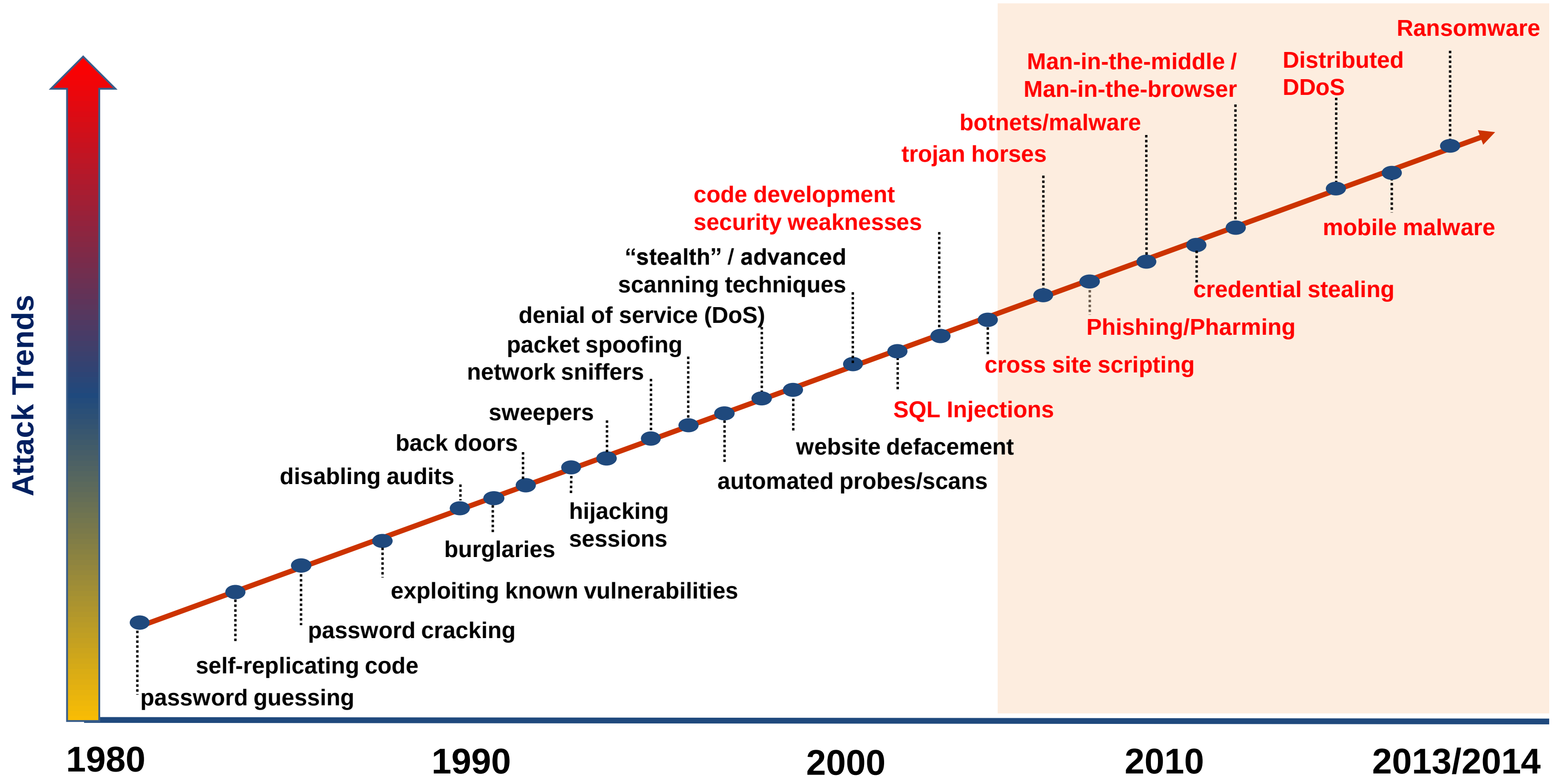
Cybersecurity Threats and Trends



Threats:

- Malware shows no sign of changing its steady growth, which has risen steeply since 2012.
- Financial Institutions are the most targeted, suffering 80% of all malware attacks.
- The trend moving forward shows increase sophistication in the mode of attack and the persistence of fraudsters.
- Mobile platforms represent a major growth area for vulnerabilities, as well as malware attacks.

Cybersecurity Regulatory Compliance outlook

- Cybersecurity Assessments
  - Type
  - Mitigating Controls
  - Effectiveness of the controls
  - Residual risk

- Vendor Risk Assessments
  - Critical services
  - Outsourcing (i.e. SaaS, IaaS, etc.)
  - Legal
  - Information Security
  - Operational Risk
  - Financial

- Incident Response
  - Develop ant test your IR Plan
  - Emergency response services (Know who to call)
  - Forensic analysis
  - Escalation procedures
  - Notification to the regulator (State, Fed, OCC, etc.)
  - Notification to law enforcement

Take Away

- Do your Part:
  - Be proactive
  - Identify and manage risks
  - Apply defense-in-depth measures
  - Ensure your vendors have the required controls in place to safeguard YOUR Bank's information - **Trust but verify**
  - Establish a culture of security
  - Join an Information Sharing support group

Be Aware - Anticipate - Adapt

Security, Compliance and Privacy in the Cloud

…Founded on Transparency and Trust

Rochelle M. Eichner, Director, Risk & Compliance
Microsoft Corporation – rochelle@microsoft.com

Microsoft

Trust considerations

Is cloud computing secure?
Where is my data and do I have access?

security

How do you support
my compliance needs?

compliance

What does privacy mean?
Is my data used for advertising?

privacy

– Forbes, 2013

Microsoft Core Values

Security

Compliance

Privacy

privacy

security

Trustworthy Computing

business practices

reliability

Office 365 Trust

Security

Best-in-class security with over a decade of experience building Enterprise software & Online services

- Physical and data security with access control, encryption and strong authentication
- Security best practices like penetration testing, Defense-in-depth to protect against cyber-threats
- Unique customer controls with Rights Management Services to empower customers to protect information

Compliance

Commitment to industry standards and organizational compliance

- Enable customers to meet global compliance standards in ISO 27001, EUMC, HIPAA, FISMA
- Contractually commit to privacy, security and handling of customer data through Data Processing Agreements
- Admin Controls like Data Loss Prevention, Legal Hold, E-Discovery to enable organizational compliance

Privacy

Privacy by design with complete separation of Enterprise and Consumer services

- No mining of data for advertising
- Transparency with the location of customer data, who has access and under what circumstances
- Customer have greater control over privacy to enable or regulate sharing based on organizational needs

Security

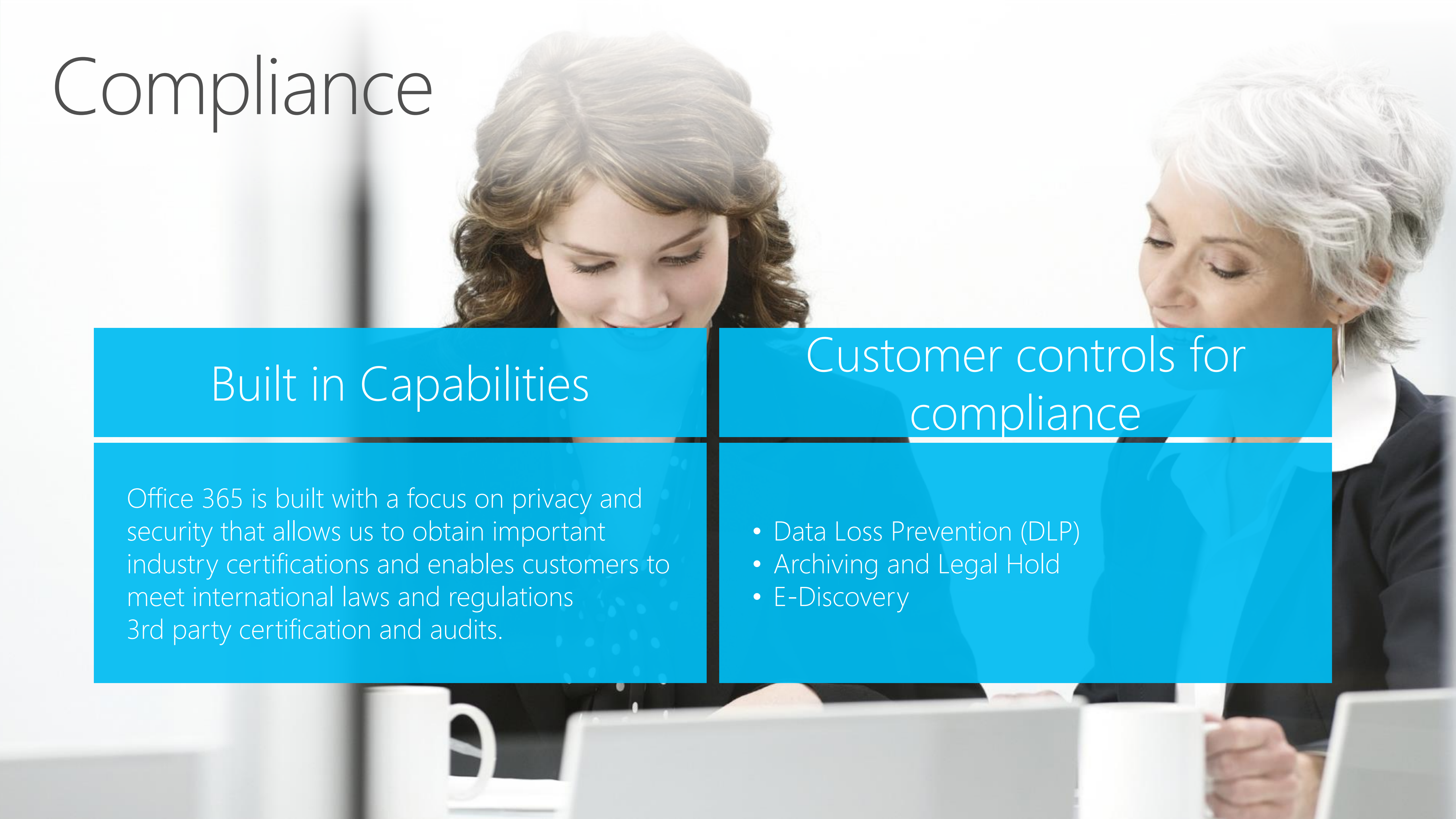
Built in Capabilities

Security best practices like penetration testing, Defense-in-depth to protect against cyber-threats

Flexible Customer Controls

- Physical and data security with access control, encryption and strong authentication
- Unique customer controls with Rights Management Services to empower customers to protect information

Compliance



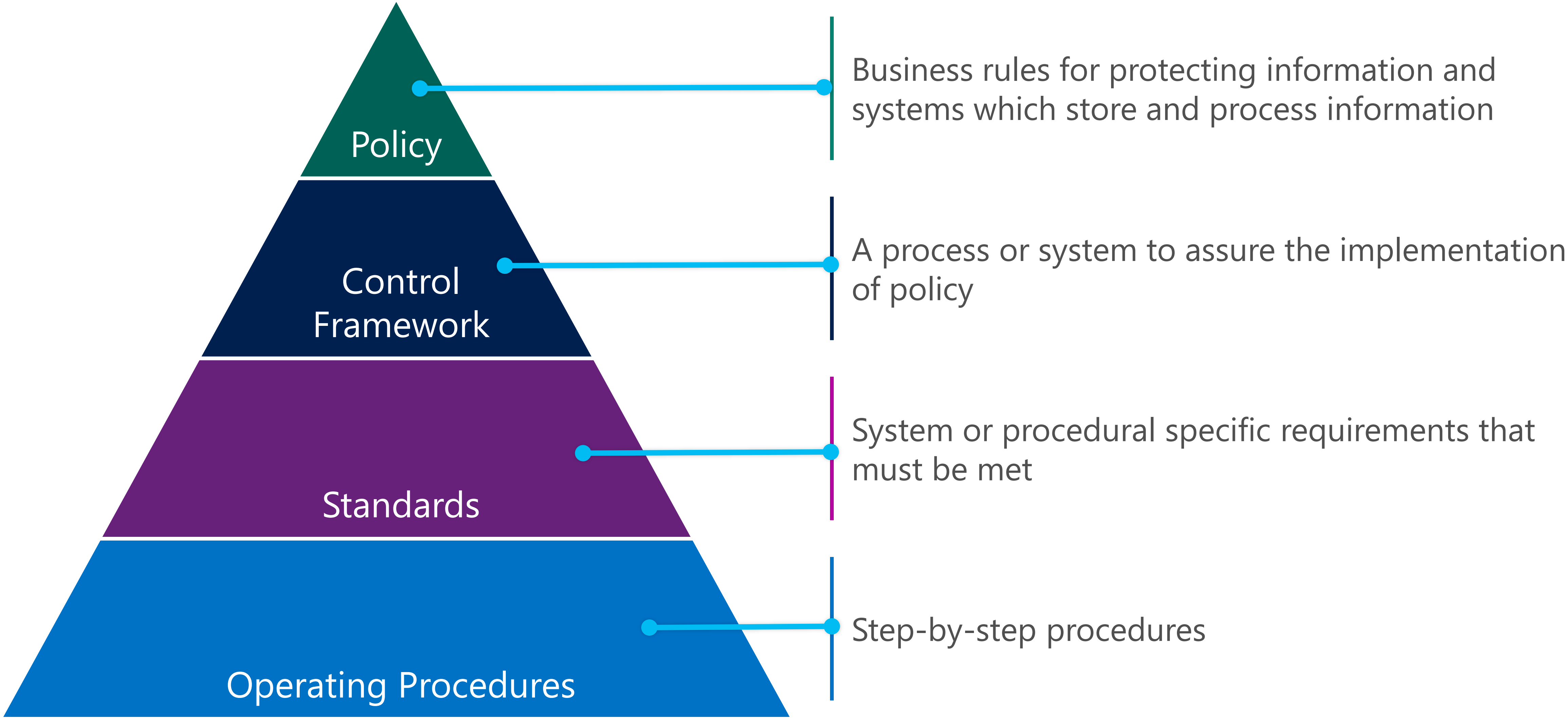
Built in Capabilities

Office 365 is built with a focus on privacy and security that allows us to obtain important industry certifications and enables customers to meet international laws and regulations
3rd party certification and audits.

Customer controls for compliance

- Data Loss Prevention (DLP)
- Archiving and Legal Hold
- E-Discovery

Compliance Management Framework



Policy

Business rules for protecting information and systems which store and process information

Control Framework

A process or system to assure the implementation of policy

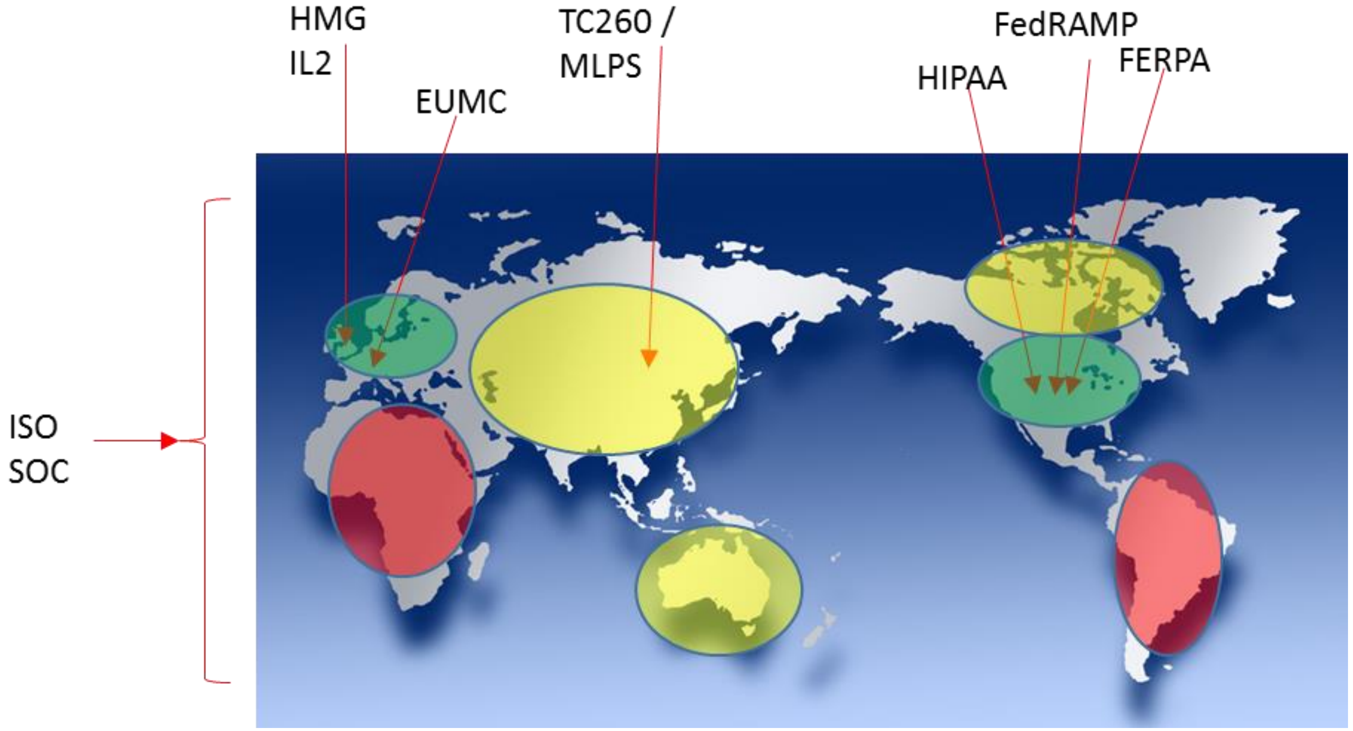
Standards

System or procedural specific requirements that must be met

Operating Procedures

Step-by-step procedures

Certifications Open New Markets



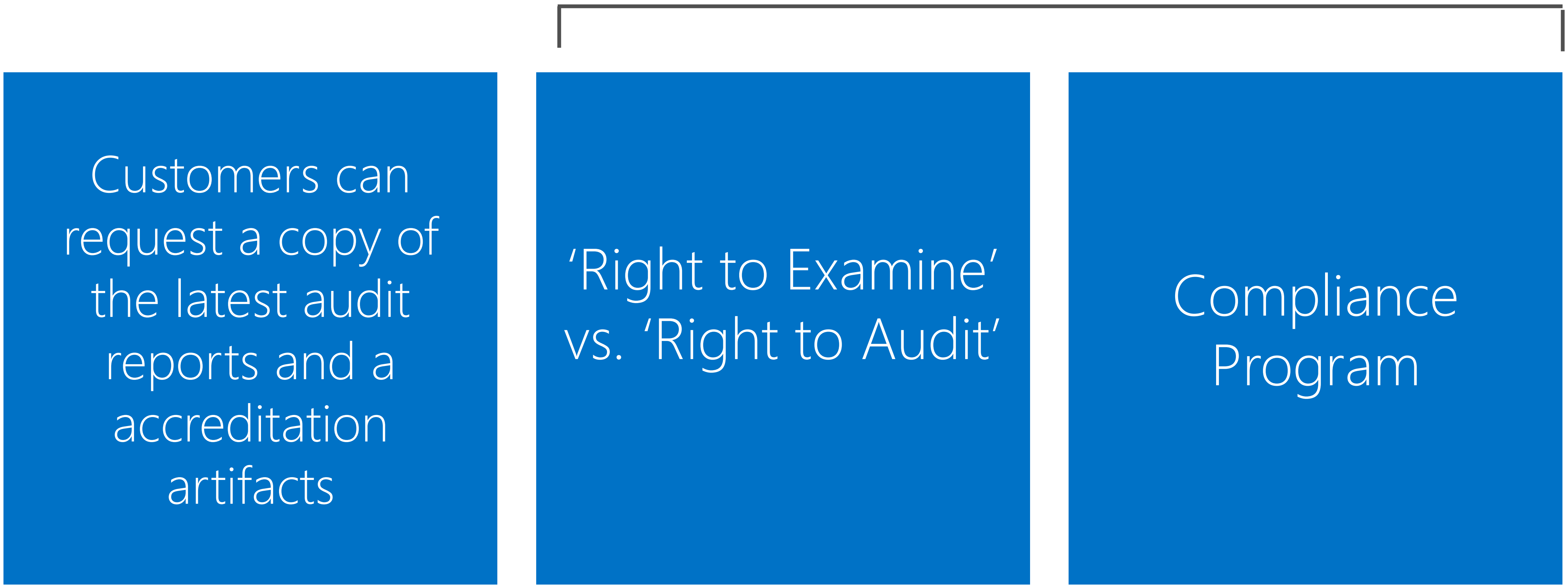
Certification Status

CERT	MARKET	REGION
SSAE/SOC	Finance	Global
ISO27001	Global	Global
EUMC	Europe	Europe
FERPA	Education	U.S.
FISMA	Government	U.S.
PCI	CardData	Global
HIPAA	Healthcare	U.S.
HITECH	Healthcare	U.S.
ITAR	Defense	U.S.
HMG IL2	Government	UK
CJIS	Law Enforcement	U.S.

Queued or In Progress

FFIEC	Finance	U.S.	FISC	Japan-Finance	U.S.
IRS 1075	Tax/Payroll	U.S.	CNSS1253	Military	U.S.

Audit Reports



Specific to Financial Institutions: regulatory requirement

Customers can request a copy of the latest audit reports and a accreditation artifacts

‘Right to Examine’ vs. ‘Right to Audit’

Compliance Program

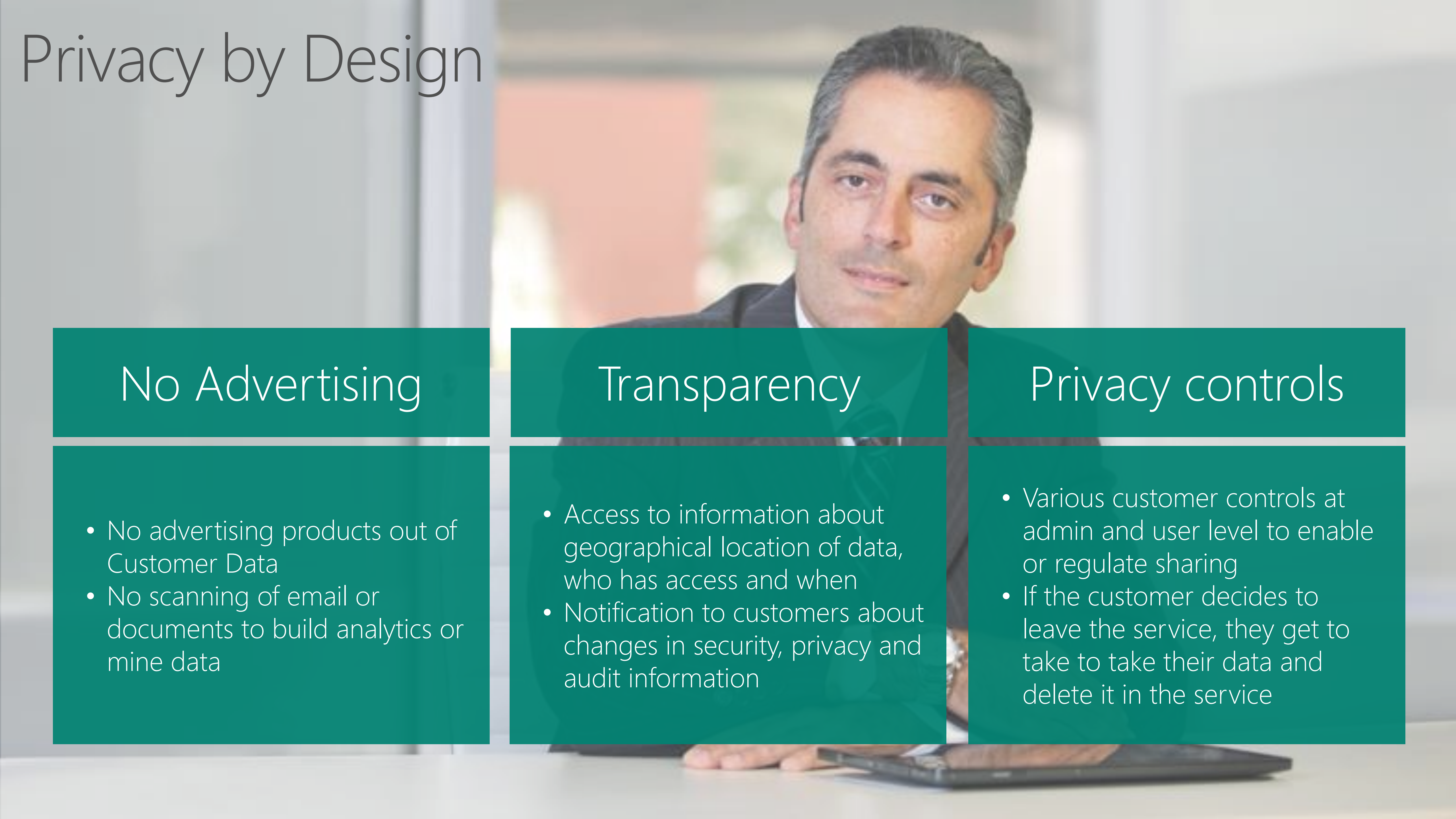
* Country Specific Regulatory Compliance Sheets map regulatory requirements to service features – Argentina, Brazil, Columbia, Chile, DR, Ecuador, Mexico, Panama, Paraguay, Peru, Venezuela, Guatemala, El Salvador, Costa Rica

Enabling Compliance

Email archiving and retention, data loss prevention

Preserve					Search
Auditing and retention policies	In-Place Archive	Governance	Hold	Data Loss Prevention	eDiscovery
Log events, view, edit, delete email messages, documents, task lists, issues lists, discussion groups, and calendars. View audit data, and report and summarize current usage	Secondary mailbox with separate quota Managed through EAC or PowerShell Available on-premises, online, or through EOA	Automated and time-based criteria Set policies at item or folder level Expiration date shown in email message	Capture deleted and edited email messages Time-Based In-Place Hold Granular Query-Based In-Place Hold Optional notification	Identify, monitor, and protect sensitive data Proactively identifies sensitive information and alerts users via “PolicyTips” Customize the level of restrictions	Web-based eDiscovery Center and multi-mailbox search Search primary, In-Place Archive, and recoverable items Delegate through roles-based administration De-duplication after discovery Auditing to ensure controls are met

Privacy by Design



No Advertising

- No advertising products out of Customer Data
- No scanning of email or documents to build analytics or mine data

Transparency

- Access to information about geographical location of data, who has access and when
- Notification to customers about changes in security, privacy and audit information

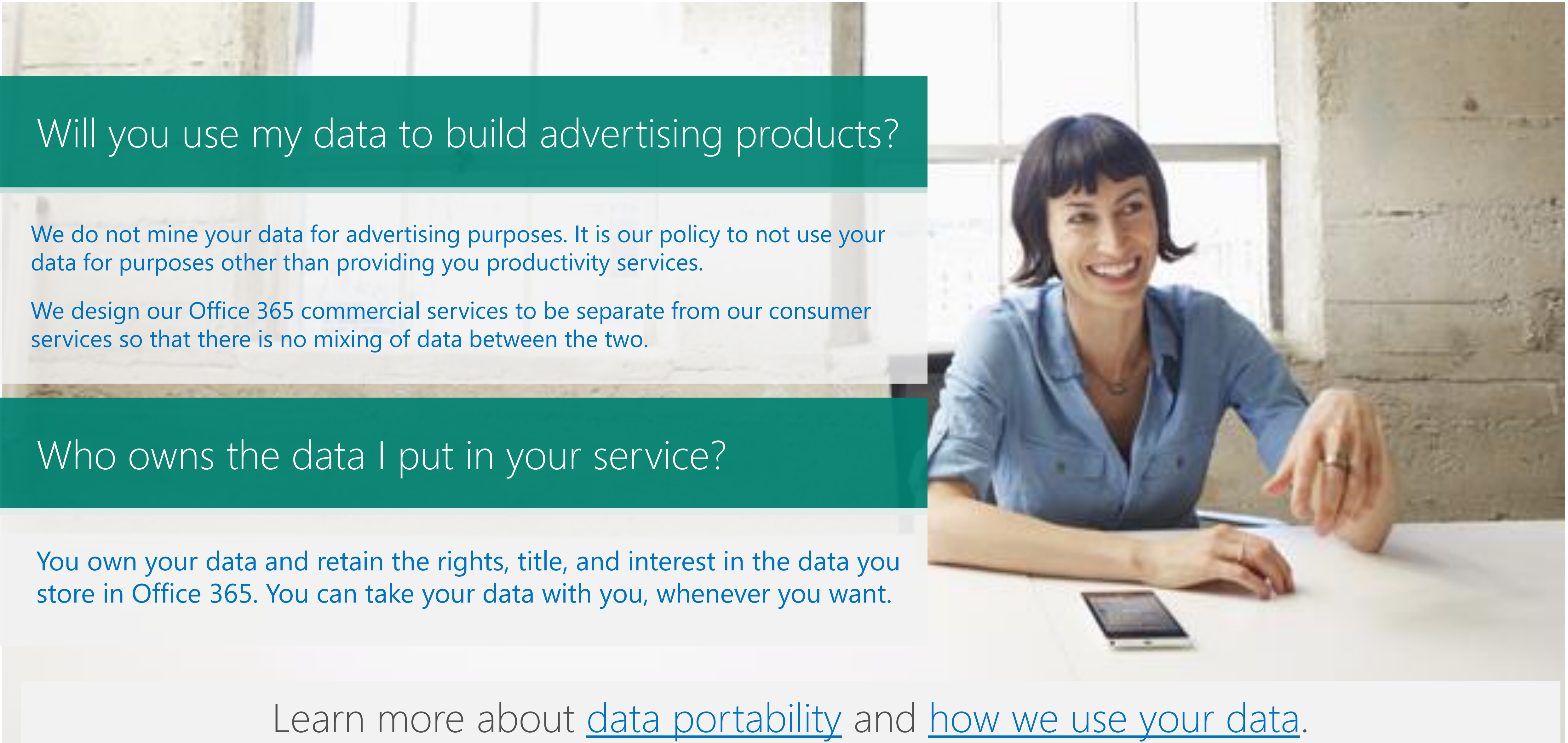
Privacy controls

- Various customer controls at admin and user level to enable or regulate sharing
- If the customer decides to leave the service, they get to take to take their data and delete it in the service

Data Sovereignty

- Microsoft will not disclose Customer Data to law enforcement unless required by law.
- Microsoft will attempt to redirect law enforcement to request data directly from Customer.
- Microsoft will notify Customer and provide a copy of the demand unless legally prohibited from doing so.
- Microsoft will continue to challenge government demands to shape the limits of the law.

No Advertising



Will you use my data to build advertising products?

We do not mine your data for advertising purposes. It is our policy to not use your data for purposes other than providing you productivity services.

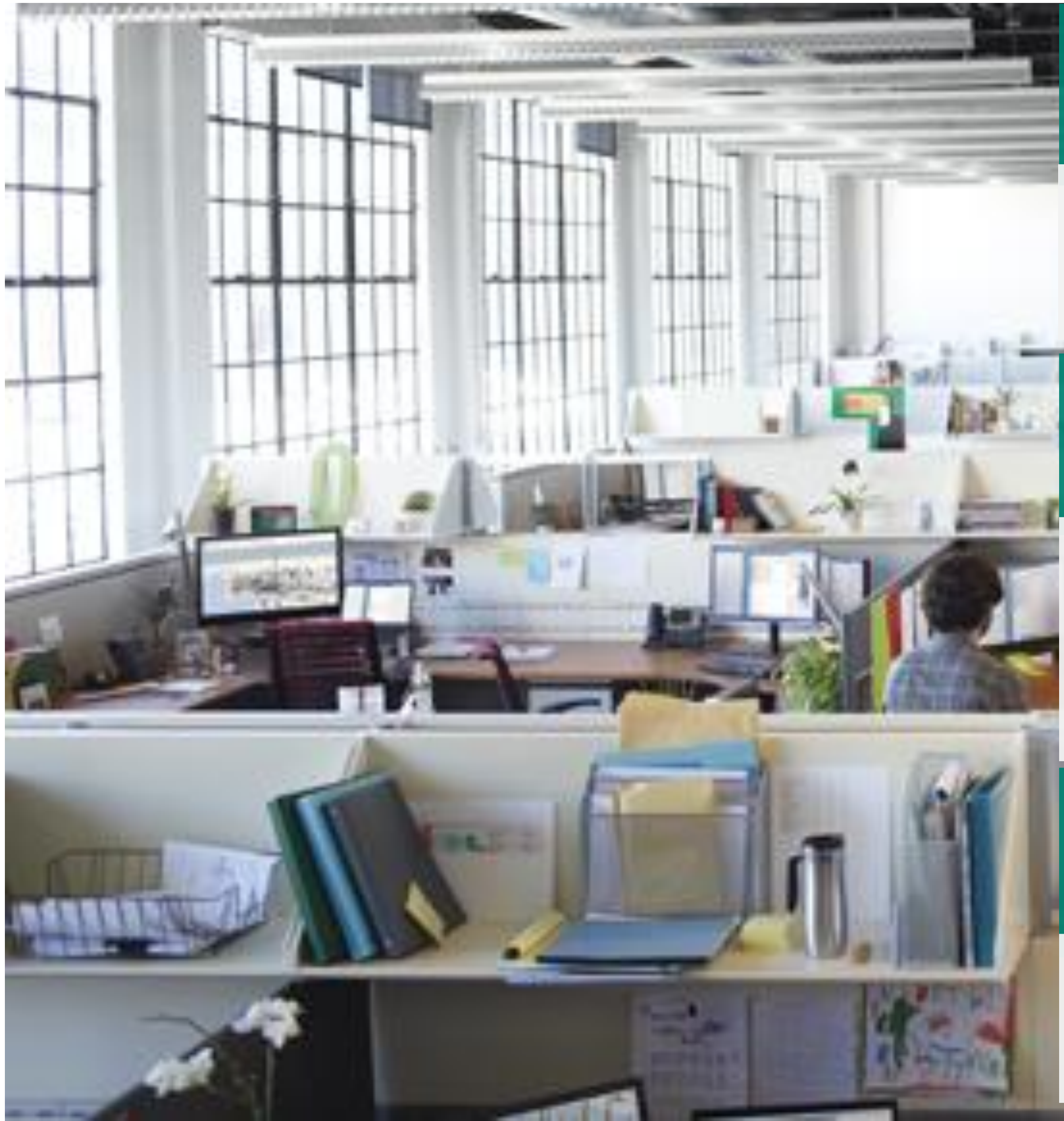
We design our Office 365 commercial services to be separate from our consumer services so that there is no mixing of data between the two.

Who owns the data I put in your service?

You own your data and retain the rights, title, and interest in the data you store in Office 365. You can take your data with you, whenever you want.

Learn more about [data portability]() and [how we use your data]().

Transparency



Where is Data Stored?

Clear Data Maps and Geographic boundary information provided
'Ship To' address determines Data Center Location

Who accesses and what is accessed?

Core Customer Data accessed only for troubleshooting and malware prevention purposes .
Core Customer Data access is limited to key personnel on an exception basis only.

Do I get notified?

Microsoft notifies you of changes in data center locations.

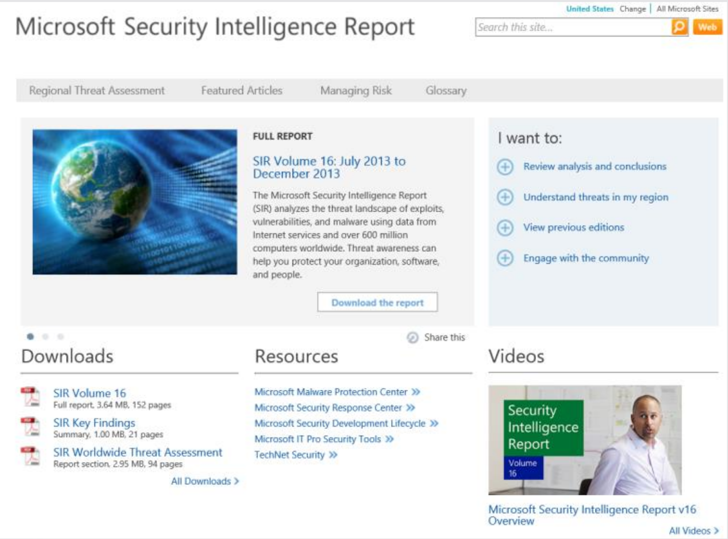
The Microsoft Difference in Operational Control

- **No persistent Administrative Accounts**
  - Admin access accounts are created to address specific support incidents and then retired.
  - Admin access is not to global infrastructure but to specific sections required for support.
  - Admin access is given a TTL (Time to Live) for the support exercise to be completed then retired.

- **Segmented Logical / Physical Access**
  - No single individual has both logical and physical access to cloud infrastructure.
  - Logical access is ONLY via the NOC which is purposefully off premises to physical infrastructure.
  - Physical access is ONLY via cleared DC personal with no logical console access to infrastructure.

- **Ongoing Red / Blue Team Exercises**
  - Microsoft Red Teams are challenged to expose vulnerabilities to platform on quarterly basis.
  - Microsoft Blue Teams are challenged to deliver vulnerability response programs based on findings.
  - Microsoft Red / Blue team methodologies are audited and overseen by 3rd party.

Microsoft’s Commitment to Transparency, Compliance & Security



Microsoft Security Intelligence Report

FULL REPORT

SIR Volume 16: July 2013 to December 2013

The Microsoft Security Intelligence Report (SIR) analyzes the threat landscape of exploits, vulnerabilities, and malware using data from Internet services and over 600 million computers worldwide. Threat awareness can help you protect your organization, software, and people.

I want to:

- Review analysis and conclusions
- Understand threats in my region
- View previous editions
- Engage with the community

Downloads

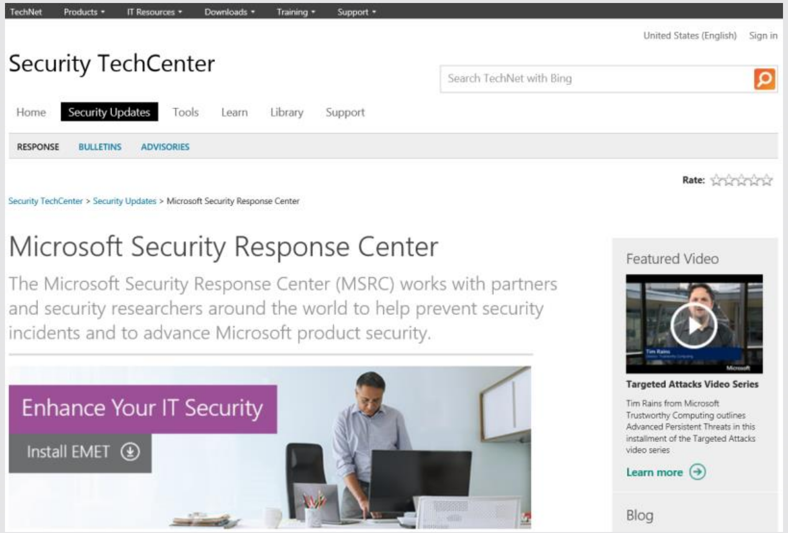
- SIR Volume 16 – Full report, 3.64 MB, 152 pages
- SIR Key Findings – Summary, 1.00 MB, 21 pages
- SIR Worldwide Threat Assessment – Report section, 2.95 MB, 94 pages

Resources

- Microsoft Malware Protection Center »
- Microsoft Security Response Center »
- Microsoft Security Development Lifecycle »
- Microsoft IT Pro Security Tools »
- TechNet Security »

Videos

Microsoft Security Intelligence Report v16 Overview



Security TechCenter

Security TechCenter > Security Updates > Microsoft Security Response Center

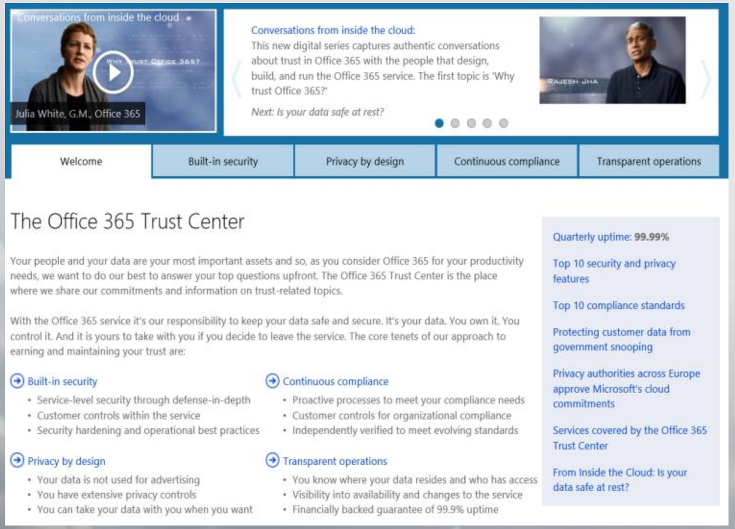
Microsoft Security Response Center

The Microsoft Security Response Center (MSRC) works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.

Featured Video

Targeted Attacks Video Series

Tim Rains from Microsoft Trustworthy Computing outlines Advanced Persistent Threats in this installment of the Targeted Attacks video series



Conversations from inside the cloud: This new digital series captures authentic conversations about trust in Office 365 with the people that design, build, and run the Office 365 service. The first topic is 'Why trust Office 365?'

Next: Is your data safe at rest?

The Office 365 Trust Center

Your people and your data are your most important assets and so, as you consider Office 365 for your productivity needs, we want to do our best to answer your top questions upfront. The Office 365 Trust Center is the place where we share our commitments and information on trust-related topics.

With the Office 365 service it's our responsibility to keep your data safe and secure. It's your data. You own it. You control it. And it is yours to take with you if you decide to leave the service. The core tenets of our approach to earning and maintaining your trust are:

Built-in security

- Service-level security through defense-in-depth
- Customer controls within the service
- Security hardening and operational best practices

Privacy by design

- Your data is not used for advertising
- You have extensive privacy controls
- You can take your data with you when you want

Continuous compliance

- Proactive processes to meet your compliance needs
- Customer controls for organizational compliance
- Independently verified to meet evolving standards

Transparent operations

- You know where your data resides and who has access
- Visibility into availability and changes to the service
- Financially backed guarantee of 99.9% uptime

Quarterly uptime: **99.99%**

Top 10 security and privacy features

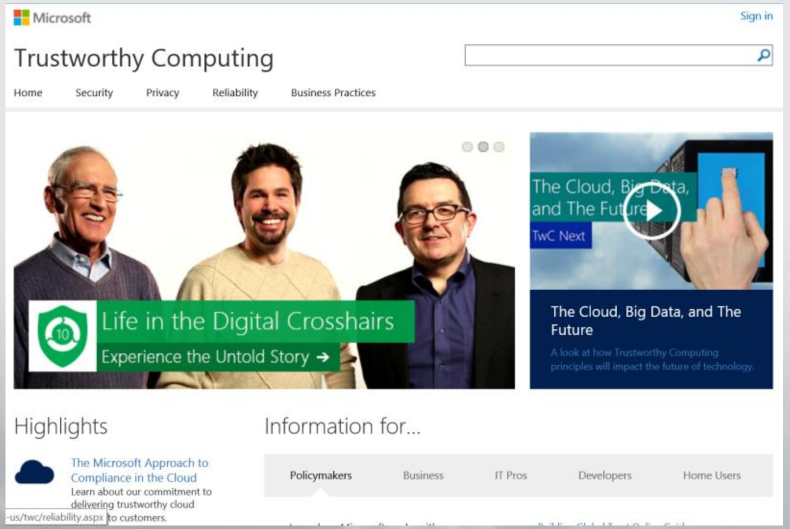
Top 10 compliance standards

Protecting customer data from government snooping

Privacy authorities across Europe approve Microsoft's cloud commitments

Services covered by the Office 365 Trust Center

From Inside the Cloud: Is your data safe at rest?



Trustworthy Computing

The Cloud, Big Data, and The Future

A look at how Trustworthy Computing principles will impact the future of technology.

Highlights

The Microsoft Approach to Compliance in the Cloud

Learn about our commitment to delivering trustworthy cloud to customers.

Information for...

- Websites committed to educating Microsoft customers on relevant regional and global security issues.
- Security Intelligence Reports summarizing recent security and compliance events.
- MSRC provides Microsoft Customers a glance into the ongoing efforts to provide our customers the most secure, compliant products and service.
- The Trust Center is the “one stop shop” for all things compliance related to Microsoft Cloud technologies.
- Ongoing audit results by our internal and third party auditors are posted here for customer review.

Office 365

Microsoft