Cl@b 2018

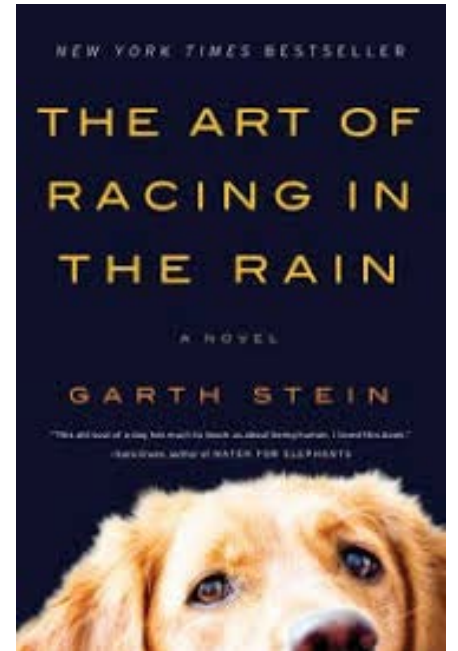18° Congreso Latinoamericano
de Tecnología e Innovación Financiera

Driving Digital Transformation Securely

Diana Kelley
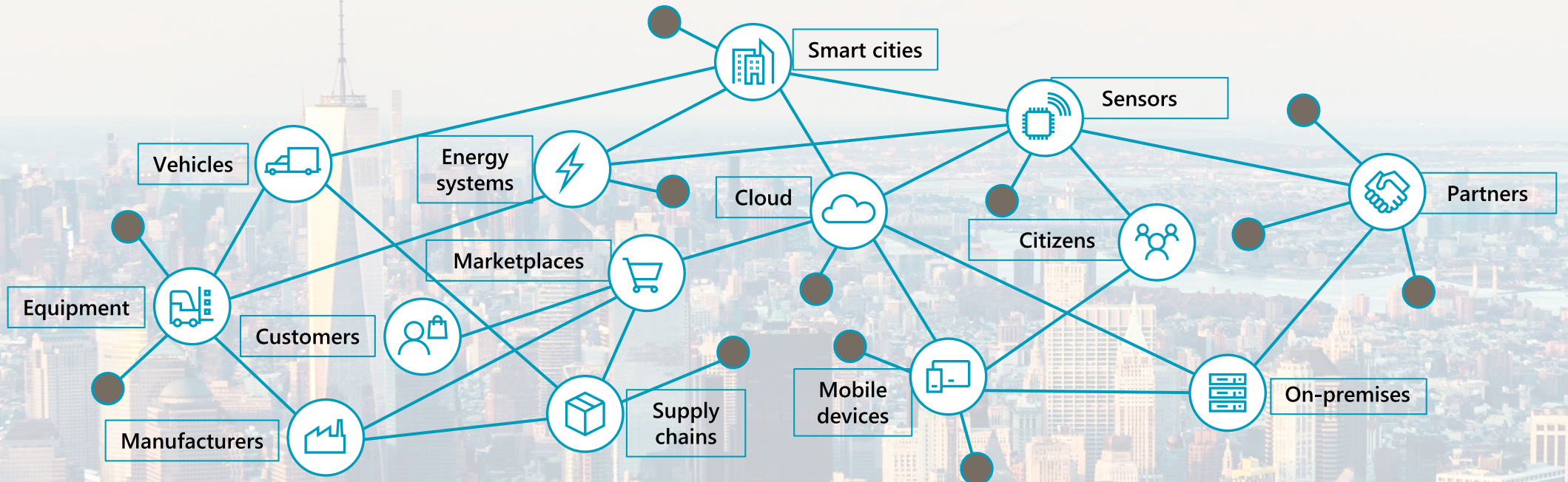Cybersecurity Field CTO, Microsoft
@dianakelley14

"This is a rule of racing:

No race has ever been won in the first corner;

many have been lost there."

The digital estate

Opportunities & Risks

→ Opportunities

Globalization: more markets, customers, and business potential

Always-on access provides **more productivity**

Ability to **analyze massive data** sets at scale and speed

Scalable, cloud based storage: efficient, cost effective, and secure

Modern engineering: allows for more agility in building capabilities, features, and in responding to threats
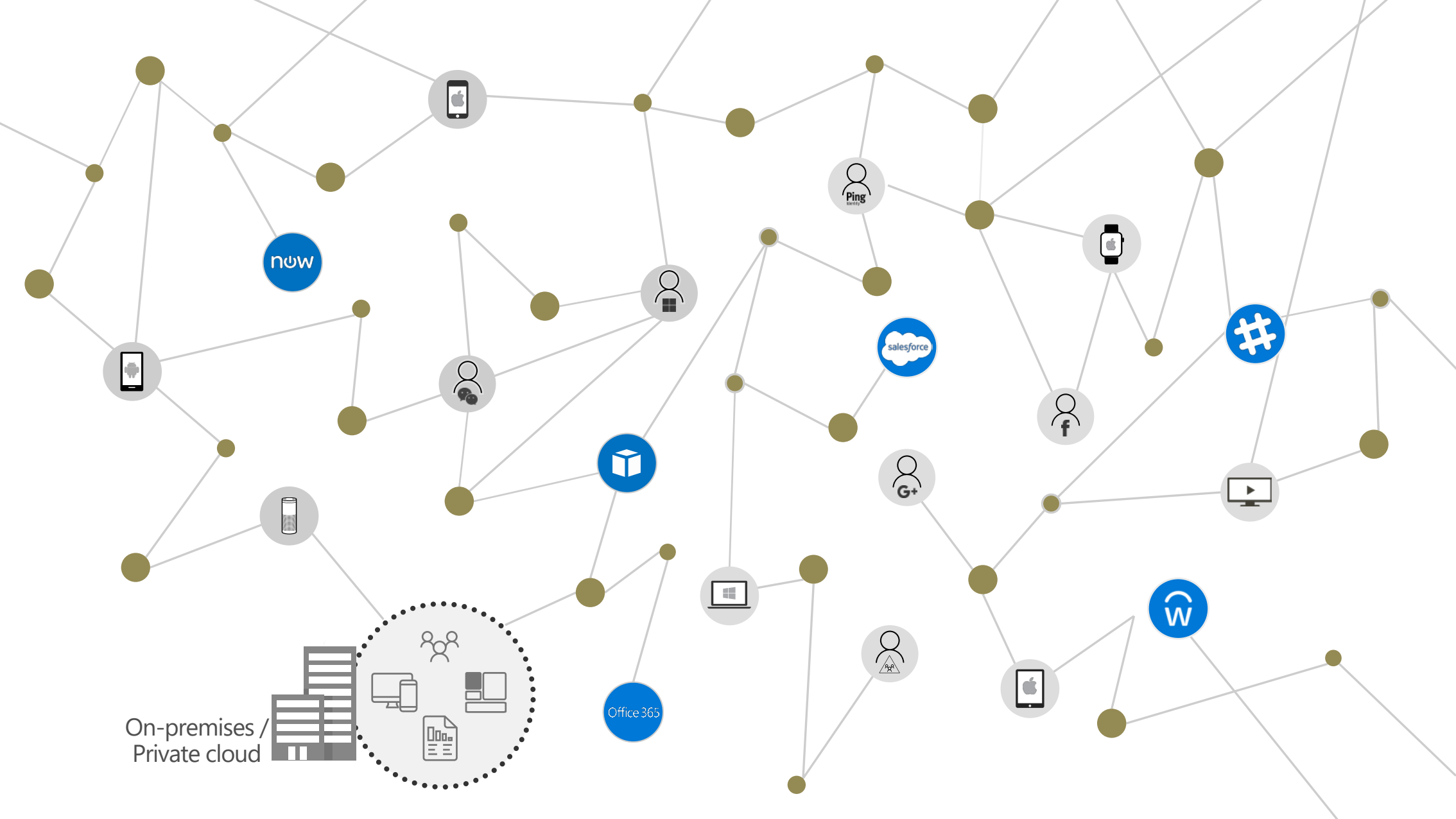
! Risks

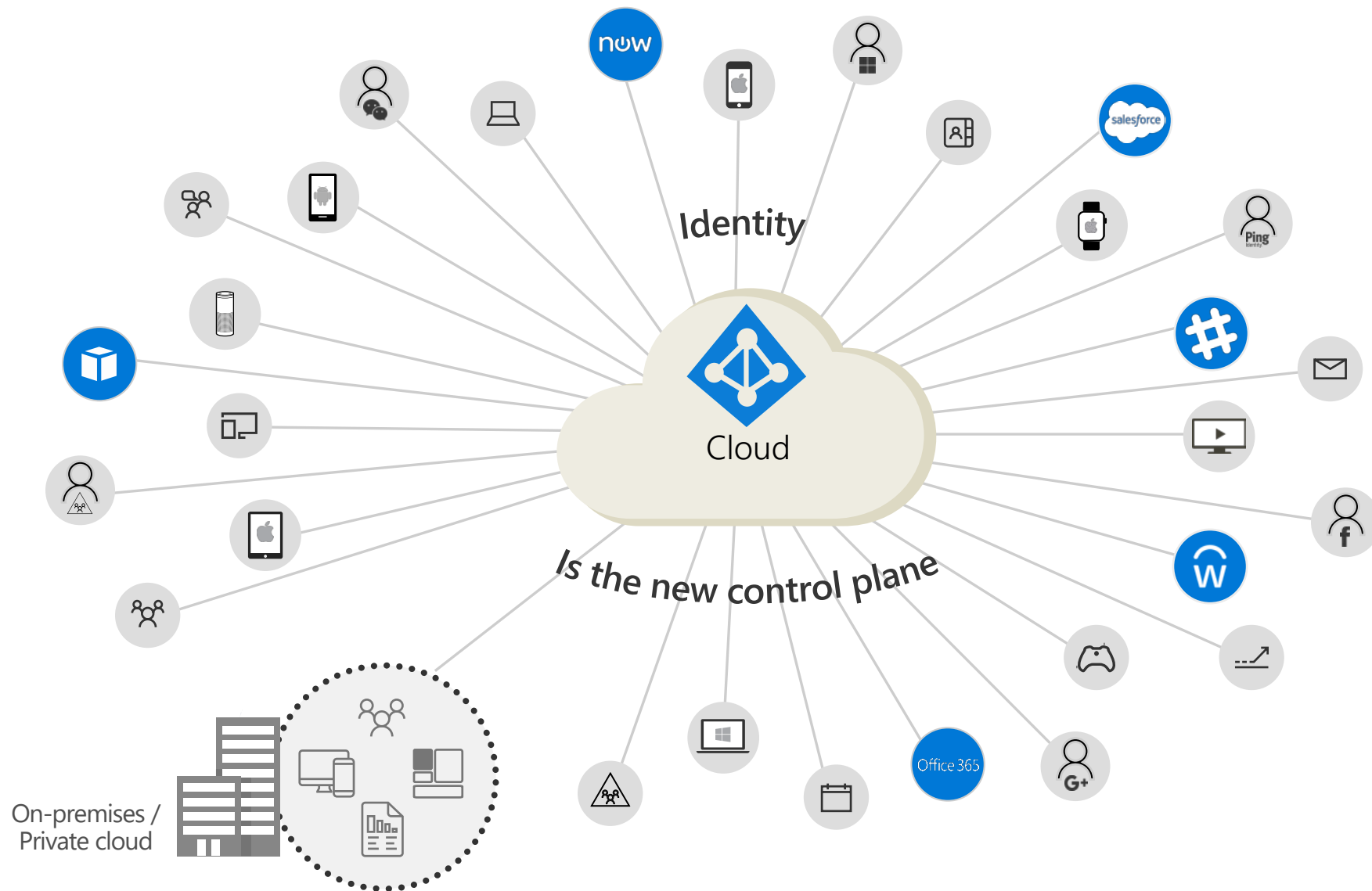Globalization can lead to **"digital xenophobia"**

More lucrative targets give rise to more **dangerous threat actors**

More surface area for attacks/exposure to harm, including **supply chain**

The client-to-cloud world requires a control shift
(Identity is the new perimeter)

On-premises /
Private cloud

Identity

Cloud

Is the new control plane

Office 365

On-premises /
Private cloud

Life before cloud

Security review queue
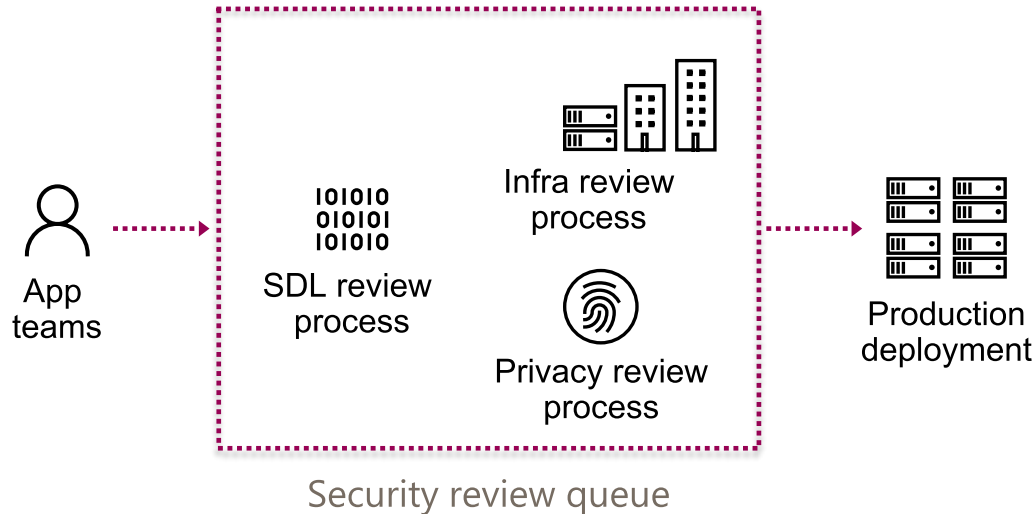
- Separate process for security reviews
- Required for any LOB apps prior to production
- Backlog determines timeline

Life with cloud
+ Mobile + Agile + DevOps

- Self provisioning & empowerment
- Rapid release schedules
- DevOps versus Central IT
- More devices & collaboration

Responsibility Zones

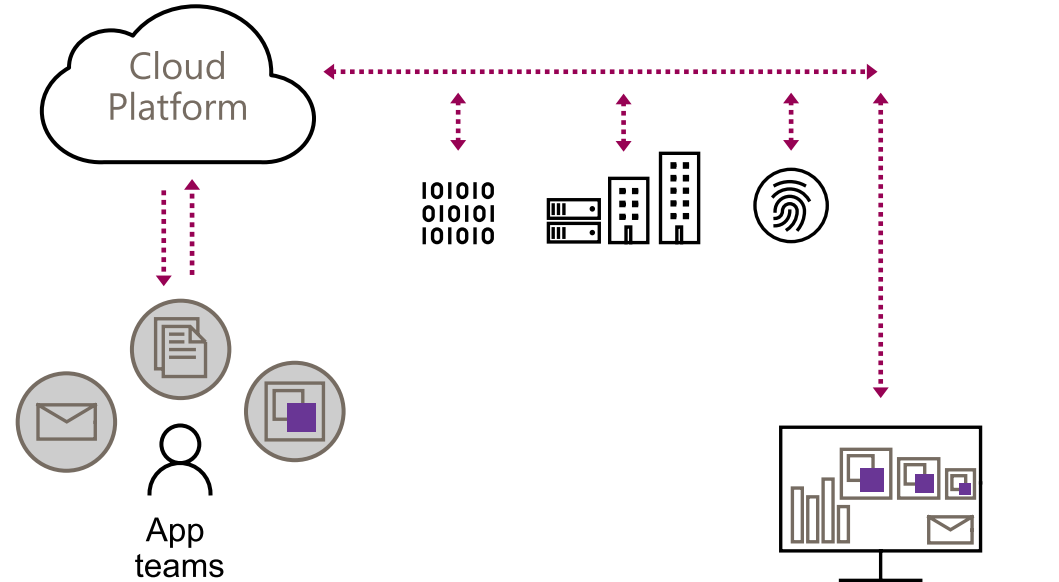| Responsibility	SaaS	PaaS	IaaS	On-prem	
Data governance & rights management	Customer	Customer	Customer	Customer	**Always retained by customer**
Client endpoints	Customer	Customer	Customer	Customer	
Account & access management	Customer	Customer	Customer	Customer	
Identity & directory infrastructure	Microsoft/Customer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

Microsoft   Customer

Multi-Dimensional Approach – Build Security In

Intelligence

Platform

Partners

INTELLIGENCE

PROTECT   DETECT   RESPOND

Physical security

Perimeter
Building
Server environment

Operational security

Continuous testing
Restricted access
Thousands of security
professionals

Customer controls

Access control
Encryption & key management
Network & DDoS protection

Platform

Secure foundation

Built in
security

Platform

Identity & access
management

Information
protection

Threat
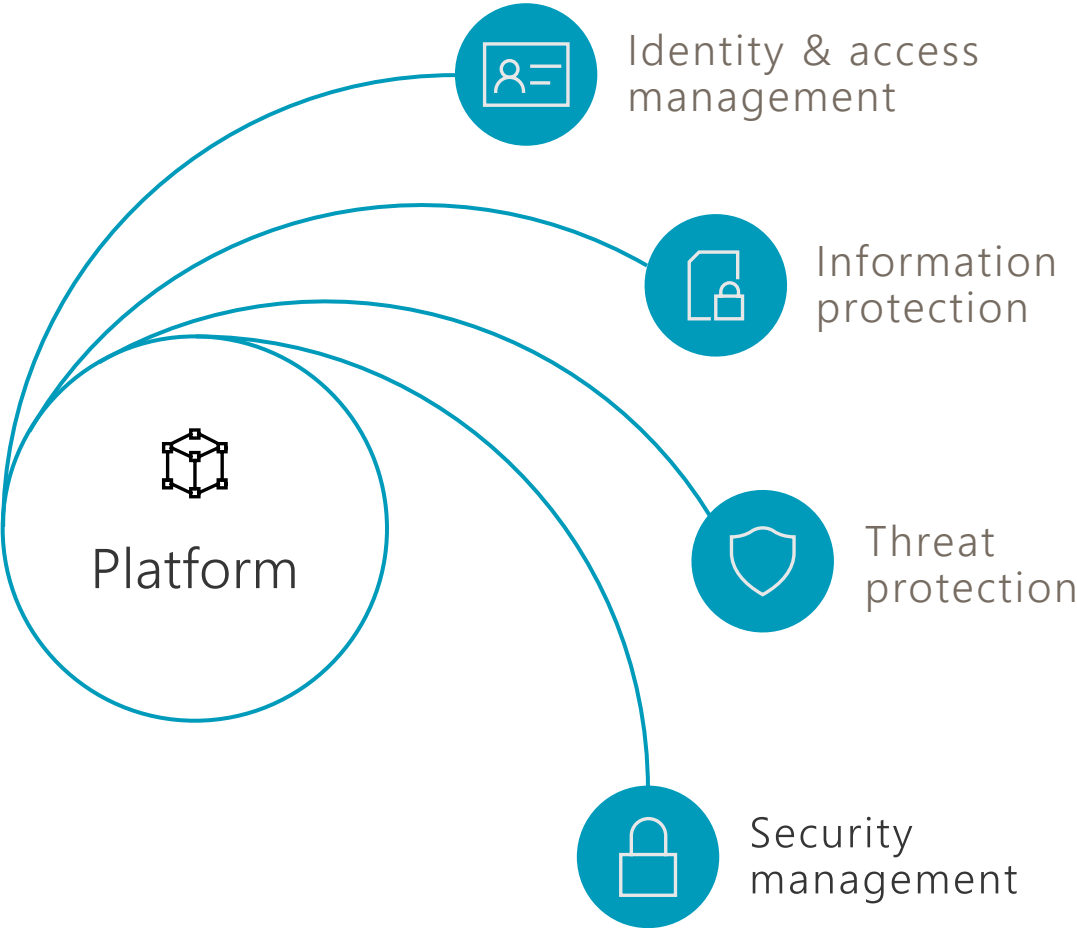protection

Security
management

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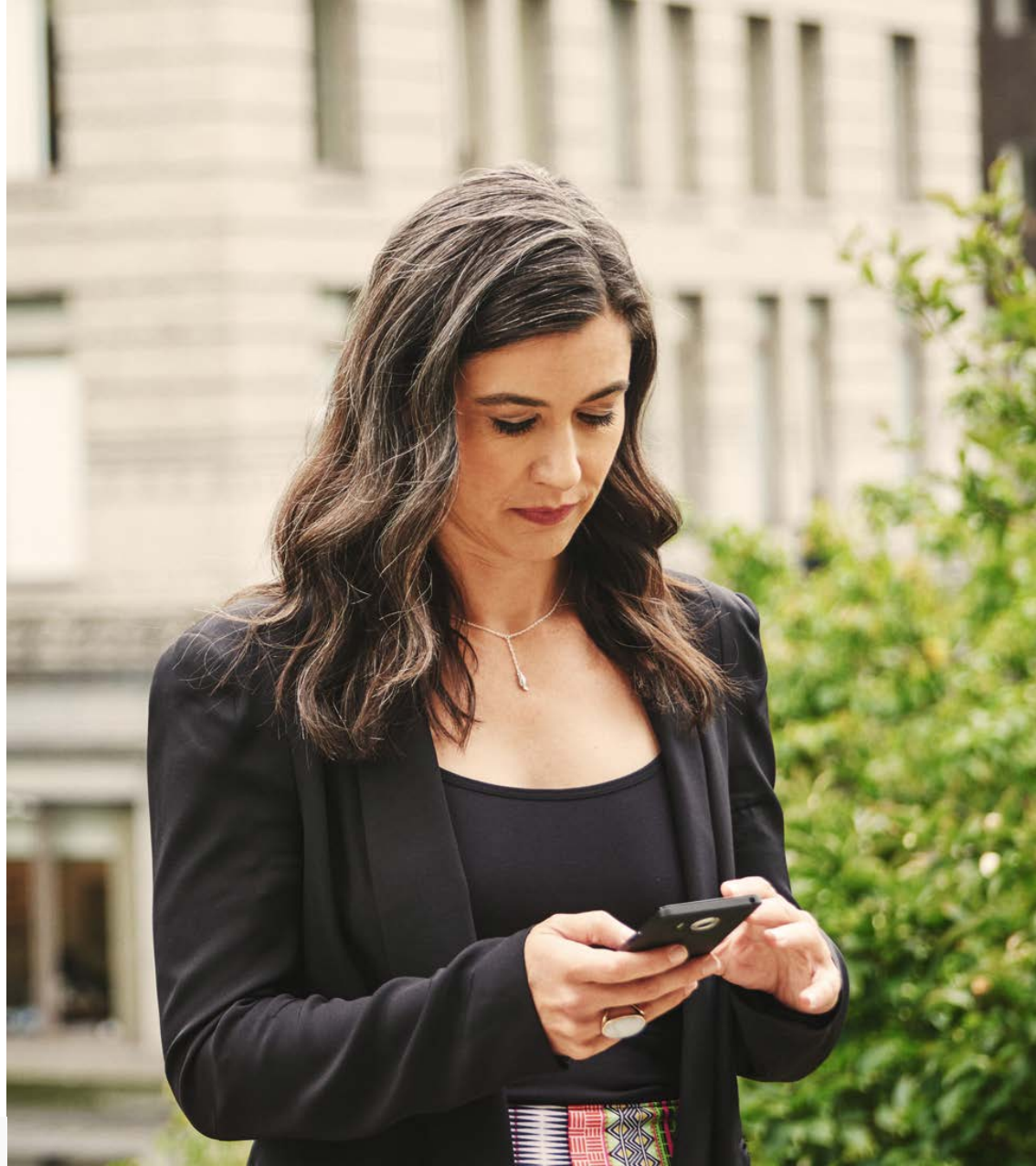
Do you have a strategy for protecting and managing **sensitive information**?

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?

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?

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?

Partner
with peers

Work with
industry alliances

Partners

Partnership
approach

Work with
government
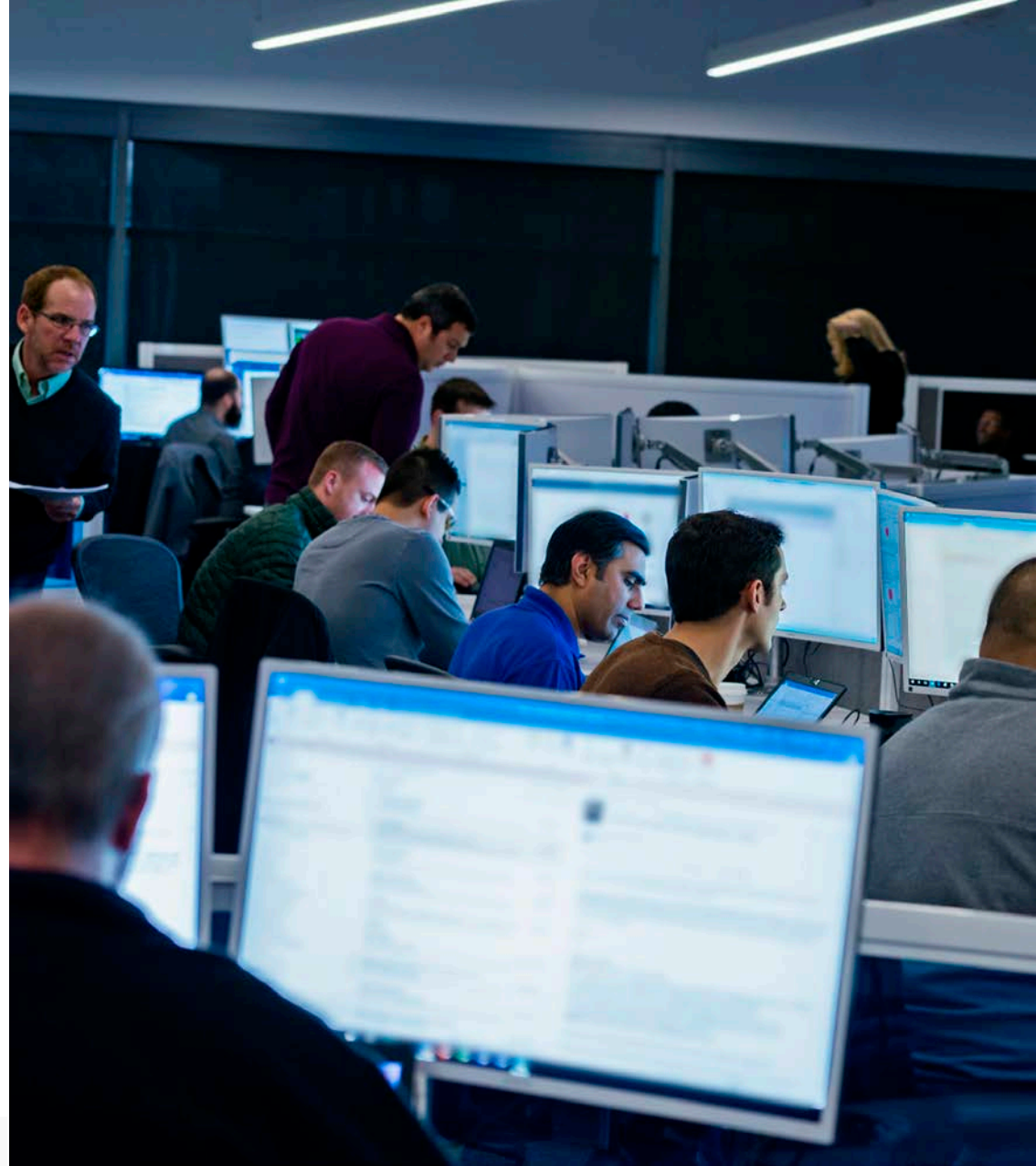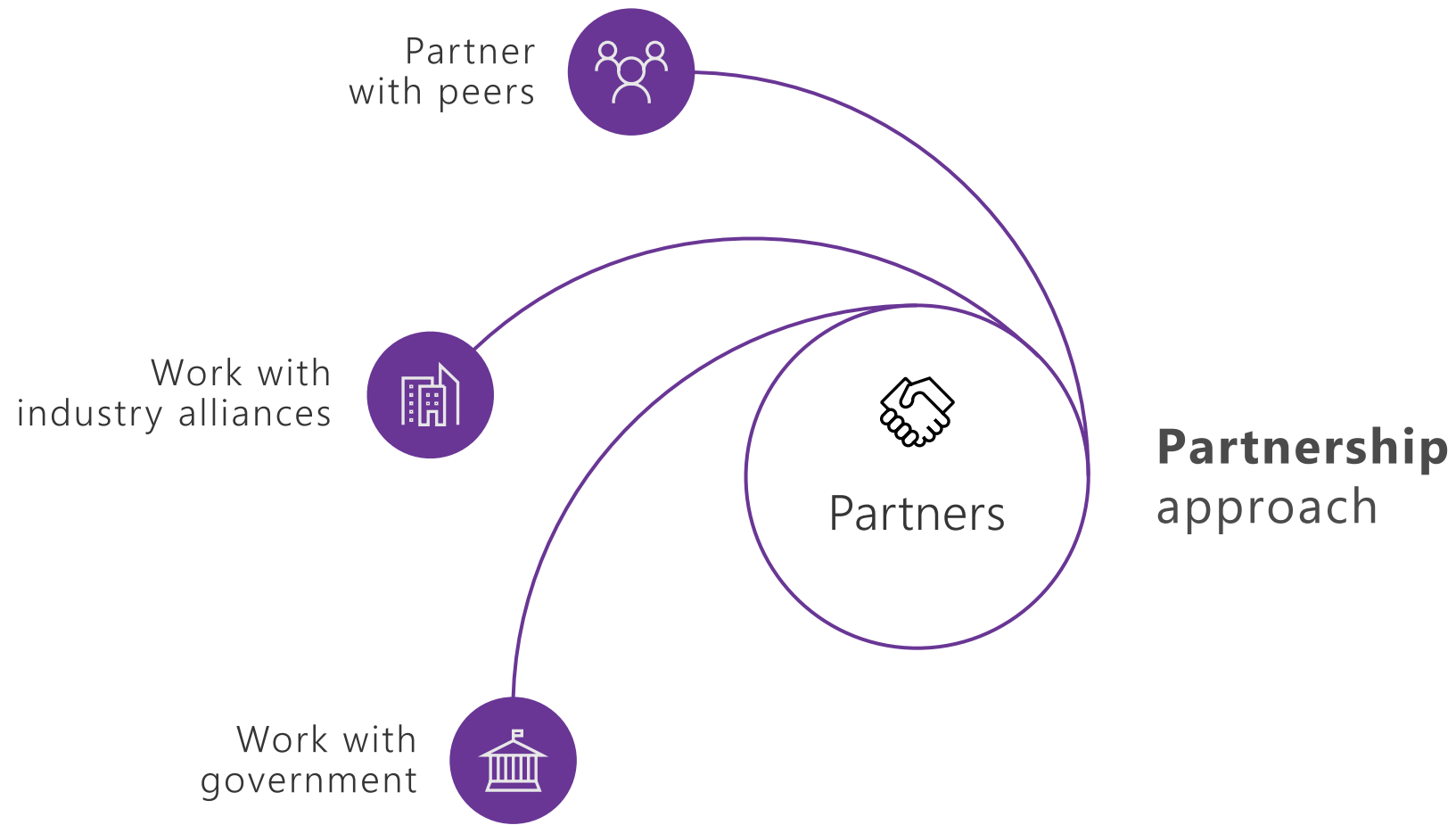
Integrating with your existing solution portfolio

Identity and access management

Omada · SailPoint · TRUSONA — When you truly need to know

SAVIYNT · Ping Identity · RSA · DUO

Information protection

SECUDE · DIGITAL GUARDIAN

Threat protection

Lookout · ZIMPERIUM

Check Point SOFTWARE TECHNOLOGIES LTD · Skycure

Security management

ArcSight An HP Company · f5 · splunk> · paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD · Qualys Continuous Security · QRadar

Microsoft Intelligent Security Graph
Unique insights, informed by trillions of signals

Shared threat data from partners, researchers, and law enforcement worldwide

Outlook

OneDrive

930M
threats detected on devices every month

400B
emails analyzed

1.2B
devices scanned each month

200+
global cloud consumer and commercial services

Windows

Botnet data from Microsoft Digital Crimes Unit

Microsoft accounts

Azure

Enterprise security for **90%** of Fortune 500

750M+
Azure user accounts

Xbox Live

18B+ Bing web pages scanned

Bing

450B
monthly authentications

Layered ML in action

Local ML models, behavior-based detection algorithms, generics, heuristics

Metadata-based ML models

Sample analysis-based ML models

Detonation-based ML models

Big data analytics

Client ML

Cloud ML

Protection in milliseconds
Just before noon, behavior-based algorithms detected a massive campaign

Protection in milliseconds
Most components of the attack were blocked at first sight by metadata-based ML models

Protection in seconds
Additional protection was provided by sample analysis-based ML models for some components

On March 6, Windows Defender Antivirus blocked more than 400,000 instances of several sophisticated trojans
http://aka.ms/dofoil

Other recent cases: Emotet | Bad Rabbit

Power of Rapid Detection & Response

Ransomware made a real-world impact in 2017, bringing down critical services like hospitals, transportation, and traffic systems. Here are few of the unprecedented and devastating ransomware families responsible for the 2017 attacks:

8 B $	850 M $	14 Minutes
WannaCrypt	Petya/NotPetya	BadRabbit

The Big Three

1. Simple

- Reduce number of solution vendors
- Alleviate friction between security & productivity

2. Smart

- Speed up detection & response with automation and ML
- Insight across the threat landscape

3. Integrated

- Built-In Security means less to deploy, fewer agents to manage
- Visibility across hybrid architectures

Microsoft Cybersecurity

Download the Microsoft Security Intelligence Report, Volume 23 for more security insights.

www.microsoft.com/sir

Microsoft