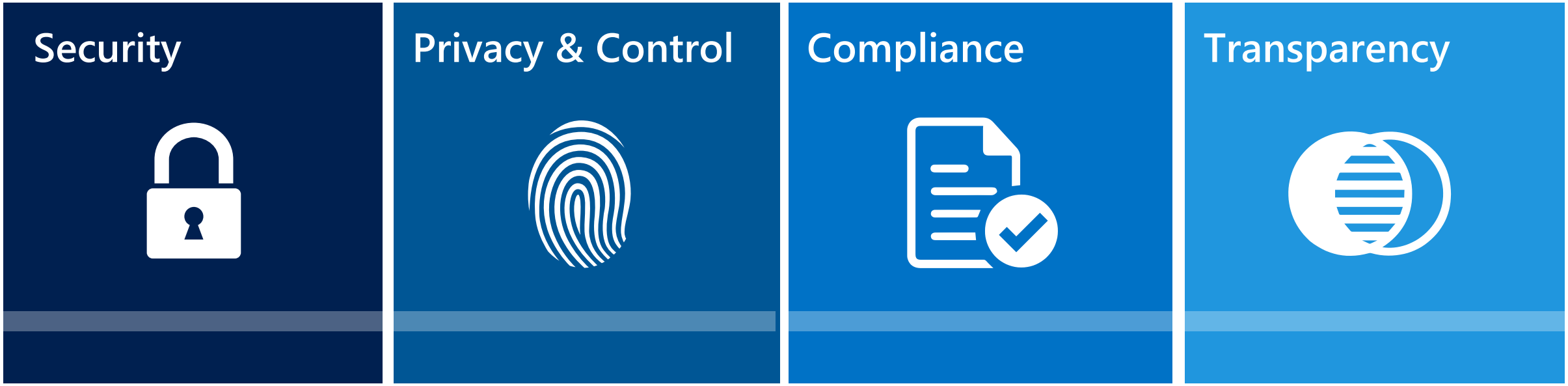
Microsoft

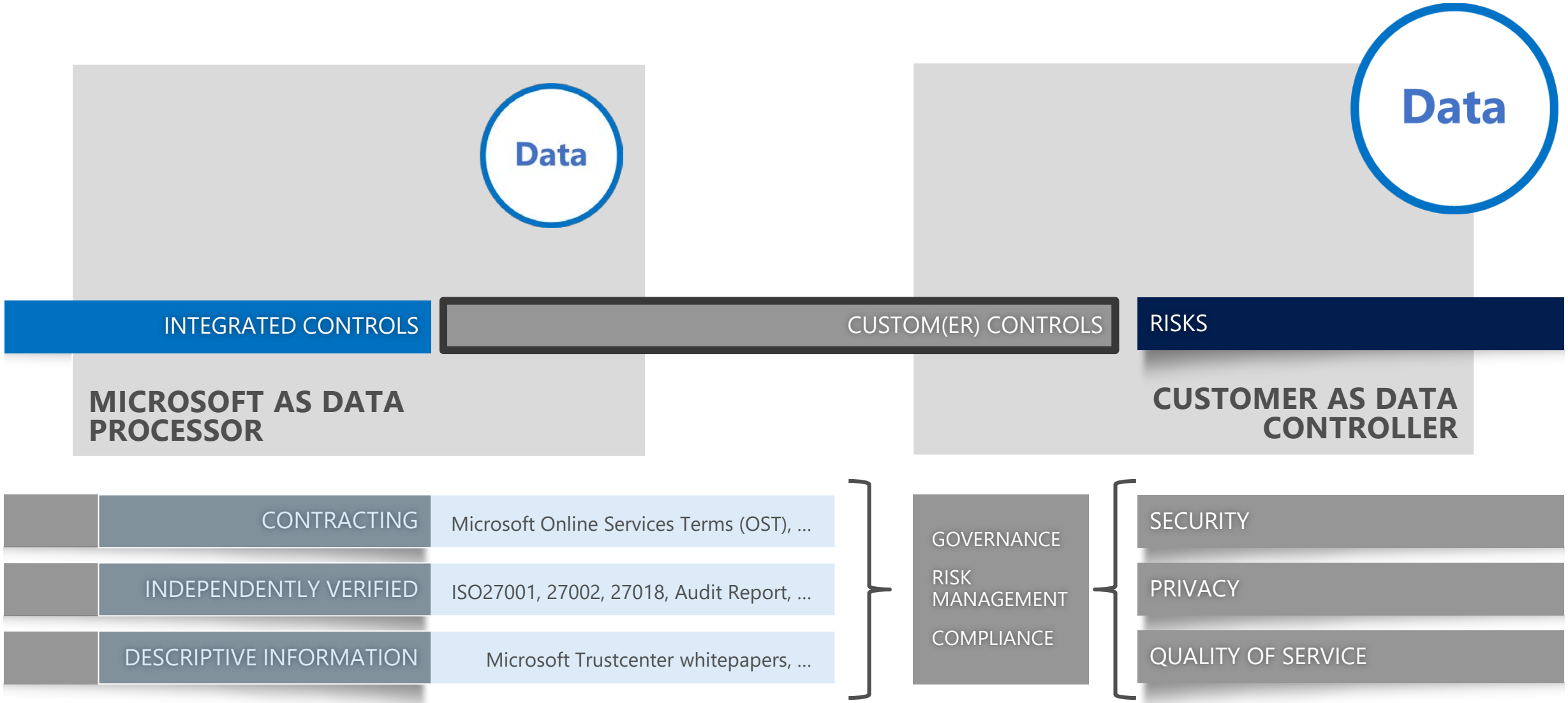
The Intelligent Security Graph

Marc Holitscher, CTO Microsoft Schweiz
Philipp Hunold, Lead Cybersecurity Specialist

Principled Approach to Trust



Integrated Control Framework



O365 Activity API

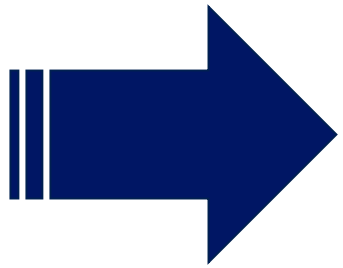
Data Center Security Cmdlet Schema

Parameters	Type	Mandatory?	Description
StartTime	Edm.Date	Yes	The start time of the cmdlet execution.
EffectiveOrganization	Edm.String	Yes	The name of the tenant that the elevati was targeted at.
ElevationTime	Edm.Date	Yes	The start time of the elevation.
ElevationApprover	Edm.String	Yes	The name of a Microsoft manager.
ElevationApprovedTime	Edm.Date	No	The timestamp for when the elevation v approved.
ElevationRequestId	Edm.Guid	Yes	A unique identifier for the elevation req
ElevationRole	Edm.String	No	The role the elevation was requested fo
ElevationDuration	Edm.Int32	Yes	The duration for which the elevation wa
GenericInfo	Edm.String	No	Used for comments and other generic

Enterprise Threat Landscape – Last 6 Months

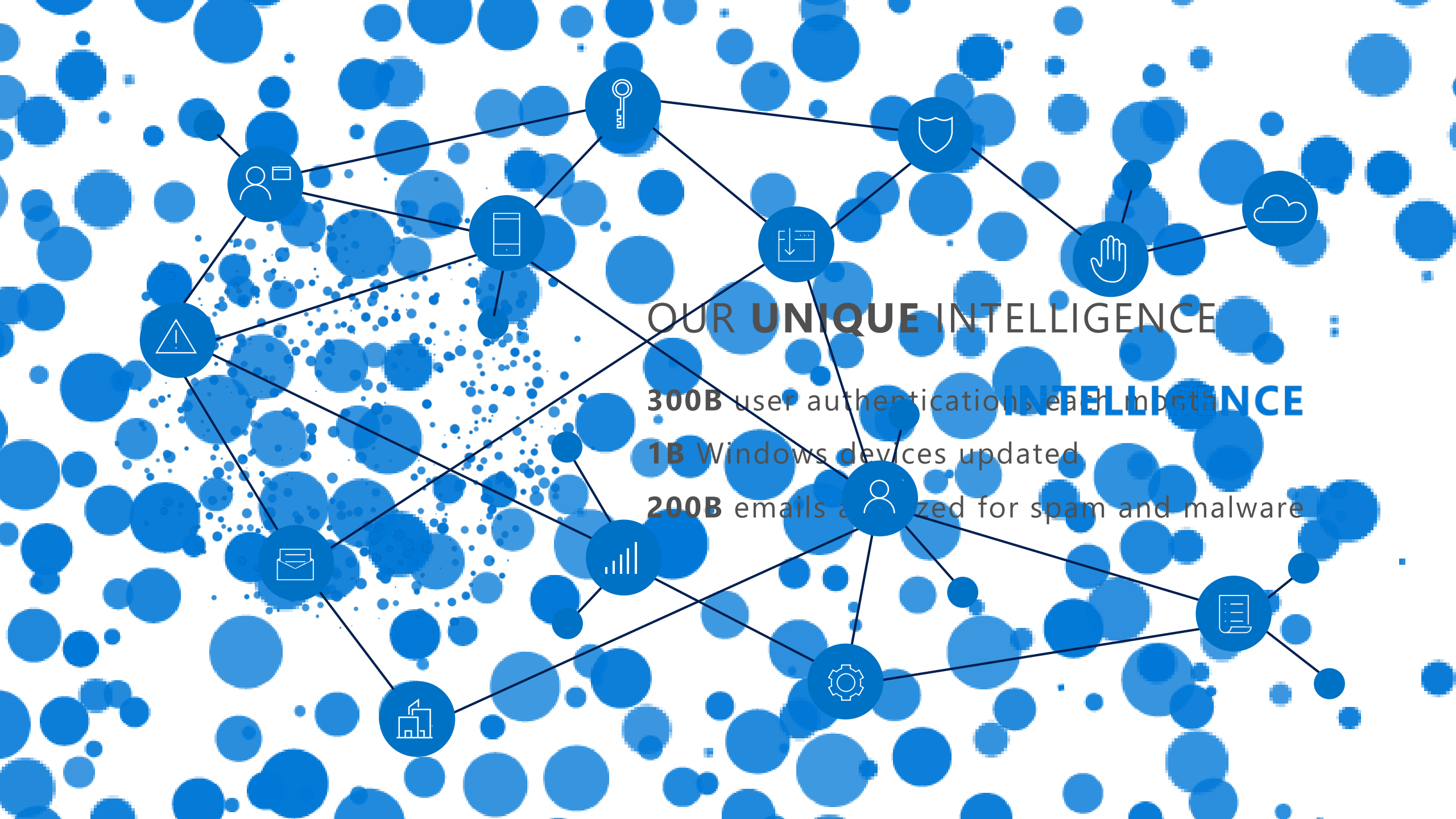
68 incidents across **8 different countries** responded to by the ECG Global Incident Response & Recovery Team

15,000 cases worked by the Cyber Defense Operations Center



85 – 90% of Incidents caused by:

1. Missing Patches for Critical Vulnerabilities
2. Excessive Use of Administrative Privileges
3. Lack of Credential Theft Mitigations



OUR **UNIQUE** INTELLIGENCE

300B user authentications each month

1B Windows devices updated

200B emails analyzed for spam and malware

INTELLIGENCE

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Legal and Corporate Affairs (LCA) Schweiz
Stand Dezember 2015

Wo werden Daten in der Microsoft Enterprise Cloud gespeichert?
Für schweizerische Kunden werden standardmässig die wesentlichen Kundendaten (Core Customer Data) der Microsoft Enterprise Services (Office 365, Microsoft Azure, CRM Online, Windows Intune) in den Microsoft Rechenzentren in Dublin und Amsterdam gespeichert. Microsoft verfolgt bei den Rechenzentren eine an den Regionen orientierte Strategie. Das Land oder die Region des Kunden, das oder die der Administrator bei der erstmaligen Einrichtung der Dienste eingibt, bestimmt den primären Speicherort für die Daten des Kunden. Weitere Informationen finden Sie hier: http://aka.ms/dataflowmap .

Die Anforderungen zur Bereitstellung der Dienste können im Einzelfall beinhalten, dass einige Daten Mitarbeitern bzw. Zulieferern von Microsoft ausserhalb der primären Speicherregion zugänglich gemacht werden. Darüber hinaus kann es vorkommen, dass sich die Mitarbeiter mit der meisten technischen Erfahrung für die Behandlung spezieller Dienstprobleme an anderen Standorten als am primären Standort befinden, und sie ggf. Zugriff auf Systeme oder Daten benötigen, um das Problem lösen zu können.

Inwiefern ist das Datenschutzrecht für Kunden von Microsoft Enterprise Cloud Services relevant?
Kunden dürfen Personendaten nur dann in der Cloud verarbeiten, wenn dafür eine rechtliche Erlaubnis besteht. Eine Erlaubnis ergibt sich bei Cloud Services in der Regel aus der sog. Auftragsdatenbeabeitung die Microsoft in seinen Verträgen abgebildet hat (siehe dazu nachstehend)

Das Datenschutzrecht gilt dabei nur für die Bearbeitung von Personendaten. Dies sind – verkürzt gesagt – Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen, wie beispielsweise Name/Firma einer Person oder deren E-Mail-Adresse. In der Praxis finden sich zumeist eine Vielzahl von Personendaten in der Microsoft Enterprise Cloud. Es gibt aber auch Fälle, in denen kaum oder keine Personendaten bearbeitet werden, beispielsweise wenn Designdaten eines Modeherstellers in Azure gespeichert werden.

Microsoft hat derzeit kein schweizerisches Rechenzentrum. Kann ein schweizerischer Kunde trotzdem datenschutzkonform Microsoft Enterprise Cloud Services nutzen?
Ja. Rechenzentren in EU-Ländern sind Rechenzentren in der Schweiz datenschutzrechtlich gleichgestellt, da diese Länder ein angemessenes Datenschutzniveau gewährleisten. Datenschutzrechtlich ist es also unerheblich, ob sich ein Rechenzentrum in der Schweiz oder der EU befindet. Ein Rechenzentrum in der Schweiz ist datenschutzrechtlich demnach nicht vorteilhafter als ein Rechenzentrum in der EU. Für den Teil der Services, die Microsoft von ausserhalb der EU erbringt, bietet Microsoft seinen Kunden die EU-Standardvertragsklauseln an. Diese begründen nach Ansicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (nachfolgend EDÖB) hierfür eine adäquate datenschutzrechtliche Lösung.


Microsoft