AGENDA

Seclore - A Brief Introduction To The Company
The Solution – Usable Dynamic Data Centric Protection
Seclore Protection - For Email, DLP and M365
Q&A - Open Discussion

Jasbir Singh, Partner and Managing Director Seclore Europe

Seclore the Company

Company Snapshot

Organization	Global HQ Milpitas CA	**~250** Employees	**100++%** Net retention rate last 5 years	**~66%** Annual growth last 3 years	**8** Sales Locations
Key Metrics	**2000++** Customers	**13** OEM Partnerships	**5 Billion** Protected Files	**15** 50,000+ user Deployments	**10 Million** End Users
Partners	FORCEPOINT / Symantec	HighQ / Datasite Where deals are made	IBM ECM / boldonjames by HelpSystems	SPIRION / HCL / Donnelley Financial Solutions	McAfee

Seclore:Leadership in Data-Centric Security Innovation

2015
First to release policy & identity federation capabilities

2016
First to achieve native 'anyness' support; all file types, devices, OSs

2017
First to deliver full agentless Enterprise Rights Mgmt

2018
First to deliver an open Data-Centric Security Platform

2019
First to deliver email encryption plus solution for persistent email protection

2020
First to deliver CASB support for automated data protection in the cloud

2021
First to provide dynamic & persistent M365 integration for Teams & SP Online
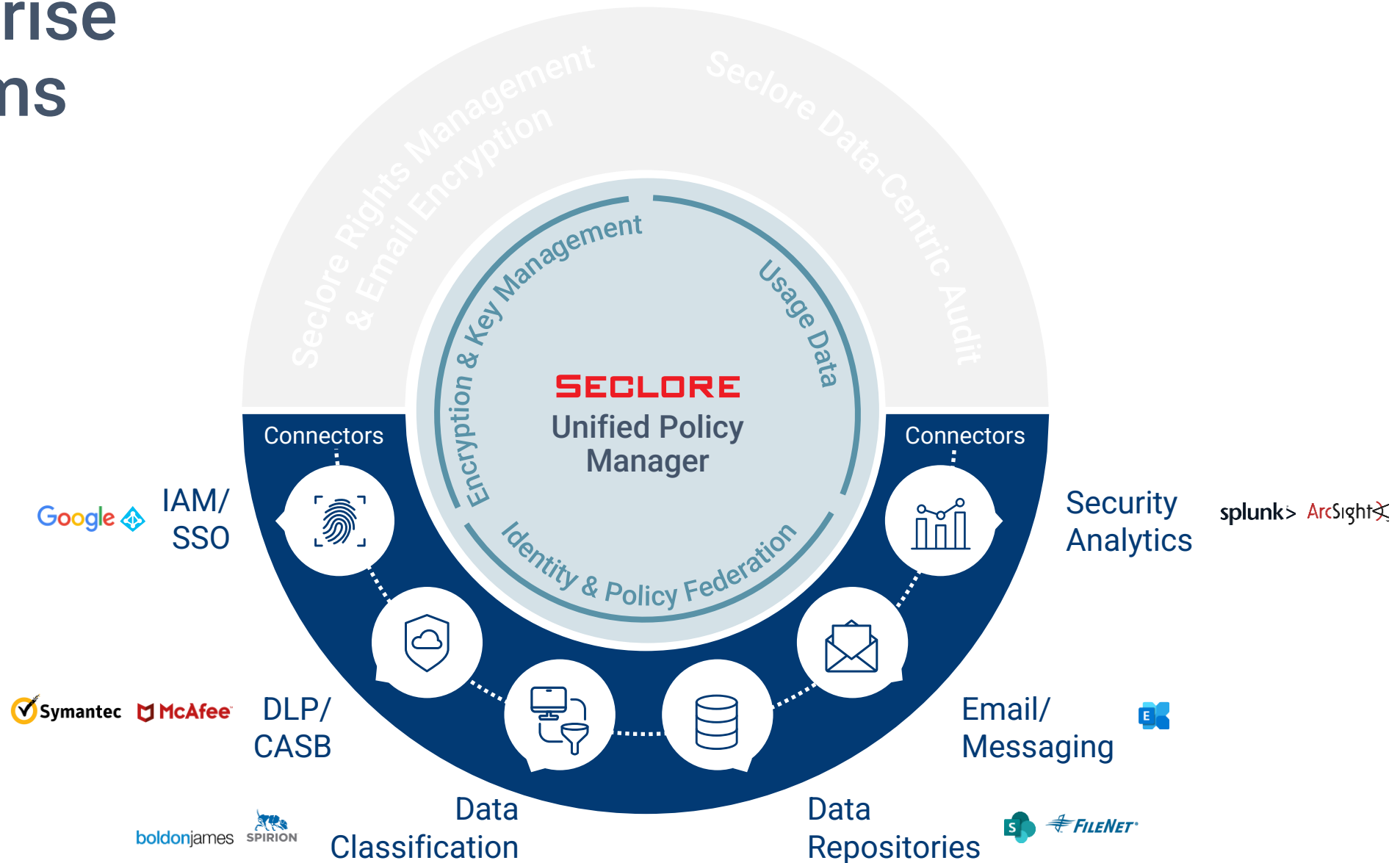
The Solution

A strong foundation for critical capabilities and continuing opportunities
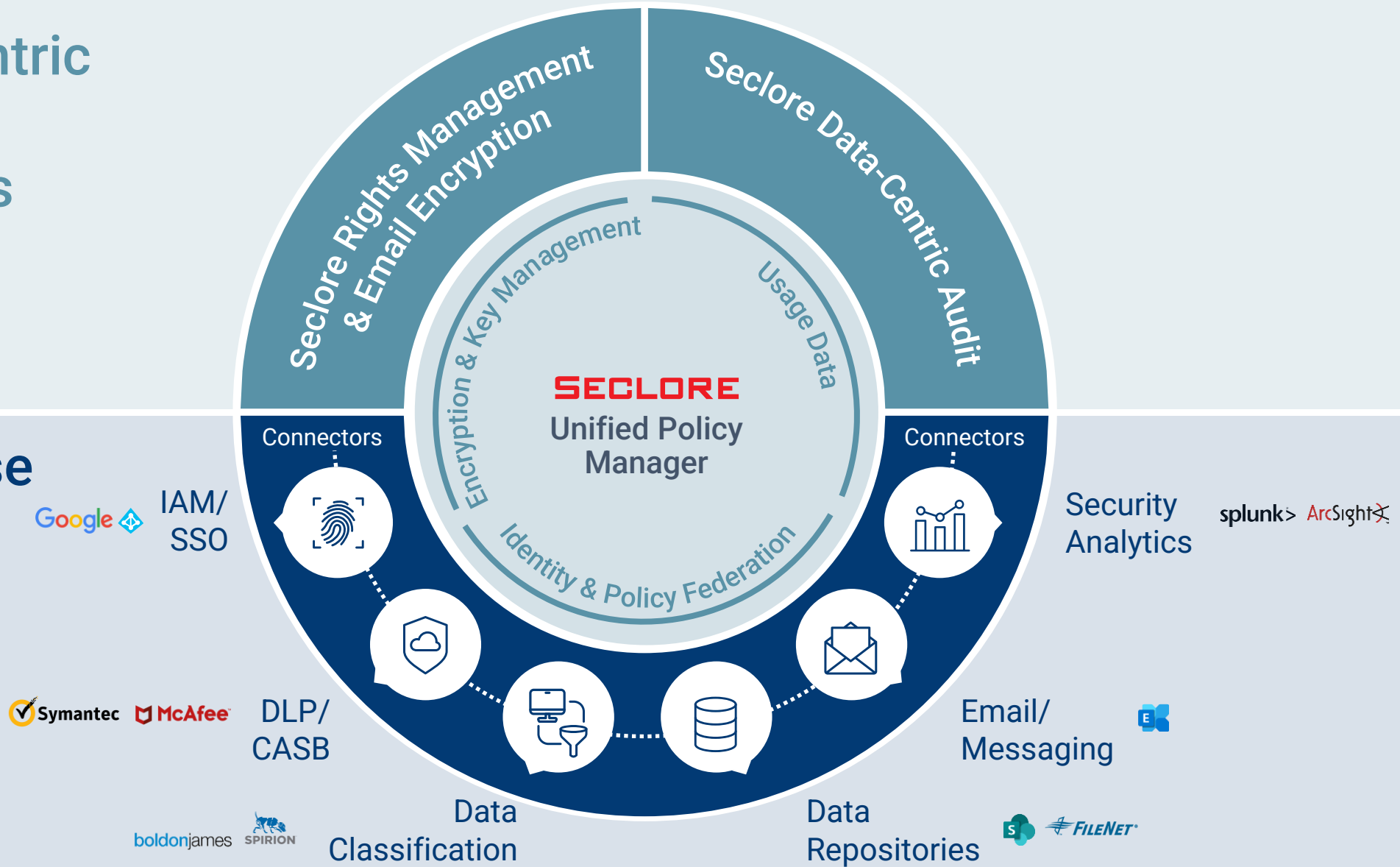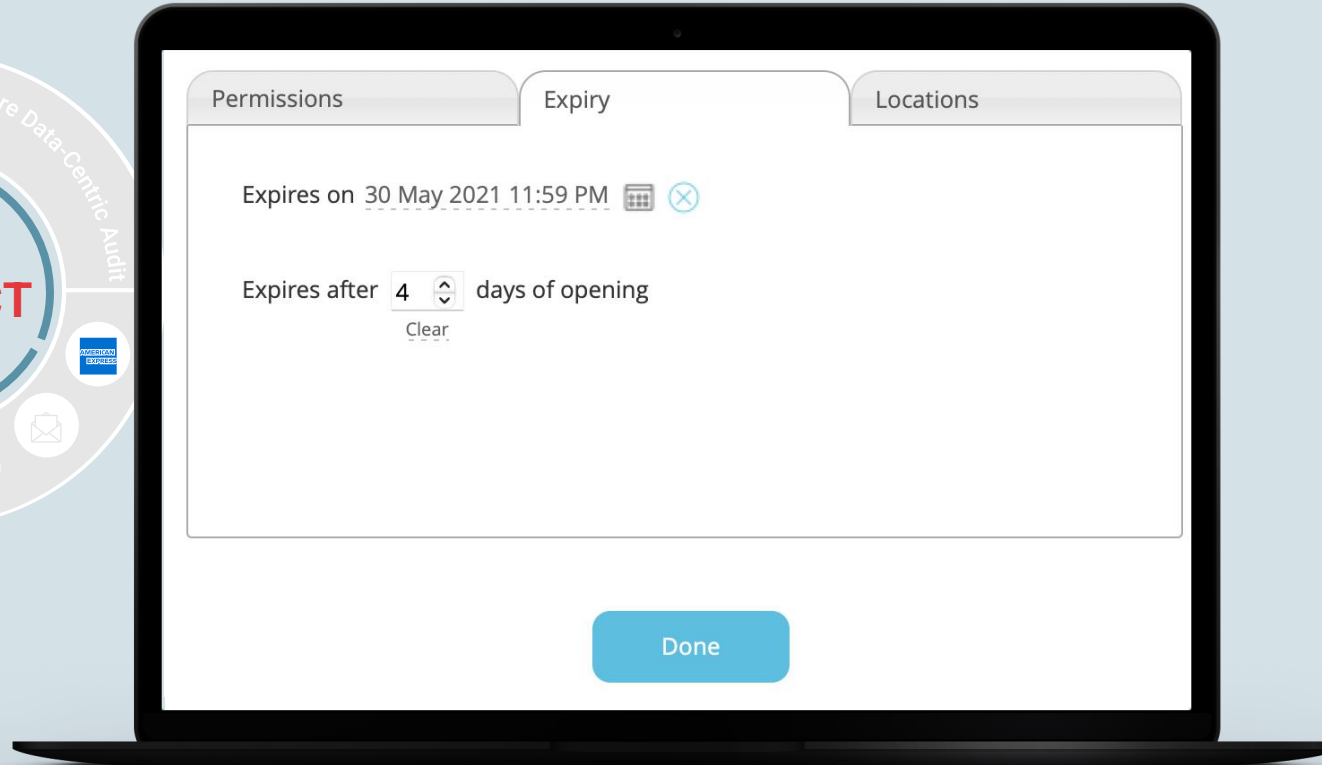
Seclore's Data-Centric Security Solutions

Seclore Rights Management & Email Encryption

Seclore Data-Centric Audit

Encryption & Key Management

Usage Data

SECLORE
Unified Policy Manager

Identity & Policy Federation

Enterprise Systems

Seclore Unified Policy Manager

PROTECT

Seclore Rights Management & Email Encryption

Seclore Data-Centric Audit

TRACK

| Permissions | Expiry | Locations |

Expires on 30 May 2021 11:59 PM

Expires after 4 days of opening

Clear

Done

Go beyond classification, encryption and DLP with granular controls

Usage data monitoring

Remotely edit permissions and rights

Encryption and key management

Seclore Unified Policy Manager

PROTECT

TRACK

Seclore Rights Management & Email Encryption

Seclore Data-Centric Audit

SECLORE

Home   Files   Activities   Policies   More ⌄

Kevin Brown ⌄
Administrator - 'POC USERS'

Admin Dashboard

License Usage

Potential Risks • June 2018

Assigned to my Organization Unit
248

⚠ Unauthorised Activities
June 2018

Assigned in Total
721 of 1000

29 Total

0 by External Users

Server License Expires on
31 Dec 2099

29
Till Today

Dec   Jan   Feb   Mar   Apr   May   Jun

Lifetime Usage

High Risk Authorised Activities
June 2018

Total Files Protected
5.2 K

6 Total

6 Unprotects

Total Activities
16 K

0 Prints

6
Till Today

0 by External Users

0 Unprotects

0 Prints

Dec   Jan   Feb   Mar   Apr   May   Jun
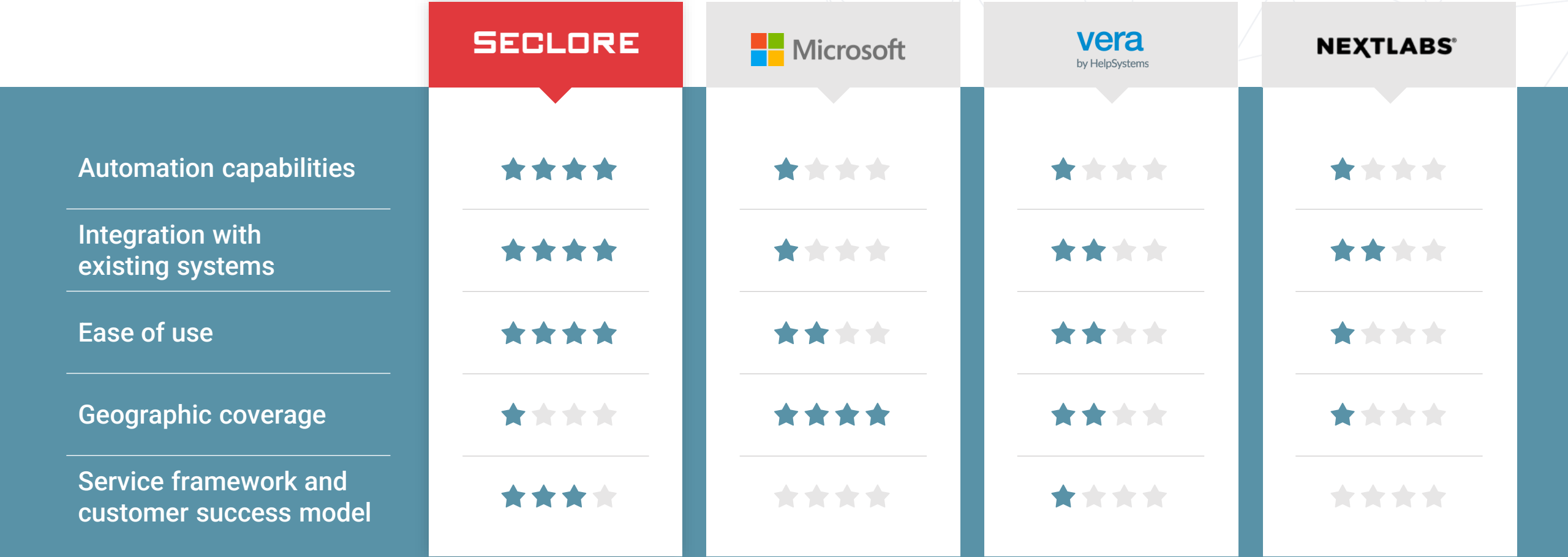
Remotely edit permissions and rights

Encryption and key management

**Go beyond classification, encryption
and DLP with granular controls**

Usage data monitoring

# Seclore is an industry leader with unmatched automation and service capabilities

	SECLORE	**Microsoft**	**vera** by HelpSystems	**NEXTLABS**
Automation capabilities	★★★★	★☆☆☆	★☆☆☆	★☆☆☆
Integration with existing systems	★★★★	★☆☆☆	★★☆☆	★★☆☆
Ease of use	★★★★	★★☆☆	★★☆☆	★☆☆☆
Geographic coverage	★☆☆☆	★★★★	★★☆☆	★☆☆☆
Service framework and customer success model	★★★☆	☆☆☆☆	★☆☆☆	☆☆☆☆

Secure Mail Collaboration

One-Click Protection, Easy Consumption, Track & Revoke

Secure Mail Collaboration: One Click Protection

Easy One-Click Protection in Outlook & OWA
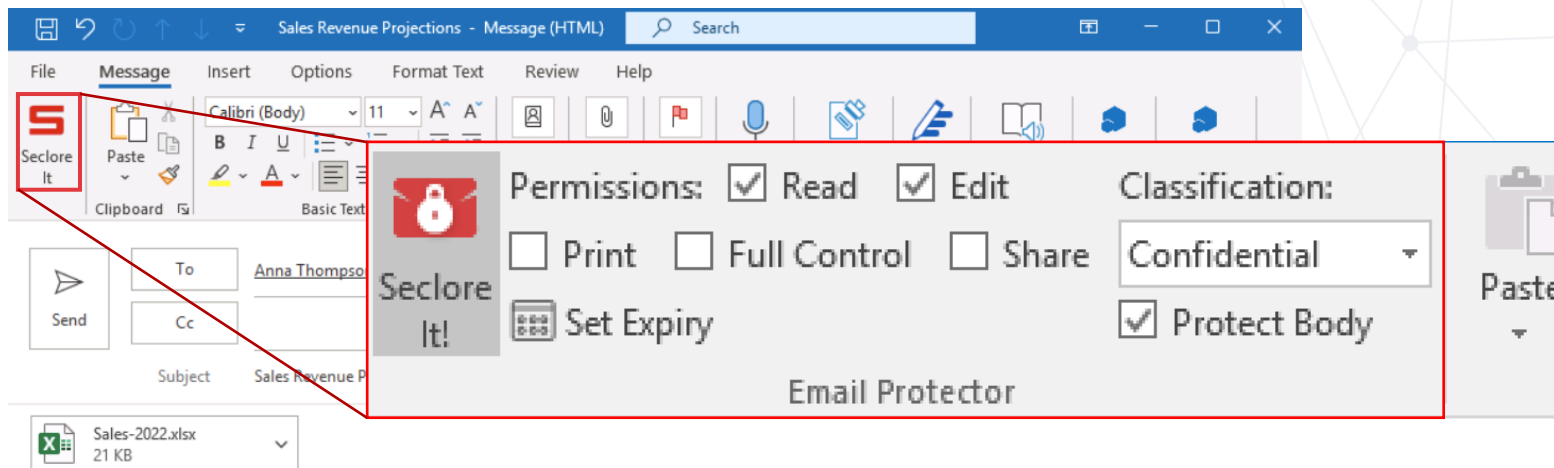
Secure your emails and keep them safe from unauthorized parties (and forwards)

Persistent Security: Security controls stay with the content regardless of where the email is sent, respective of email client or device.

Granular Protection: Protection is granular and can be customized depending on your use case.

'Smart' Sharing: If protected emails are forwarded, any additional content will get protected automatically

Secure Mail Collaboration: Consumption

VIA Seclore Client

Seamless Integration
- Protected Mails open in Outlook
- Direct attachment access

Secure Communication
- Replies are protected
- Smart Sharing with other users

VIA Browser

Browser-based Access
- Agentless Access for Email Body and attachments

Secure Collaboration
- Users can securely reply on mails
- Allow users to work on protected files without an agent

VIA Mobile

Mobile Access
- Compatible with all major EMM application vendors

Business Benefits
- Extend your security and governance framework
- Maintain complete data privacy

Secure Mail Collaboration: Track and Revoke

Easily Manage protected mails directly from Outlook

Activity Tracking: Details on emails and attachments are being tracked in real time wherever they go

Expiry and Remote Control: Access to emails / attachments can be revoked at any time – even after they are sent.

Sales Revenue Projections

Kevin Brown
To   Anna Thompson; linda.jones83@hotmail.com

↩ Reply   ↩ Reply All   → Forward

Tue 6/14/2022 2:38 PM

🔒 Seclore   ✕

◎ Track   ⓘ

Time ^	Recipients	Activity	File
14.Juni.2022, 04:41 nachm.	kevin.brown	Opened	Email_Sales Revenue Projections.smail
14.Juni.2022, 04:41 nachm.	anna.thompson	Opened	Email_RE_ Sales Revenue Projections.smail
14.Juni.2022, 04:40 nachm.	anna.thompson	Opened	Email_Sales Revenue Projections.smail
14.Juni.2022, 04:40 nachm.	anna.thompson	Edited	Email_Sales Revenue Projections.smail

<   1   >   Total Records: 16

◎ Track   👤 Revoke

🔒 Seclore   ✕

👤 Revoke Access   ⓘ

☐ Select All

Recipients

☐ anna.th

☐ linda.jo

👤 Revoke Access

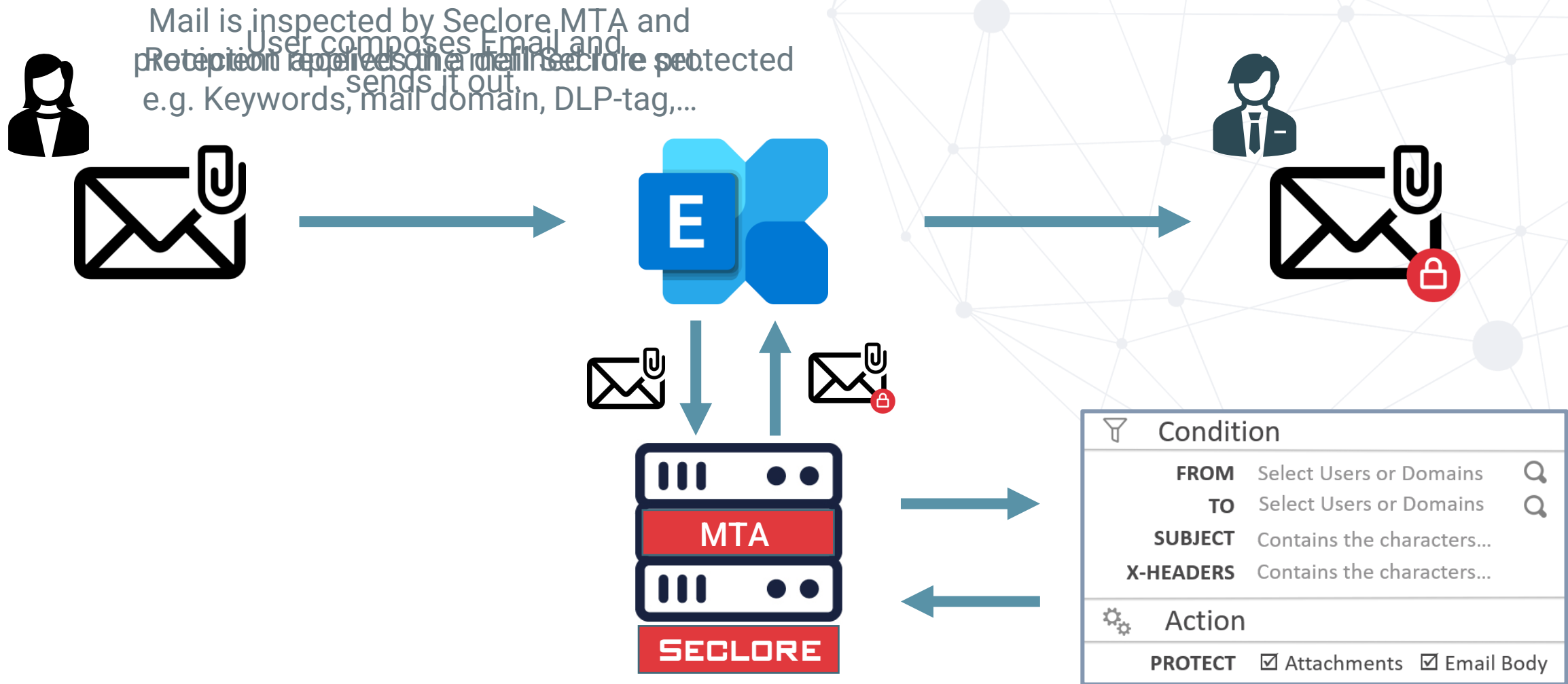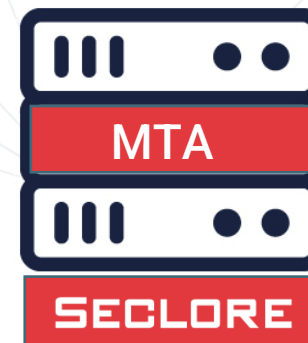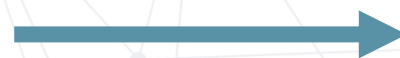✅ 1 recipient's access was successfully revoked

Close

Revoke   Back to Email

How it Works: Automated Protection - Mail

Mail is inspected by Seclore MTA and
protection applied as per defined policy
User composes Email and Recipient opens the mail Seclore protected
sends it out.
e.g. Keywords, mail domain, DLP-tag,…

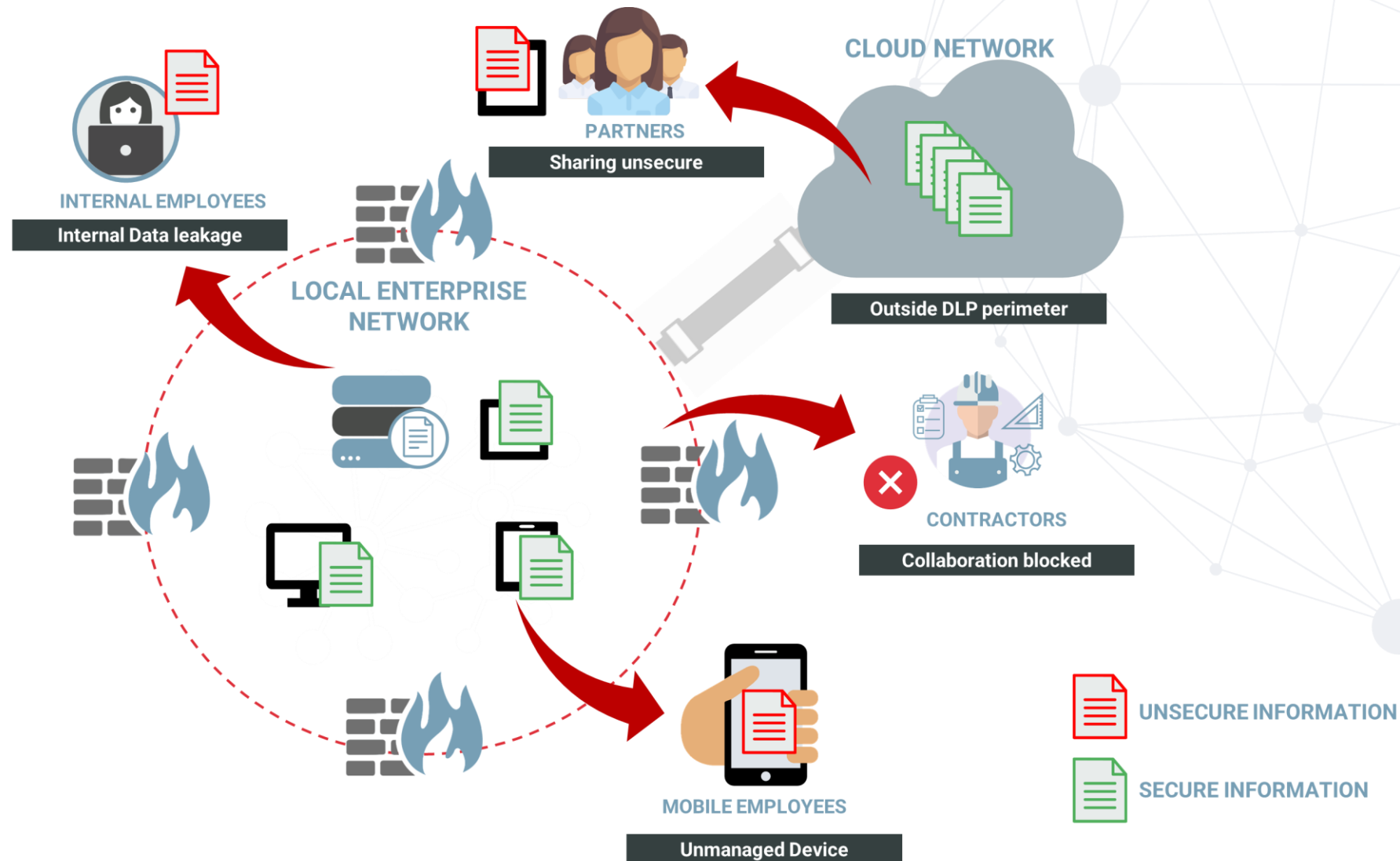| ⧩ Condition		
FROM	Select Users or Domains	🔍
TO	Select Users or Domains	🔍
SUBJECT	Contains the characters…	
X-HEADERS	Contains the characters…	
⚙ Action		
PROTECT	☑ Attachments	☑ Email Body

How it Works: Automated Protection - Mail

Key Benefits

✓ **Automate:** Automatically protect emails without user intervention.

✓ **Extend Email Protection with DLP:** Add usage controls to sensitive data that is discovered in emails and attachments

✓ **Persistent Security:** The security controls stay with the content regardless of where the email is sent.

✓ **On-the-Fly User Registration:** User registration and onboarding happens via automatic workflows when the email is sent.
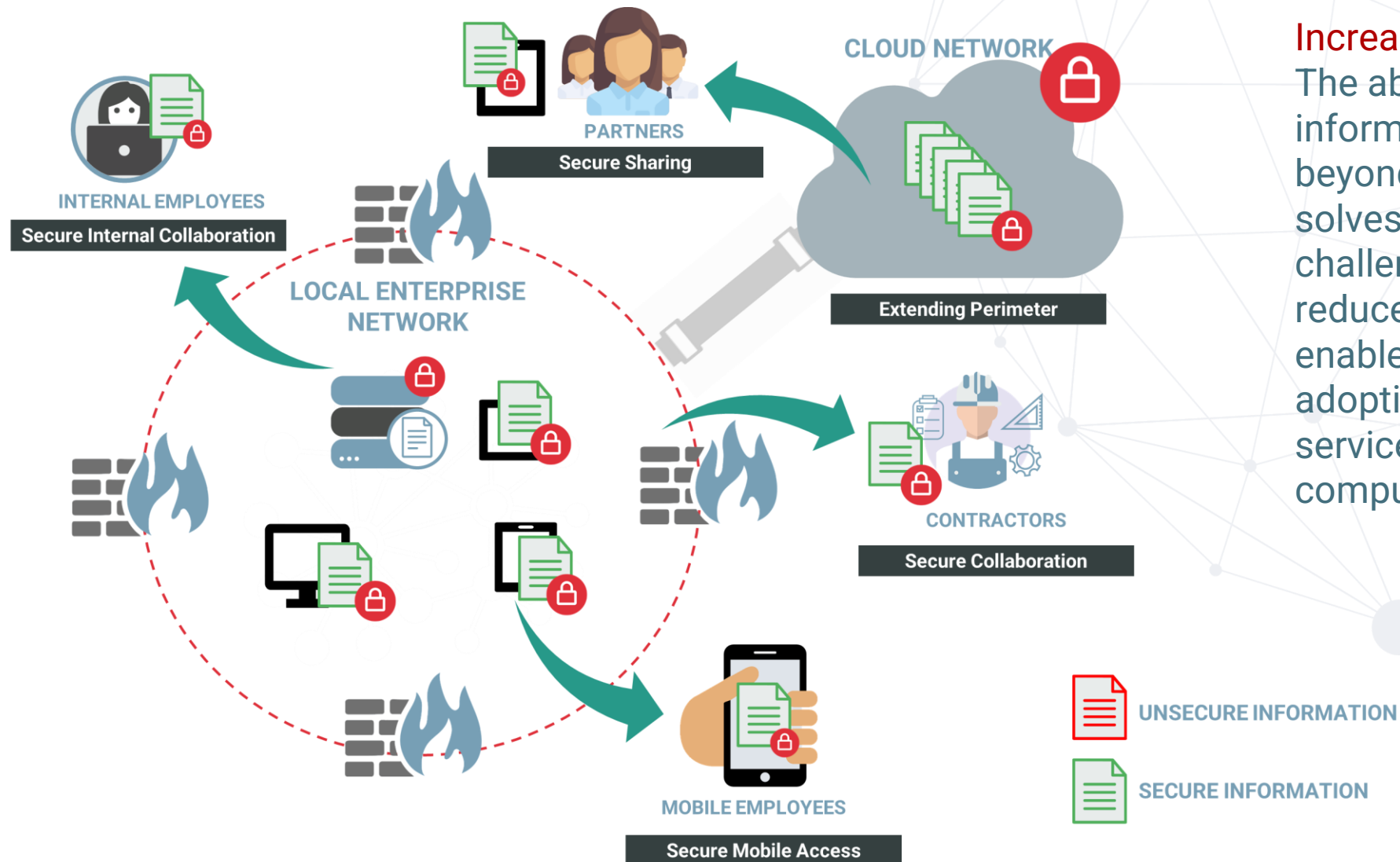
MTA

SECLORE

Seclore for DLP

Extend protection beyond the enterprise

Seclore & DLP: Without Seclore Protection

CLOUD NETWORK

PARTNERS
Sharing unsecure

INTERNAL EMPLOYEES
Internal Data leakage

LOCAL ENTERPRISE NETWORK

Outside DLP perimeter

CONTRACTORS
Collaboration blocked

MOBILE EMPLOYEES
Unmanaged Device

UNSECURE INFORMATION

SECURE INFORMATION

Seclore & DLP: With Seclore Protection

PARTNERS
Secure Sharing

CLOUD NETWORK

Extending Perimeter

INTERNAL EMPLOYEES
Secure Internal Collaboration

LOCAL ENTERPRISE NETWORK

CONTRACTORS
Secure Collaboration

MOBILE EMPLOYEES
Secure Mobile Access

UNSECURE INFORMATION

SECURE INFORMATION

Increased Business Agility:
The ability to secure information that travels beyond corporate borders solves a thorny compliance challenge, significantly reduces security risks, and enables the safe and secure adoption of file-sharing services, BYOD and cloud computing.

Seclore & DLP: How it works

1 | File / Email with sensitive data is, created on an **Endpoint**, moved on a **Network Share,** send via **Email** or copied on a **USB drive**

2 | DLP **scans** for keywords and patterns. Instead of blocking a file, DLP can now **invoke** Seclore

3 | Seclore automatically encrypts the file and applies usage controls

4 | File is **protected** and can be shared securely in- and outside the company's perimeter.

Key Benefits

- ✓ Extend protection beyond the enterprise
- ✓ Secure email, cloud and other file sharing
- ✓ Reduce false positives
- ✓ Dynamically assign and revoke granular file permissions
- ✓ Gain comprehensive data reports for compliance

Seclore for Microsoft

Automatic Protection, Seamless Access , Policy Federation

Protection on desktop
Seamless access in native apps

Classification driven protection
Sensitivity labelling driven protection

Email protection
User-driven and automated

Desktop app   **Web app**   **Online**

Securing collaboration and productivity apps

Securing mobile data sharing

Identity Federation
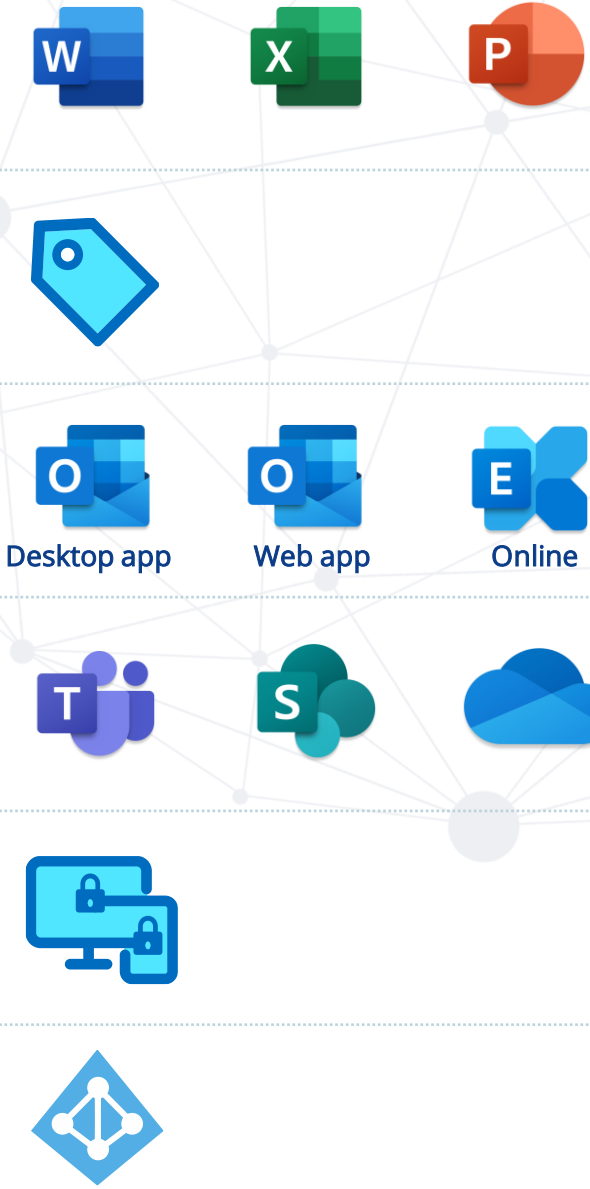
Seamless Integration into Azure AD

Enterprise ID Federation
Seamless identity federation with Azure allow employees and external users to authenticate using Enterprise Azure Identity solution to access Seclore protected files.

Securely Collaborate Within Microsoft Intune
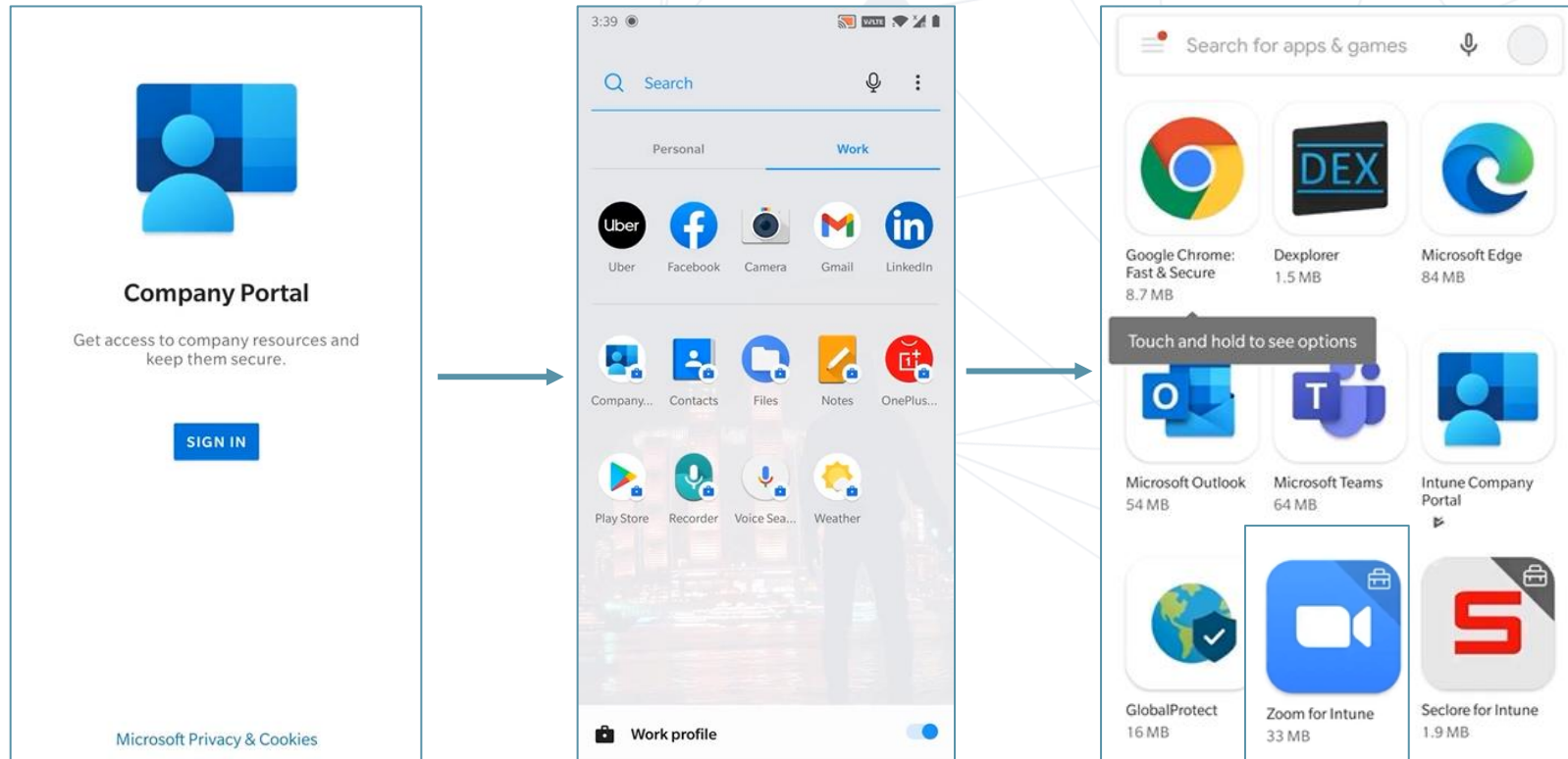
Seamless Security
Ensures Data-Centric Security works seamlessly with existing perimeter-based security tools.

Easy Administration
Self-service options available for end-user on-boarding
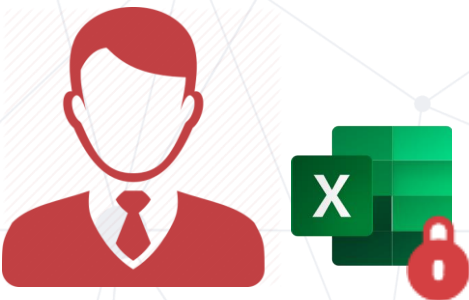
No Maintenance
Ongoing updates are automatic with no end-user or admin intervention

Seclore supports a variety of different other MDM solutions

How it Works: Teams Integration

SSO with Azure Identity

Single Click open from Teams

Secure access via Browser and Client

Edit and Save Back to Application

EASE OF USE
Single Click Access

SECURE ACCESS
Client & Browser

Lower TCO
No MS Office License

ONLINE EDITOR — Read-only — Edit

ONLYOFFICE — Revenue_Projections_2019-2020.xlsx — Kevin Brown

File | Home | Insert | Layout | Formula | Data | Collaboration

	A	B	C	D	E	F	G	H	I	J
1	SALES PROJECTIONS FOR FY 2016-17 (All figures in USD)									
2		Q1	Q2	Q3	Q4		Total			
3	Northeast US	2.1	2.4	2.1	2.9		9.5			
4	Southeast US	0.9	1.2	1.1	1.4		4.6			
5	Midwest US	1.2	1.4	1	1.5		5.1			
6	West US	2.6	3	2.5	3.2		11.3			
7	Canada	0.7	0.9	1	1.5		4.1			
8	Mexico	1	1	1	1.5		4.5			
9	South America	3.9	4	3.8	10		21.7			
10										
11										
12	Total Revenue						60.8			
13										
14	TOP 5 ACCOUNTS									
15		Renewal	Growth							
16	Airlogic	1.3	0.5							
17	VCC Group	1.1	0.7							
18	EgSystems	0.9	0.9							
19	Zenna	0.9	0.7							
20	Jupiter LLC	0.8	0.6							
21										

Sales Projection — Zoom 100%

SECLORE CONFIDENTIAL

Policy Federation
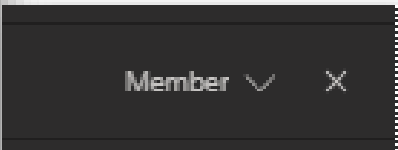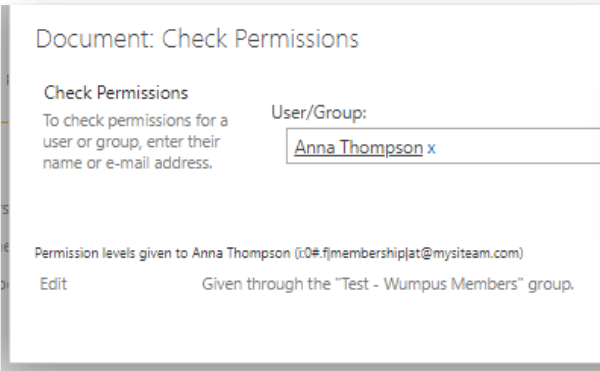
Dynamic Rights , Instant Revoke
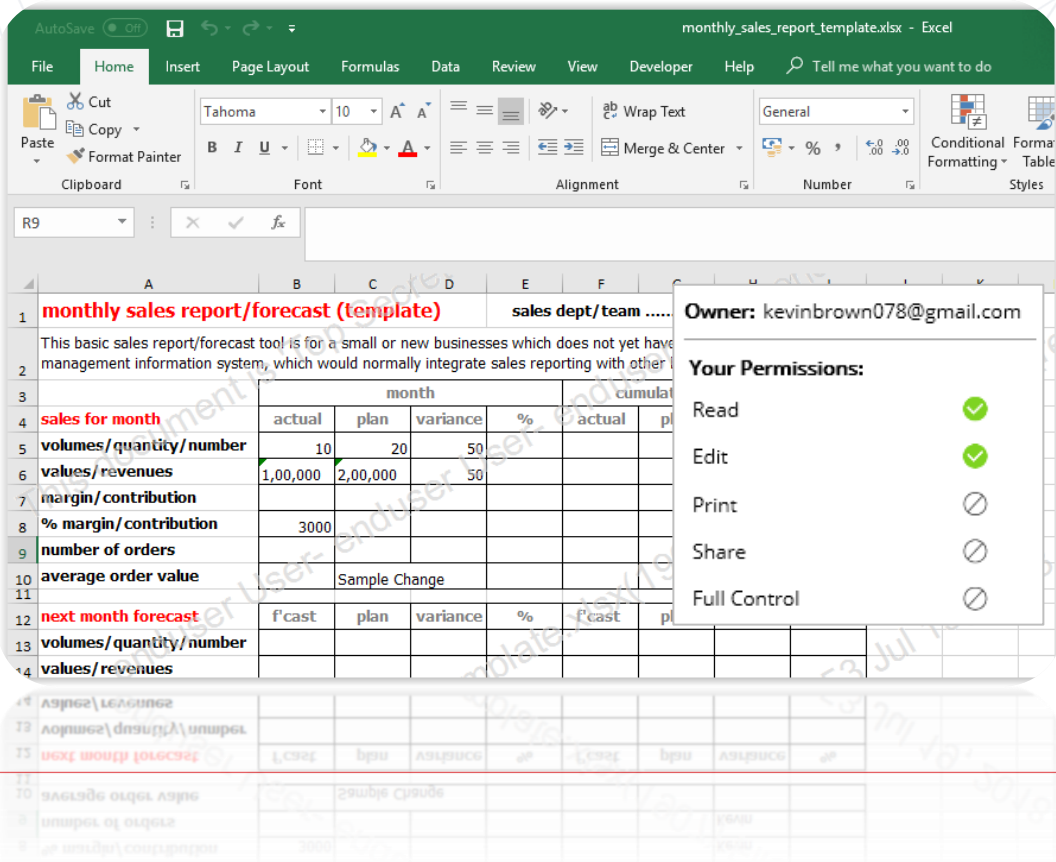
How it Works: Policy Federation

Read + Edit
in SharePoint

Or Member Role
in Team

Enforce Read + Edit
even outside SharePoint

How it Works: Policy Federation

~~Read + Edit in SharePoint~~

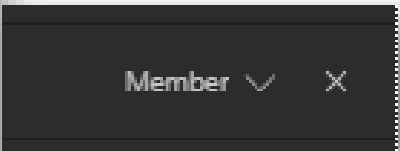~~Or Member Role in Team~~

Document: Check Permissions

Check Permissions
To check permissions for a user or group, enter their name or e-mail address.

User/Group:
Anna Thompson x

Permission levels given to Anna Thompson (i:0#.f|membership|at@mysiteam.com)

Edit   Given through the "Test - Wumpus Members" group.

Member ⌄ ✕

~~Revoke access automatically~~
~~even outside SharePoint too!~~

Before Read + Edit on the downloaded copy

SECLORE IRM

No access

Sorry you don't have access to
SalesProjections.xlsx

You can request access from the File owner
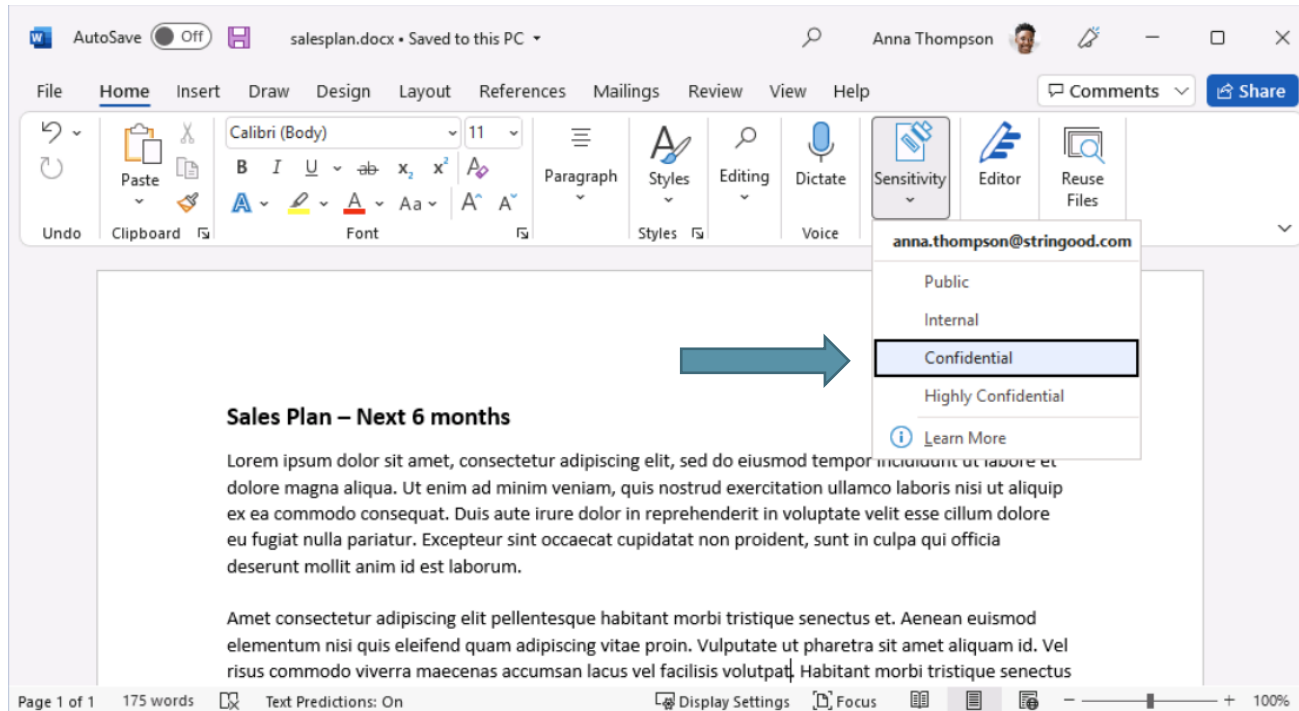Chiranjeev Sethi (chiranjeev.sethi@seclore.com)

Add a note...

Request access

Seclore for
Microsoft Sensitivity Labels
Office & Mail

How it Works: Label-based Protection - Office

User classifies the document,
saves and closes the file

How it Works: Label-based Protection - Office

User classifies the document and automatically
applies protection based on the label

Seclore reads file classification and automatically
applies preset policies to the file

Label	Seclore Policy
Public	No Protection
Internal	Protection - Internal Policy
Confidential	Protection - Confidential Policy
Highly Confidential	Protection - Highly Confidential Policy

How it Works: Label-based Protection - Office

Seclore reads file classification and automatically applies protection based on the label

File is classified and Seclore protected
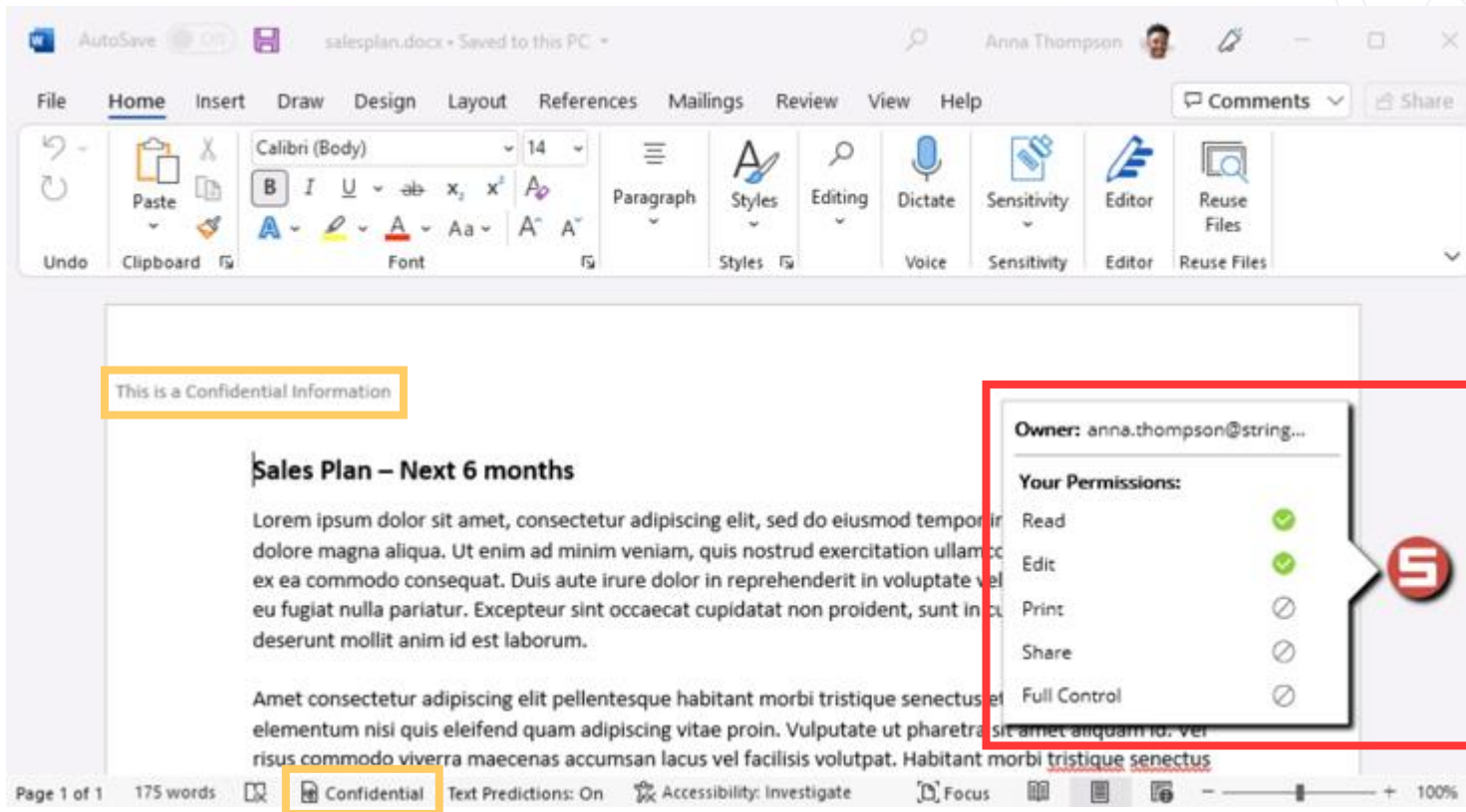
Full Interoperability
Seclore protection enforced as-soon-as users or automation classifies sensitive content
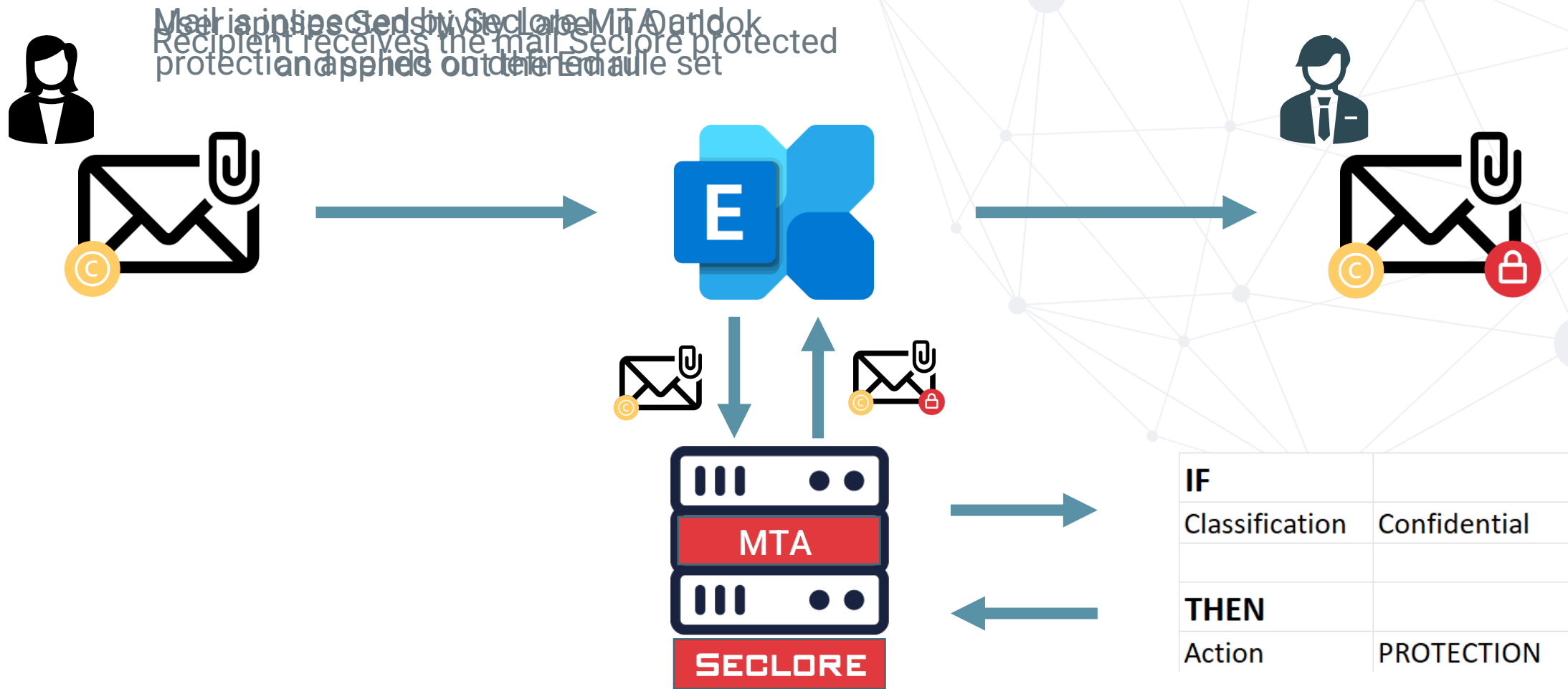
Full Security
Seclore offers flexibility to host the system on-cloud or on-prem. Gain control of your keys, server and metadata

Seamless User Experience
Users can access secured documents directly in their desktop applications or in Seclore's Agentless browser-based Editor

How it Works: Label-based Protection - Mail

Mail is inspected by Seclore MTA
User applies Sensitivity Label Outlook
Recipient receives the mail Seclore protected
protection and appends outside Email rule set

IF	
Classification	Confidential
THEN	
Action	PROTECTION

Automation	**Automatic Protection** once Uploaded to SharePoint , Teams Automatic Policy Federation from Microsoft 365
Any-ness	Automatic Protection of **Any File**
Ease of Use	Agentless Browser Based File Access Desktop/Native File access for Office and PDF on Windows Minimal Admin Overheard through Policy Federation
Security	Security inside Microsoft 365 On-Premise and On-Cloud support Policy Federation
Lower TCO	**Minimal Admin Overhead** for Policy Management Agentless access eliminates need to have MS App Licenses

Thank You