Protecting, Detecting, Responding & Insuring Cyber Threats

Robert Hayes
Senior Director, Strategy & Partnerships,
Microsoft Enterprise Cybersecurity Group
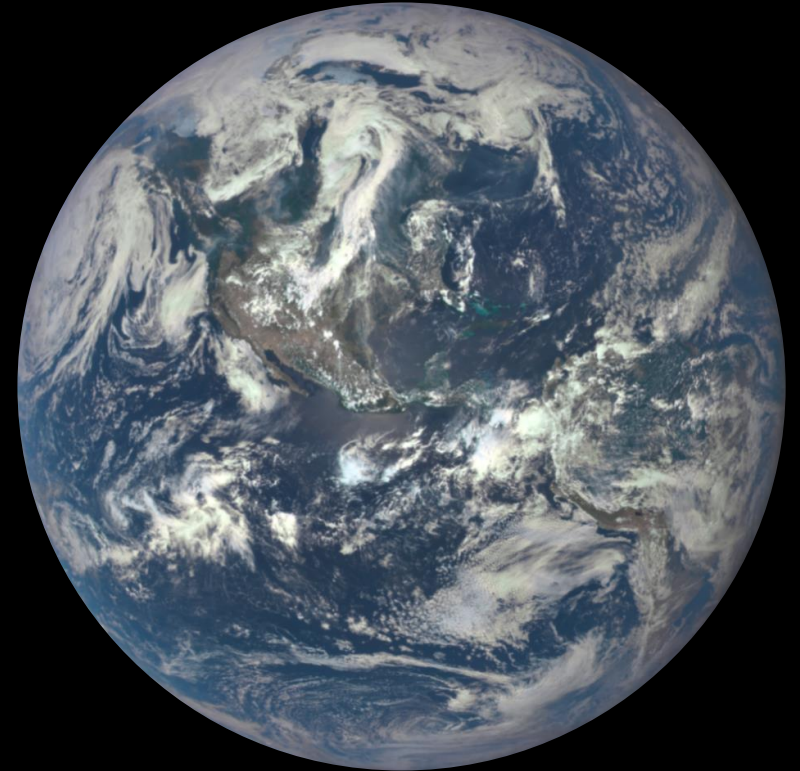
Microsoft

OUR COMMITMENT TO **TRUST**

TRANSPARENCY

PRIVACY

2015 A ROUGH YEAR IN SECURITY

160 MILLION customer records

229 DAYS between infiltration and detection

$3 TRILLION of market value destroyed

2016 NOT STARTING ANY BETTER!

MOSSACK FONSECA:

11.5m documents

210,000 companies

21 offshore jurisdictions

YOUR
IT ENVIRONMENT

YOUR
IT ENVIRONMENT

YOUR
IT ENVIRONMENT

YOUR
OPPORTUNITY

YOUR
IT ENVIRONMENT

SECURE YOUR ENTERPRISE / BUILD AN APPROACH

	PROTECT	DETECT	RESPOND
Identity	Eliminate passwords, use multi-factor auth, move to risk based conditional access	Proactive notification of suspicious behavior and unusual authentication	Automatically elevate access requirements based on risks
Device	Device encryption, management of devices, consistent compliance	Auto-identify suspicious or compromised end points	Block, quarantine suspicious devices
Apps & infrastructure	Identify unsanctioned apps & enforce policies on cloud resources, monitor cloud data	Detect any deviations from baseline, policies, or behavior	Deploy new controls & block risky apps
Data	Policy based data separation, containment, classification & encryption	Notification of any attempts for unauthorized data access	Revoke unauthorized access to documents, wipe device data

Identity

Device

Apps & infrastructure

Data
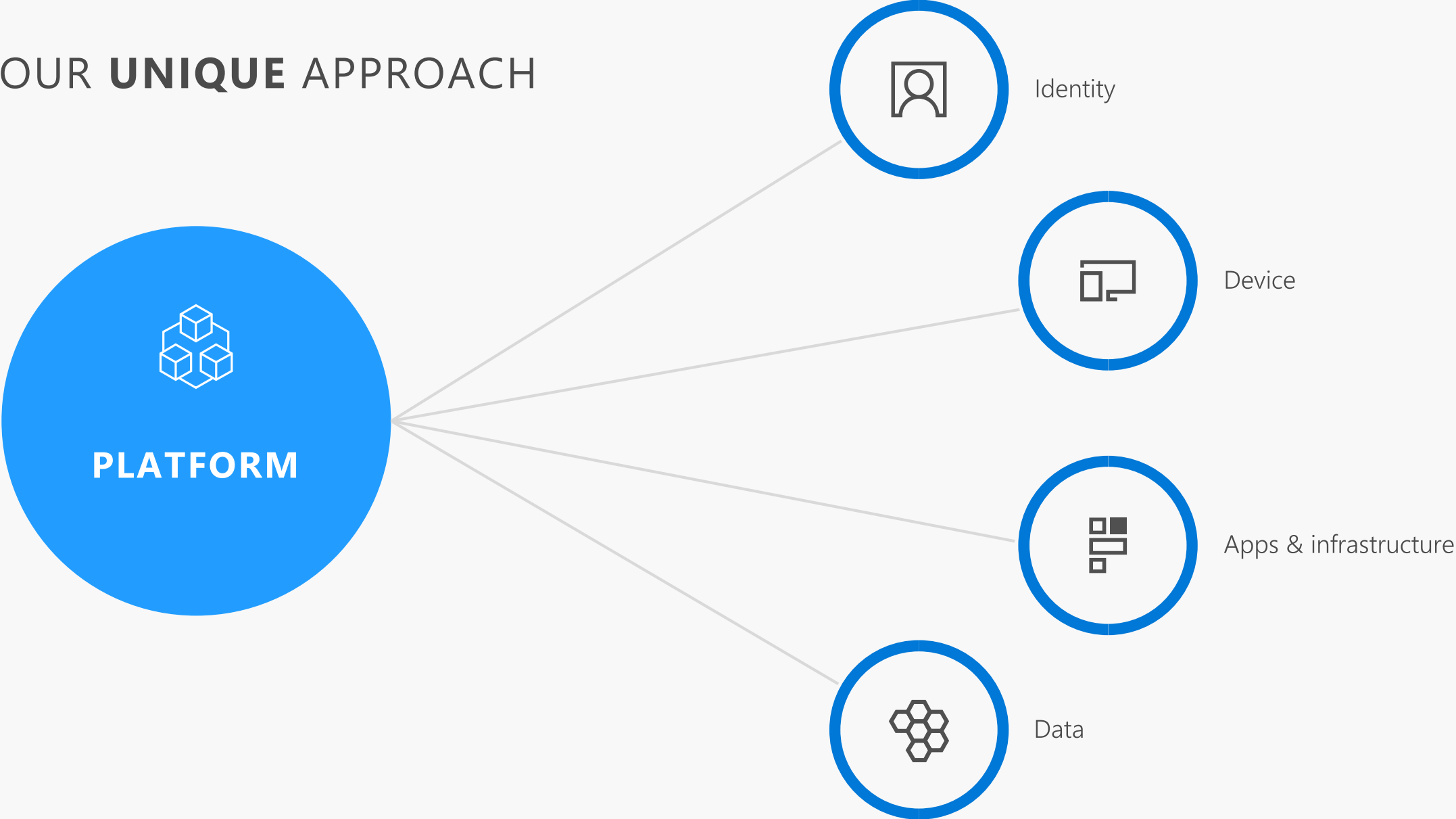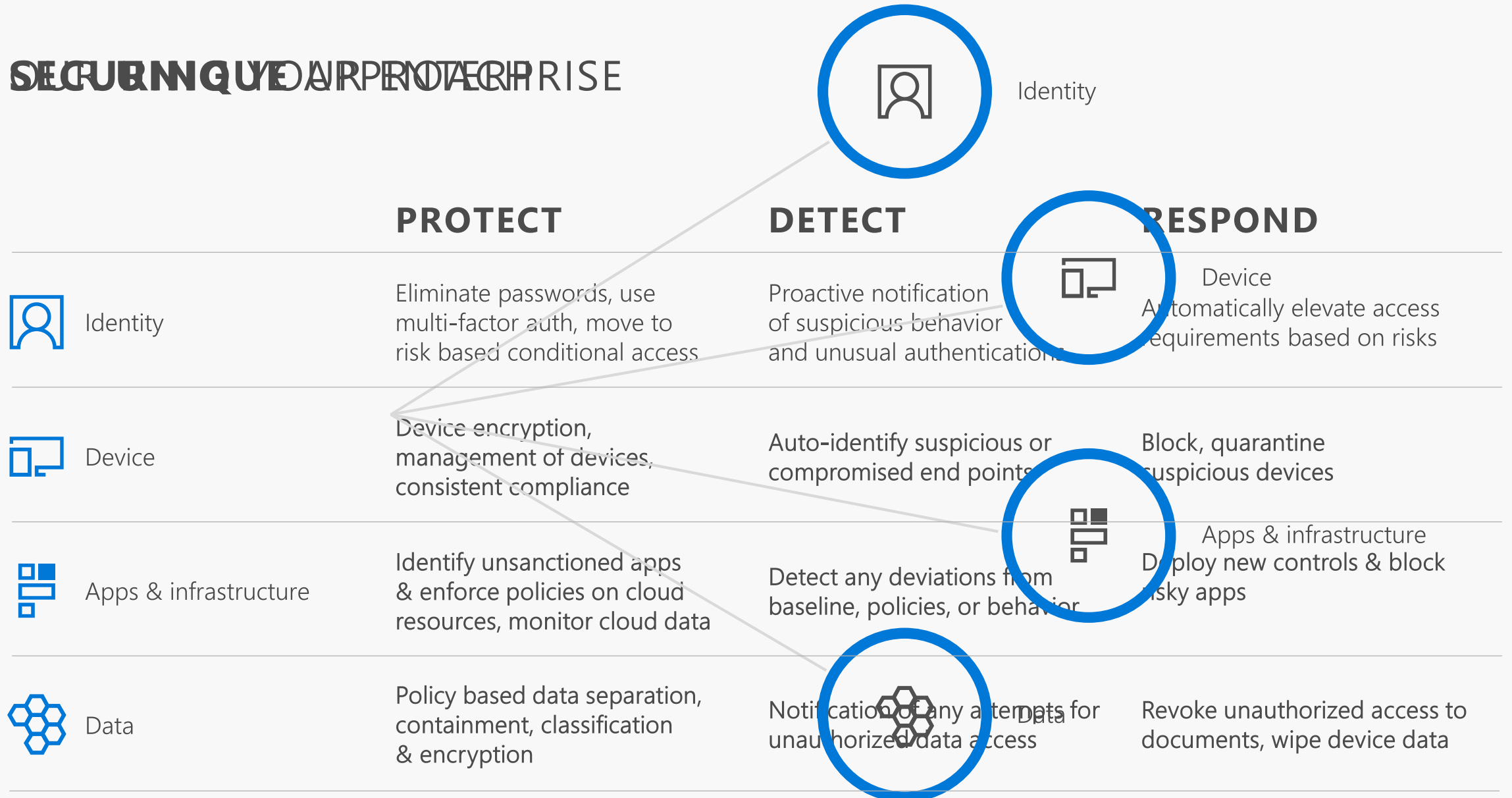
THE MICROSOFT **SECURITY PLATFORM**

|	**PROTECT**	**DETECT**	**RESPOND**
Identity			
Device	Azure Active Directory, Microsoft Advanced Threat Analytics, Windows 10, Microsoft Intune, Office 365		
Apps & infrastructure	Azure, Microsoft Cloud App Security, Office 365, Operations Management Suite, SQL Server 2016, Windows Server 2016		
Data	Azure Rights Management, Windows 10, Office 365, SQL Server 2016, Windows Server 2016		
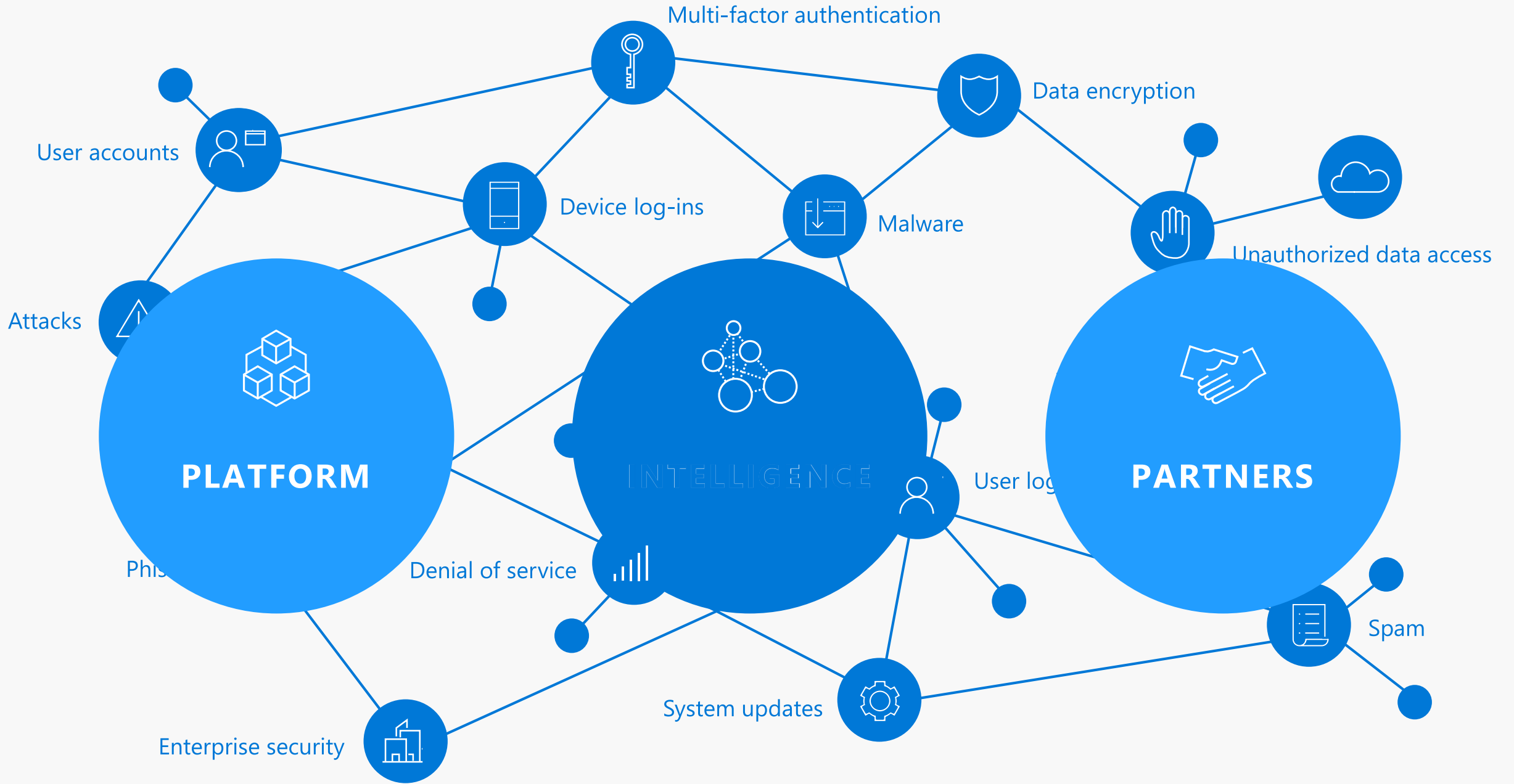
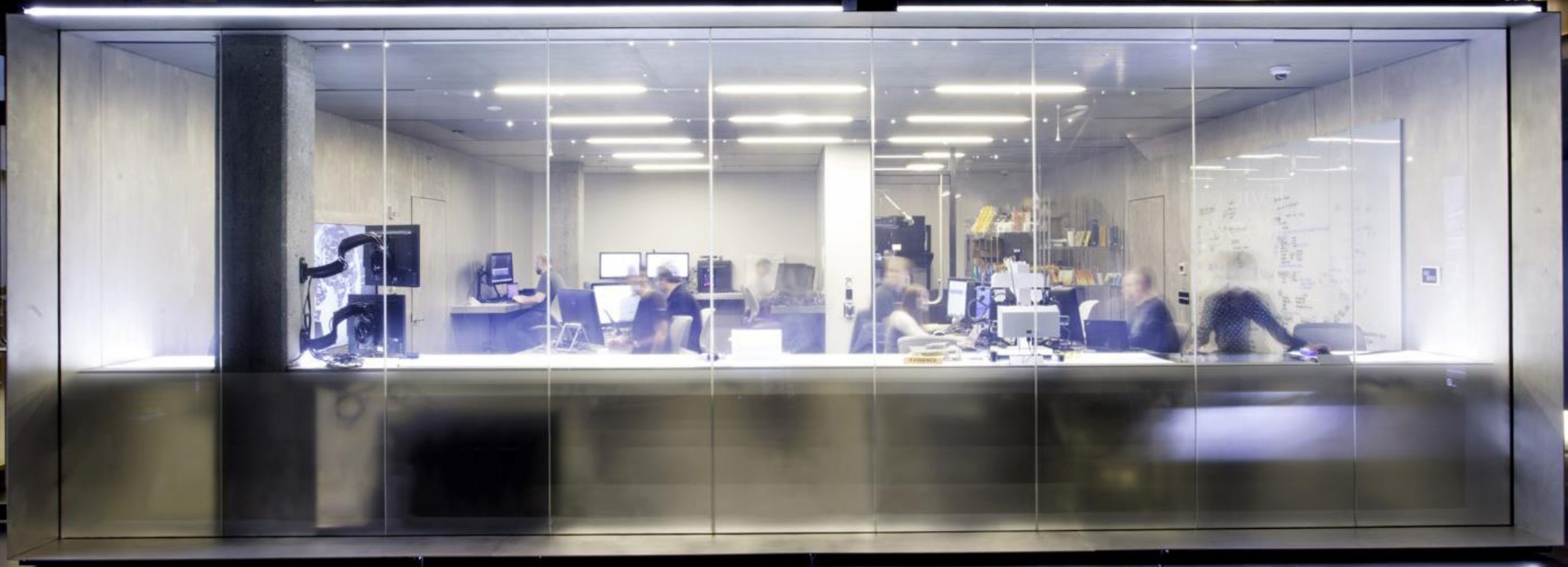OUR **UNIQUE** PERSPECTIVE

INTELLIGENCE

300B user authentications each month

1B Windows devices updated

200B emails analyzed for spam and malware

OUR **INTELLIGENCE**

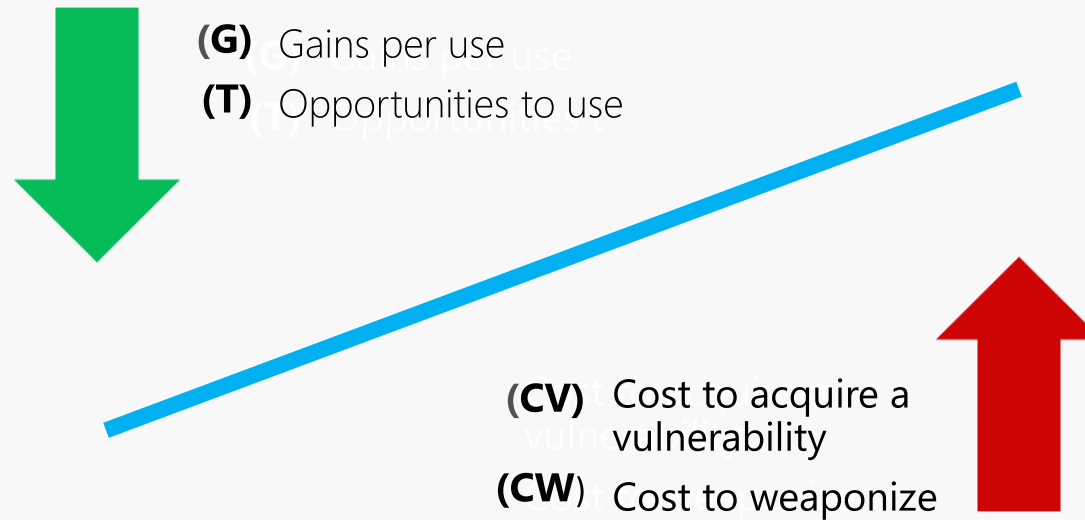# The Microsoft Cyber Defense Operations Center

- Protect Microsoft's cloud infrastructure, customer-facing cloud services, products and devices, and internal resources 24 x 7 x 365

- Unite personnel, technology, and analytics in a central hub

- Provide world-class security protection, detection, and response

- More than 50 Security Experts and Data Scientists

- Connected to >3500 Security Professionals across Microsoft

- Tight partnerships with Microsoft Research and the Security Development Lifecycle (SDL) team

Cyber Economics

Goal: increase attacker costs

(G) Gains per use
(T) Opportunities to use

(CV) Cost to acquire a vulnerability
(CW) Cost to weaponize

Attacker's ROI = (G x T) − (CV + CW)
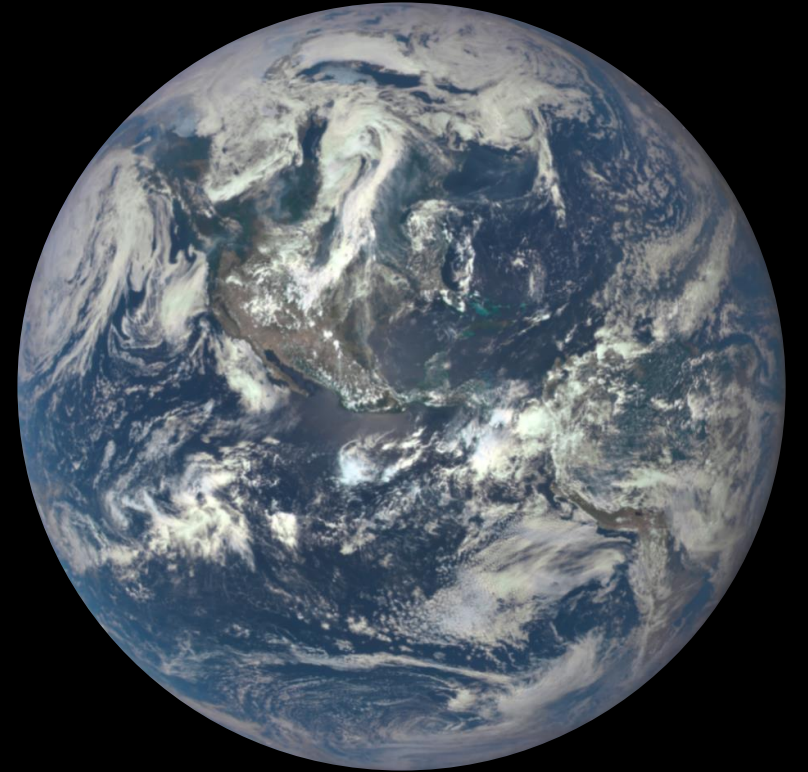
Microsoft &
The Insurance Sector

Insuring Against Cyber Threats – why it is difficult?

- Difficult to assess the baseline security risk of organisations seeking cybersecurity insurance

- Average time before an attacker is discovered is over 200 days, are you insuring a broken system?

Insuring Against Cyber Threats – where we want to help

- Difficult to assess the baseline security risk of organisations seeking cybersecurity insurance

- Infrastructure assessment, network & telemetry monitoring, analysis against the intelligent security graph

- Average time before an attacker is discovered is over 200 days, are you insuring a broken system?

- Dynamic monitoring & detection, threat analytics, real time alerting driven by powerful inference engine

Insuring Against Cyber Threats – why we think we can add value

- Enable you to make better decisions on assessing the risk profile of organisations seeking cybersecurity insurance

- By detecting & removing attackers quickly from networks before they can do real damage we can help reduce your exposure

- By helping you understand the security of reference architectures

- By potentially taking a share of the risk??

Is there an appetite for this type of partnership?

Questions

robert.hayes@microsoft.com