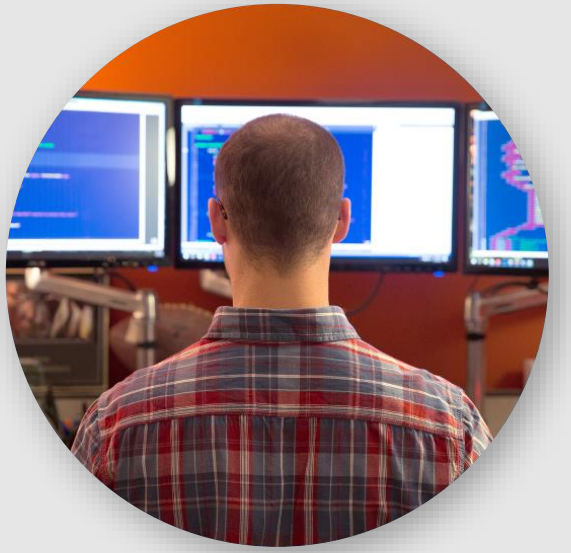
БИТВА ЗА ДОМЕН

Microsoft

Как облака помогают нам стать более безопасными

Дмитрий Узлов
Компания «ТЕХНОПОЛИС»

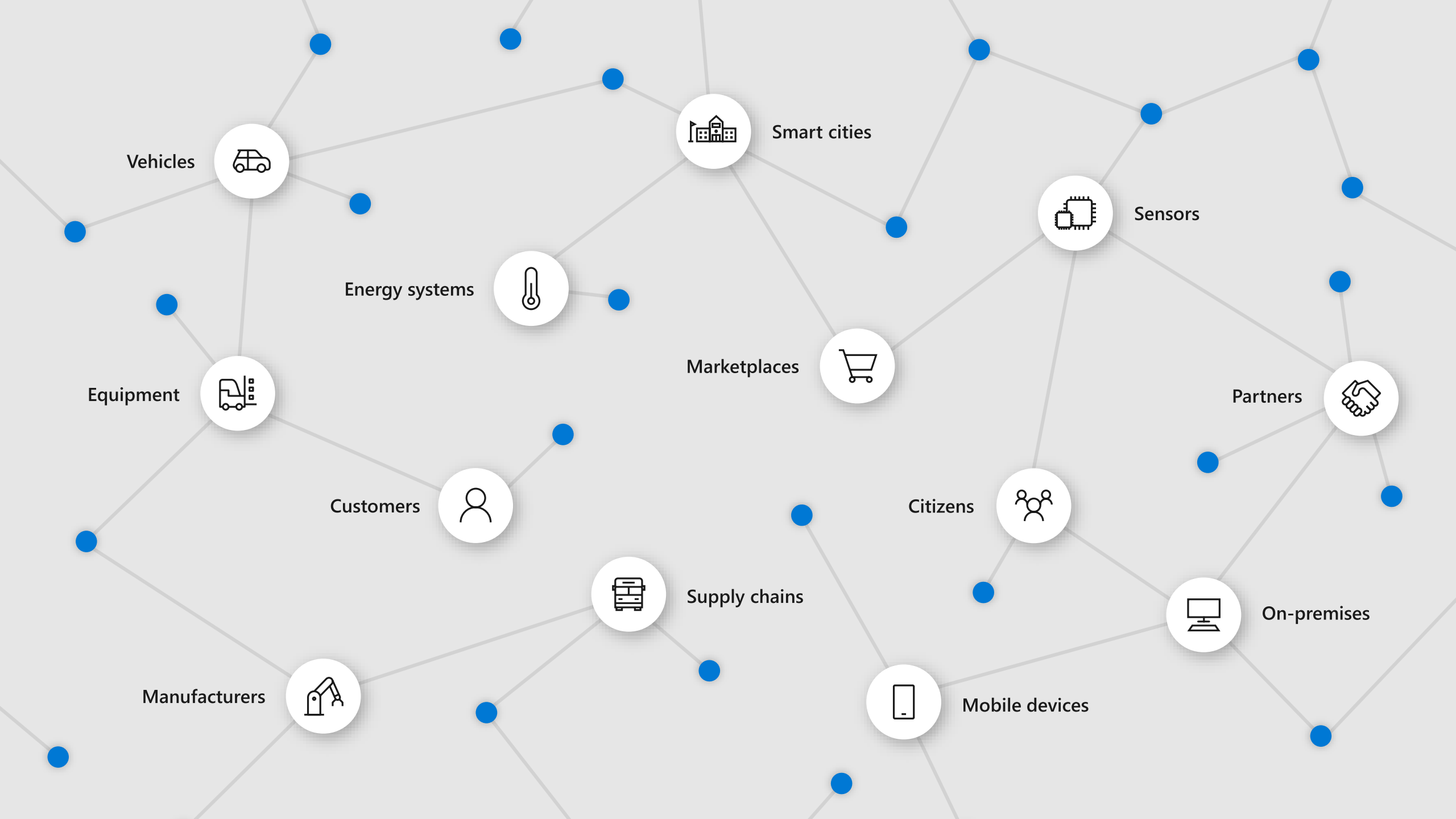
The cybersecurity landscape is rapidly changing

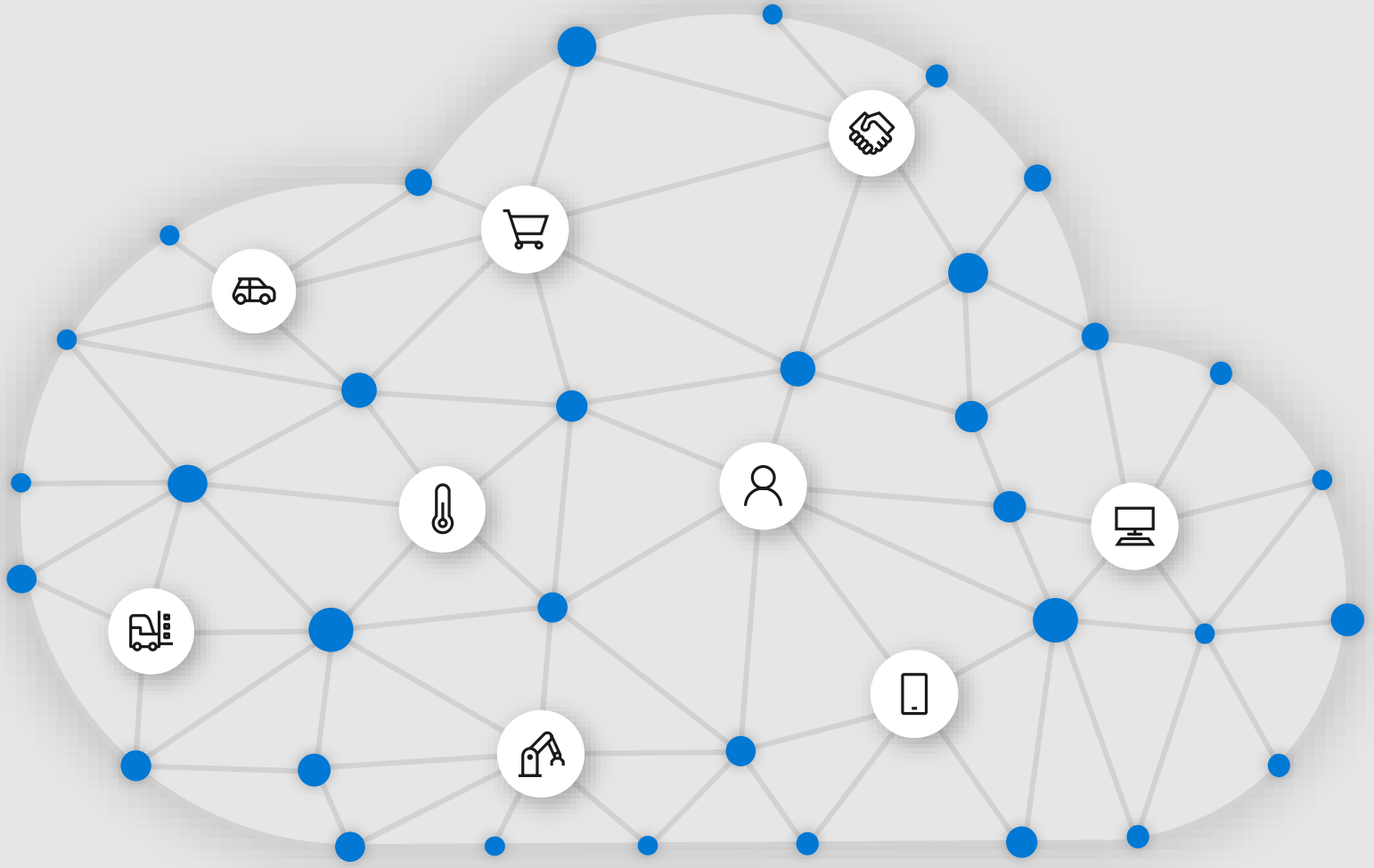


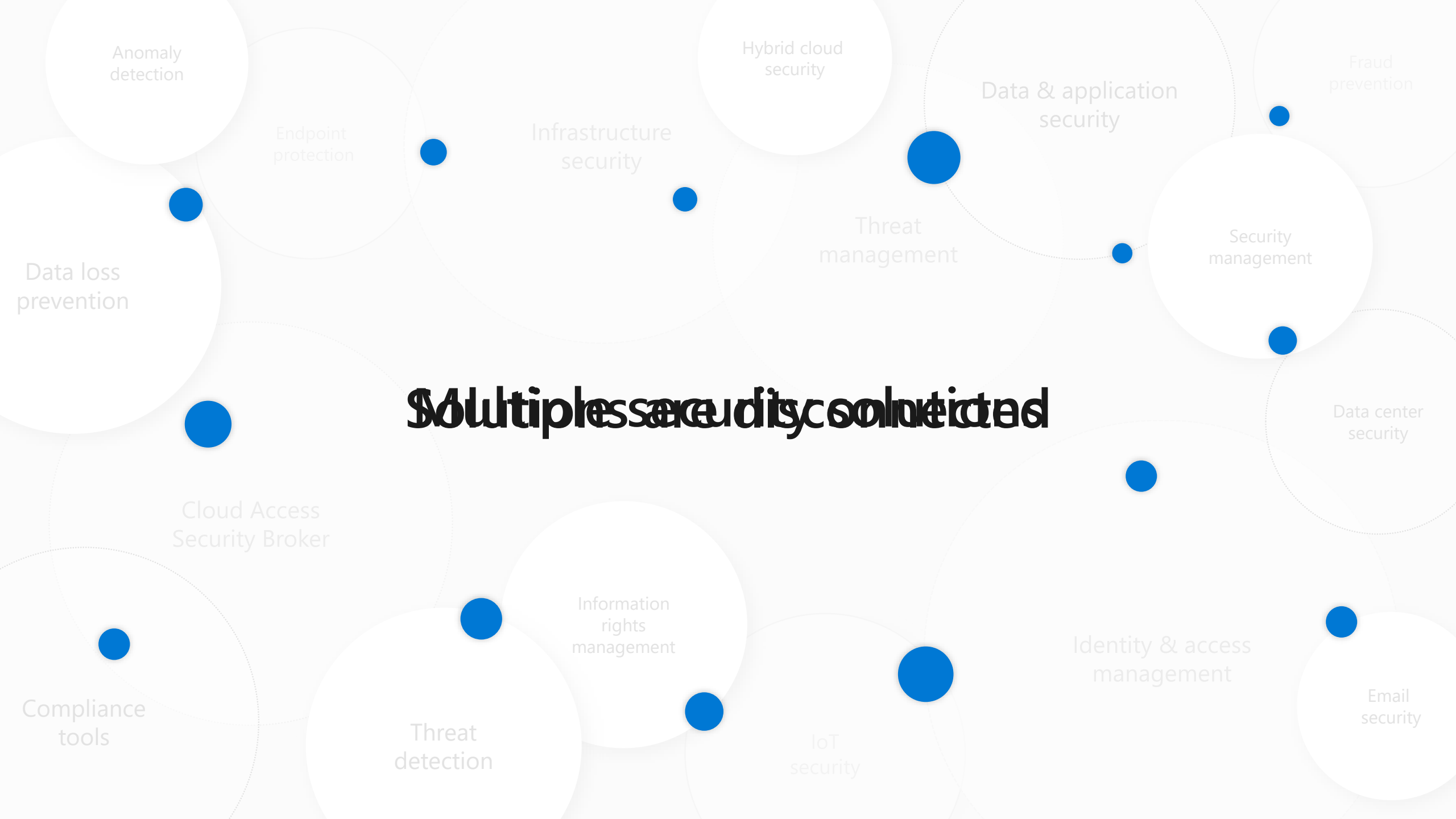
Cyberspace is the new battlefield

Security skills are in short supply

Virtually anything can be attacked


Vehicles
Smart cities
Sensors
Energy systems
Marketplaces
Equipment
Partners
Customers
Citizens
Supply chains
On-premises
Manufacturers
Mobile devices





Multiple security solutions

Operations

Security operations that work for you

Technology

Enterprise-class technology

Partnerships

Partnerships for a heterogeneous world

Operations

Security operations that work for you

Technology

Enterprise-class intelligent security

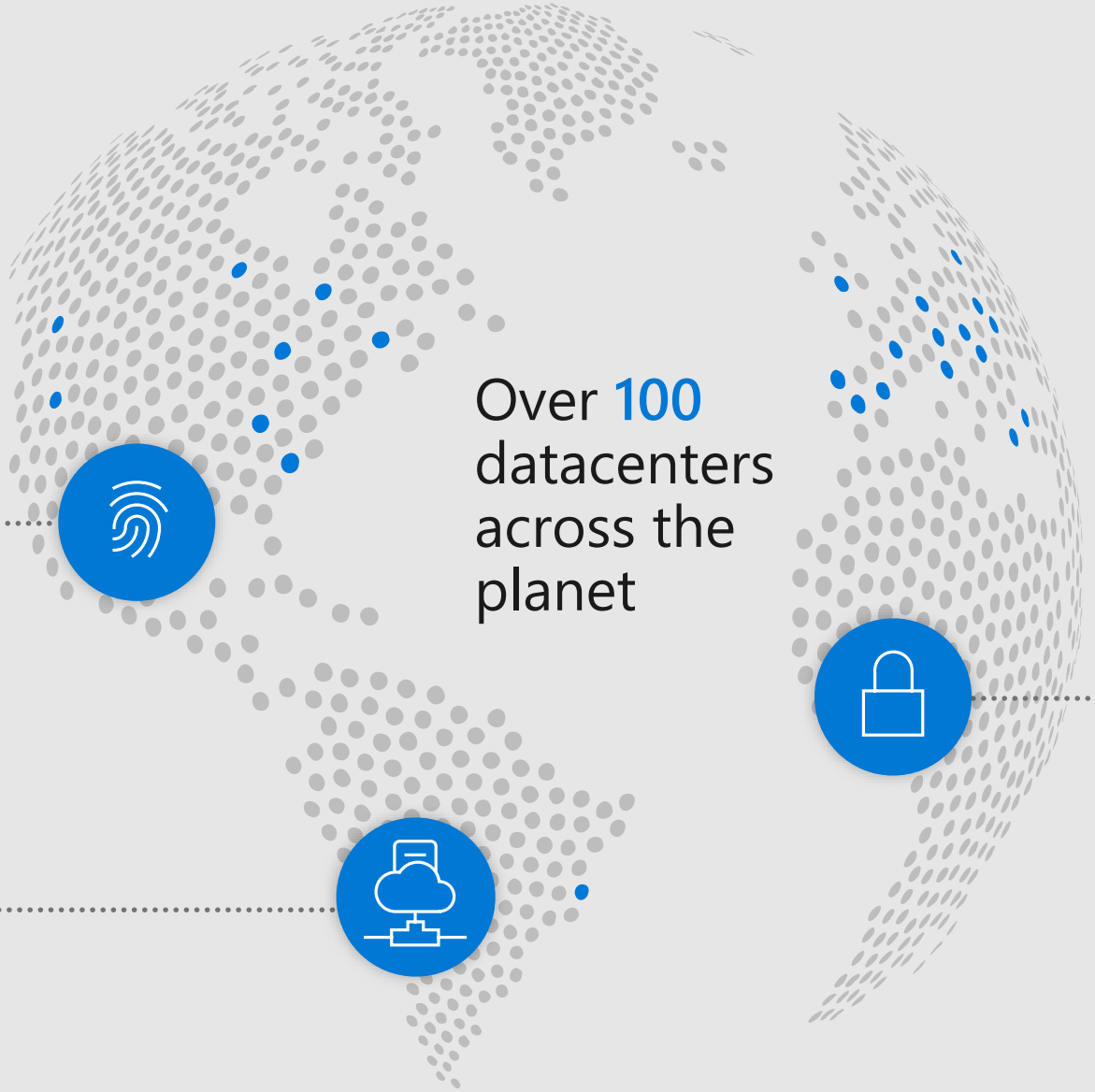
Partnerships

Partnerships for a heterogeneous world

A secure foundation at global scale

Each **physical datacenter** protected with world-class, multi-layered protection

Global cloud infrastructure with custom hardware and network protection



Over **100** datacenters across the planet

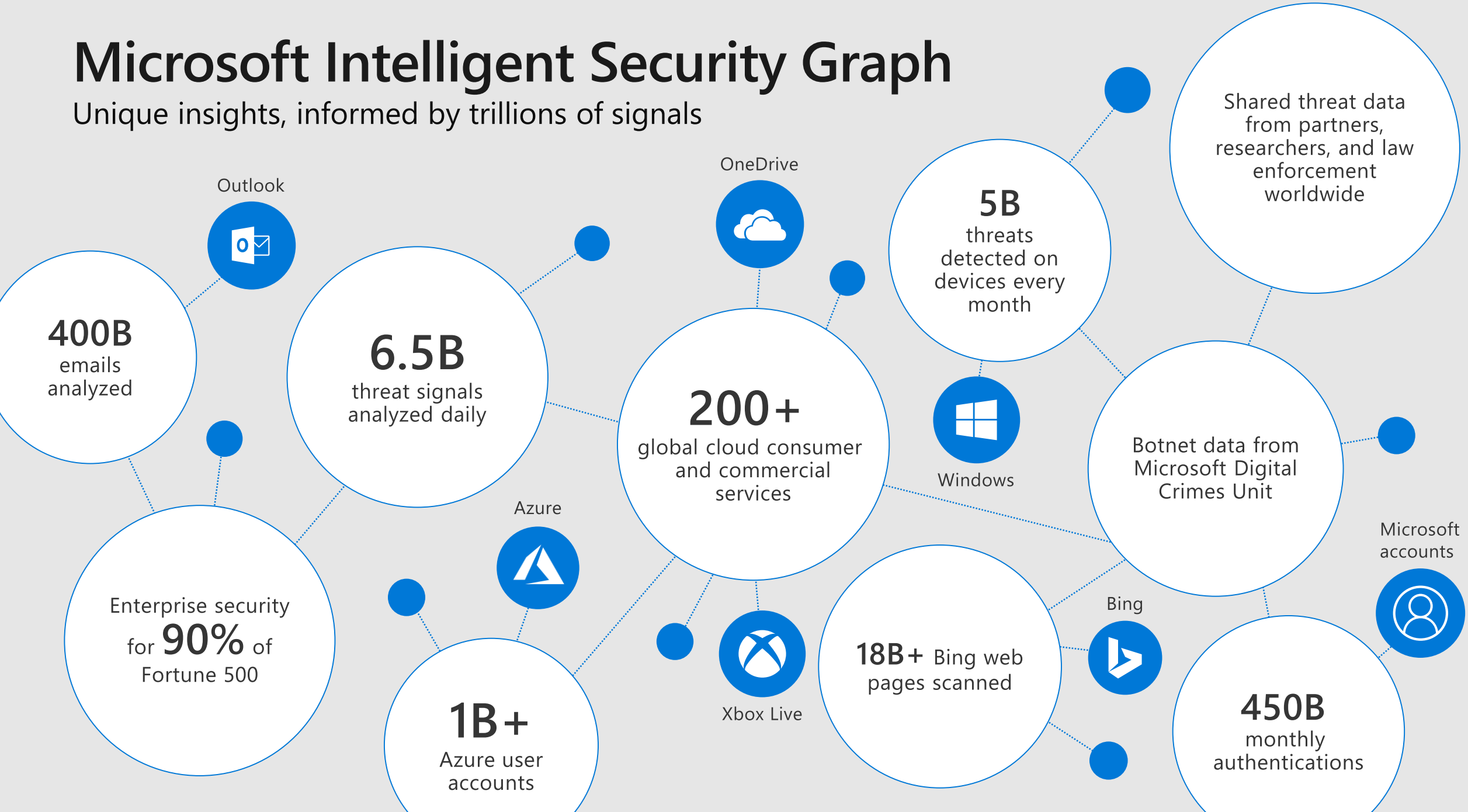
Secured with cutting-edge **operational security**

- Restricted access
- 24x7 monitoring
- Global security experts


Security operations that work for you

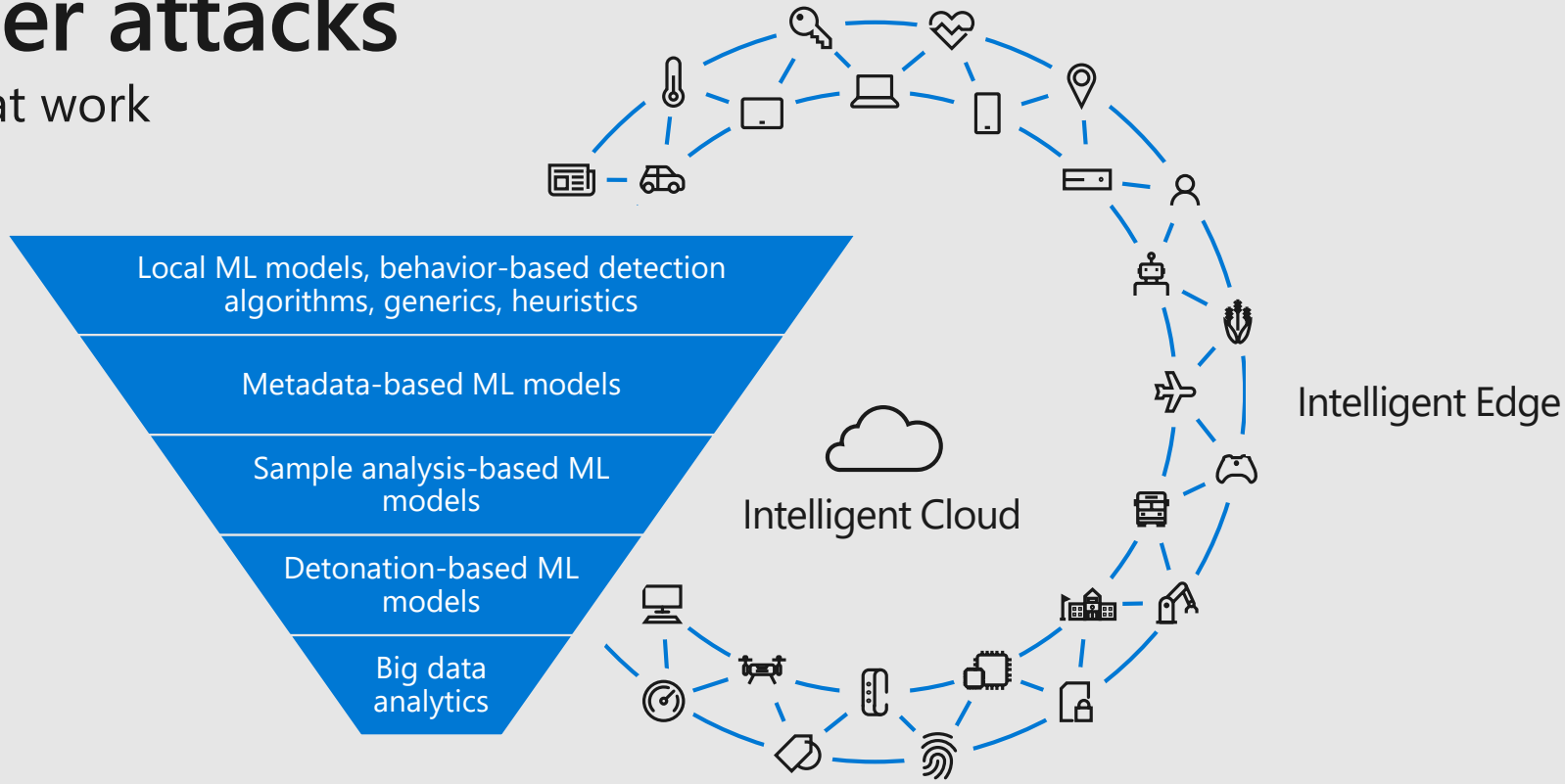
Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



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

Stopping cyber attacks

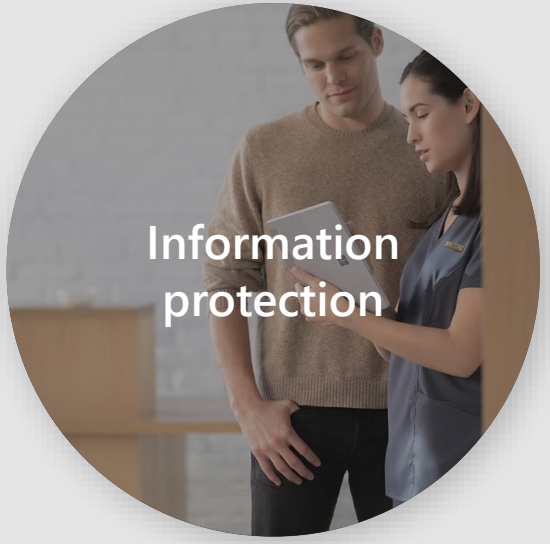
Real-world intelligence at work

- Emotet: Patient zero to quarantine in milliseconds
- Ursnif: Spotting the needle in the haystack
- Phishing campaigns


Operations
Security operations that work for you
Microsoft Security
Technology
Enterprise-class intelligent security
Partnerships
Partnerships for a heterogeneous world

Enterprise-class intelligent security

Secure identities to reach zero trust



Locate and classify information anywhere it lives

Help stop damaging attacks with integrated and automated security

Strengthen your security posture with insights and guidance

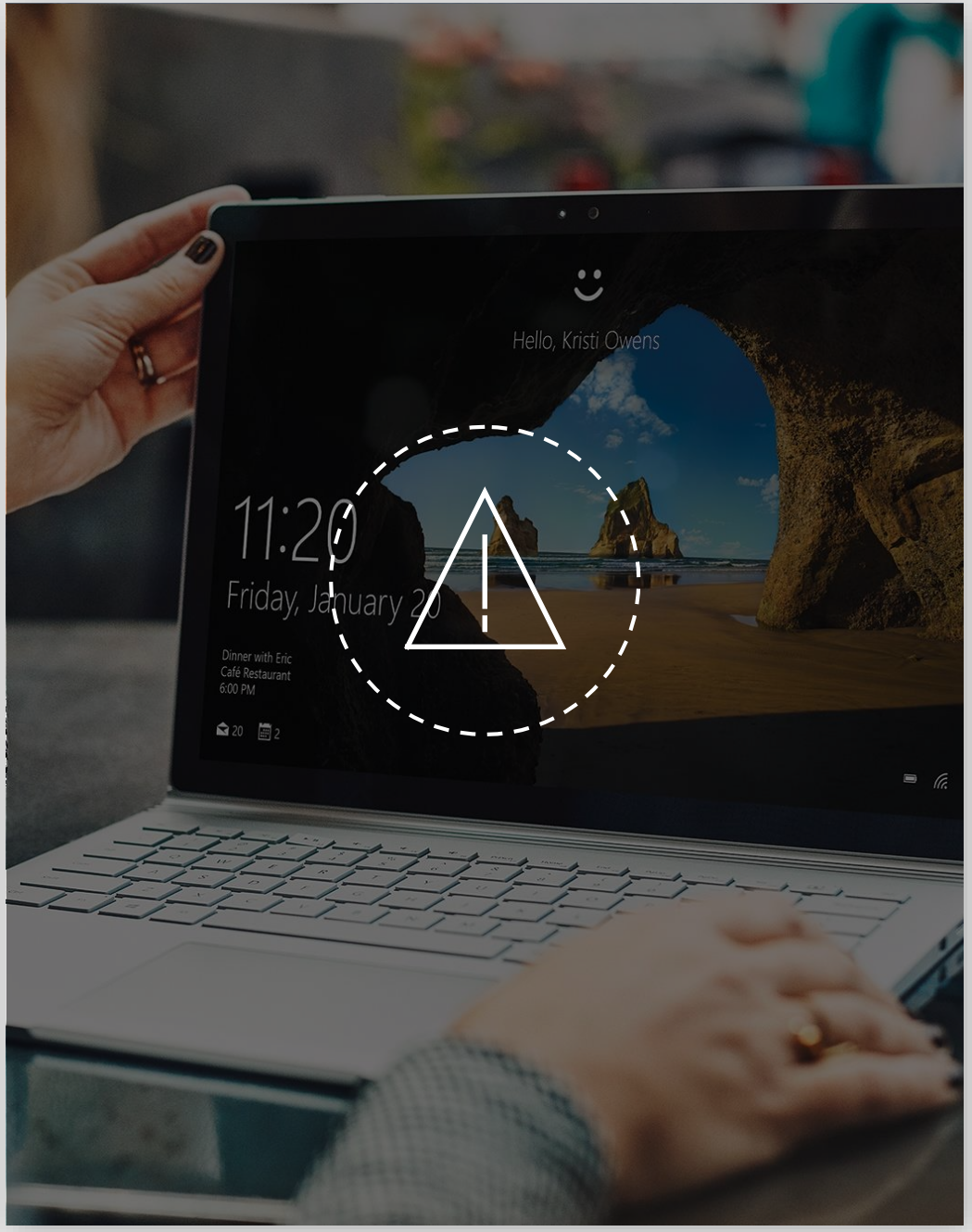
Identity & access management

Identity & Access Management

Passwords = weakest link → **Secure Authentication**

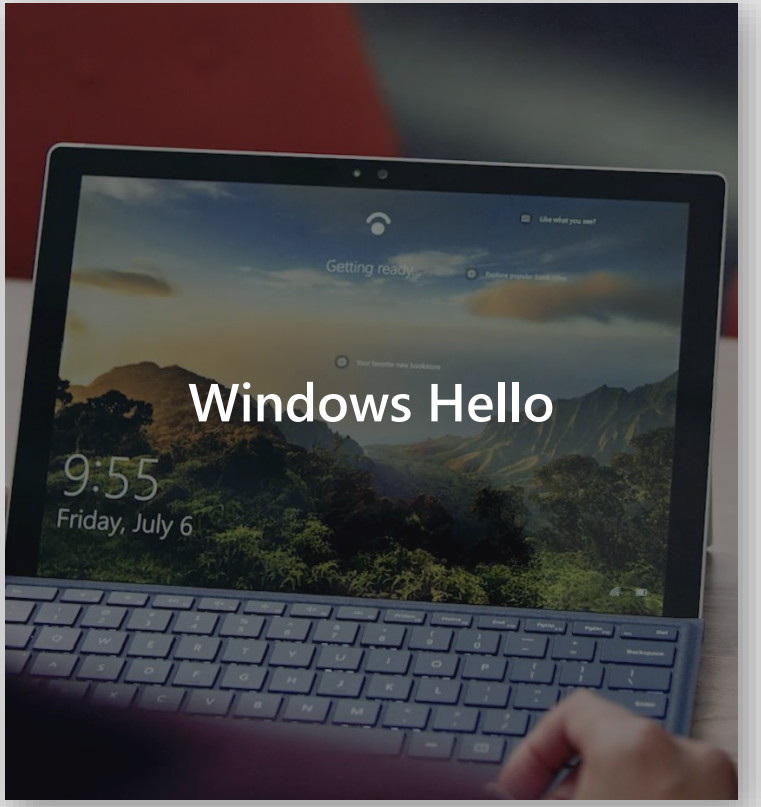
How do I get Zero Trust? → **Conditional Access**

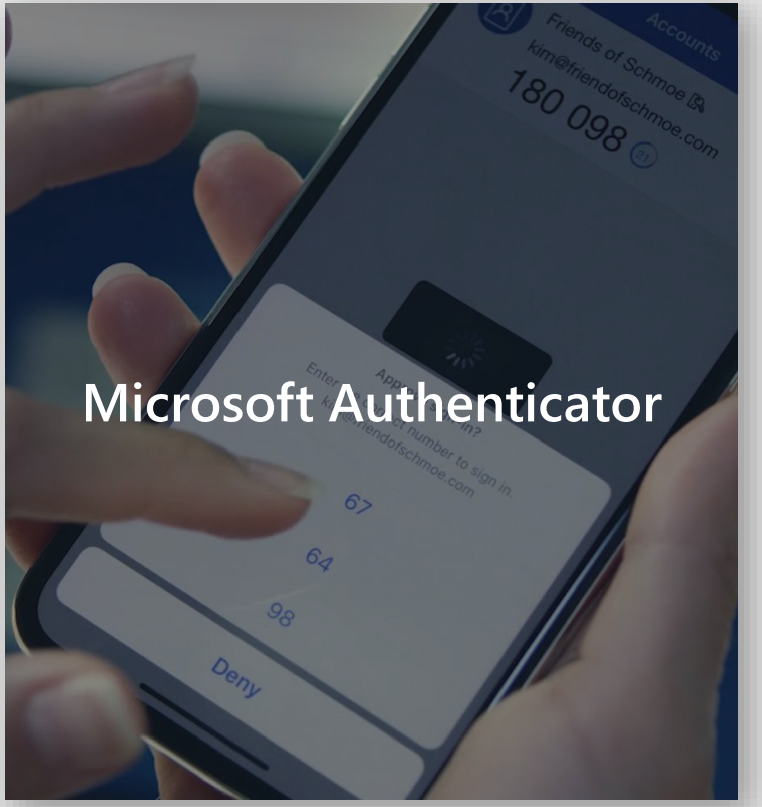
Identities are constantly at risk → **Identity Protection**

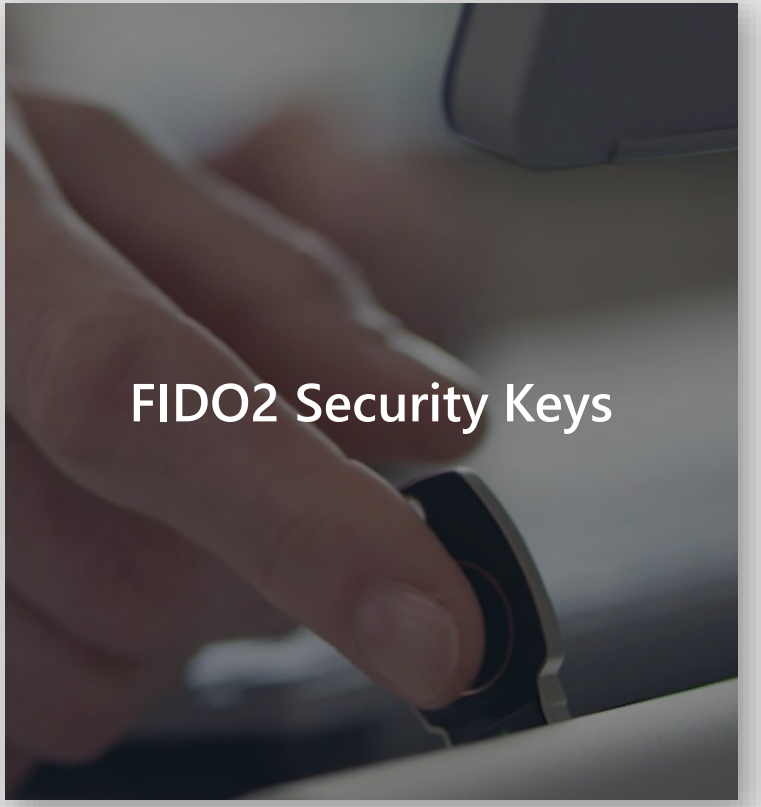


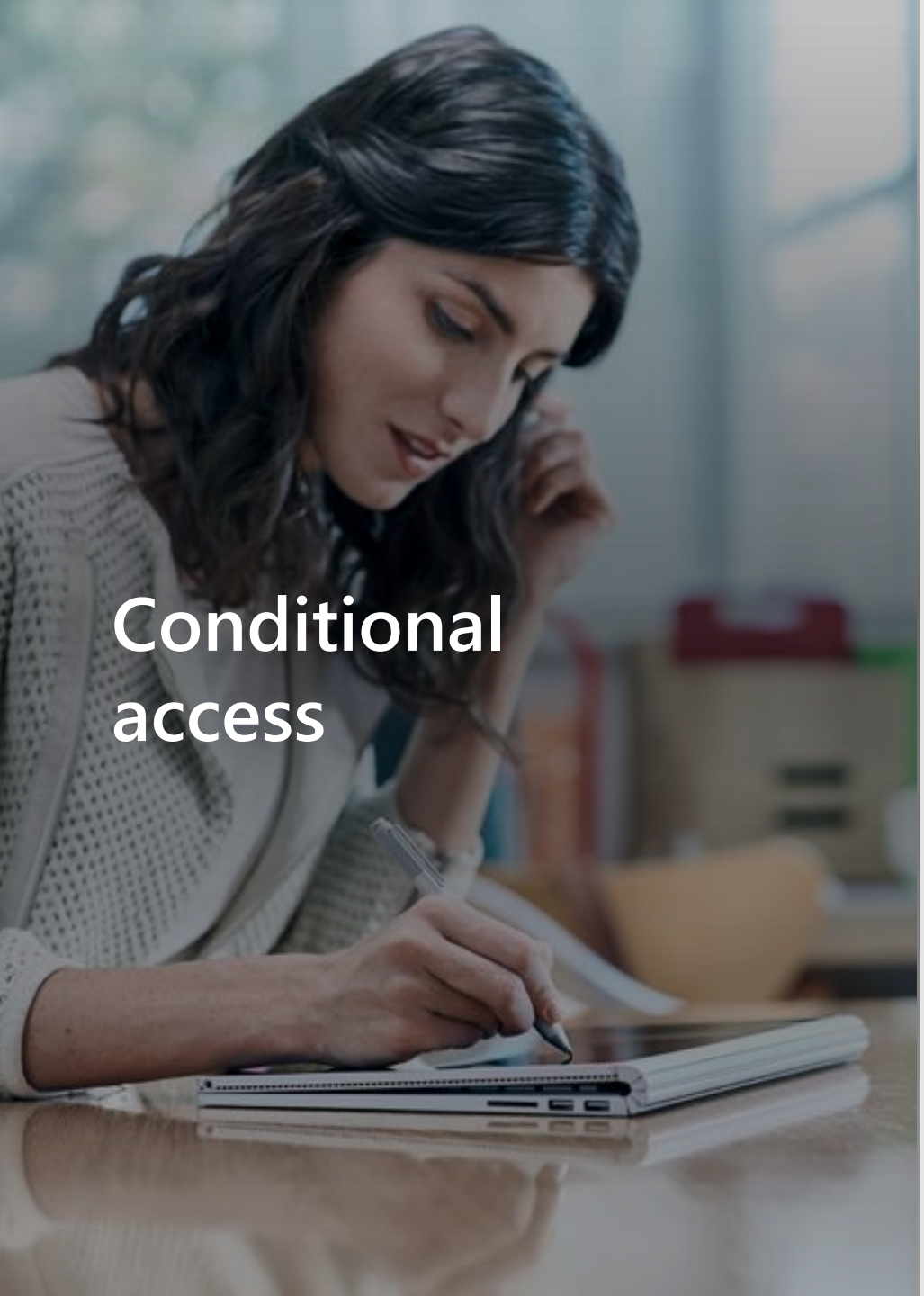
Secure authentication

Getting to a world without passwords

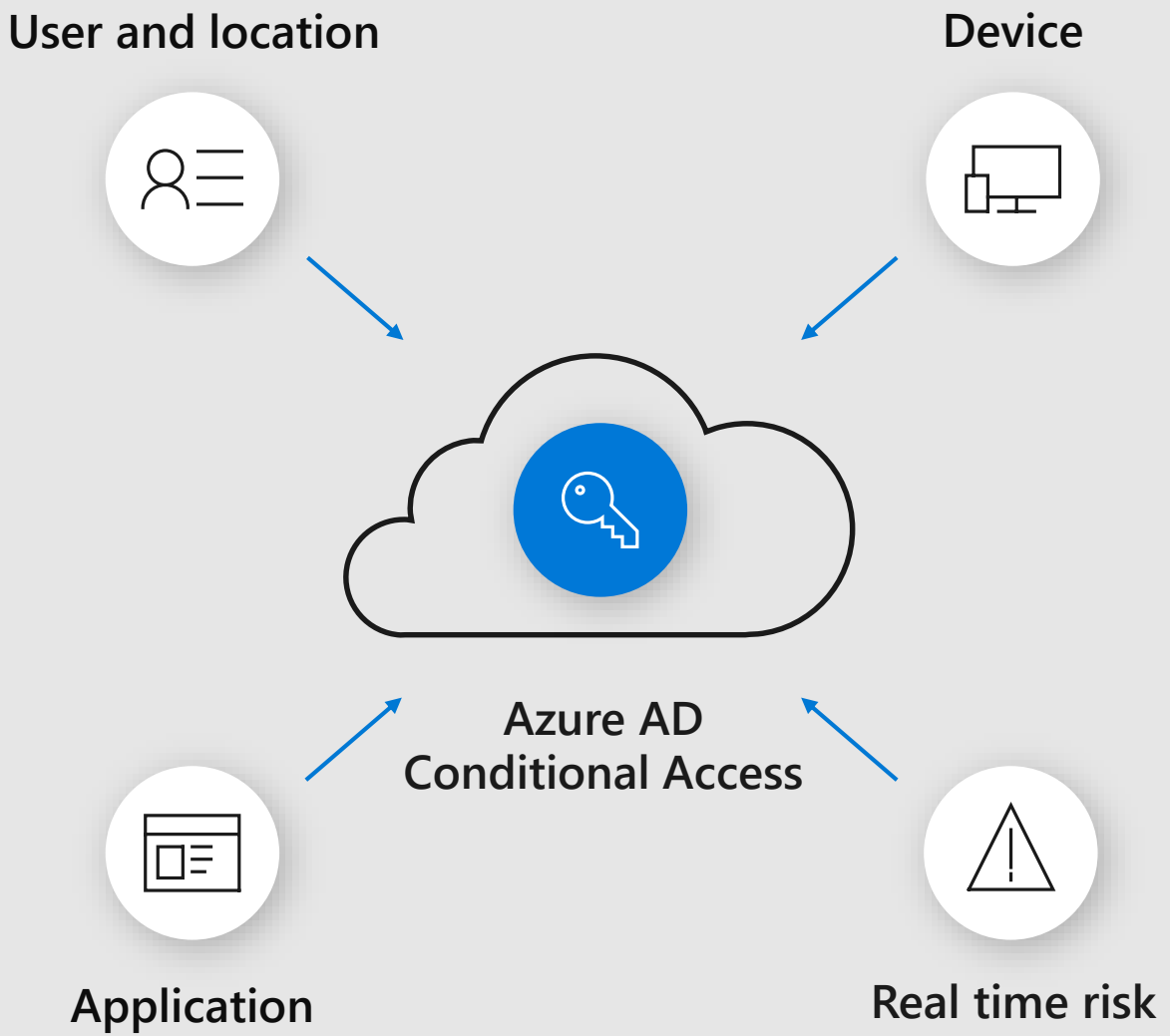


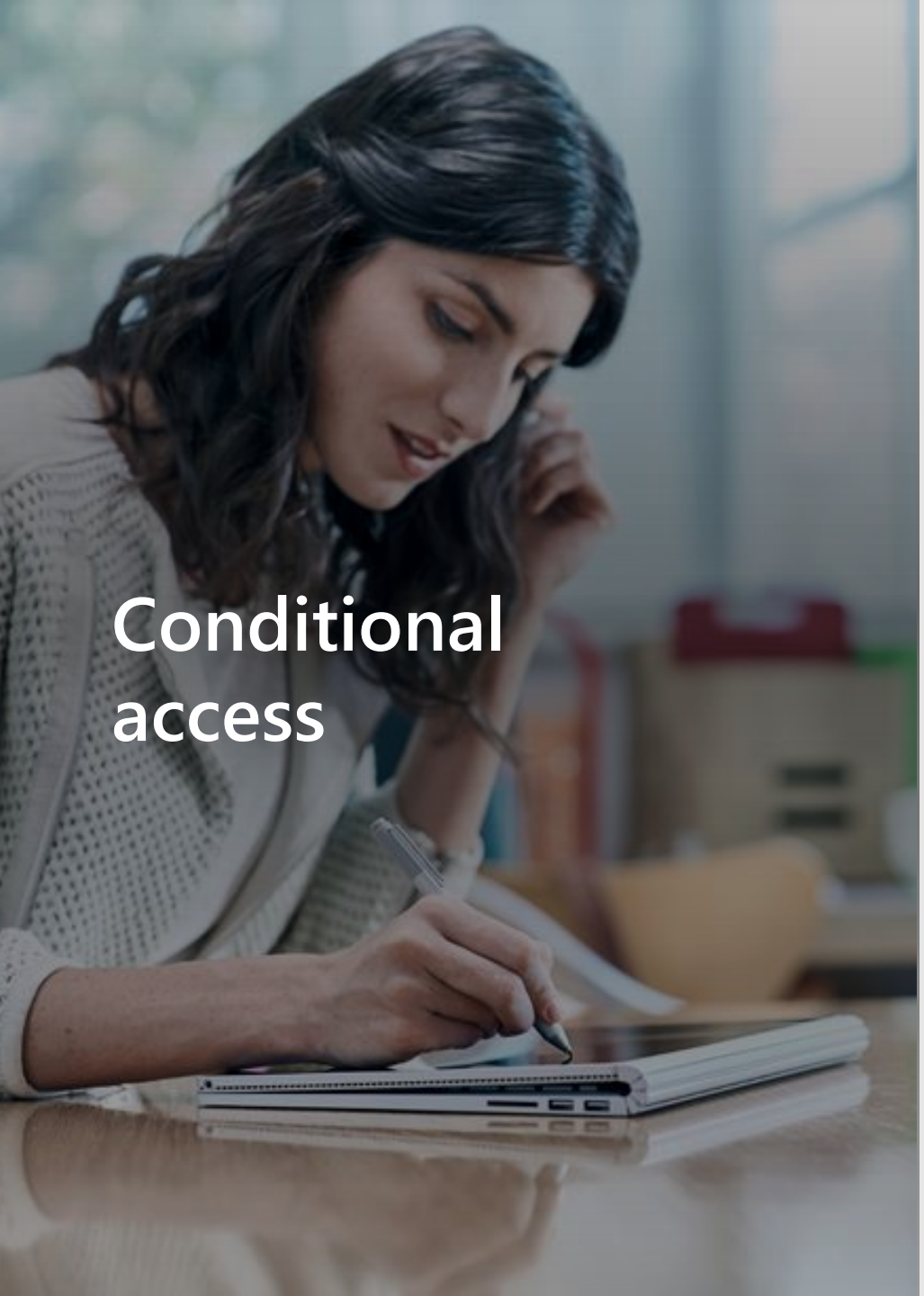




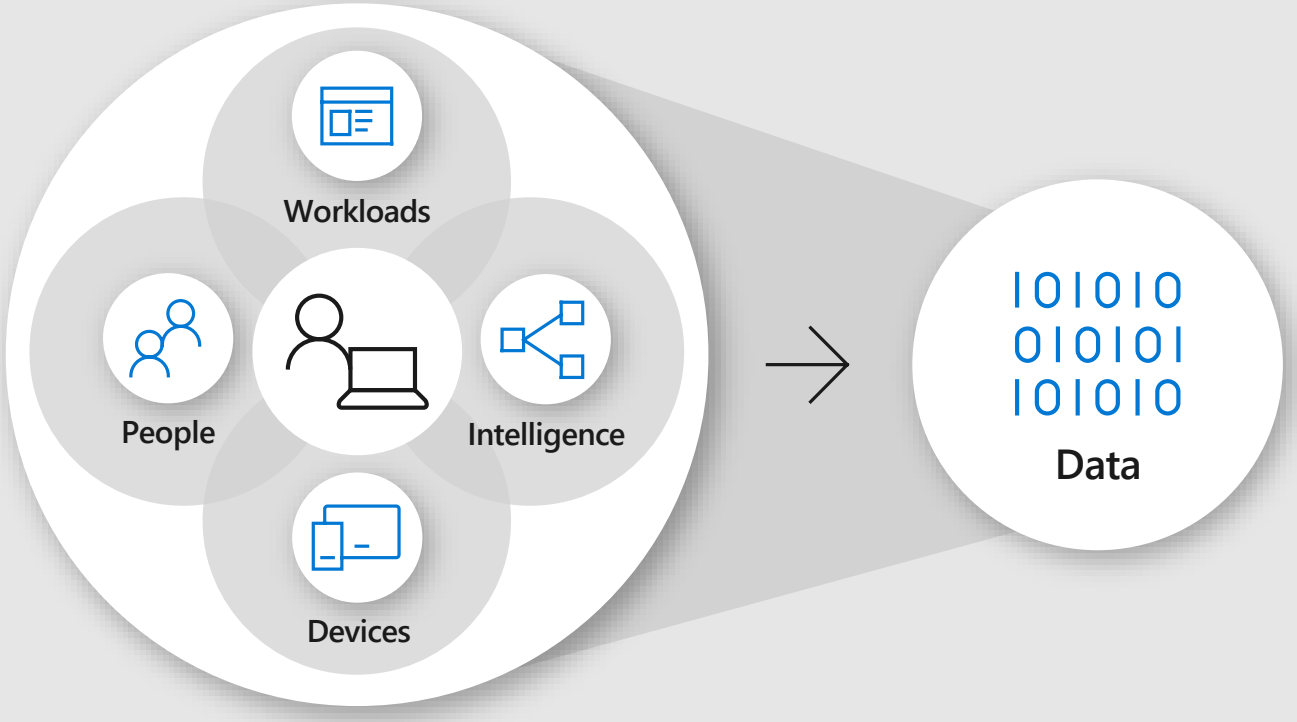


Conditional access





Conditional access



Implement Zero Trust with
Azure AD Conditional Access

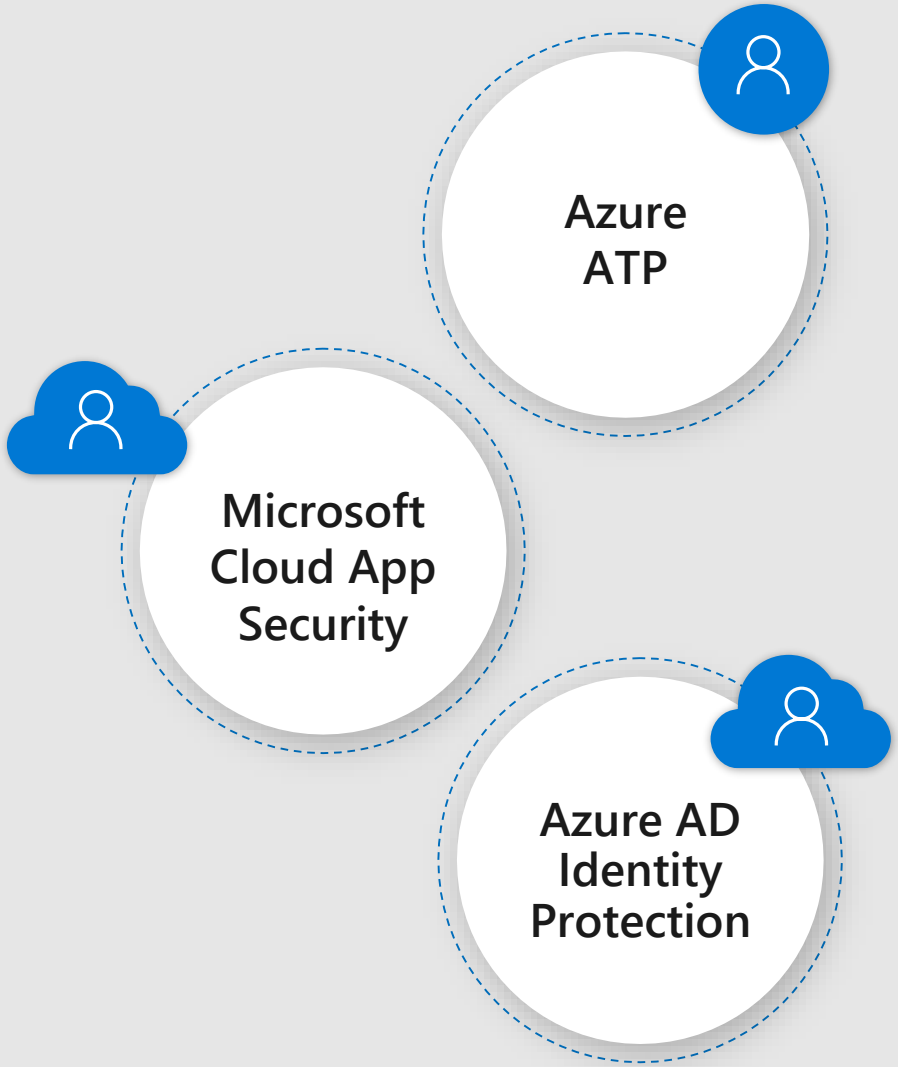
Identity protection

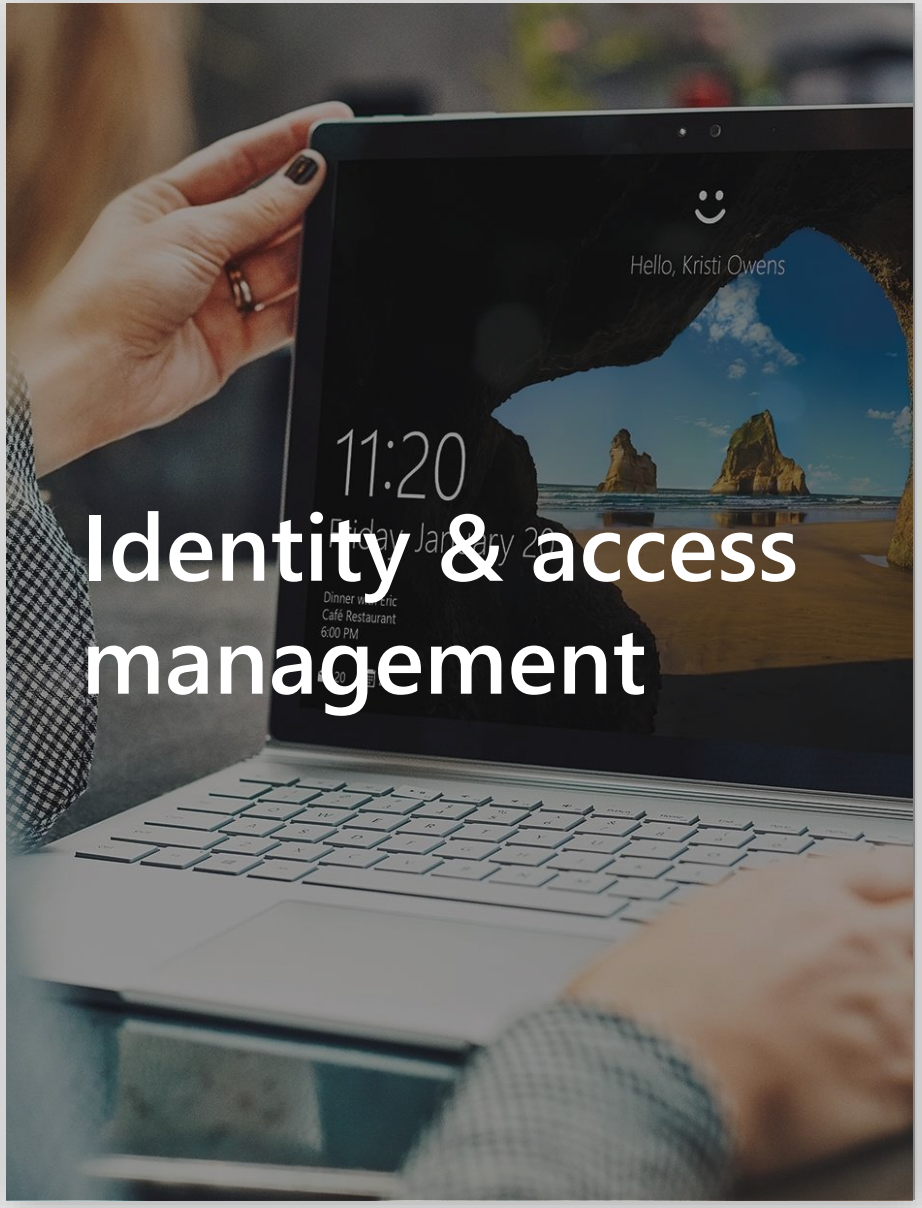
An integral component of Microsoft Threat Protection

One SecOps experience to **investigate identity activities across on-premises & the cloud**

Consolidated view of user information and insights

Investigation priority based on User and Entity Behavior Analytics





Identity & access management

- Turn on MFA
- Protect your apps with Azure AD conditional access
- Begin your password-less journey

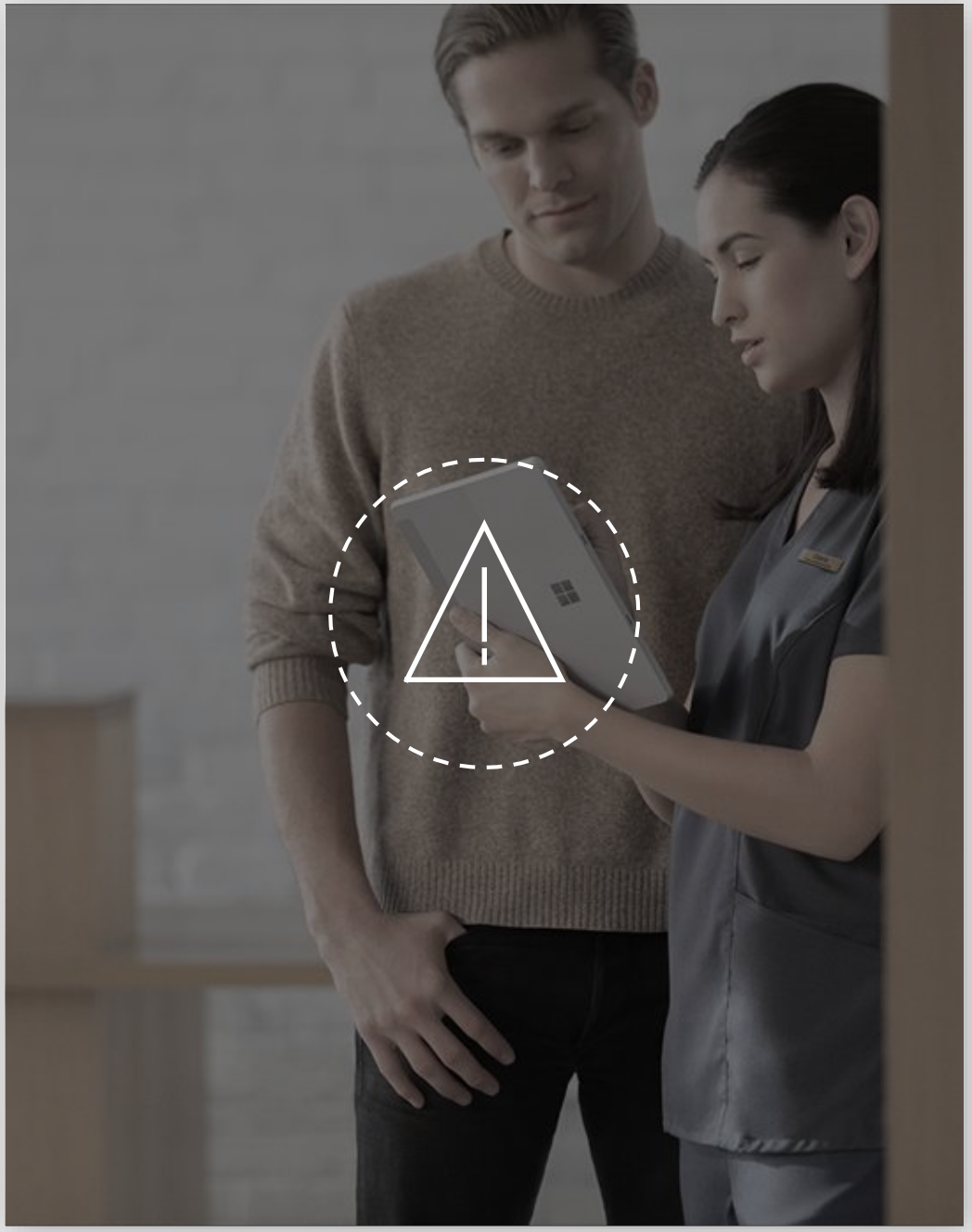
Information protection

Information protection

Fragmented policy → **Unified taxonomy**

Scattered knowledge → **Rich dashboards**

Poor user enforcement → **Intuitive experiences**



Microsoft Information Protection

Locate and classify information anywhere it lives

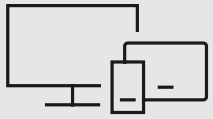
Discover & classify sensitive information

Apply protection based on policy

Monitor & remediate

Accelerate Compliance

Across



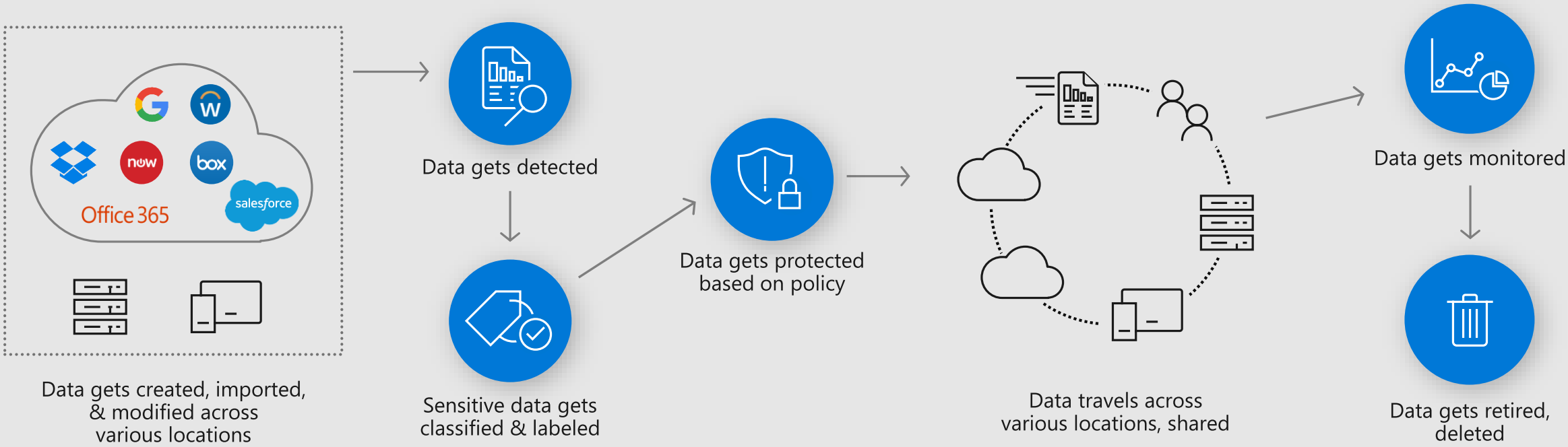
Devices

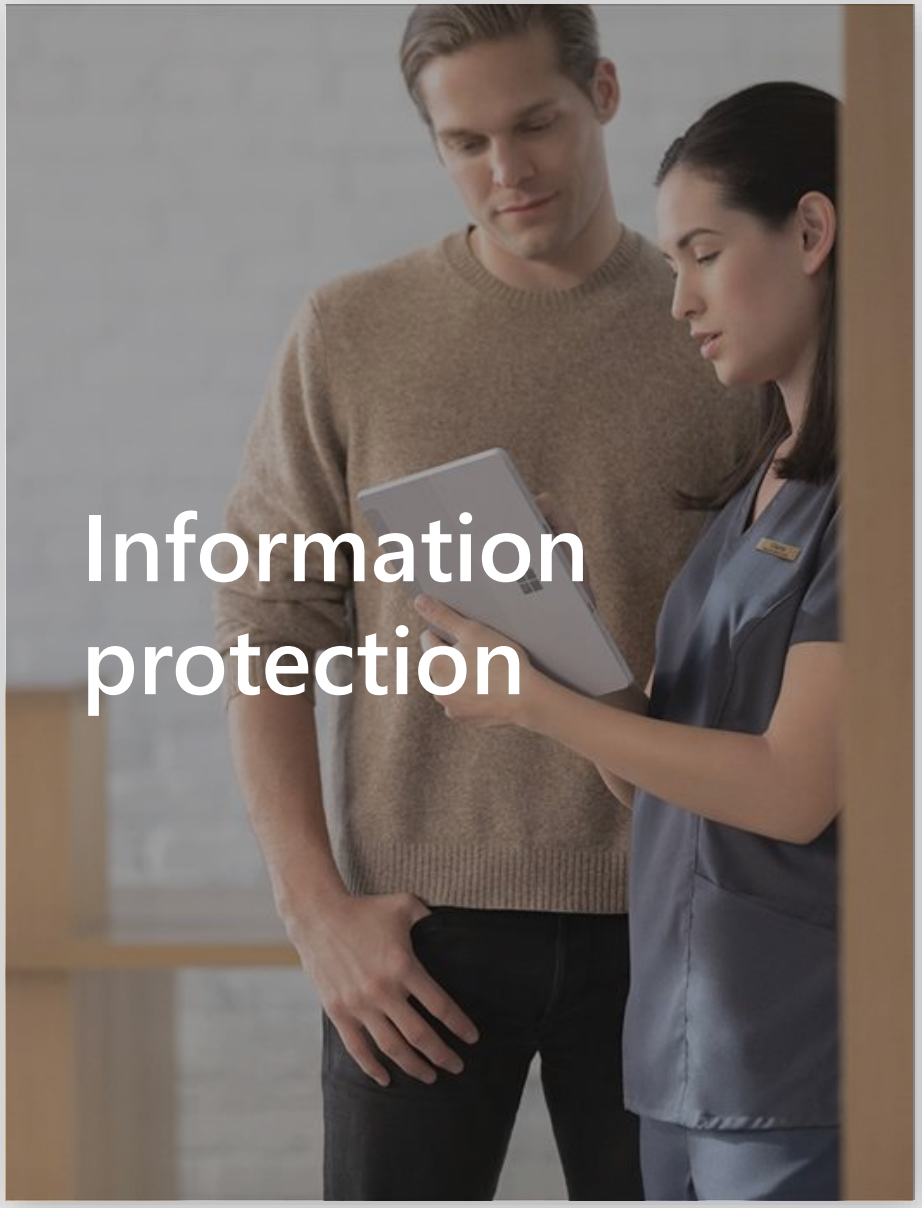
Apps

Cloud services

On-premises

Follow the data—throughout its lifecycle





Start classifying content

Deploy Microsoft Cloud App Security

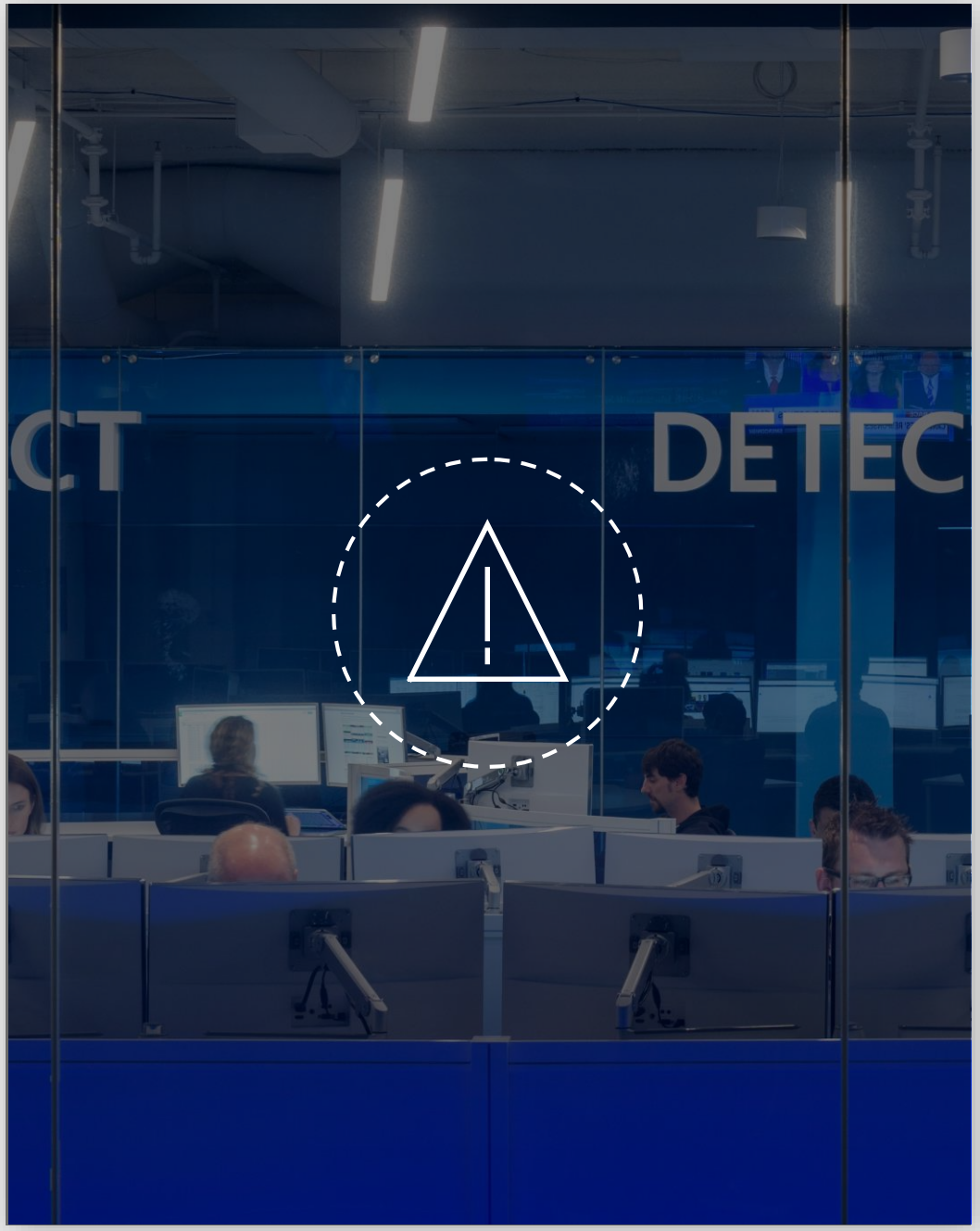
Threat protection

Threat protection

Disconnected tools → **Integrated experiences**

Alert fatigue → **Correlated insights**

Task overload → **Automated workflows**



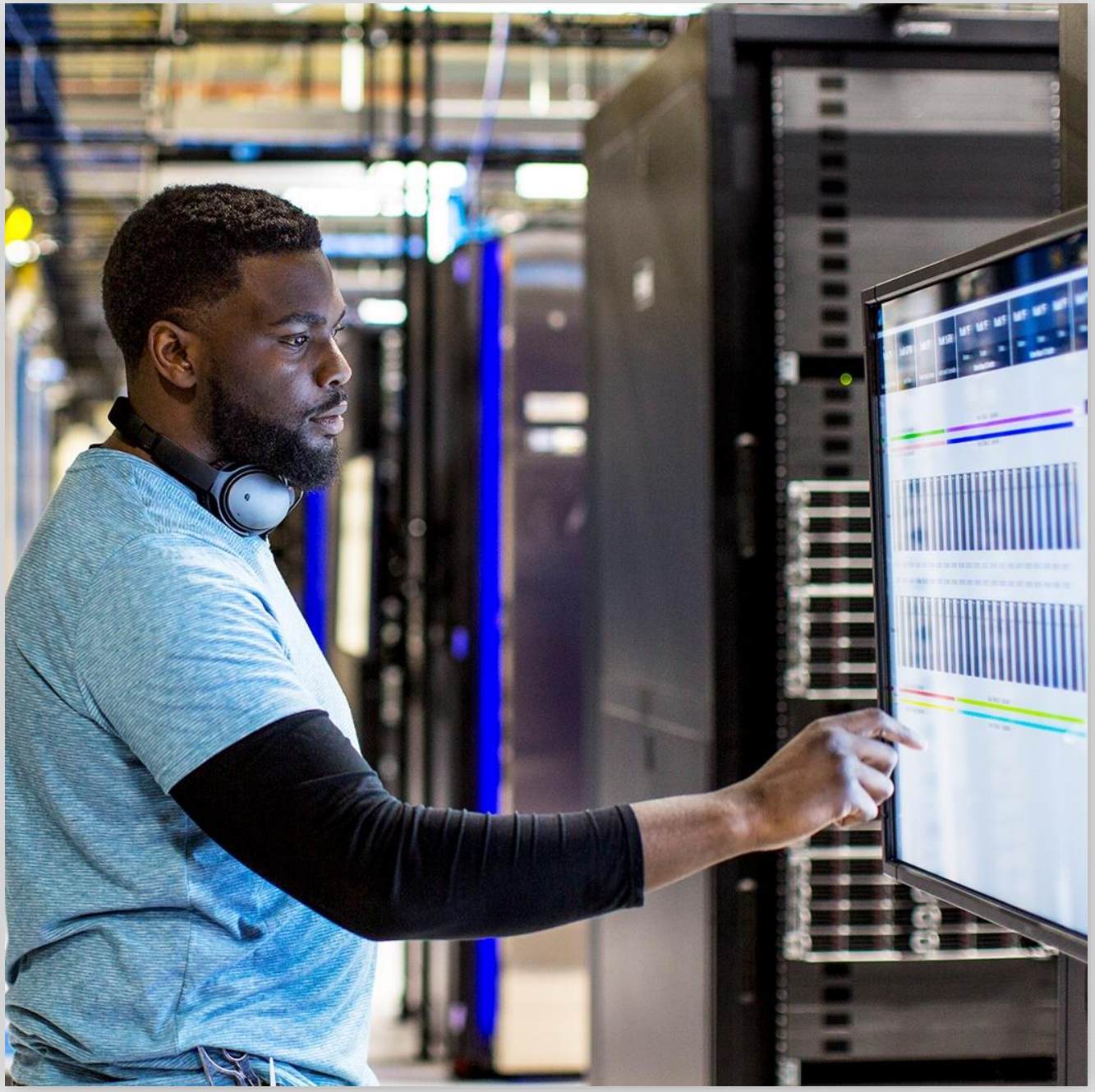

Microsoft Threat Protection
Identities
Endpoints
User Data
Cloud Apps
Infrastructure
Intelligent Security Graph | 6.5 TRILLION signals per day

Check out Microsoft Threat Protection at
security.microsoft.com

Deploy Office 365 ATP,
Windows Defender ATP, & Azure ATP

Turn on Azure Security Center

Security management



Security management

Uncertain configuration → **Understood posture**

Option overload → **Prioritized plan**

Unknown status → **Quantified impact**

Security management

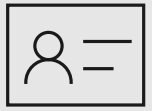
Strengthen your security posture with insights and guidance

Visibility

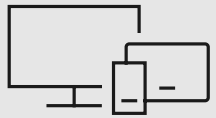
Control

Guidance

Across



Identity



Devices

Apps & data

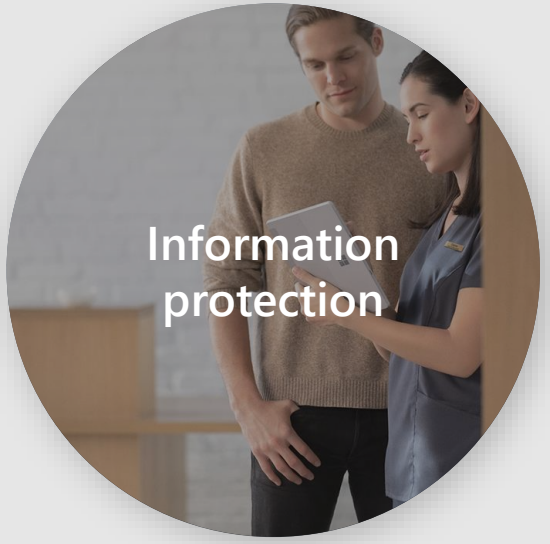
Infrastructure

Visit securescore.microsoft.com to see your score

Make a plan to improve your score!

Enterprise-class intelligent security

Azure AD
Conditional Access



Microsoft
Information Protection

Microsoft Threat Protection
Azure Security Center

Microsoft Secure Score
Azure Security Center

Operations

Security operations that work for you

Technology

Enterprise-class intelligent security

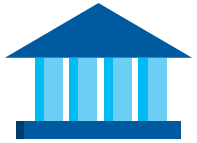
Partnerships

Partnerships for a heterogeneous world

Partnerships for a heterogeneous world

Partner with peers

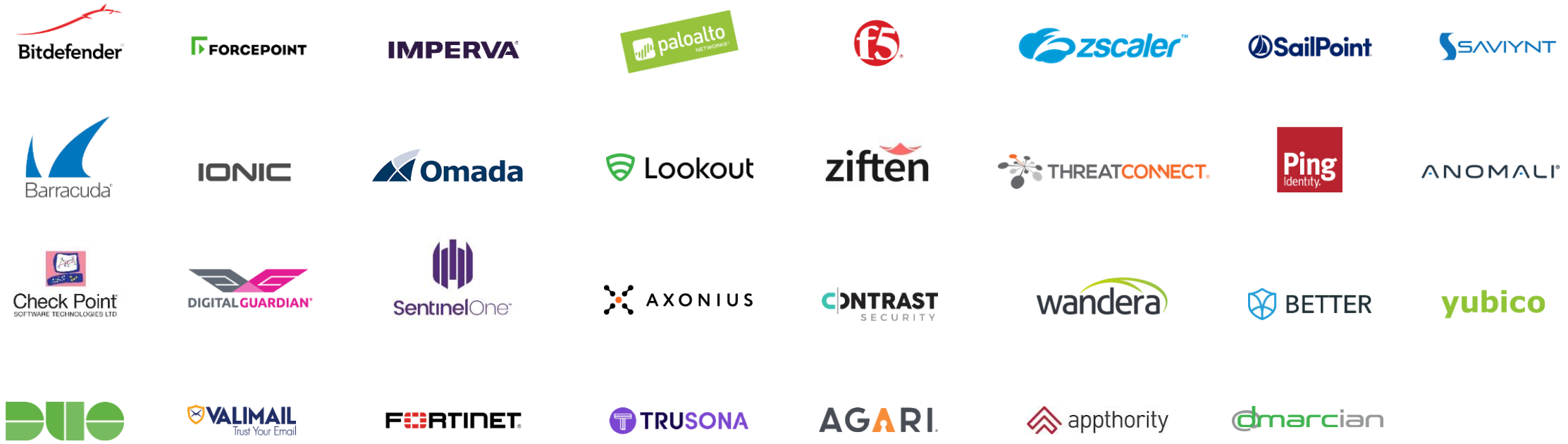
Work with industry alliances



Work with government

Microsoft Intelligent Security Association

Collaboration strengthens protection



Teaming up with our security partners to build an ecosystem of intelligent security solutions that better defend against a world of increased threats

Fast identity online—the FIDO Alliance

The world's largest ecosystem for standards-based, interoperable authentication

Security on-premises and web	Secure mobile user credentials	Secure authentication

FIDO board members