



# Microsoft Trust

Built on Compliance, Security, Privacy  
and Transparency

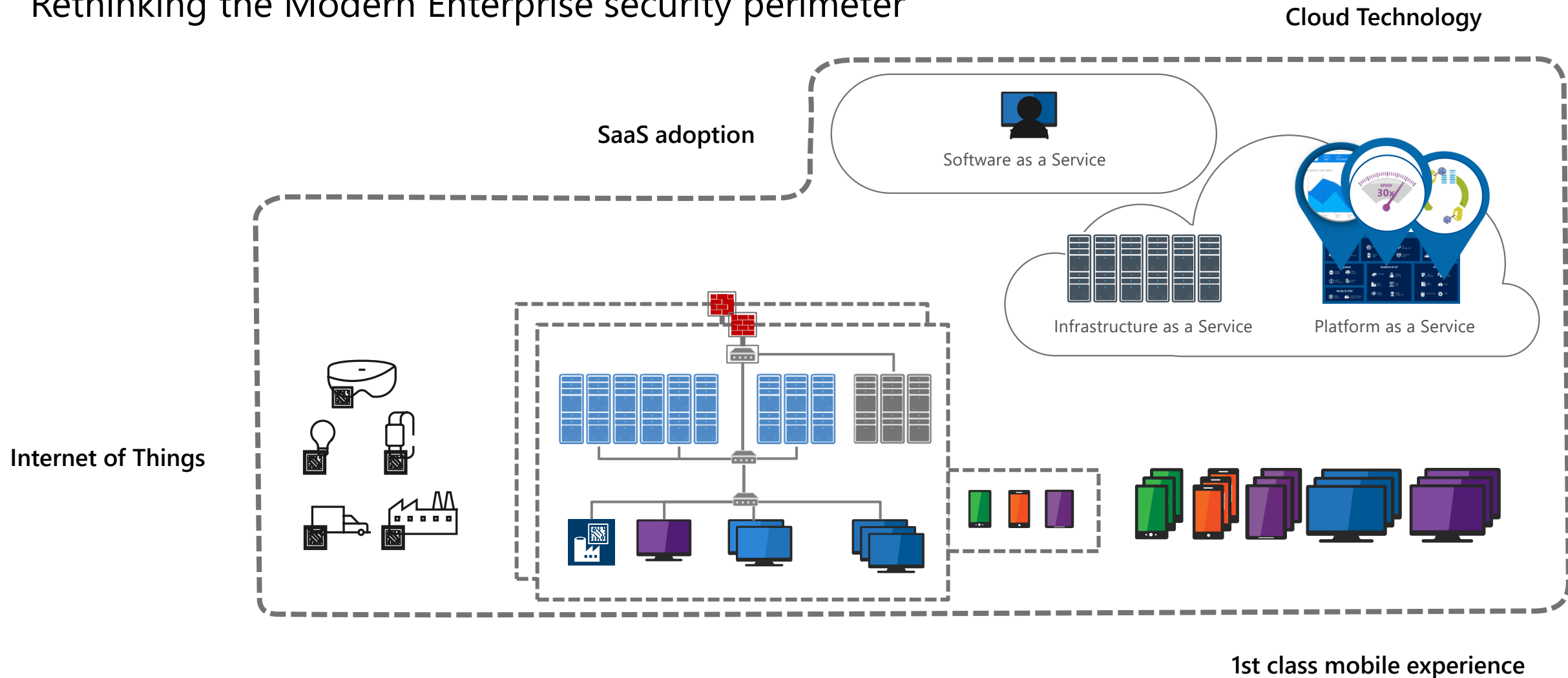


# Tech intensity

$$= (\text{Tech adoption} \times \text{Tech capability})^{\text{Trust}}$$

# Your organization in transformation

Rethinking the Modern Enterprise security perimeter



# Risk-based approach – opportunities and concerns





Microsoft Trust principles to guide your assessment



Compliance



Security



Privacy



Transparency

Bring it all together

# Compliance

“Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law and Data Protection Requirements.”(1)

We have a very comprehensive compliance coverage.

---

We can handle customers’ most sensitive data and help satisfy the needs of even the most stringent data protection regulations.

---

We are committed to sharing our experiences in complying with complex regulations.

---

We make resources available to help our customers along their Compliance journey.

(1) Microsoft Data Protection Addendum: <https://aka.ms/dpa>





## Global

- ✓ ISO 27001:2013
- ✓ ISO 27017:2015
- ✓ ISO 27018:2014
- ✓ ISO 22301:2012
- ✓ ISO 9001:2015
- ✓ ISO 20000-1:2011
- ✓ SOC 1 Type 2
- ✓ SOC 2 Type 2
- ✓ SOC 3
- ✓ CSA STAR Certification
- ✓ CSA STAR Attestation
- ✓ CSA STAR Self-Assessment
- ✓ WCAG 2.0 (ISO 40500:2012)
- ✓ ISO 27701:2019

**NEW!**

## US Gov

- ✓ FedRAMP High
- ✓ FedRAMP Moderate
- ✓ EAR
- ✓ DFARS
- ✓ DoD DISA SRG Level 5
- ✓ DoD DISA SRG Level 4
- ✓ DoD DISA SRG Level 2
- ✓ DoE 10 CFR Part 810
- ✓ NIST SP 800-171
- ✓ NIST CSF
- ✓ Section 508 VPATs
- ✓ FIPS 140-2
- ✓ ITAR
- ✓ CJIS
- ✓ IRS 1075

## Industry

- ✓ PCI DSS Level 1
- ✓ GLBA
- ✓ FFIEC
- ✓ Shared Assessments
- ✓ FISC (Japan)
- ✓ APRA (Australia)
- ✓ FCA (UK)
- ✓ MAS + ABS (Singapore)
- ✓ 23 NYCRR 500
- ✓ HIPAA BAA
- ✓ HITRUST

## Regional

- ✓ Argentina PDPA
- ✓ Australia IRAP Unclassified
- ✓ Australia IRAP PROTECTED
- ✓ Canada Privacy Laws
- ✓ China GB 18030:2005
- ✓ China DJCP (MLPS) Level 3
- ✓ China TRUCS / CCCPPF
- ✓ EN 301 549
- ✓ EU ENISA IAF
- ✓ EU Model Clauses
- ✓ EU – US Privacy Shield
- ✓ GDPR
- ✓ Germany C5
- ✓ Germany IT-Grundschutz workbook
- ✓ India MeitY
- ✓ Japan CS Mark Gold
- ✓ Japan My Number Act
- ✓ Netherlands BIR 2012
- ✓ New Zealand Gov CC Framework
- ✓ Singapore MTCS Level 3
- ✓ Spain ENS
- ✓ Spain DPA
- ✓ UK Cyber Essentials Plus
- ✓ UK G-Cloud
- ✓ UK PASF

## Industry

- ✓ 21 CFR Part 11 (GxP)
- ✓ MARS-E
- ✓ NHS IG Toolkit (UK)
- ✓ NEN 7510:2011 (Netherlands)
- ✓ FERPA
- ✓ CDSA
- ✓ MPAA
- ✓ DPP (UK)
- ✓ FACT (UK)
- ✓ SOX

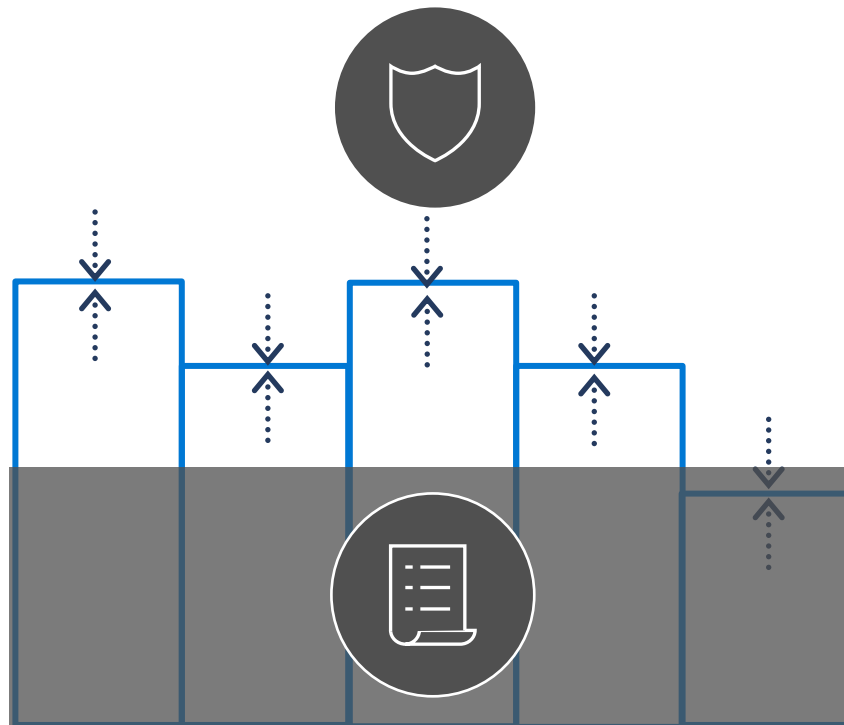
# Compliance Standards certification

Complete and actual overview can be found here:

<https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>

# Compliance ≠ Security

---



## Compliance

Meets a specific standard or regulation at a point in time



## Security

Lowers business risk to acceptable level



# Security

We will help you protect your data

We develop, implement & maintain a very comprehensive security posture.

---

We have a large, dedicated workforce of security professionals to secure datacenters and hunt down attackers based on our unique insights into the threat environment.

---

2.5 billion daily cloud-based detections blocked almost 6 billion threats on endpoints in 2020.

---

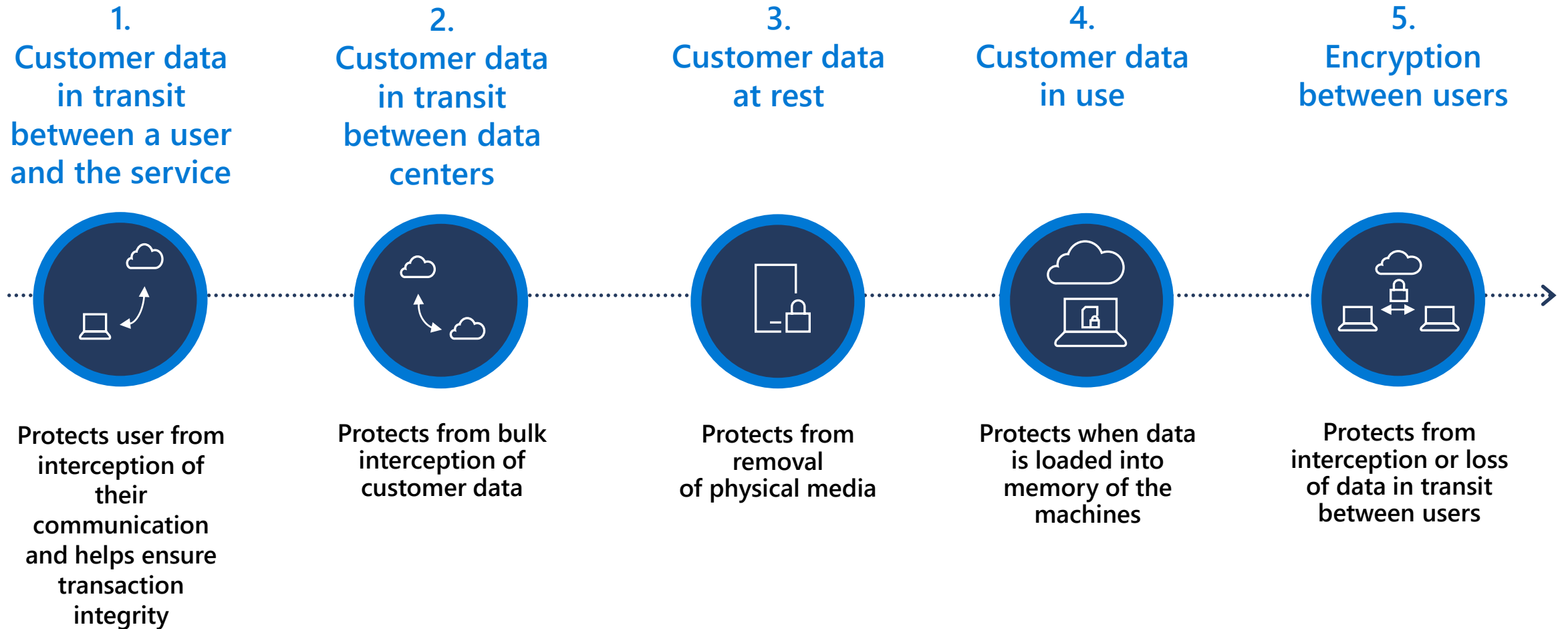
More than 30 billion email threats were blocked in 2020.

---

We continuously develop & provide customers innovative security controls, to ensure optimal resilience.



# Security – Data encryption



Microsoft controlled encryption:  
<https://aka.ms/msazureencryption>  
<https://aka.ms/o365contentencryption>

Customer controlled encryption:  
<https://aka.ms/msazureprotection>  
<https://aka.ms/mscloudCMkryptering>

Double Key Encryption:  
<https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption?view=o365-worldwide>

# Privacy differs from Security

Protecting Personal data

## Security controls

Robust access control management, data classification and data encryption

---

## Laws and regulations

Getting privacy right starts with abiding the law

---

## Customer contracts or agreements

Understanding the agreements made to commercial customers

---

## Individual expectations

What is the product/service needed and how will Personal Data be used

# Microsoft privacy principles

You control your data



You choose where your data is located



Microsoft secures your data at rest and in transit



Microsoft defends your data





# Our commitments to commercial customers

---

## Controlled by you

We commit to strong privacy protections through greater user control and transparency

## No data profiling

We will not share or use your data for marketing, advertising, or other commercial purposes

## Strong legal protection

We do not provide governments with "back doors," encryption keys, or assistance to break encryption


## GDPR for all customers

We extend GDPR data protection rights to all customers worldwide, not just in Europe

## Listening to customers

We actively collaborate with customers and regulators to foresee and shape compliance regulations

These commitments are backed by our contractual agreements that govern how we process data and protect data privacy for commercial customers. [Learn more.](#)



While **privacy** is about appropriate collection and use of data, **transparency** is all about providing visibility to what happens with your data.

# Transparency

We are transparent about our processes and the use and the protection of customer data

We provide information about the geographic locations where customer data is stored.

---

We publish the number of legal demands for customer data that we receive from law enforcement agencies.

---

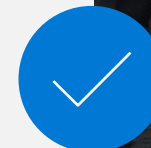
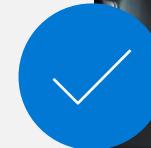
We provide visibility into what we do with customer data, how we protect it, and how they are in control.

---

We collaborate with National Cyber Security entities around the globe to provide them insights into our platform, source code, and processes

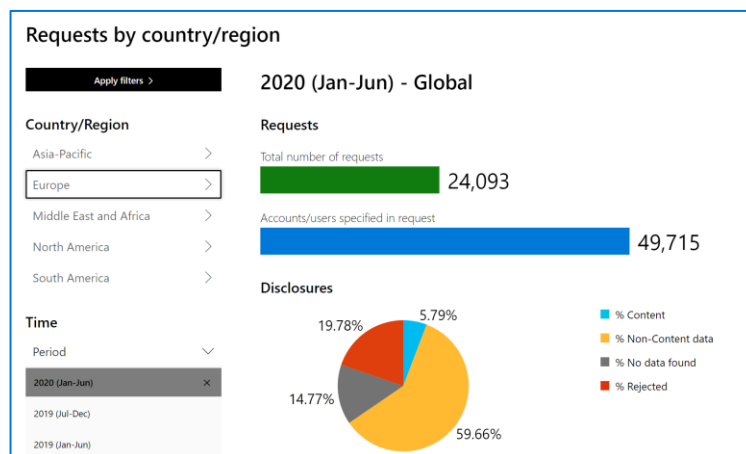
---

We provide customers with the tools necessary to gain real-time insights into how their data is used and accessed and how they can remain in control.



# Government requests for customer data

We contractually commit that we do not provide any government with direct, unfettered access to Customer Data. If a government demands Customer Data from us, it must follow applicable legal process. Additional contractual commitments to defend Customer data: [new steps to defend your data](#)



Microsoft information about government demands for Customer Data: <https://aka.ms/MSLERR>

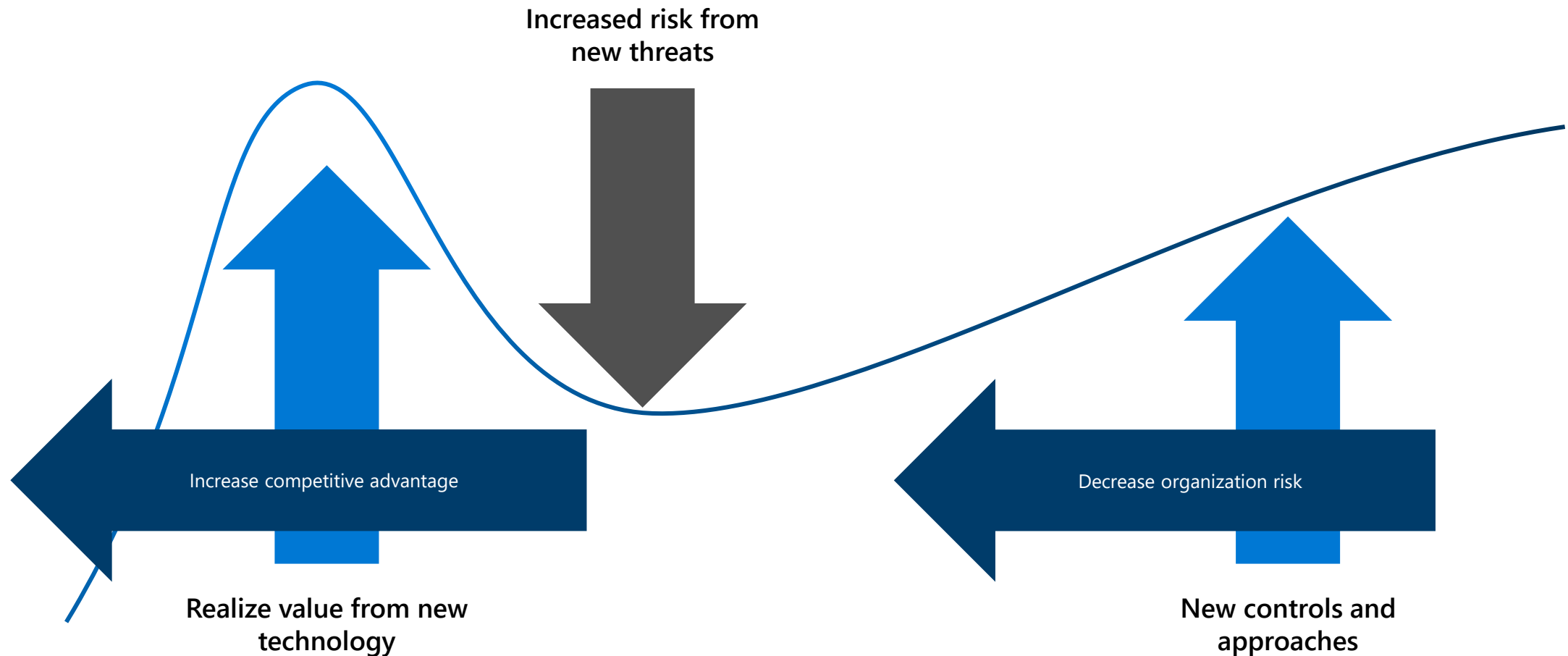
- Jan-Jun 2020: 24093 requests, 91 for accounts associated with enterprise cloud customers
- 42 cases rejected, withdrawn or redirected; 49 compelled to provide information
- In 25 cases non-content was disclosed, 24 involved some customer content
- Of the 24 instances, 20 associated U.S. law enforcement, **2 warrants** concerned content data stored outside the U.S.



# Three Major Forces in Digital Transformation

---

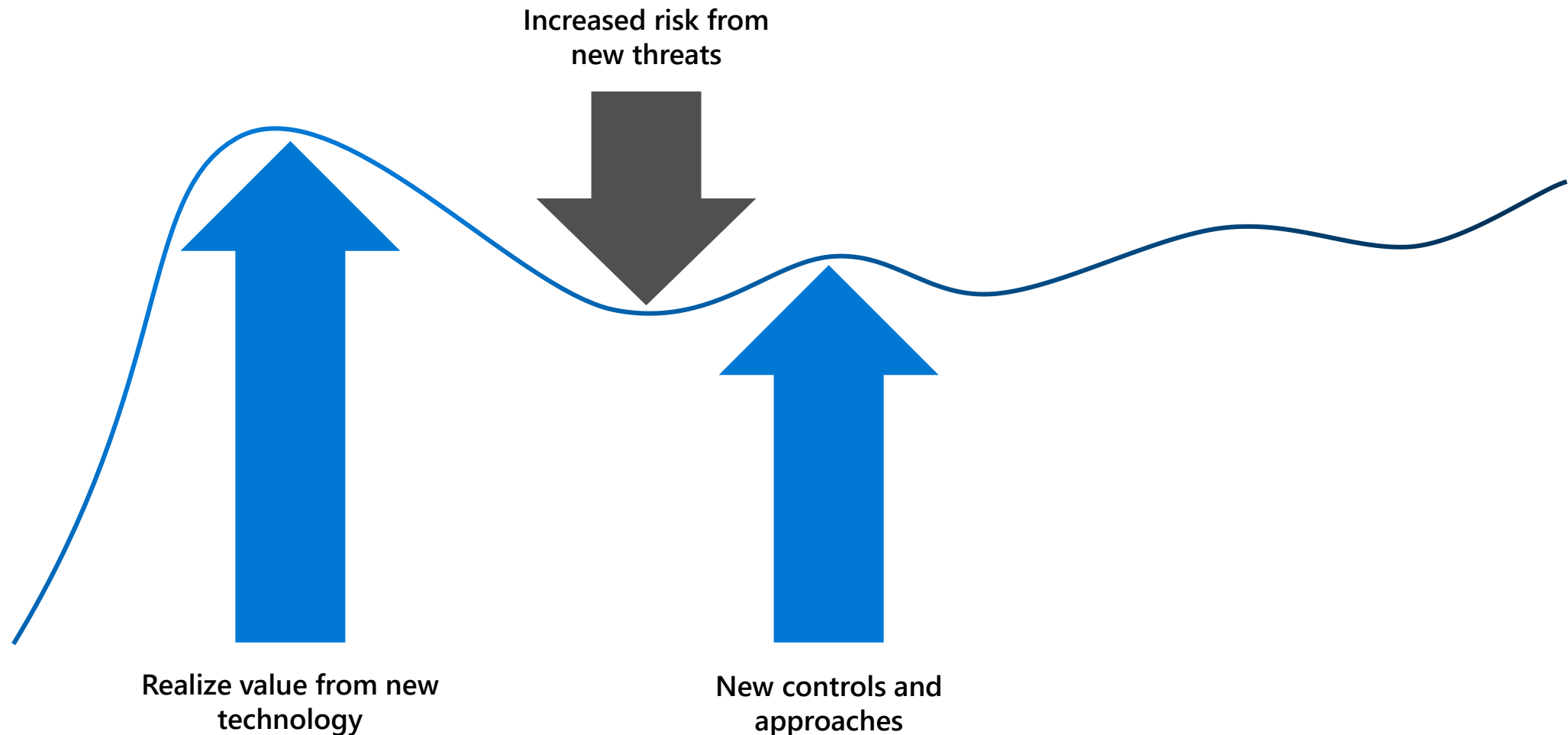
Adoption Speed impacts Benefit/Risk curve



# Three Major Forces in Digital Transformation

---

Adoption Speed impacts Benefit/Risk curve



# Risk-based approach – opportunities and concerns





Thank you

