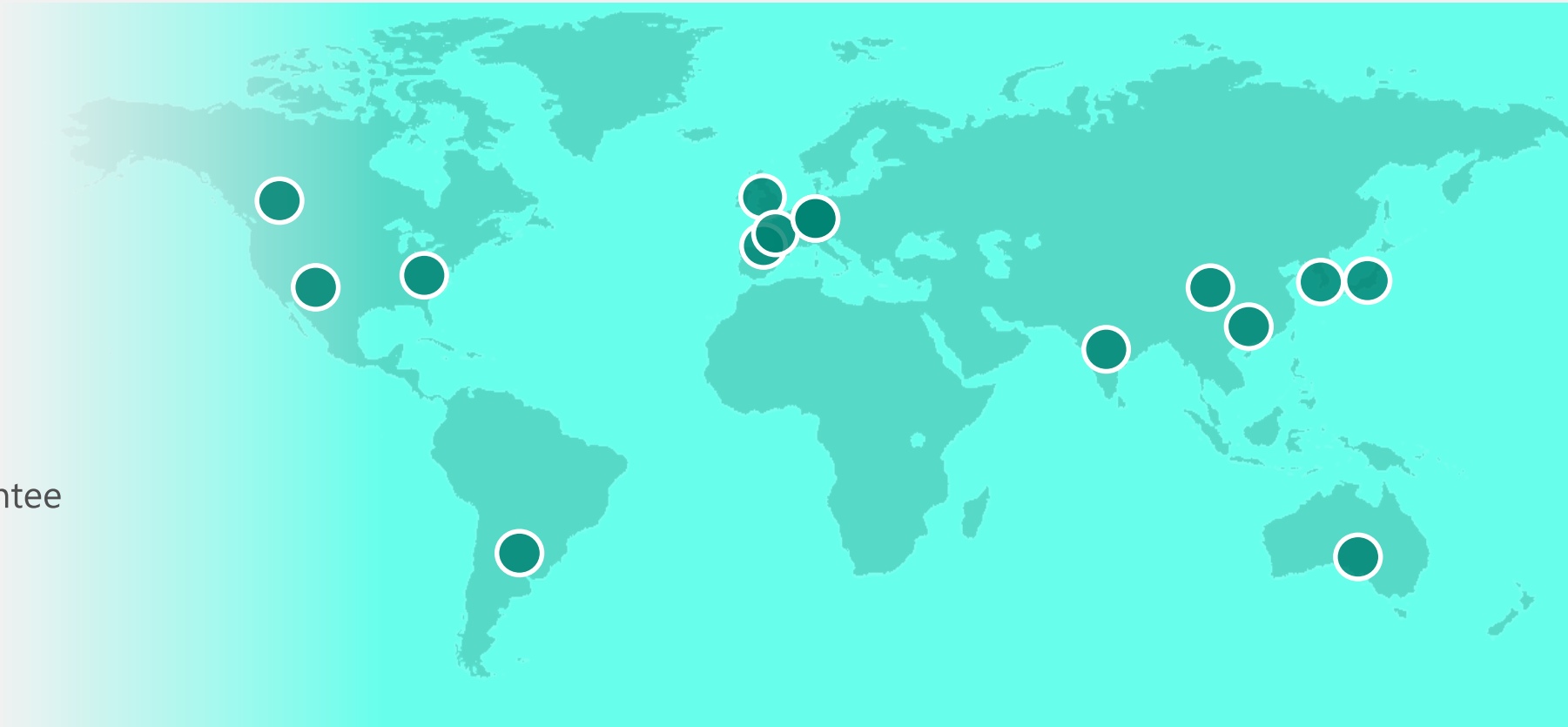
Office 365:

No standing access to data,

transparent operational model, and 99.9% financial-backed uptime guarantee

Security by design

operationalized at the physical, logical, and data layers



Digital Crimes Unit

Leading the fight against cybercrime

Protecting people, organizations and our cloud through **global disruptions** and **enforcement actions** against cybercriminals

Investigations, forensics, and analytics

Machine learning, AI, and data visualization

Public and private partnerships

Creative legal strategies



Ethics and your Data

We have built a culture of strong **privacy principles** and leading **security practices**



"We do not provide anyone with direct, unfettered access to customer data."

-Brad Smith, General Counsel



We provide governments with the ability to review source code and reassure themselves of its integrity at our Transparency Centers



We put people first with privacy by design

"Most trusted company for privacy"

-Ponemon Institute's Most Trusted Companies for Privacy Study



TRUSTED CLOUD

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

March
2017

GLOBAL



ISO 27001



ISO 27018



ISO 27017



ISO 22301



ISO 9001



SOC 1
Type 2



SOC 2
Type 2



SOC 3



CSA STAR
Self-Assessment



CSA STAR
Certification



CSA STAR
Attestation

US GOV



Moderate
JAB P-ATO



High
JAB P-ATO



DoD DISA
SRG Level 2



DoD DISA
SRG Level 4



DoD DISA
SRG Level 5



SP 800-171



FIPS 140-2



Section 508
VPAT



ITAR



CJIS



IRS 1075

INDUSTRY



PCI DSS
Level 1



CDSA



MPAA



FACT UK



Shared
Assessments



FISC Japan



HIPAA /
HITECH Act



HITRUST



GxP
21 CFR Part 11



MARS-E



IG Toolkit UK



FERPA



GLBA



FFIEC

REGIONAL



Argentina
PDPA



EU
Model Clauses



UK
G-Cloud



China
DJCP



China
GB 18030



China
TRUCS



Singapore
MTCS



Australia
IRAP/CCSL



New Zealand
GCIO



Japan My
Number Act



ENISA
IAF



Japan CS
Mark Gold



Spain
ENS



Spain
DPA



India
MeitY



Canada
Privacy Laws



Privacy
Shield



Germany IT
Grundschutz
workbook



Our commitment to you



Security



Privacy & control



Compliance



Transparency



Reliability

Microsoft Secure

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships

