Office 365 Security, Privacy and Compliance

Robert Crane

http://about.me/ciaops

Agenda

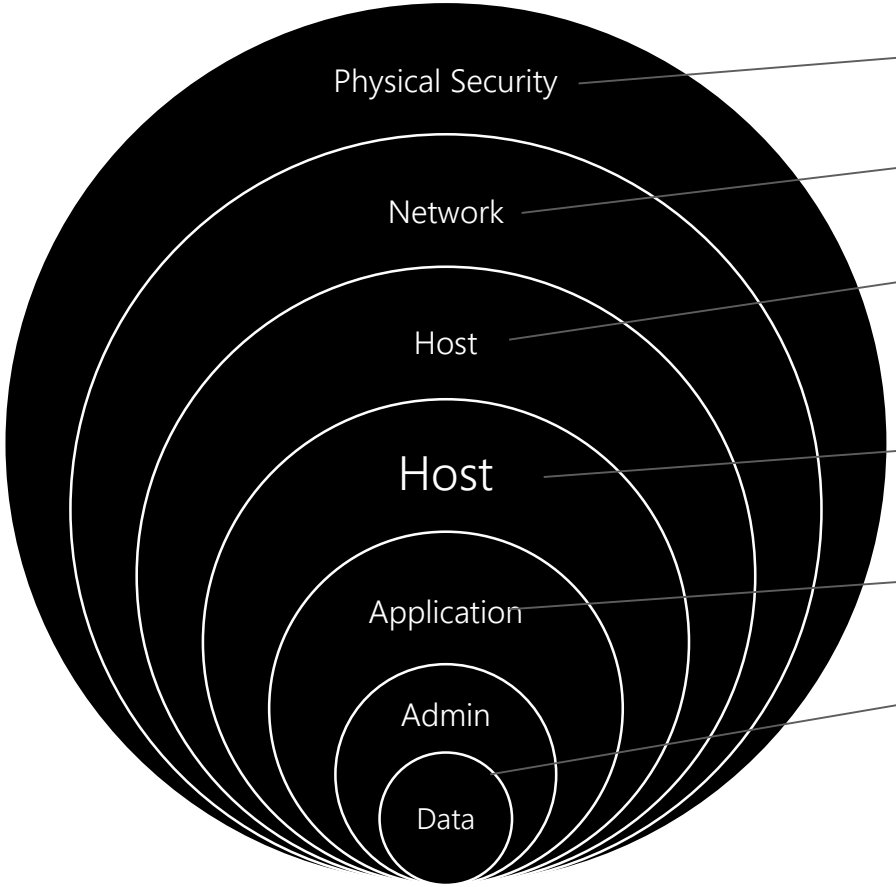
- Common Business Requirements
- Security features of Office 365
- Compliance features of Office 365
- Security and compliance within plans
- Configuration of security and compliance options
- Best practices.
- Take aways.

Common Business Requirements

- Security
  - Is my information safe?
- Retention
  - What happens when an employee leaves?
- Policies
  - How do we manage our information?
- Auditing
  - What's happening to the information?
- Control
  - Who has access to the information?
- Reporting
  - How do I know what's happening with the information?

Security

Defense in depth



Physical controls, video surveillance, access control

Edge routers, firewalls, intrusion detection, vulnerability scanning

Access control and monitoring, anti-malware, patch and configuration management

Secure engineering (SDL), access control and monitoring, anti-malware

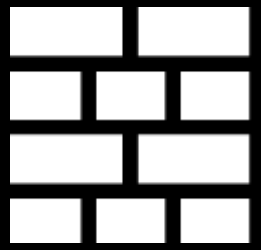
Account management, training and awareness, screening

Threat and vulnerability management, security monitoring, and response, access control and monitoring, file/data integrity, encryption

Independently verified to meet key standards – ISO 27001, SSAE 16, FISMA

Physical security

Perimeter security



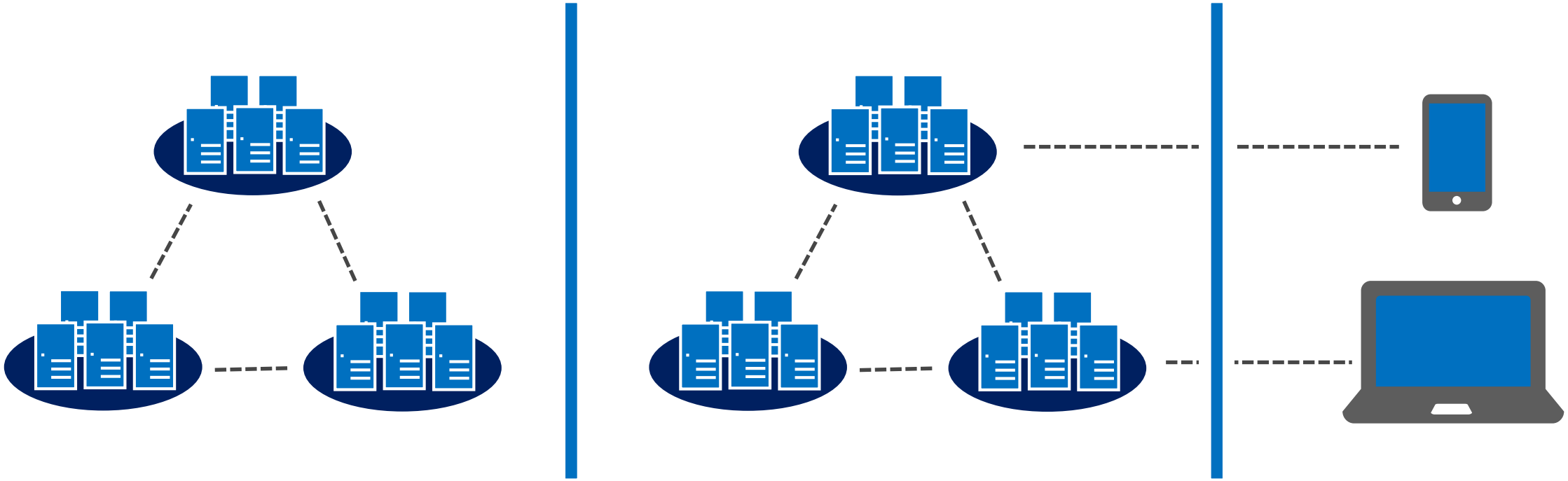
Fire suppression

Multi-factor authentication

Extensive monitoring

- Seismic bracing
- 24x7 onsite security staff
- Days of backup power
- Tens of thousands of servers

Network security



Host/application

Patching/malware protection

Whitelisted processes

Security development lifecycle

Automated tooling for routine activities

Zero standing permissions in the service

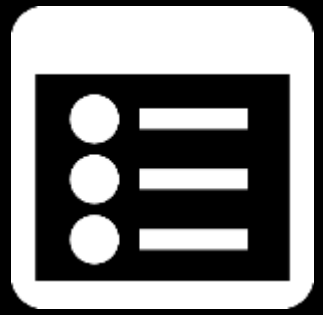
Auditing of all operator access and actions

Administrators

Personnel

Background checks
Screening

Account management



Automatic account deletion
Unique accounts
Zero access privileges

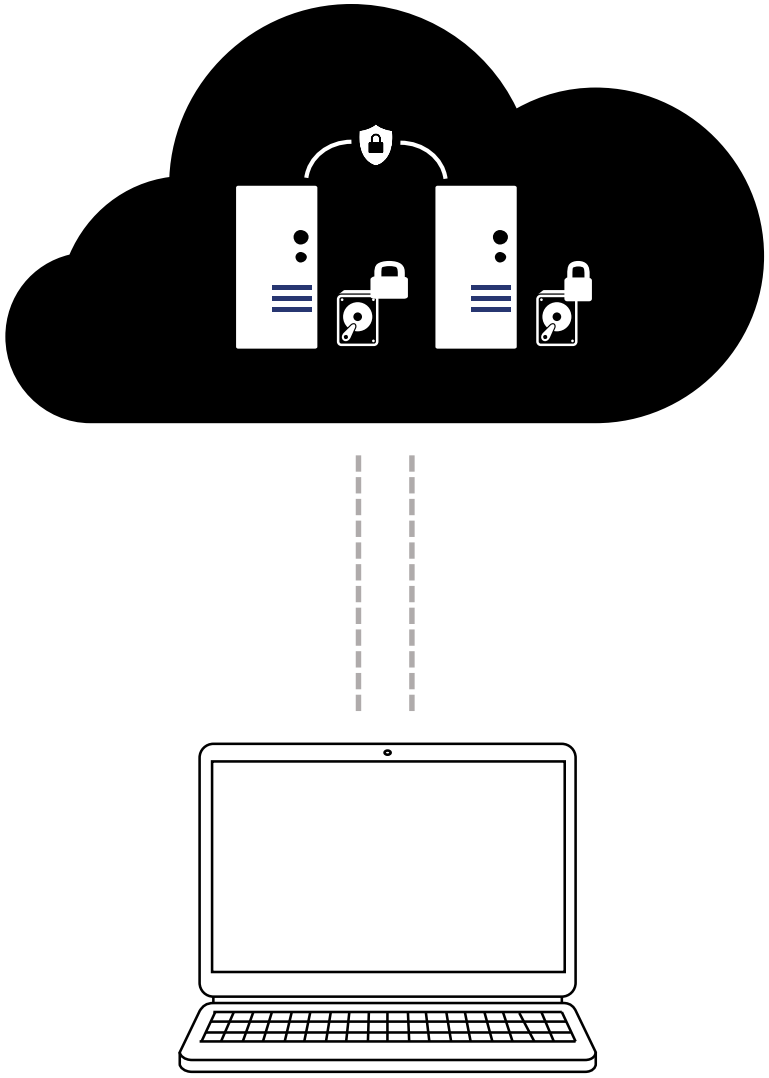
Training, policies, and awareness

SDL
Annual training

Default Encryption

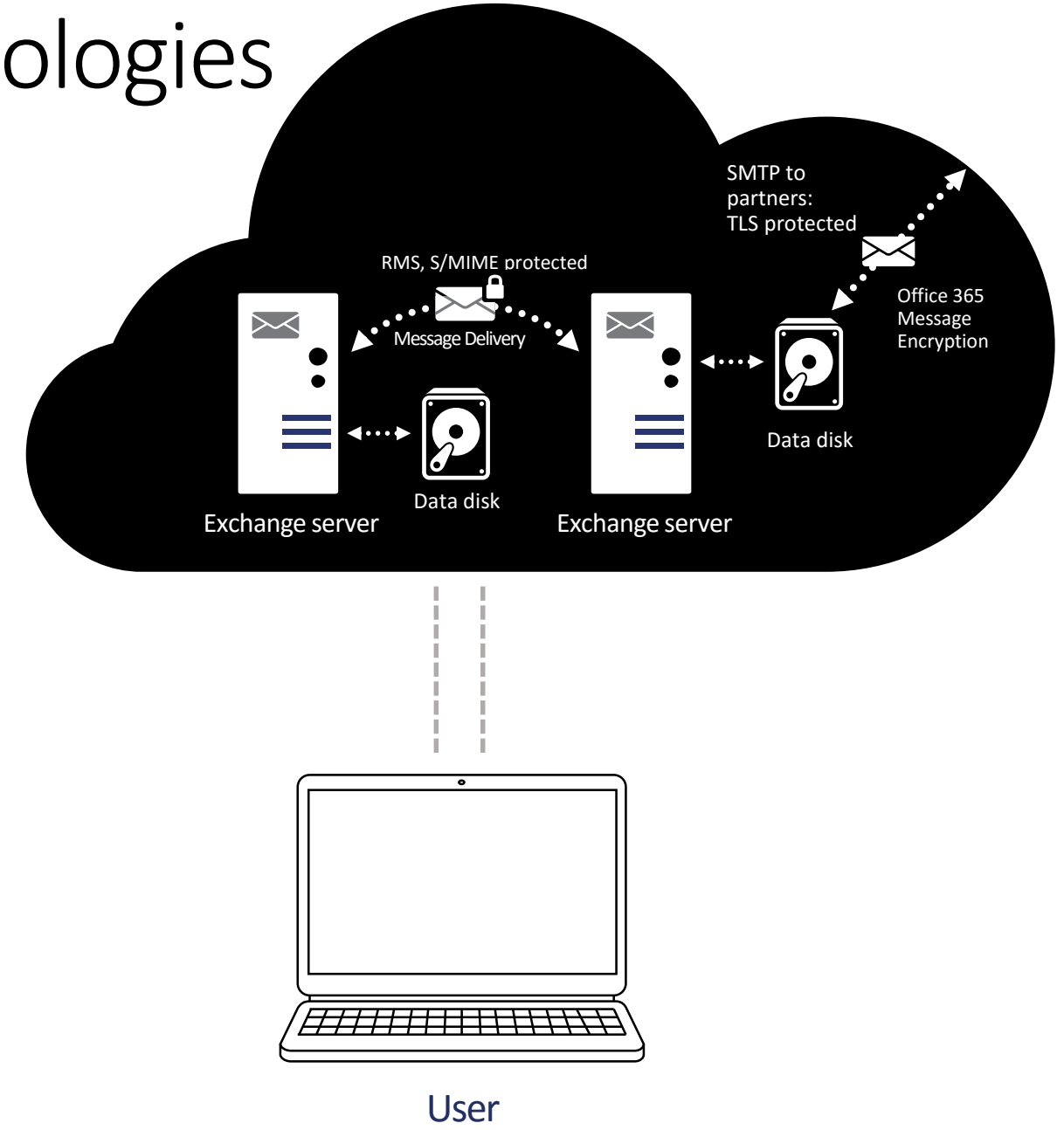
- Data in transit
- Strong SSL/TLS cipher suite
- Perfect Forward Secrecy
- Datacenter-to-datacenter encryption

- Data at rest
- BitLocker disk encryption
- Per-file encryption for customer content



Additional Encryption technologies

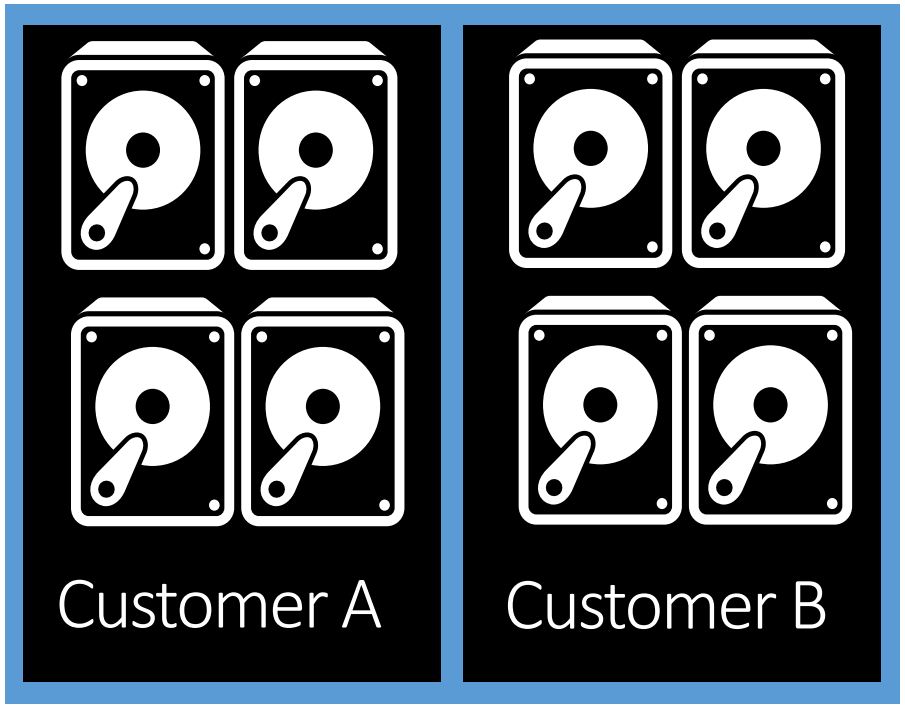
- Rights Management Service
- S/MIME
- Office 365 Message Encryption
- Transport Layer Security



Anti Spam/ Anti Virus

- Multi-engine antimalware protects against 100% of known viruses.
- Continuously updated anti-spam protection captures 98%+ of all inbound spam.
- Advanced fingerprinting technologies that identify and stop new spam and phishing vectors in real time.
- Mark all bulk messages as spam.
- Block unwanted email based on language or geographic origin.

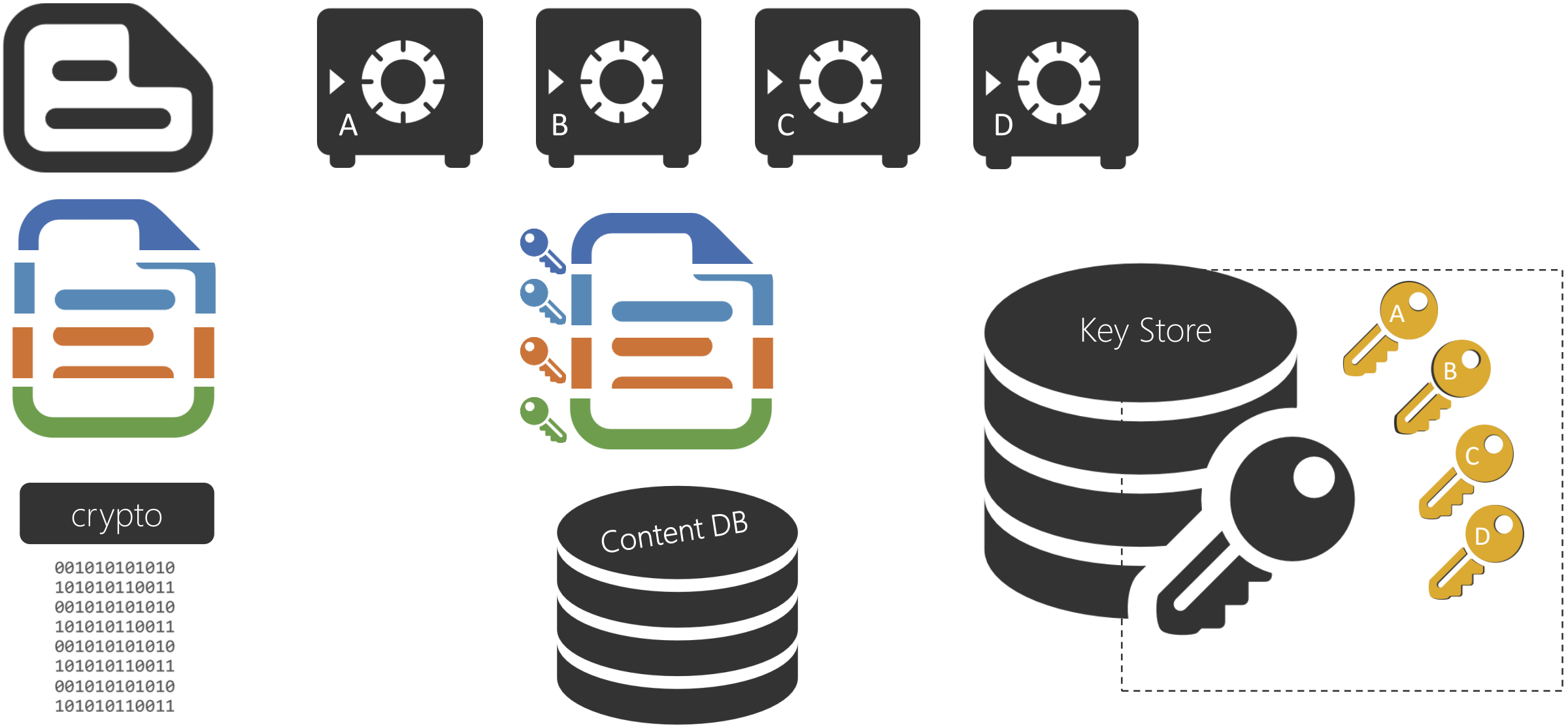
Customer data isolation



Designed to support logical isolation of data that multiple customers store in same physical hardware.

Intended or unintended mingling of data belonging to a different customer/tenant is prevented by design using Active Directory organizational units

Encryption at rest with Per-file Encryption



Breach simulations

Multi-factor authentication using any phone

Mobile Apps

Push Notification
One-Time-Passcode
(OTP) Token

Phone Calls

Out-of-Band* Call

Text Messages

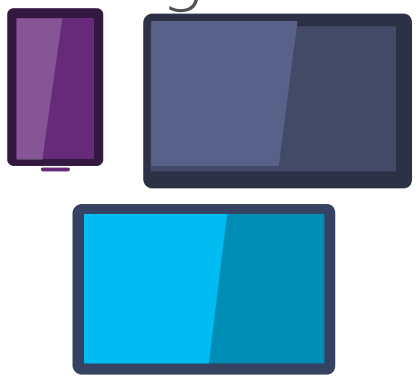
Text
One-Time Passcode
(OTP) by Text

*Out of band refers to being able to use a second factor with no modification to the existing app UX.

Mobile Device Management

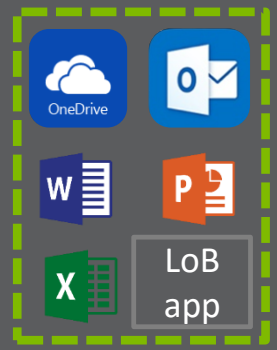
Conditional Access

Device Management



Selective Wipe

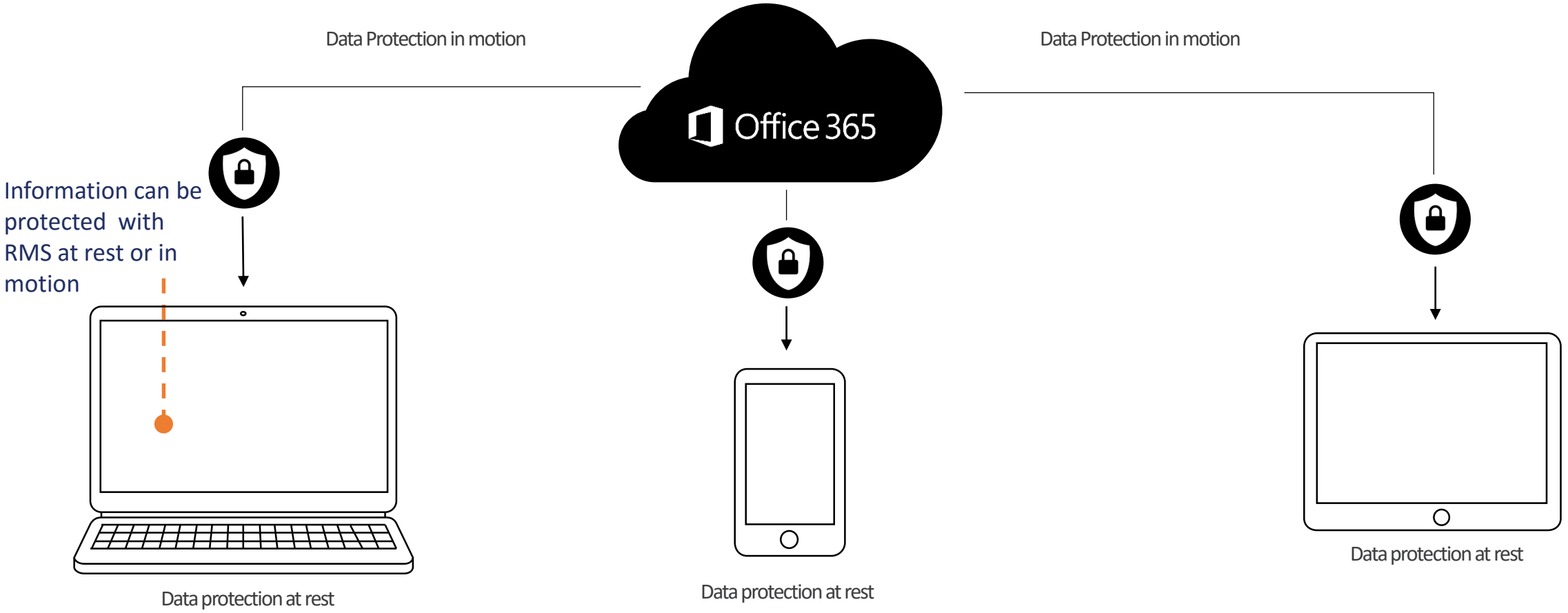
Advanced Application Management



MDM Office 365 Built-in

Microsoft Intune

Rights Management Service



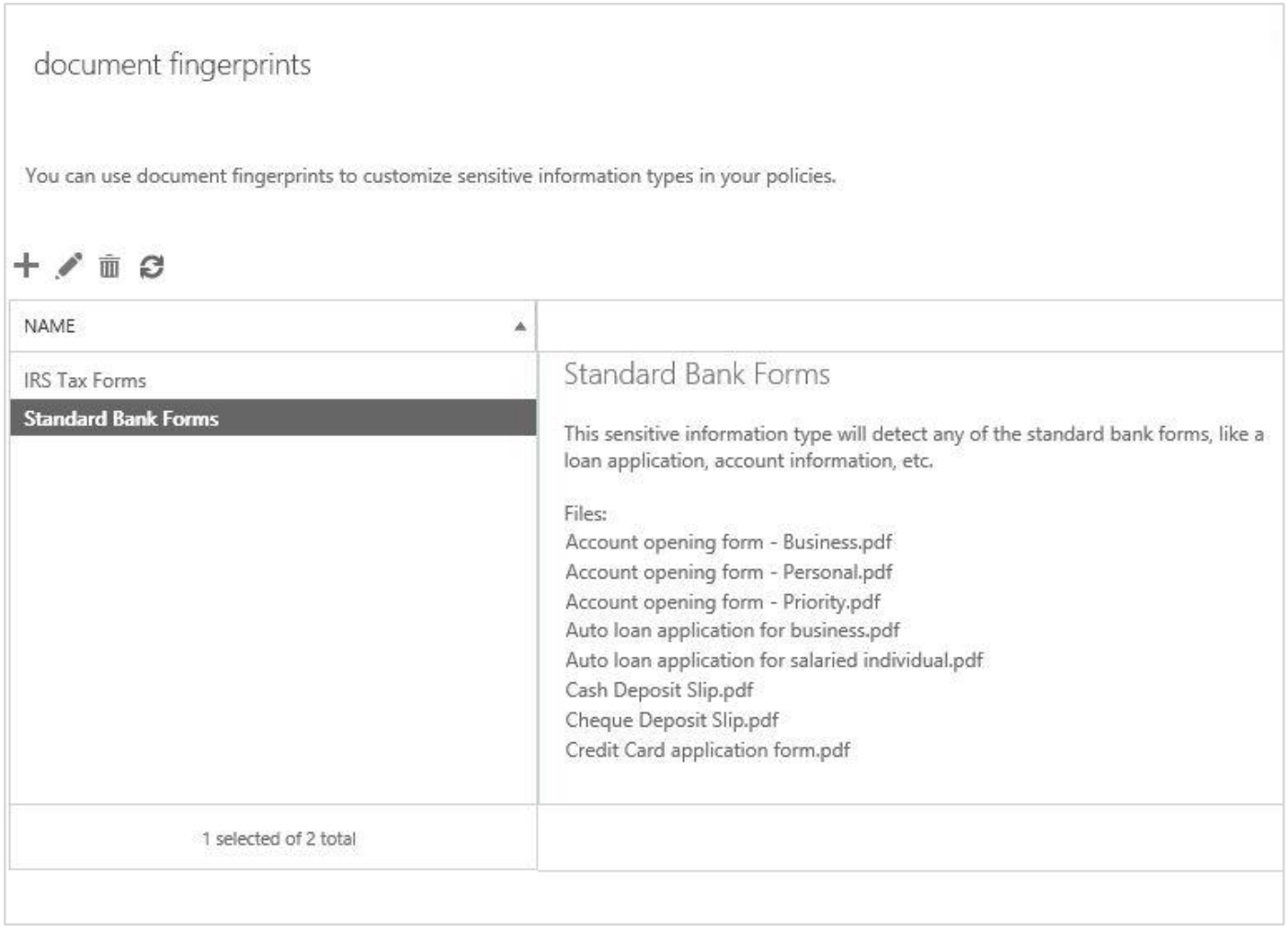
RMS can be applied to any file type using RMS app

DLP document fingerprinting

Scan email and attachments to look for patterns that match document templates

Protect sensitive documents from being accidently shared outside your organization

No coding required; simply upload sample documents to create fingerprints



Email archiving and retention

Preserve

In-Place Archive

- Secondary mailbox with separate quota
- Managed through EAC or PowerShell
- Available on-premises, online, or through EOA

Governance

- Automated and time-based criteria
- Set policies at item or folder level
- Expiration date shown in email message

Hold

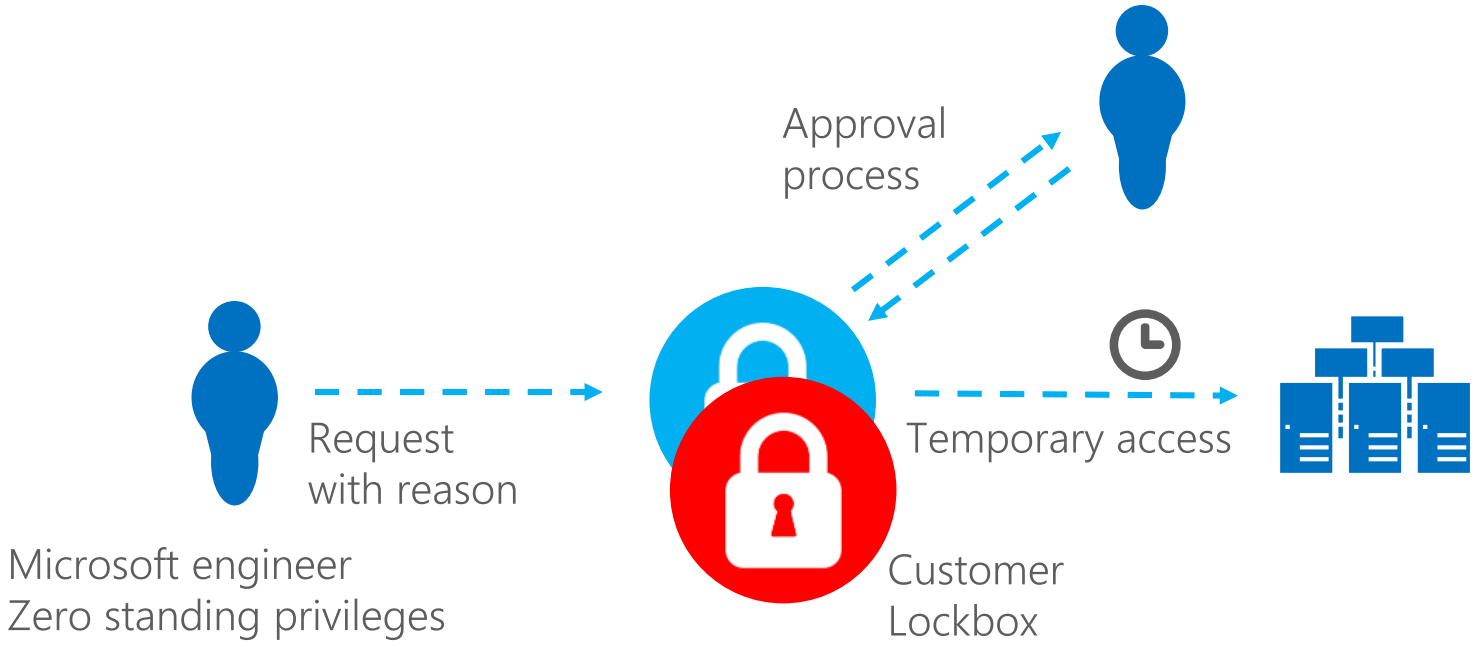
- Capture deleted and edited email messages
- Time-Based In-Place Hold
- Granular Query-Based In-Place Hold
- Optional notification

Search

eDiscovery

- 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

Just-in-time access

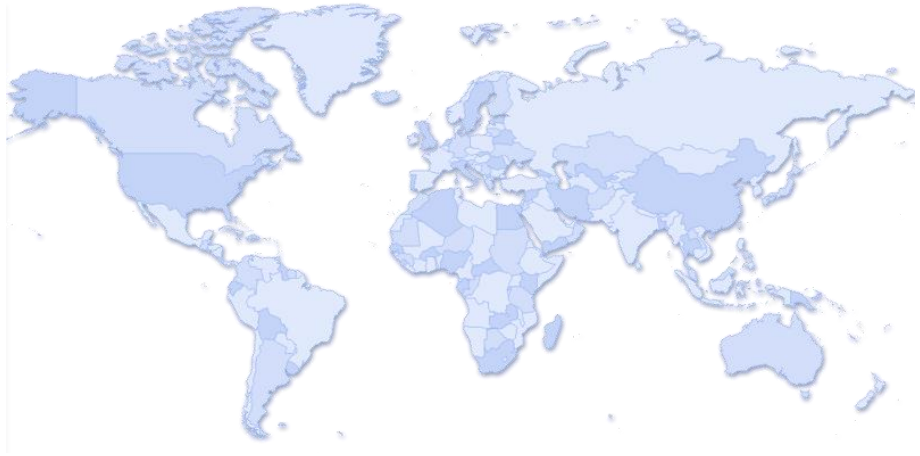


Engineers must have current background check, fingerprinting, security training.

System grants least privilege required to complete task.

Compliance

Standards & Certifications



Standards Certifications	Market	Region
SSAE/SOC	Finance	Global
ISO 27001:2013	Global	Global
ISO 27018	Global	Global
EUMC	Europe	Europe
FERPA	Education	U.S.
FedRAMP/FISMA	Government	U.S.
HIPAA	Healthcare	U.S.
HITECH	Healthcare	U.S.
ITAR	Defense	U.S.
HMG IL2	Government	UK
CJIS	Law Enforcement	U.S.
Article 29 [+]	Europe	Europe
SOC 2	Global	Global

Security, Audits and certifications - http://www.microsoft.com/online/legal/v2/?docid=27

[+]EU Data Protection Authorities validate Microsoft's approach to privacy

Privacy

Privacy by design means that we do not use your information for anything other than providing you services

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

On government snooping…

Here's what Microsoft does, and doesn't do:

We don't provide any government with direct, unfettered access to your data

We don't assist any government's efforts to break our encryption or provide any government with encryption keys

We don't engineer back doors into our products and we take steps to ensure governments can independently verify this

If as reports suggest there is a bigger surveillance program we aren't involved

eDiscovery and In-Place Hold in Office 365

Integrated tools to help you preserve, expire, and discover data

Hold

Keep the data you do want

- Data Held In-Place
- Customize holds based on filters
- Hold across multiple products in a single action
- Capture deleted & edited messages

Deletion

Delete the data you don't want

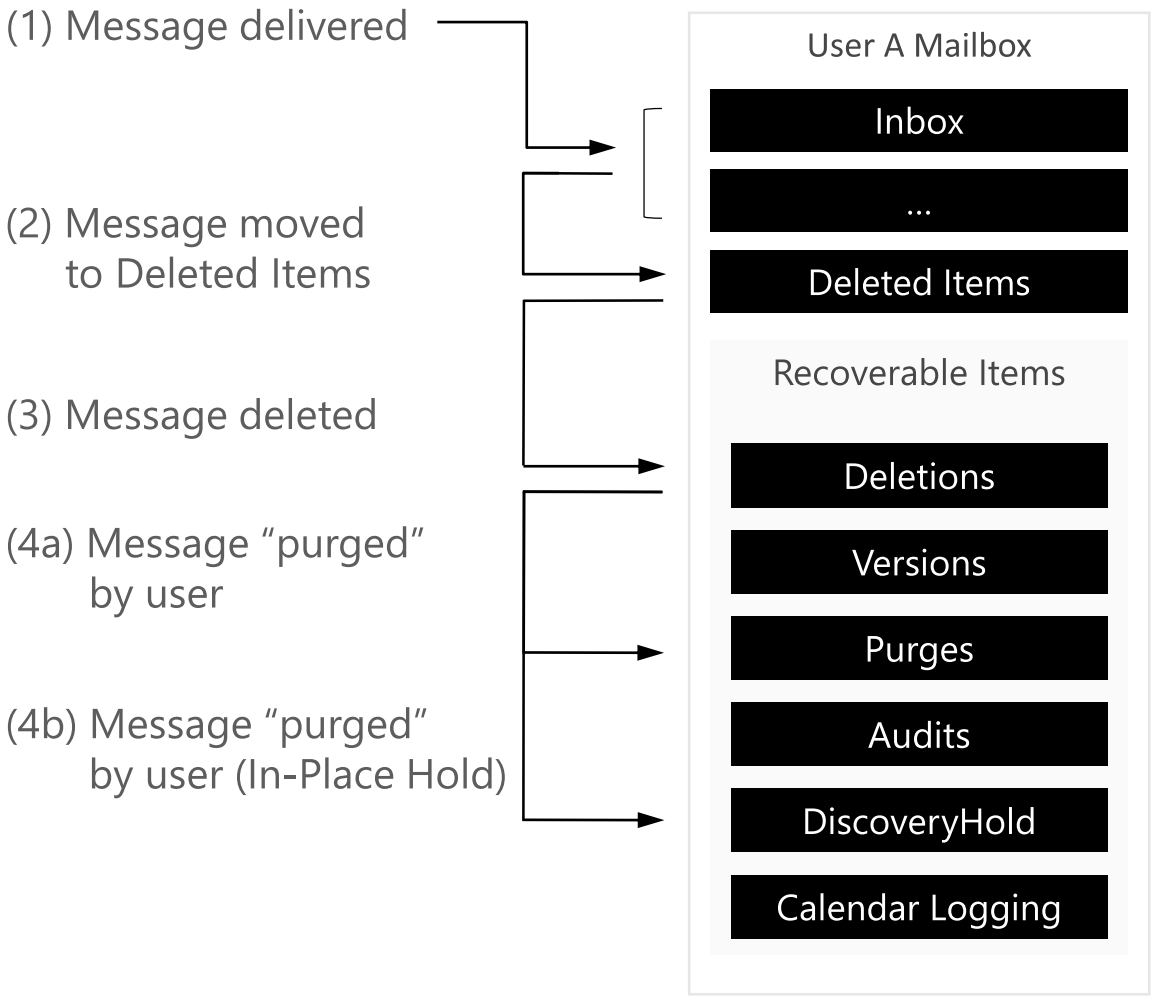
- Automated time-based criteria to delete
- Set policies at item or folder level – admin or user
- Set site level retention polices

Search

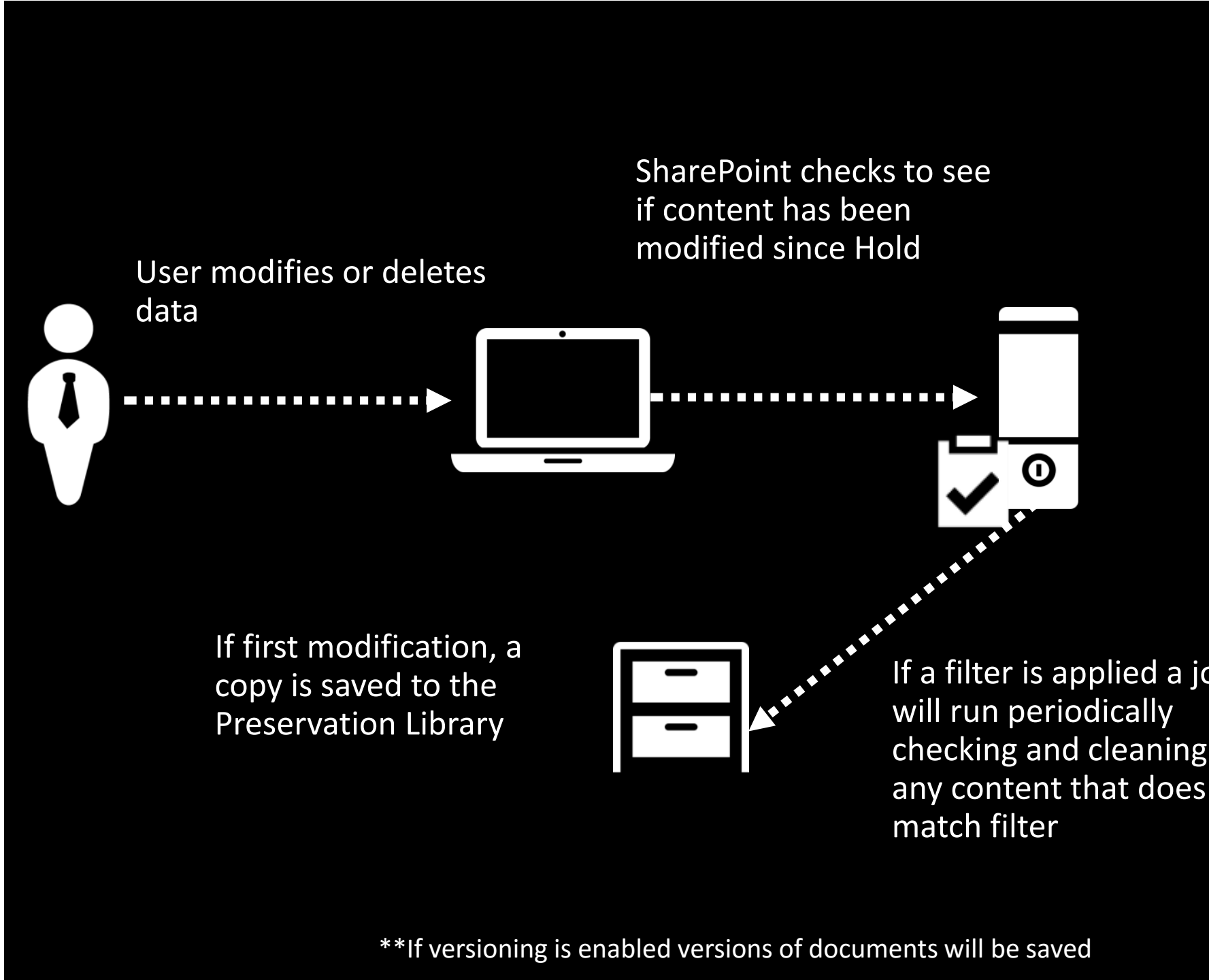
Find the data you need

- Search across multiple products
- De-duplication & search statistics
- Case management
- Export search results

How does Exchange Hold Work?

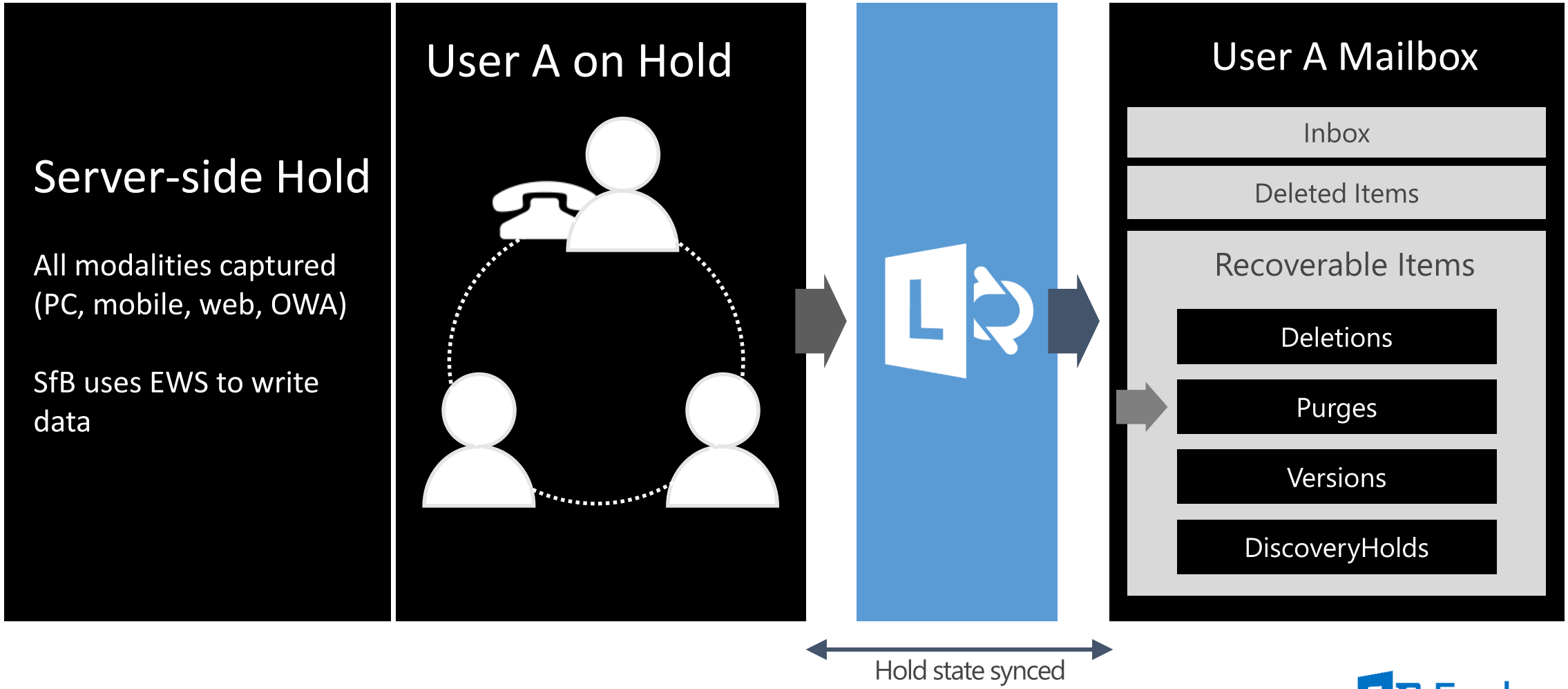


How does SharePoint Hold Work?



**If versioning is enabled versions of documents will be saved

How does Skype for Business Hold Work?



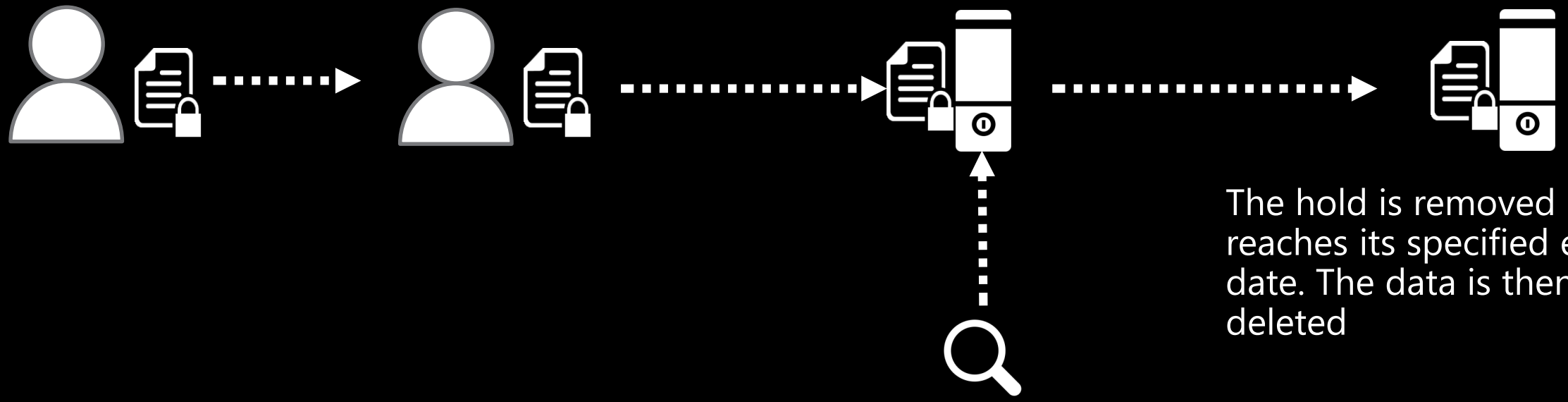
Exchange

How does hold work for inactive users?

User is placed on hold

User leaves company, AD object is deleted

The license will be released, and the In-Place Hold remains enabled



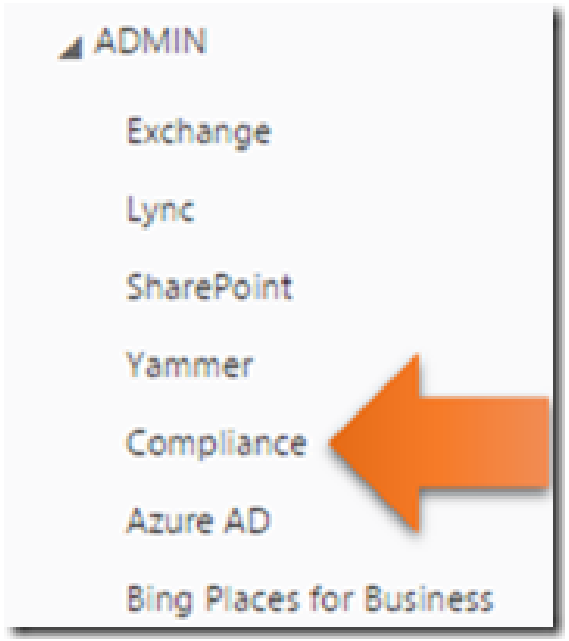
The hold is removed or reaches its specified end date. The data is then deleted

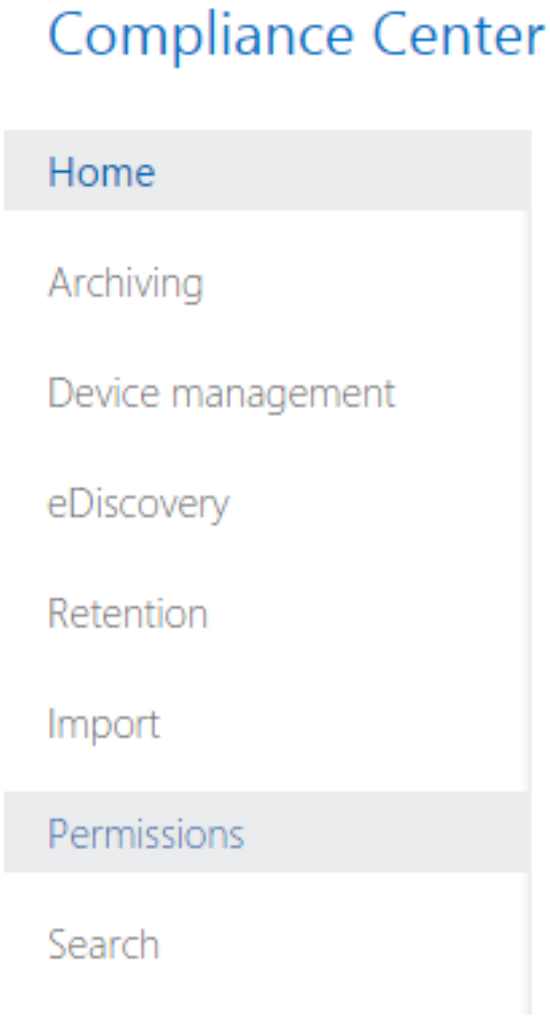
Inactive data can now be searched and accessed only through eDiscovery

Full plan lineup

		Business			Enterprise		
		Business	Business Essentials	Business Premium	ProPlus	E1	E3
Target customer	Price (per year) $AUD	$158	$68	$167	$230	$107	$338
	Seat Cap	300 (for each plan)			Unlimited		
	24/7 phone support from Microsoft	Critical issues			All issues		
Security	Antivirus / Anti-malware	●	●	●	●	●	●
	Encryption at rest	●	●	●	●	●	●
	Multi factor	●	●	●	●	●	●
	Mobile Device Management	●	●	●	●	●	●
Email Security	Message encryption						●
	Unlimited email archiving						●
	Litigation hold						●
	Message tracing		●	●		●	●
Advanced services	Active Directory integration	●	●	●	●	●	●
	Supports hybrid deployment				●	●	●
	Rights Management						●
	Full eDiscovery (hold)						●
	Data Loss Prevention						●

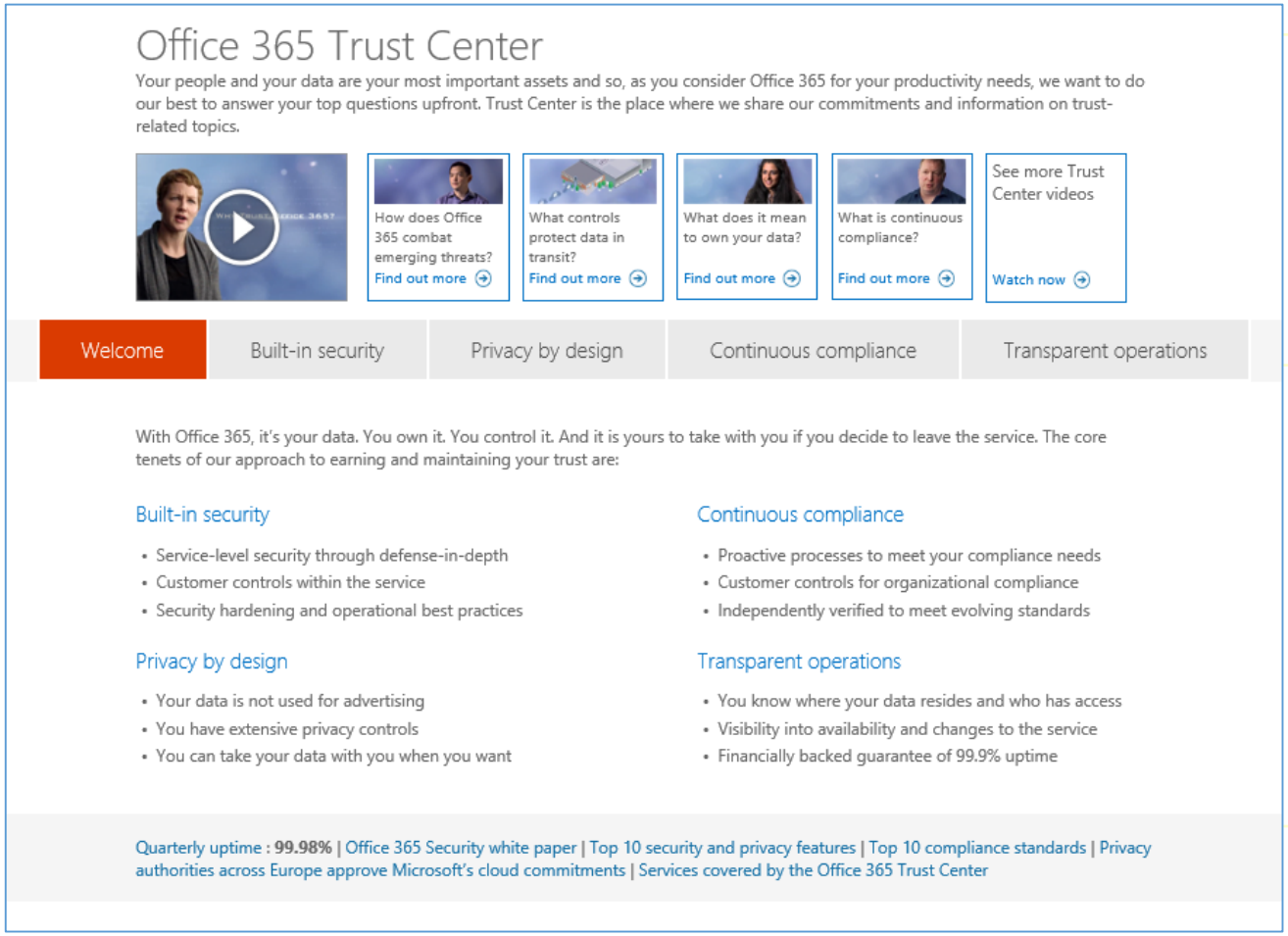
New Compliance centre





DEMO

Resources



Two resources you must know

Office 365 Trust Center http://trust.office365.com

Office 365 Blog http://blogs.office.com/

Best practices

- Understand the customer need for security and compliance.
- Sell the right plan to meet these needs.
- Automate security and compliance configuration.
- Look to enable all the security and compliance options.

Take aways

- Understand what security and compliance options offer.
- Enhance pitch by asking about security and compliance.
- If targeting a vertical know the industry security and compliance requirements.
- Office 365 security and compliance is always being enhanced. Stay up to date.

Resources

- Customer Lockbox - https://blogs.office.com/2015/04/21/announcing-customer-lockbox-for-office-365/
- Office 365 Compliance - https://technet.microsoft.com/en-au/library/office-365-compliance.aspx
- Office 365 Security, Audits and Certifications – http://www.microsoft.com/online/legal/v2/?docid=27
- Beyond MDM – https://www.youtube.com/watch?v=_X3-LEYc8Y8
- Roadmap for information protection in Office 365 and beyond - https://www.youtube.com/watch?v=FhmCYyCgeG4
- Overview of Advanced Threat protection in Exchange - https://www.youtube.com/watch?v=GEE5y9sE_t4
- Office 365 Message encryption - http://blog.ciaops.com/2014/11/office-365-message-encryption.html

QUESTIONS / FEEDBACK?

director@ciaops.com

@directorcia