



Education Tech Summit 2021
- Security & Compliance med Office 365

Sikkerhed & compliance for uddannelsesinstitutioner med Microsoft Office 365

Agenda

- Er Security & Compliance vigtig for uddannelsesinstitutioner?
- Overblik over Microsofts Security & Compliance features
- anbefalinger til at øge sikkerheden og sikre optimal databeskyttelse
- Værktøjer til at komme i gang

Security

PROTECTING YOUR
VALUABLE ASSETS



45

Er digital sikkerhed nødvendig for skoler?

22-09-2020

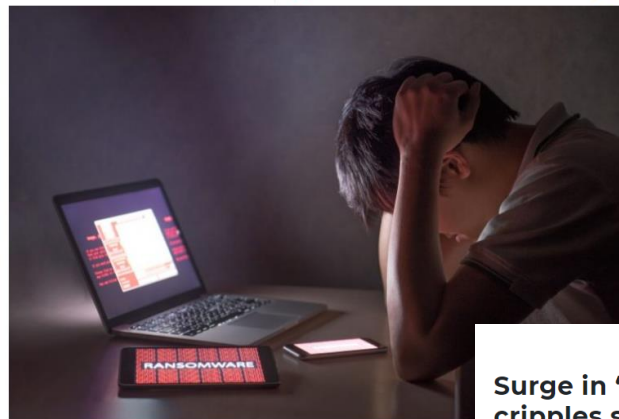
Stor stigning i cyberangreb på skoler



Hackerne ser studerende, der vender tilbage til virtuelle lektioner som enkle kan omfatte ondsindet phishing, såkaldte "Zoombombs" og endda ransomware.

Hvorfor skete der cyberangreb i Baltimore County skoler?

I Zaib December 7, 2020 Computer Security Danish



50 britiske skoler inficeret med ransomware



...ket ude af deres mail-konti, efter ondsindede hackere har inficeret systemerne med

News

Surge in 'devastating' ransomware attacks cripples schools

James Carr

Alert: Further targeted ransomware attacks on the UK education sector by cyber criminals

The NCSC is responding to further targeted ransomware attacks on the education sector by cyber criminals.

School cyber-attack affects 40,000 pupils' email

© 29 March



“The challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. In nearly all cases, it is the user – not the cloud provider – who fails to manage the controls used to protect an organization’s data.

‘Through 2022, at least 95% of cloud security failures will be the customer’s fault.’”

Microsoft Security

1/4

Only a quarter of Microsoft customers are actively using the security products they've purchased

Microsoft 365 Security & Compliance features

Office 365 data loss prevention for Exchange Online, SharePoint Online, and OneDrive for Business

Communication Data Loss Prevention for Teams

Compliance Manager

Office 365 Cloud App Security

Office 365 Message Encryption

Azure Active Directory Identity Protection

Double Key Encryption for Microsoft 365

Microsoft Defender for Identity

Records Management

Information barriers

Advanced Audit

Microsoft Graph APIs for Teams Data Loss Prevention (DLP)

Communication Compliance

Microsoft Defender for Endpoint

Insider Risk Management



Office 365 Customer Key

Microsoft Cloud App Security

Azure Active Directory Identity Governance

Office 365 Customer Lockbox

Microsoft 365 data classification analytics: Overview Content & Activity Explorer

Conditional Access policies

Microsoft Defender for Office 365

Information Protection

Information Governance

Privileged access management in Office 365

Microsoft Security technology



Identity and access management

Secure access for a connected world



Threat protection

Stop sophisticated attacks



Information protection

Protect sensitive data



Device Management

Safeguard your devices and applications

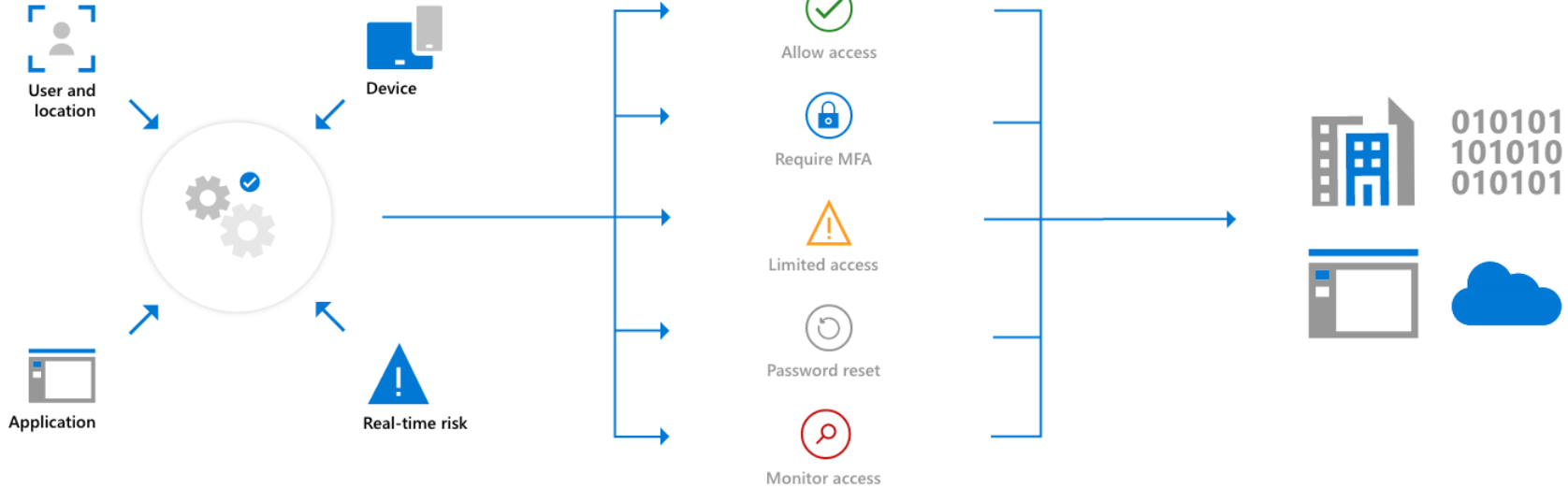


Azure AD Conditional Access

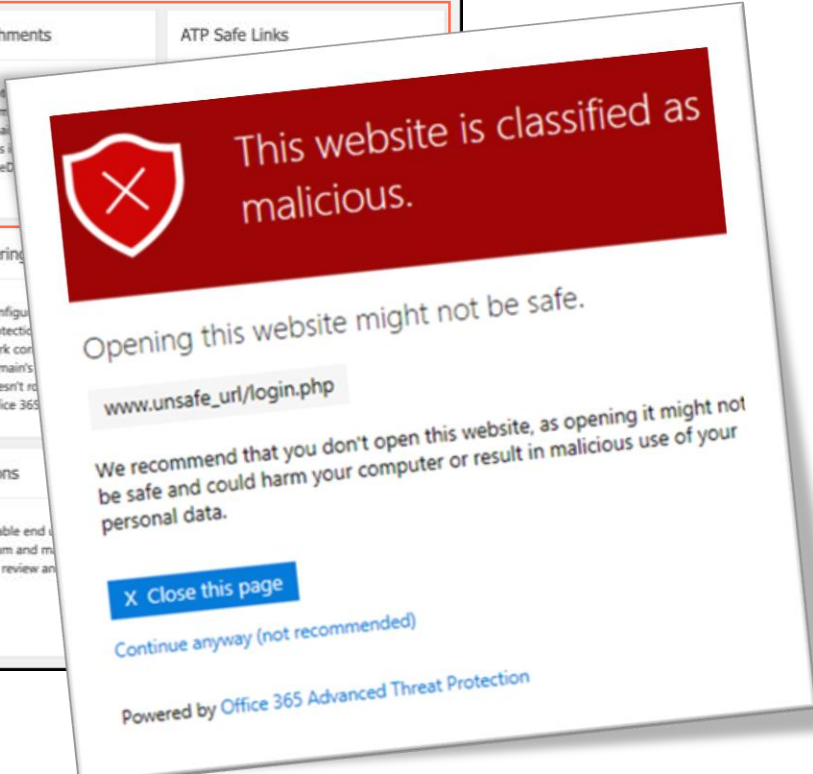
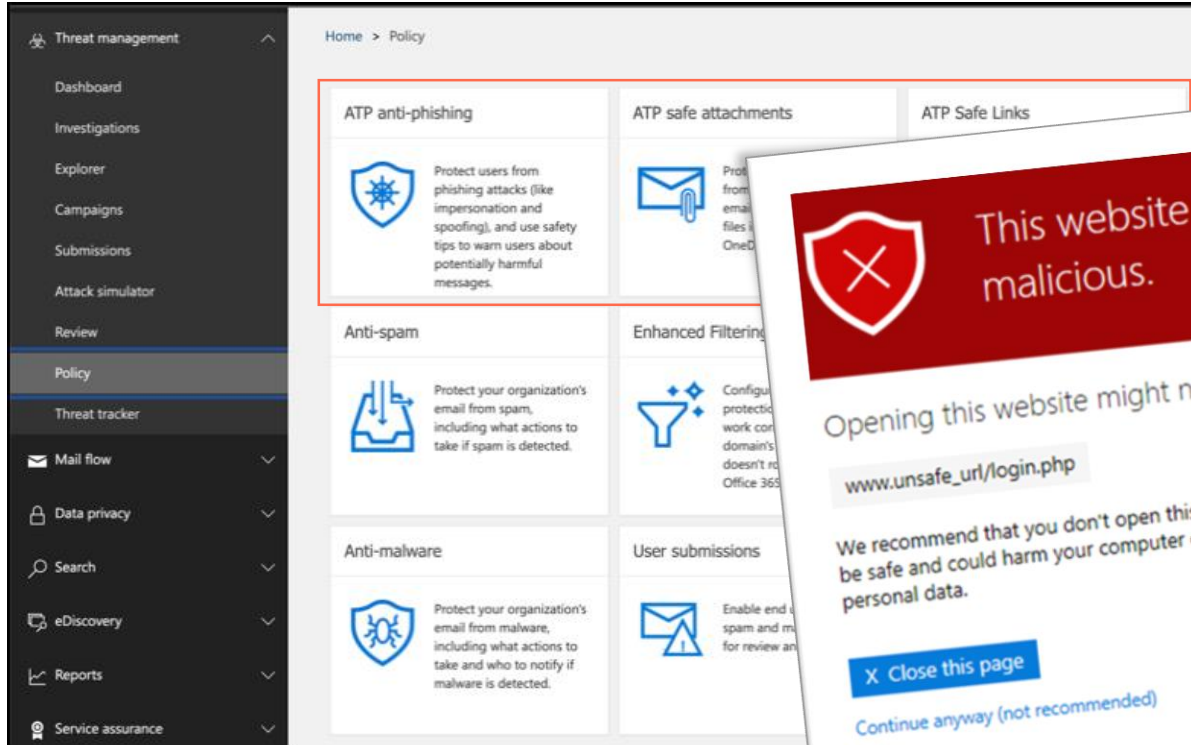
Signals

Verify every access attempt

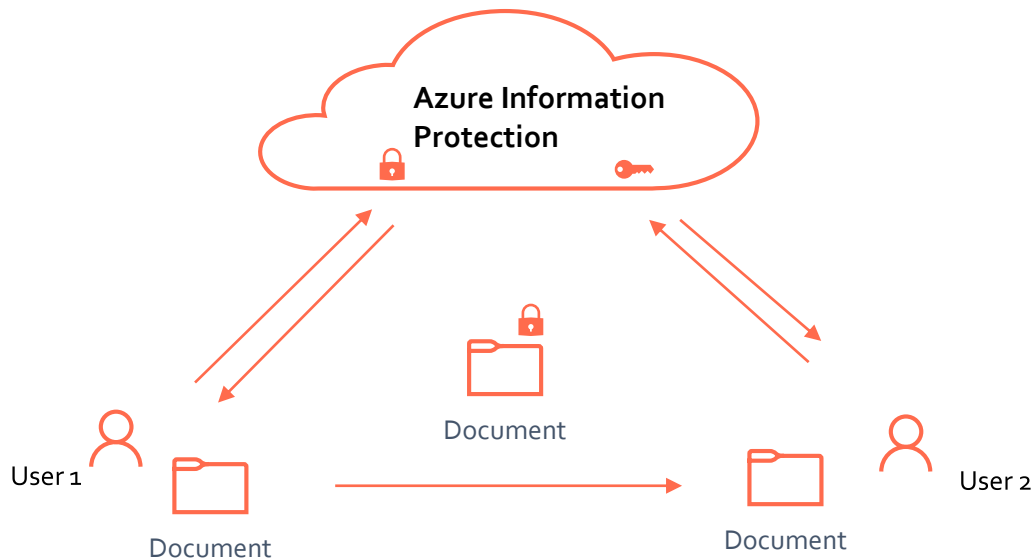
Apps and Data



Microsoft Defender for Office 365



Azure Information Protection



Classification & Labeling: "Highly Confidential"
Encryption
Tracking
Revocation

Azure Information Protection

Classification & Labeling:

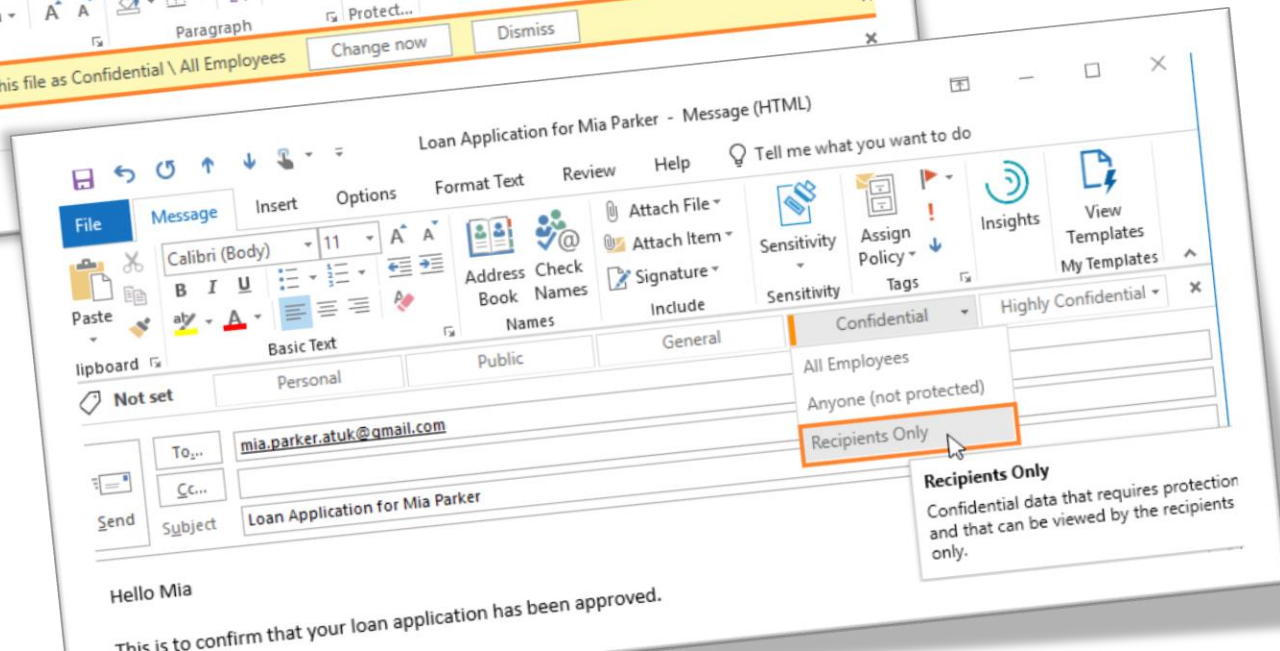
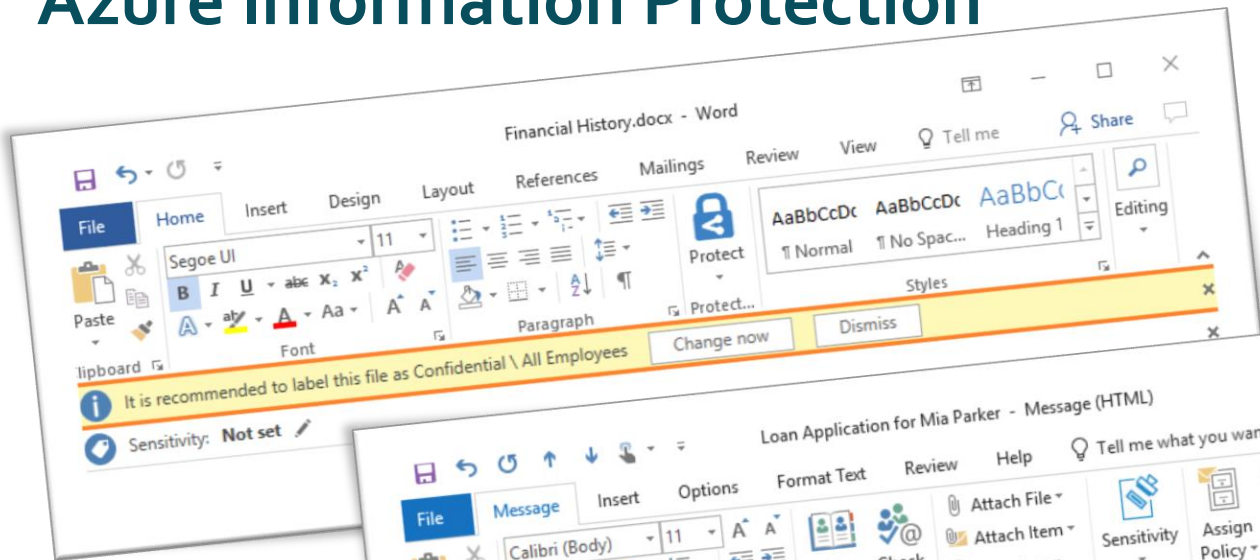
Manually classify documents based on labels like "Highly Confidential" that is associated with a certain group access

Encryption: The encryption follows classification labels

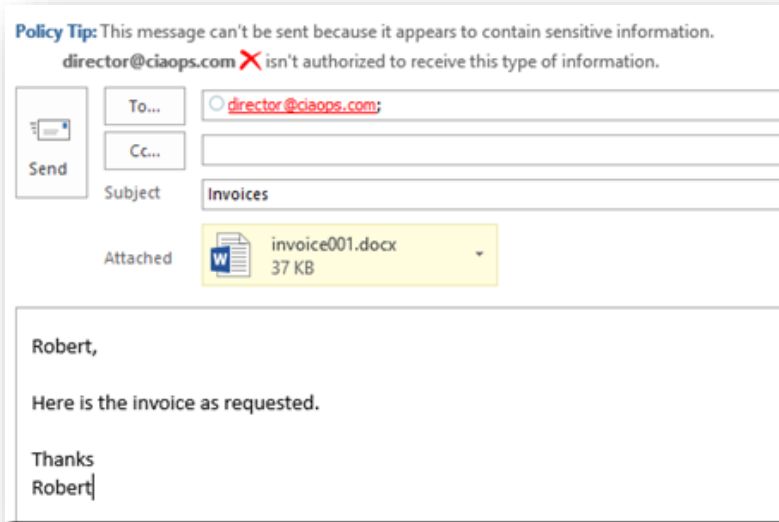
Tracking: who/where document is accessed

Revoke access previously granted

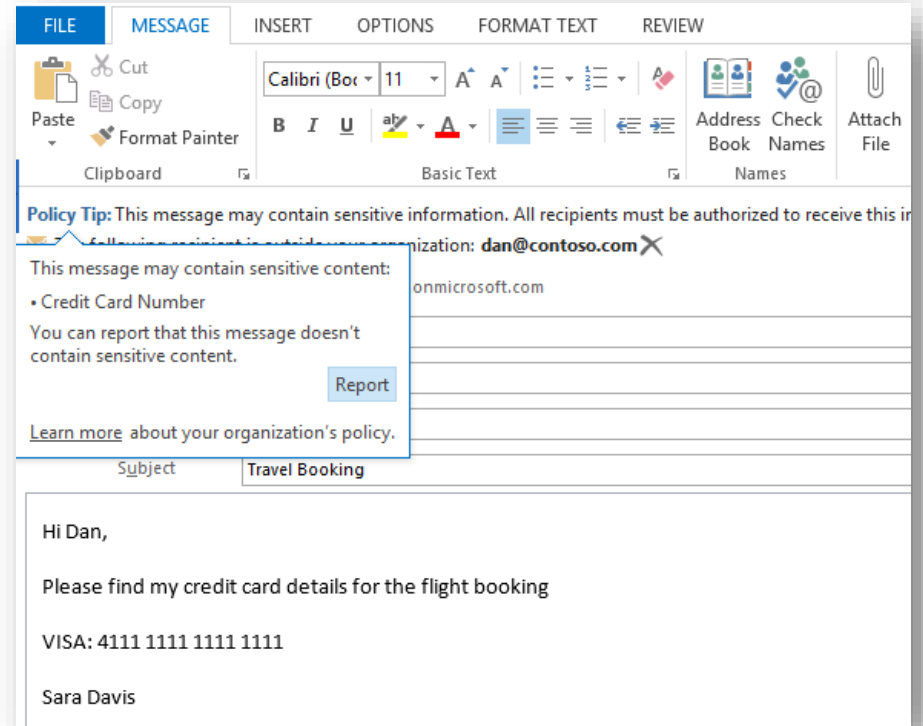
Azure Information Protection



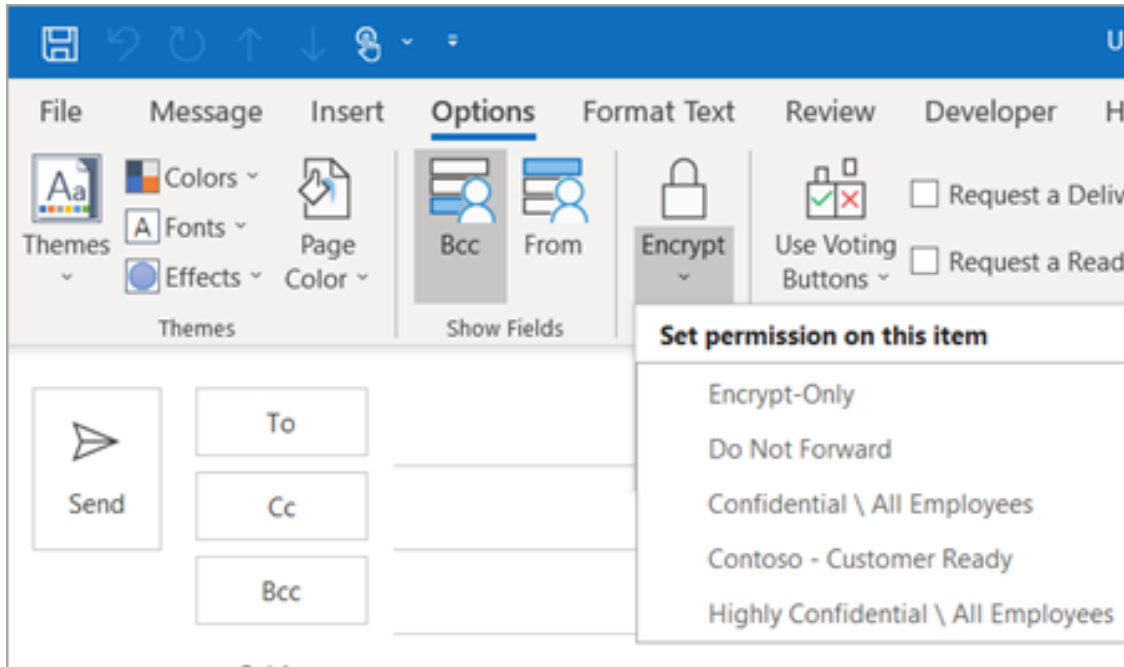
Data Loss Prevention



The DLP feature in Office 365 will automatically classify data and use the set policies to stop an email from being sent and block unauthorized access to classified content.



Office Message Encryption

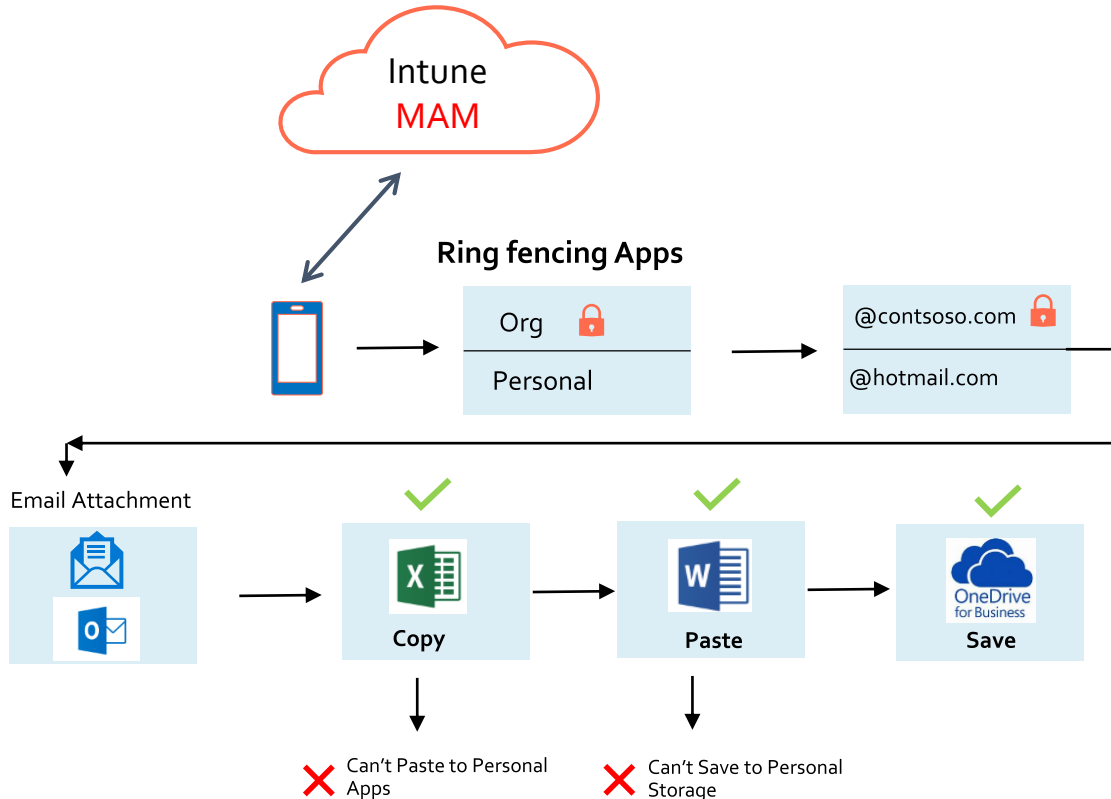


When you need to protect the privacy of an email message, encrypt it.

Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading.

Any recipient without the corresponding private key, however, sees indecipherable text.

Intune – Mobile Application Management



Intune MAM does two things without requiring Device Enrollment:

1. Separates company managed apps from personal apps, and set policies on how data is accessed from managed apps
2. Ensures corporate data cannot be copied and pasted to personal apps within the device

SECURE SCORE

Microsoft Security

93%

of all breaches could have been avoided if basic cyber hygiene had been in place¹

Next step: Strengthen your security posture

VISIBILITY AND GUIDANCE WILL HELP YOU TAKE FULL ADVANTAGE OF YOUR SECURITY PLATFORM

Com Report metrics and trends to leadership and propose future improvements

Your Secure Score zone

Secure Score: 42%

Score zones are customized based on your organization's goals and definitions of each score range.

■ Bad (<10%)
 ■ Okay (10%-30%)

▲ 1/3 ▼

[Edit score zones](#)

Comparison trend

How your organization's Secure Score compares to others' over time.

■ Your score
 ■ Organizations like yours
 ■ Custom comparison

[Manage comparisons](#)

Regression trend

Timeline of points that have regressed due to configuration, user, or device changes.

■ Points regressed

[View current regressed actions](#)

[View related history](#)

Score changes

▼ **8% decrease**

Changes	Points
Points achieved	▲ 80
Points regressed	▼ 16

[View history](#)

Microsoft Compliance technology



Information Protection & Governance

Protect and govern data wherever it lives



Insider Risk Management

Identify and take action on critical insider risks



Discover & Respond

Quickly investigate and respond with relevant data



Compliance Management

Simplify compliance and reduce risk



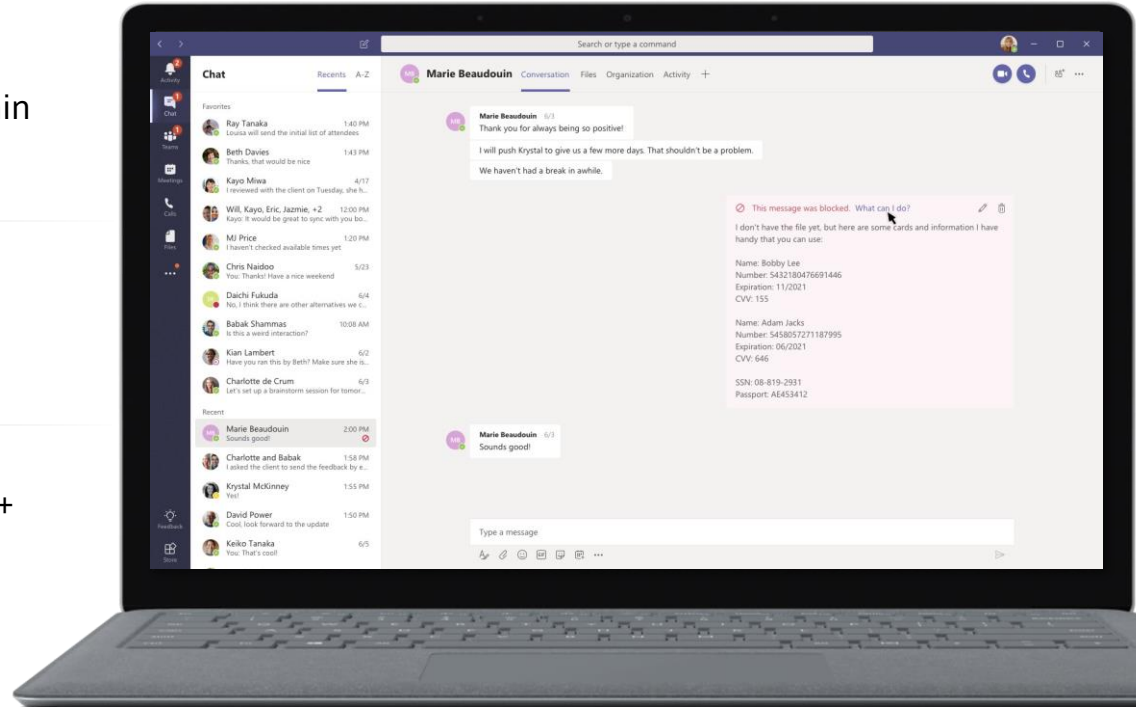
Data Loss Prevention for Microsoft Teams

PREVENT SHARING SENSITIVE INFORMATION IN A CHANNEL OR CHAT SESSION

Automatically block messages which contain sensitive information

Educate and guide end-users with notifications and “policy tips”

Unified classification engine supporting 90+ sensitive information types and custom sensitive info type creation



Microsoft Information Governance

INTELLIGENT AND BUILT-IN DATA AND RECORDS MANAGEMENT

In-place management

Retain data and manage records where your users collaborate

Automated policy

Classify and govern data at scale with pattern recognition and trainable classifiers

Ongoing data ingestion

Manage chats, social, and collaboration data beyond Microsoft with high-fidelity import

Enhanced defensibility

Demonstrate compliance with proof of disposals, defensible disposition, and rich audit trails

Information Governance

Keep what you need and delete what you don't



Records Management

Manage high value content and meet recordkeeping obligations



Insider Risk Management

IDENTIFY AND TAKE ACTION ON CRITICAL INSIDER RISKS

Rich insights via tailored templates

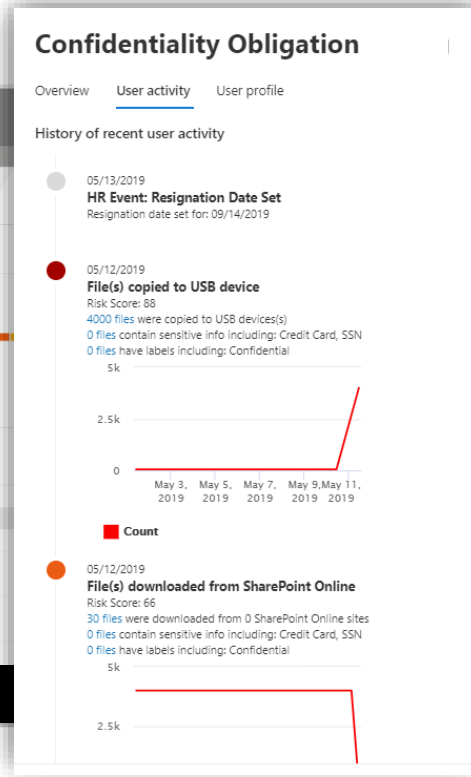
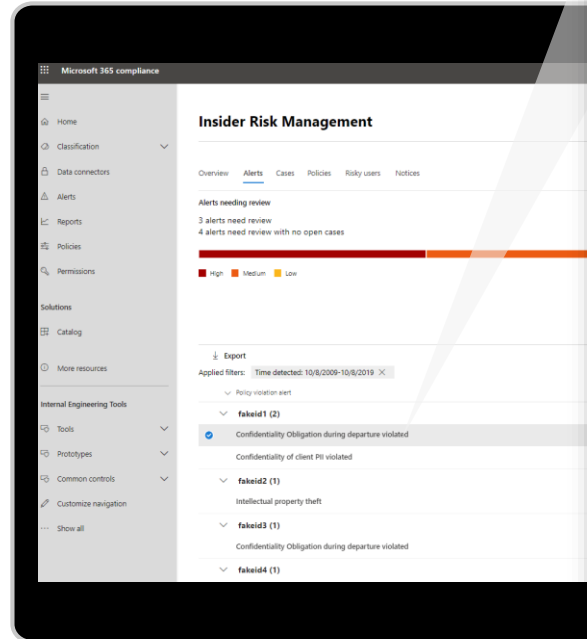
Machine learning correlates native and third-party signals to identify insider risks

Privacy built-in

Anonymity controls ensure data about risks is appropriately managed

End-to-end investigations

Integrated investigation workflows allow for collaboration across IT, HR, and legal



Communication Compliance

QUICKLY IDENTIFY AND REMEDIATE CORPORATE CODE-OF-CONDUCT POLICY VIOLATIONS

Intelligent customizable playbooks

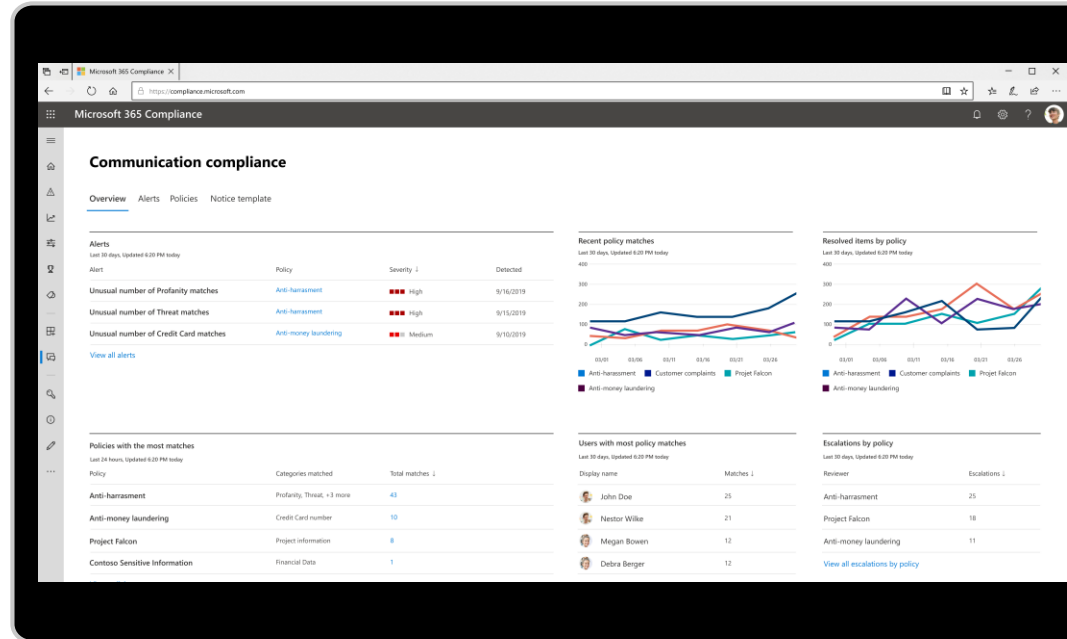
Leverage machine learning to detect violations across Teams, Exchange and third-party content

Flexible remediation workflows

Remediation workflows to quickly act on violations

Actionable insights

Interactive dashboard with policy violations, actions, and trends



Advanced eDiscovery

QUICKLY FIND AND RESPOND WITH ONLY THE RELEVANT INFORMATION

Custodian Management and Communications

Preserve content by custodian, send hold notifications and track acknowledgements

Deep crawling and indexing

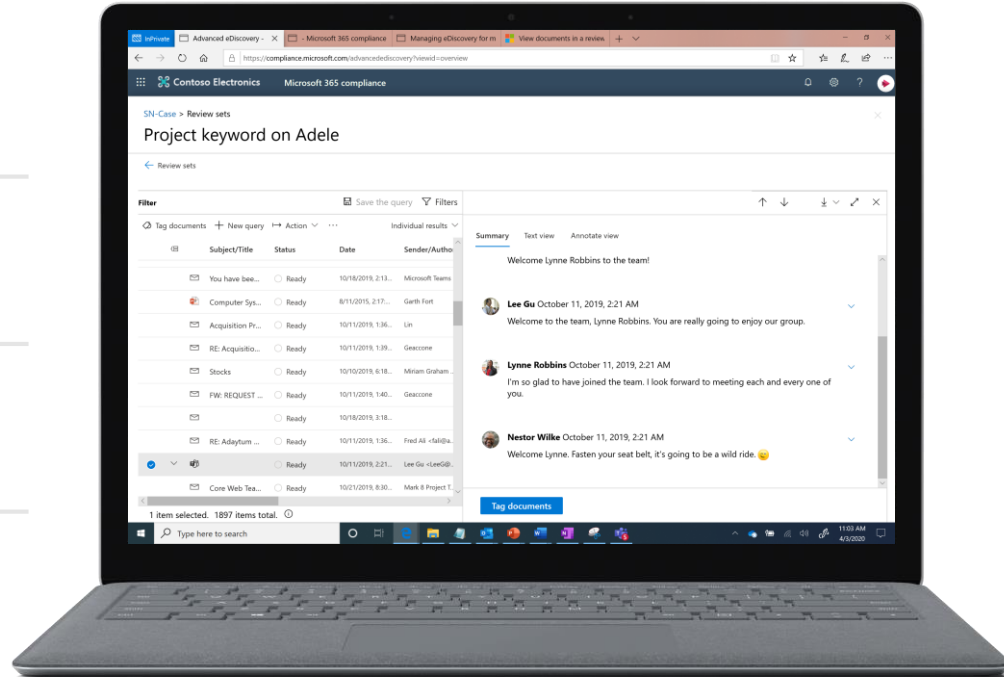
Deep processing (e.g., much higher size limits, non-Microsoft file types) to extract and index text and metadata

Review and manage case data

Manage static sets of documents within a case, that can be independently searched, analyzed, shared, and acted upon

Cull your data intelligently with ML

Near duplicate detection, email threading, themes, and ML models to identify potential high value content



Microsoft Compliance Manager

SIMPLIFY COMPLIANCE AND REDUCE RISK

Continuous assessments

Detect and monitor control effectiveness automatically with a risk-based score

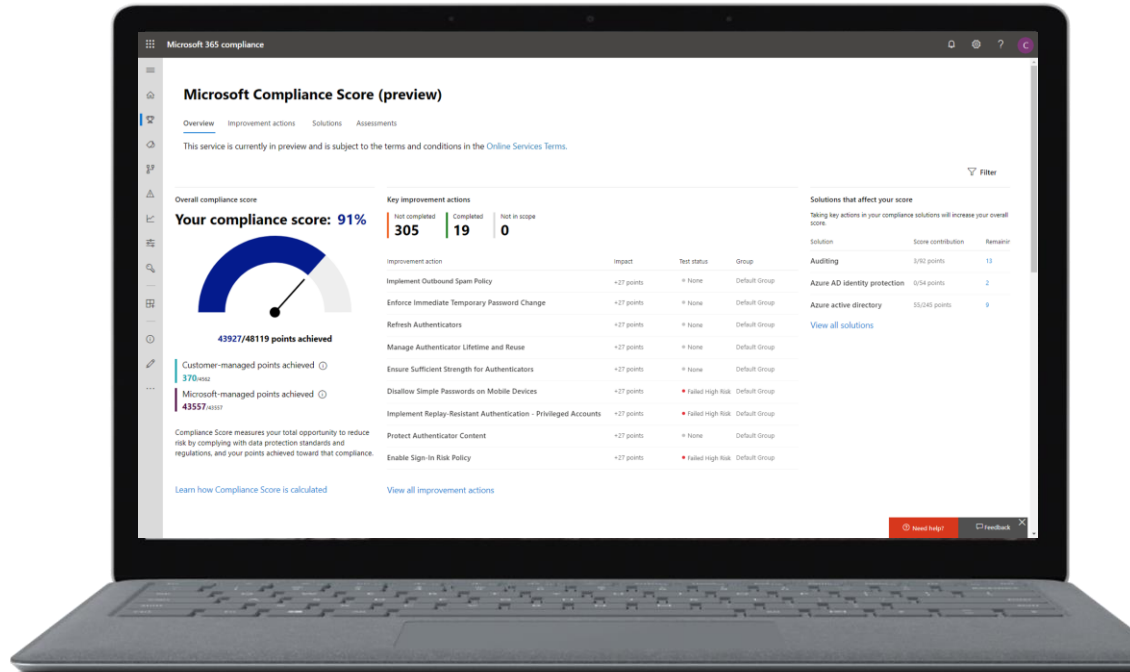
Recommended actions

Reduce compliance risks with actionable guidance

Built-in control mapping

Scale your compliance efforts with built-in mapping across regulations and standards

Compliance Score is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Microsoft 365 Education licenseroverblik

Office 365

Audit Logging & Alerting	Data Loss Prevention	Delve	eDiscovery	Exchange Online Plan 1+	Exchange Online Protection
Information Protection (Office 365)	Kaaba Pro (testing)	Microsoft Forms	Microsoft Link	Microsoft Teams	Microsoft To-Do
Microsoft Whiteboard	Office for the Web	Office Mobile Apps	OneDrive for Business Plan 2	OneNote Class Notebook	Planner
PLC Groups	Power Apps for Office 365	Power Automate for Office 365	Retention Policy	School Data Sync	SharePoint Online Plan 1+
Steps for Business Plan 2 (testing)	Stream for Office 365	Sway	Yammer Academic		

Bookings	Exchange Online Plan 2	Use Events	Microsoft 365 Apps for Education	Microsoft Dynamics for Teams	Office 365 Cloud App Security
Power Virtual Agents for Teams	SharePoint Online Plan 2				

Microsoft 365 A5 Security

Application Guard for Office (preview)	Defender for Endpoint (Mac)	Safe Documents
--	-----------------------------	----------------

Anti-Phishing
Safe Attachments

Microsoft Defender for Office 365 Plan 1

Safe Links		
Attack Simulator	Automated Investigation & Response	Campaign Views

Compromised User Detection	Threat Explorer	Threat Trackers
----------------------------	-----------------	-----------------

Microsoft Defender for Office 365 Plan 2

Microsoft 365 A5 Compliance

Information Protection & Governance	Insider Risk Management	eDiscovery & Audit
Endpoint DLP	Insider Risk Management	
Trainable Classifiers (preview)		

Advanced Message Encryption	Customer Key	Compliance	Advanced Audit	Audio Conferencing
Double Key Encryption	Information Governance	Customer Lockbox	Advanced eDiscovery	MyAnalytics (Full)
Records Management	Rule-Based Classification (Office 365)	Information Barriers		Phone System
Teams Data Loss Prevention		Privileged Access Management		Power BI Pro

Office 365

Enterprise Mobility + Security (EMS)

Azure AD for Office 365	Intune for Education
-------------------------	----------------------

Active Directory RMS	Advanced Threat Analytics (testing)	Advanced Security Reports & Alerts	App Proxy, including PingAccess	Azure AD B2B (previously partner access)	Azure AD Connect Health
Azure SMS	Information Protection	Azure AD Password Protection	Cloud App Discovery	Conditional Access	Enterprise State Roaming
Microsoft Endpoint Config Manager	System Center Endpoint Protection	Microsoft Identity Manager	Multi-Factor Auth (MFA)	Self-Service Password Reset in AD	Self-Service Group Management
Windows Server CAL Rights		Shared Account Password Roll-Over	Single-Sign-On to other SaaS	Terms of Use	3 rd Party SSOA Integration

Azure AD Premium Plan 1

Microsoft Defender for Identity	Microsoft Cloud App Security
---------------------------------	------------------------------

Access Reviews	Azure Identity Protection	Privileged Account Management
Privileged Identity Management	Risk-Based Conditional Access	Self-Service Password Reset

Azure AD Premium Plan 2 (includes Plan 1 features)

Microsoft Cloud App Security	Rule-Based Classification (ADP Client & Scanner)
------------------------------	--

Enterprise Mobility + Security (EMS)

Windows 10

Application Control	Application Guard	Azure AD & Domain Joints	BitLocker & BitLocker to Go	Conditional Access	Cortana
Edge for Business	MDM	Microsoft Defender Antivirus	Microsoft Store for Business	Voice, Pen, Ink, and Gesture	Windows Autopilot
Windows Firewall	Windows Hello for Business	Windows Information Protection	Windows Update for Business		

Always On VPN	AppLocker	App Assure	App-V	BranchCache	Credential Guard
Desktop Analytics	Device Guard	DirectAccess	Long Term Servicing Channel	MDOP	Persistent Memory
Resident File System (RFS)	SMB Direct	Unified Write Filter	Universal Print	User Experience Index	Windows to Go

Advanced Hunting	Automated Investigation & Response	Block at First Sight
Cloud App Security Integration	Defender for Endpoint (Android)	Defender for Endpoint (iOS)
Endpoint Detection & Response	Evolution Lab	Microsoft Threat Explorer

Windows 10

Velkommen til sikkerdigital.dk

Din guide til en sikker digital hverdag

[Borger](#)

[Virksomhed](#)

[Myndighed](#)

På sikkerdigital.dk har Digitaliseringsstyrelsen og Erhvervsstyrelsen samlet vigtig viden om informationssikkerhed. Du finder råd og vejledning, hvad enten du er borger, virksomhed eller myndighed.



Tusind tak for jeres deltagelse!

Nogle spørgsmål?

