



Ignite recap Microsoft 365

Dutch Microsoft & Security Meetup 14 november 2019

@maarteneekels

Portiva.

Aangenaam :)



Portiva.



Microsoft
Regional Director



Contact

 @maarteneekels
meekels@portiva.nl
www.eekels.net

Agenda

- Security baseline for Office 365 ProPlus
- Office cloud policy service + security policy advisor
- Safe documents
- Application guard
- Sensitivity labels in SharePoint and Office web apps
- Information barriers in Microsoft Teams
- Insider risk management
- Communication compliance
- Microsoft Compliance Score
- More news

New security baseline for Office 365 ProPlus

<https://aka.ms/officesecbaseline>

 Aaron Margosis Microsoft

09-24-2019 11:09 AM

Security baseline for Office 365 ProPlus (v1908, Sept 2019) - FINAL

Microsoft is pleased to announce the *final* release of the recommended security configuration baseline settings for Microsoft Office 365 ProPlus, version 1908. Please evaluate this proposed baseline and send us your feedback through the [Baselines Discussion site](#).

This baseline builds on the overhauled [Office baseline we released in early 2018](#). The highlights of this baseline include:

- Componentization of GPOs so that “challenging” settings can be added or removed as a unit.
- Comprehensive blocking of legacy file formats
- Blocking Excel from using Dynamic Data Exchange (DDE)

Also see the announcements at the end of this post regarding the new Security Policy Advisor and Office cloud policy services.

Download the content from the [Security Compliance Toolkit](#).

The downloadable baseline package includes importable GPOs, a script to apply the GPOs to local policy, a script to import the GPOs into Active Directory Group Policy, a custom administrative template (ADMX) file for Group Policy settings, all the recommended settings in spreadsheet form and as Policy Analyzer rules. The recommended settings correspond with the Office 365 ProPlus administrative templates version 4909 released on September 5, 2019 that can be downloaded [here](#).

Componentization of GPOs

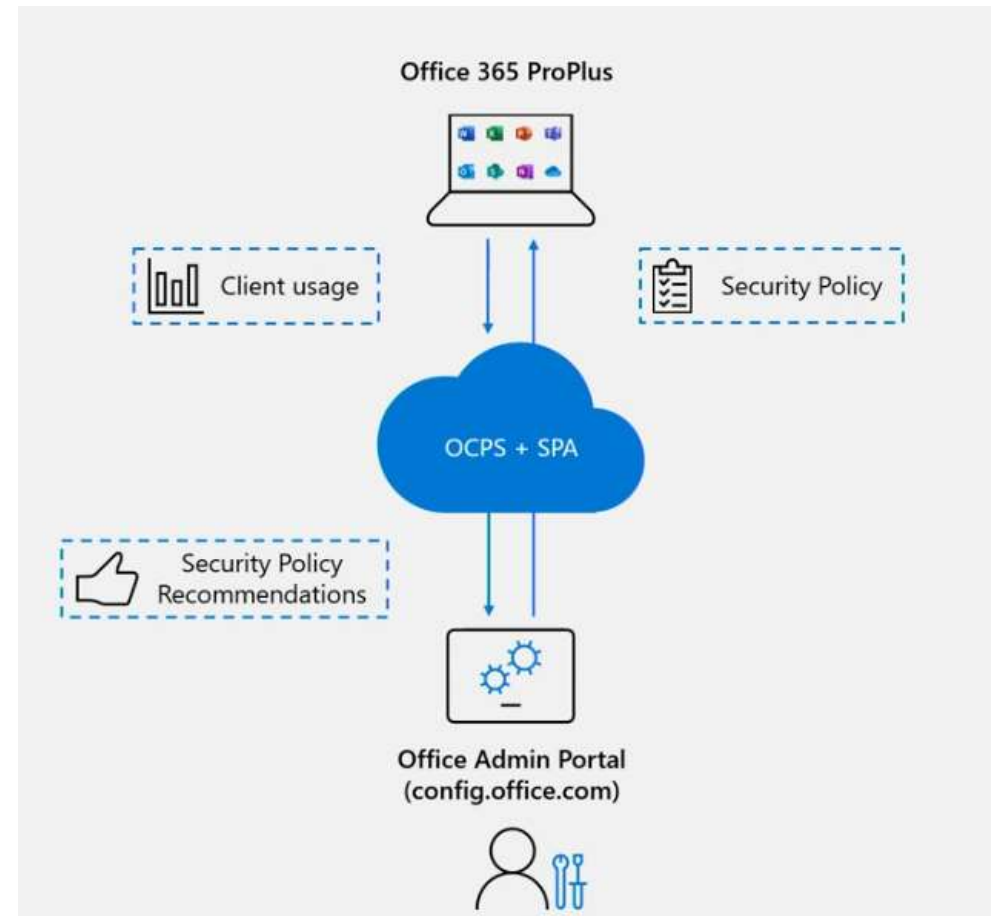
Most organizations can implement most of the baseline’s recommended settings without any problems. However, there are a few settings that will cause operational issues for some organizations. We have broken out related groups of such settings into their own GPOs to make it easier for organizations to add

Office cloud policy service + Security policy advisor

General available and public preview

<https://config.office.com>

- Roams with user
- From version 1908



DEMO




Safe Documents

Public preview

AutoSave ACHAuthoriza... - Saved Bhanu Paruchuri

File Home Insert Design Layout References Mailings Review View Help

PROTECTED VIEW This file has been verified by Microsoft Defender Advanced Threat Protection and found to be malicious.



ACH Debit Enrollment/Authorization Form

I. General Information (Please Print)

Account Holder Information Joint-Account Holder Information

First Name	First Name
Last Name	Last Name
Address	Address (if different from Account Holder)
City, State, Zip	City, State, Zip

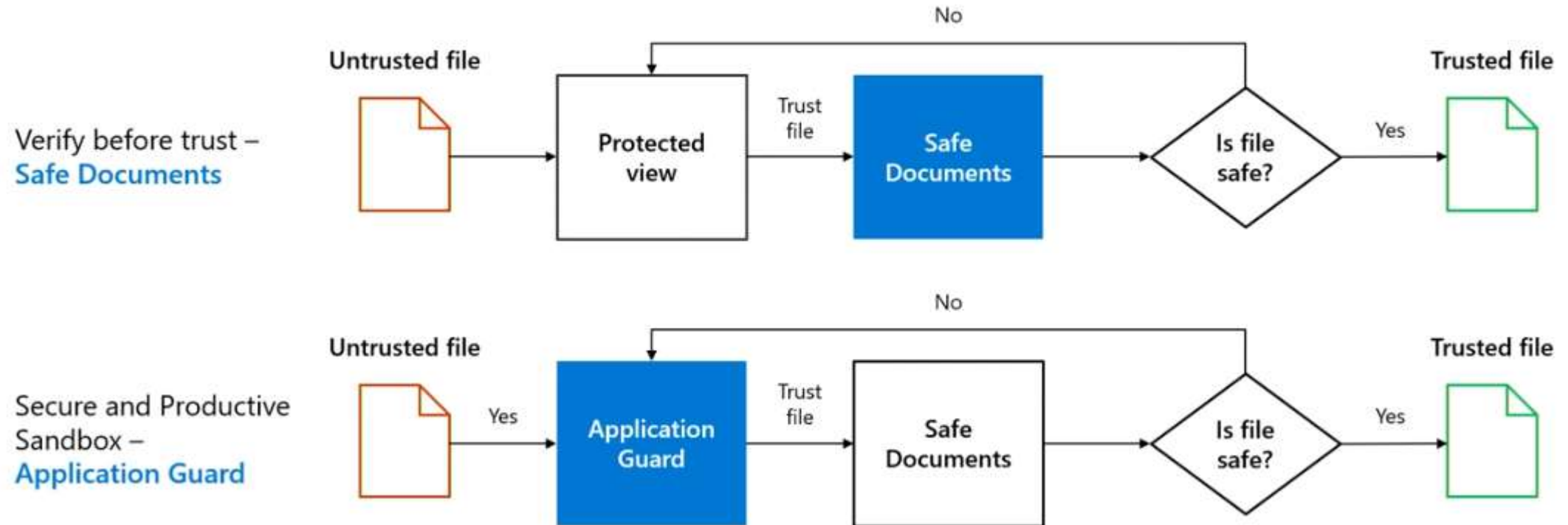
II. Name(s) of Child(ren): _____

III. Tuition Payment Plan Schedule: Debit to occur in accordance with terms set forth by the payment plan selected on the Enrollment Agreement(s).

_____ I/we authorize to debit from my/our bank account as supplied below. The amount to be debited shall be the amount set forth by the payment plan selected on the Enrollment Agreement(s).

Application Guard

Private preview



When available?

Safe Documents – Spring 2020

In preview now: <https://aka.ms/safedocspreview>

Application Guard for Office – Summer 2020

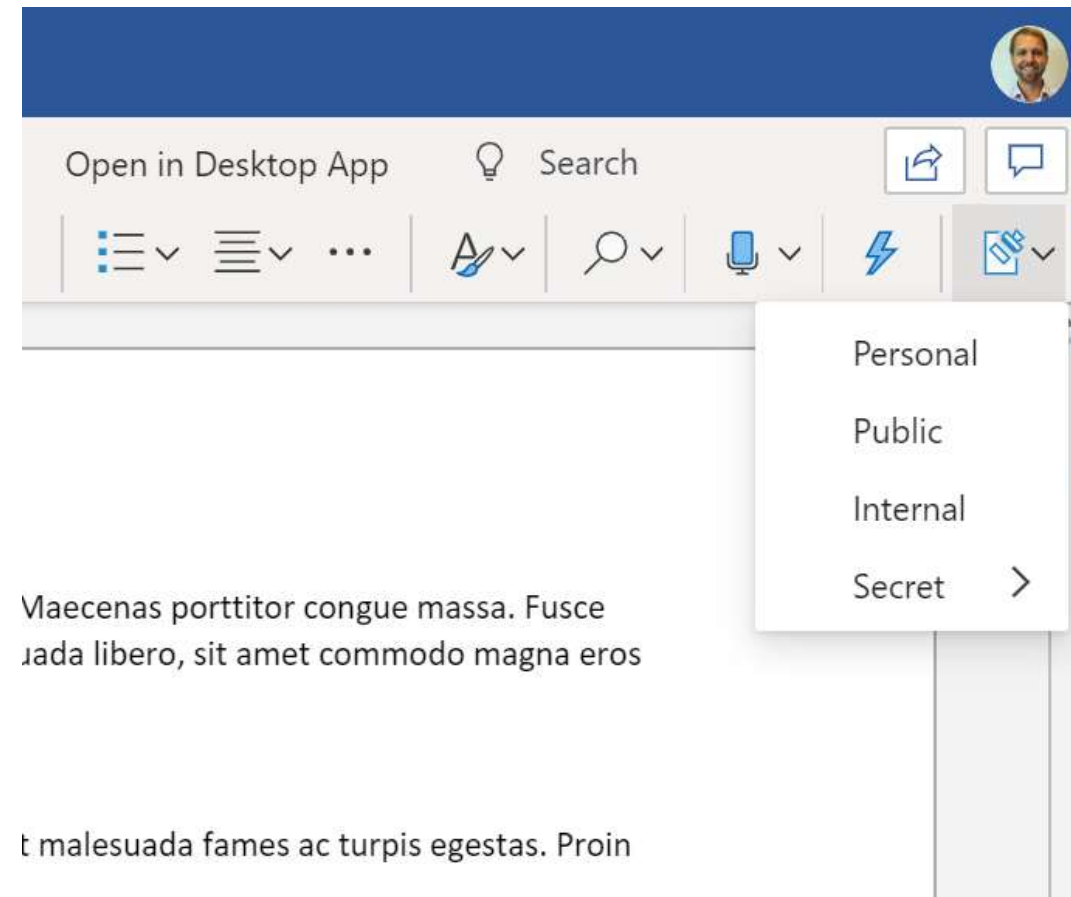
In limited preview now: <https://aka.ms/appguardpreview>

Sensitivity labels in SharePoint and Office web apps

Public preview

Set-SPOTenant -EnableAIPIIntegration \$true

<https://docs.microsoft.com/en-gb/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files>



DEMO



Information Barriers in Microsoft Teams

General available

Restrict communications between two groups to avoid a conflict of interest from occurring in your organization.

- Searching for a user
- Adding a member to a team
- Starting a chat session with someone
- Starting a group chat
- Inviting someone to join a meeting
- Sharing a screen
- Placing a call

It takes about 30 mins for policies to be applied
Or longer for large orgs (1 hour per 5000 users)

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies>

Information Barriers deployment

Give admin consent to the Information Barriers app:

```
Login-AzureRmAccount
```

```
$appId="bcf62038-e005-436d-b970-2a472f8c1982"
```

```
$sp=Get-AzureRmADServicePrincipal -ServicePrincipalName $appId
```

```
if ($sp -eq $null) { New-AzureRmADServicePrincipal -ApplicationId $appId }
```

```
Start-Process "https://login.microsoftonline.com/common/adminconsent?client_id=$appId"
```

Create segments:

```
New-OrganizationSegment -Name "Sales" -UserGroupFilter "Department -eq 'Sales'"
```

Create policies:

```
New-InformationBarrierPolicy -Name "Sales-Research" -AssignedSegment "Sales" -SegmentsBlocked  
"Research" -State Inactive
```

Apply policies:

```
Get-InformationBarrierPolicy
```

```
Set-InformationBarrierPolicy -Identity <GUID> -State Active
```

```
Start-InformationBarrierPoliciesApplication
```

Insider Risk Management

Private preview

- Obtain real-time native signals across Office, Windows and Azure, including file activity, communications sentiment and abnormal user behaviors
- Additional third-party signals from HR systems such as SAP and Workday can be integrated via connectors
- Includes configurable playbooks tailored for risks, such as digital IP theft and confidentiality breach

Insider risk management

Show in navigation

Pseudonymize On

Overview Alerts Cases Policies Users Notices

Alerts needing review

Medium 2 Low 1

Policy matches	Severity	User	Time detected
Confidentiality obligation during departure	Medium	Anony65KF-34...	2 months ago
Project Osiris Confidentiality	Medium	Anony04IS-34...	2 years ago
Anti-harrasment policy	Low	AnonyF3FD-34...	2 years ago

View all alerts

Users

Display name	Severity	Active case
AnonyIS8-978	High	Case 884: (RO) Potential IP theft
AnonyDB4-135	Low	Case 893: (FO) Potential IP theft
Anony65KF-34DF	Low	Case 448: Potential IP theft

View all users

Active cases

Active 2

Case name	Status	User	Last updated
Case 884: (RO) Potential IP theft	Active	AnonyIS8-978	a month ago
Case 893: (FO) Potential IP theft	Active	AnonyDB4-135	a month ago

View all cases

Policies with most activity

Policy name	Active alerts	Total confirmed alerts
Project Osiris Confidentiality	1	0
Confidentiality obligation during departure	1	0
Anti-harrasment policy	1	3

View all policies

Insider risk management

Show in navigation

Pseudonymize On

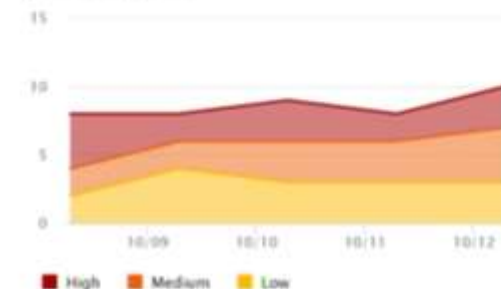
Overview Alerts Cases Policies Users Notices

Alerts needing review

3 alerts need review
3 alerts need review with no open cases



Open alerts over time



Statistics

Average time to resolve high severity alerts a day

Average time to resolve medium severity alerts a day

Average time to resolve low severity alerts a day

Export

6 items Search Filter

	Status	Severity	Time detected	Active case	Case status
Policy match alert					
Anony85KF-34DF (1) Alert: Confidentiality obligation during departure	Needs review	Medium	2 months ago	Case 254: Possible data leak	Active
Anony04J5-34PP (1) Alert: Project Osiris Confidentiality	Needs review	Medium	2 years ago		No case found
AnonyF3FD-34PK (1) Alert: Anti-harassment policy	Needs review	Low	2 years ago		No case found
AnonyI58-978 (1) Alert: Confidentiality obligation during departure	Confirmed	High	2 months ago	Case 884 (RIC) Potential IP theft	Active
AnonyDB4-I35 (1)					

Insider risk management

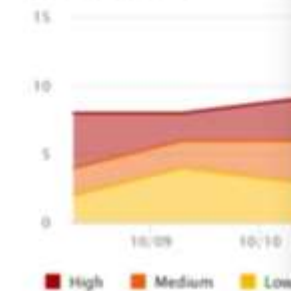
Overview Alerts Cases Policies Users Notices

Alerts needing review

3 alerts need review
3 alerts need review with no open cases



Open alerts over time



Export		Status	Severity
Policy match alert			
Anony85KF-34DF (1)			
<input checked="" type="checkbox"/>	Alert: Confidentiality obligation during departure	 Needs review	 Medium
Anony04J5-34PP (1)			
	Alert: Project Osiris Confidentiality	 Needs review	 Medium
AnonyF3FD-34PK (1)			
	Alert: Anti-harrasment policy	 Needs review	 Low
AnonyI58-978 (1)			
	Alert: Confidentiality obligation during departure	 Confirmed	 High
AnonyDB4-135 (1)			
	Alert: Confidentiality obligation during departure	 Confirmed	 Low

Alert: Confidentiality obligation during departure

Overview User activity User profile

Alert information

Status

Needs review

Time detected

2 months ago

Policy matches

Confidentiality obligation during departure

Severity

Medium

Active case

Case 234: Possible data leak

Confirm alert to an existing case

Dismiss as benign

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

Insider risk management

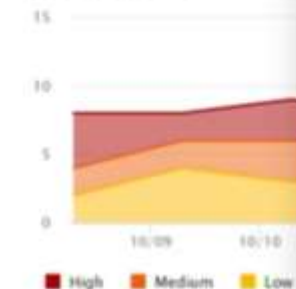
Overview Alerts Cases Policies Users Notices

Alerts needing review

3 alerts need review
3 alerts need review with no open cases



Open alerts over time



Export

Policy match alert	Status	Severity
<div>Anony85KF-34DF (1)</div> <div>Alert: Confidentiality obligation during departure</div>	Needs review	Medium
<div>Anony04J5-34PP (1)</div> <div>Alert: Project Osiris Confidentiality</div>	Needs review	Medium
<div>AnonyF3FD-34PK (1)</div> <div>Alert: Anti-harrasment policy</div>	Needs review	Low
<div>AnonyI58-978 (1)</div> <div>Alert: Confidentiality obligation during departure</div>	Confirmed	High
<div>AnonyDB4-135 (1)</div> <div>Alert: Confidentiality obligation during departure</div>	Confirmed	Low

Alert: Confidentiality obligation during departure

Overview User activity User profile

History of recent user activity

- 10/21/2019
HR Event: Resignation Date Set
Resignation date set for: Last Friday at 5:00 PM
- 10/20/2019
File(s) printed
Risk Score: 65
10 file(s) were printed
6 file(s) contain sensitive info including: ABA Routing Number
4 file(s) have labels including: Internal Only
- 10/20/2019
File(s) copied to USB device
Risk Score: 92
113 file(s) were copied to USB device(s)
47 file(s) contain sensitive info including: ABA Routing Number
54 file(s) have labels including: Internal Only
- 10/20/2019
File(s) downloaded from SharePoint Online
Risk Score: 34
113 file(s) were downloaded from 1 SharePoint Online site(s)
47 file(s) contain sensitive info including: ABA Routing Number
54 file(s) have labels including: Internal Only

Confirm alert to an existing case

Dismiss as benign

Insider risk management

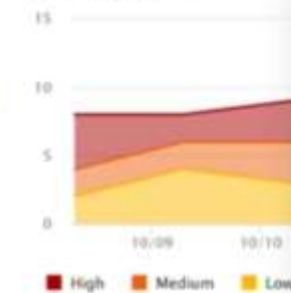
Overview Alerts Cases Policies Users Notices

Alerts needing review

3 alerts need review
3 alerts need review with no open cases



Open alerts over time



Export		Status	Severity
▼	Policy match alert		
▼	Anony85KF-34DF (1)		
✓	Alert: Confidentiality obligation during departure	Needs review	Medium
▼	Anony04J5-34PP (1)		
	Alert: Project Osiris Confidentiality	Needs review	Medium
▼	AnonyF3FD-34PK (1)		
	Alert: Anti-harassment policy	Needs review	Low
▼	AnonyI58-978 (1)		
	Alert: Confidentiality obligation during departure	Confirmed	High
▼	AnonyDB4-135 (1)		
	Alert: Confidentiality obligation during departure	Confirmed	Low

Alert: Confidentiality obligation during departure

Overview User activity User profile

Name and title

Anony85KF-34DF

User email

Organization or department

Confirm alert to an existing case

Dismiss as benign

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management**
 - Communication compliance
 - More resources
 - Customize navigation
 - Show less

Insider risk management

Show in navigation

Pseudonymize ☒ On

Overview Alerts Cases Policies Users Notices

Active cases

Active
2



Cases over time



Statistics

Average time in active
a few seconds

Export

6 items Search Filter

Case name	Status	User	Time case opened	Total policy violation alerts	Last updated	Last updated by
Case 784: Tented Case	Closed	AnonyJ4F3-53DF	a month ago	0	a month ago	Adam Arndt
Case 123: Possible HR violation	Closed	AnonyIS8-978	7 months ago	1	7 months ago	Mod Tejavaniya
Case 449: Potential IP theft	Closed	Anony8SKF-34...	7 months ago	1	7 months ago	Mod Tejavaniya
Case 342: Possible data leak	Closed	AnonyIS8-978	2 months ago	1	2 months ago	Andy Carson
Case 884: (RO) Potential IP theft	Active	AnonyIS8-978	a month ago	1	a month ago	Erin Miyake
Case 893: (FO) Potential IP theft	Active	AnonyDB4-I35	a month ago	1	a month ago	Erin Miyake

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

Insider risk management > Case > Case 893: (FO) Potential IP theft

Pseudonymize ☐ On ☒ Open investigation

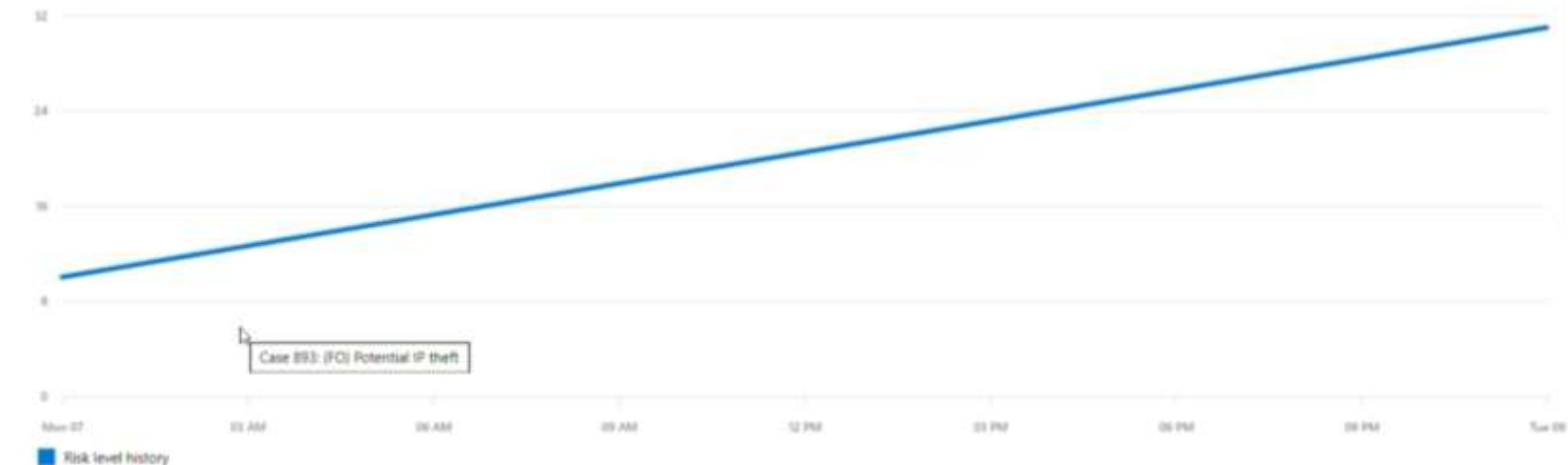
Case overview Alerts User activity Content explorer Social graph Case notes Contributors

Alerts

Policy matches	Status	Severity	Time detected
Confidentiality obligation during departure	Confirmed	Low	a month ago

[View all alerts](#)

Risk level history



Case details User details

About this case

Case name
Case 893: (FO) Potential IP theft

Case status
Active

Current risk level



Alerts confirmed
Alert: Confidentiality obligation during departure

Content at risk
Sensitivity type & labels

SharePoint & Teams

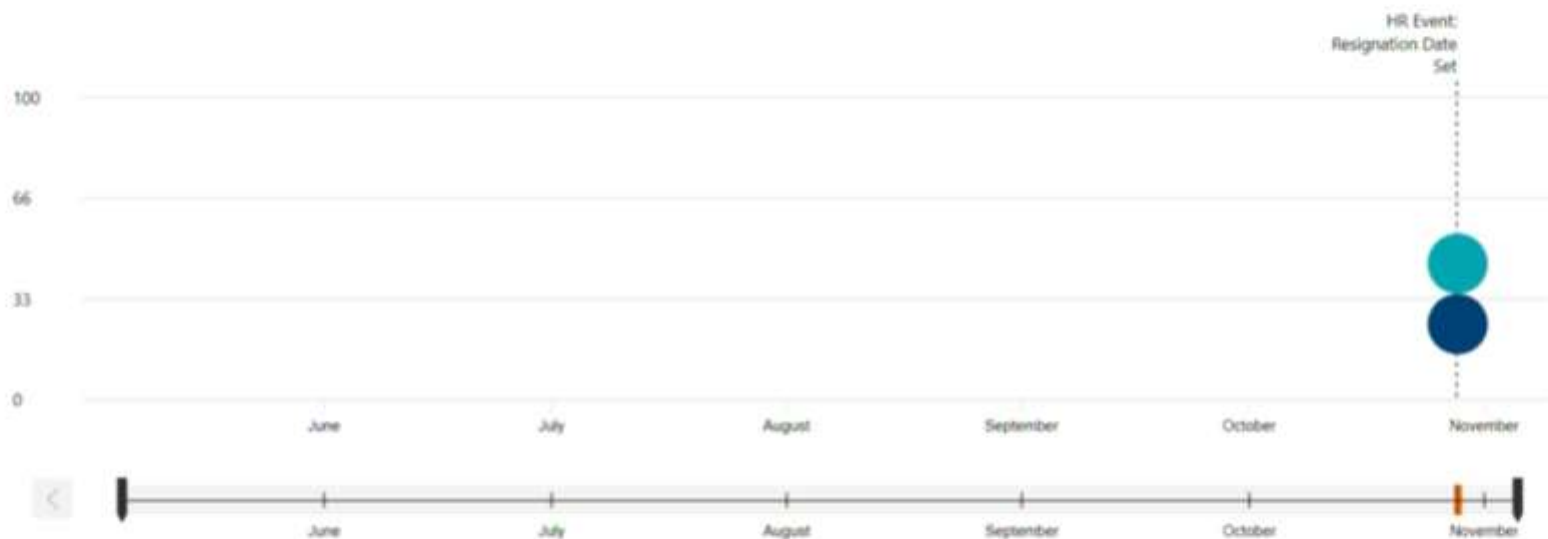
Insider risk management > Case > Case 893: (FO) Potential IP theft

Pseudonymize ☐ On ☒ Open investigation

Case overview Alerts User activity Content explorer Social graph Case notes Contributors

Export

05/05/2019 - 11/05/2019 3 risky activities Filter



10/28/2019
File(s) copied to USB device
Risk Score: 45
197 file(s) were copied to USB device(s)
0 file contains sensitive info
0 file has labels

10/28/2019

Case details User details

About this case

Case name
Case 893: (FO) Potential IP theft

Case status
Active

Current risk level



Alerts confirmed
Alert: Confidentiality obligation during departure

Content at risk
Sensitivity type & labels

SharePoint & Teams

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

Insider risk management > Case > Case 893: (FO) Potential IP theft

Pseudonymize On Open investigation Send e-mail notice Resolve case

Case overview Alerts User activity Content explorer Social graph Case notes Contributors

Export

05/05/2019 - 11/05/2019 3 risky activities Filter

33

0



- SharePoint Online (Download, Sharing)
- File(s) copied
- File(s) printed
- Email(s) sent externally
- Security tampering or harmful software
- Offensive language detected
- Others
- Compound

- 10/28/2019
File(s) copied to USB device
Risk Score: 43
197 file(s) were copied to USB device(s)
0 file contains sensitive info
0 file has labels
- 10/28/2019
File(s) downloaded from SharePoint Online
Risk Score: 25
243 file(s) were downloaded from 0 SharePoint Online site(s)
0 file contains sensitive info
0 file has labels
- 10/28/2019
HR Event: Resignation Date Set
Resignation date set for Friday at 2:17 PM

Case details User details

About this case

Case name
Case 893: (FO) Potential IP theft

Case status
Active

Current risk level



Alerts confirmed
Alert: Confidentiality obligation during departure

Content at risk
Sensitivity type & labels

SharePoint & Teams

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

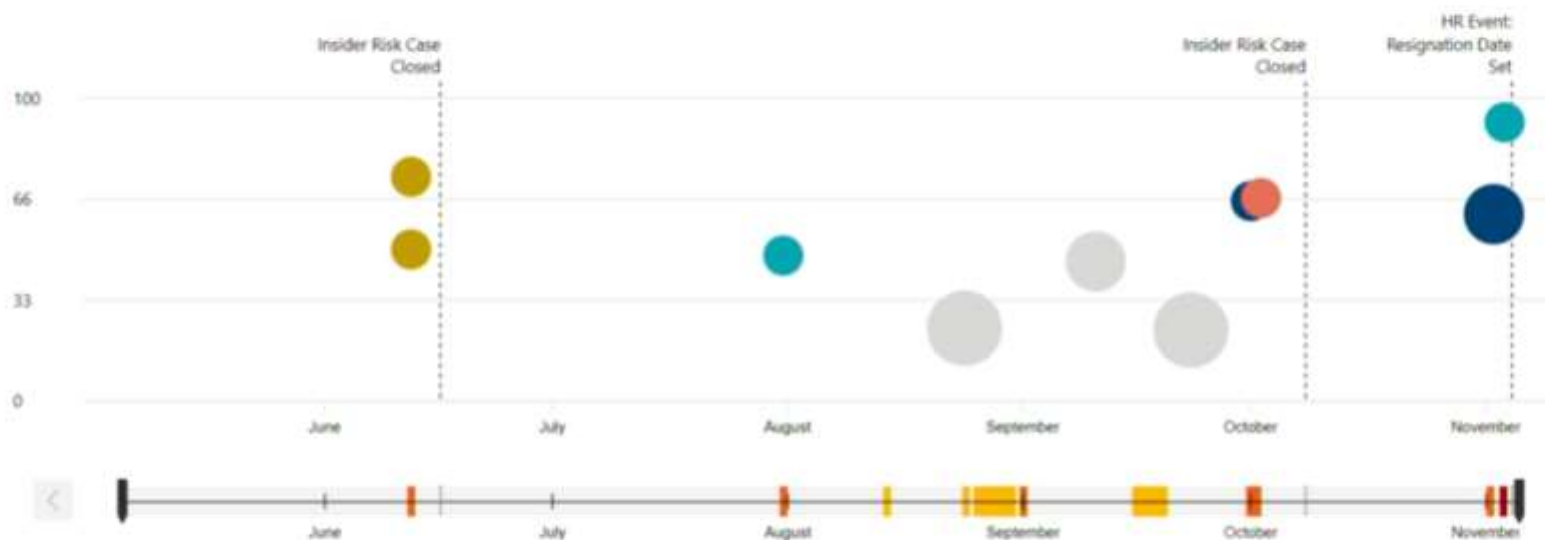
Insider risk management > Case > Case 884: (RO) Potential IP theft

Case overview Alerts **User activity** Content explorer Social graph Case notes Contributors

Pending review ☐ On ☒ Open investigation ☐ Send e-mail notice ☒ Resolve case

Export

05/05/2019 - 11/05/2019 25 risky activities Filter



SharePoint Online (Download, Sharing)
File(s) copied
File(s) printed
Email(s) sent externally
Security tampering or harmful software
Offensive language detected
Others
Compound

- Yesterday at 11:17 AM
HR Event: Resignation Date Set
Resignation date set for: 11/15/2019
- Last Sunday at 12:46 PM
File(s) copied to USB device



Alerts confirmed
Alert: Confidentiality obligation during departure

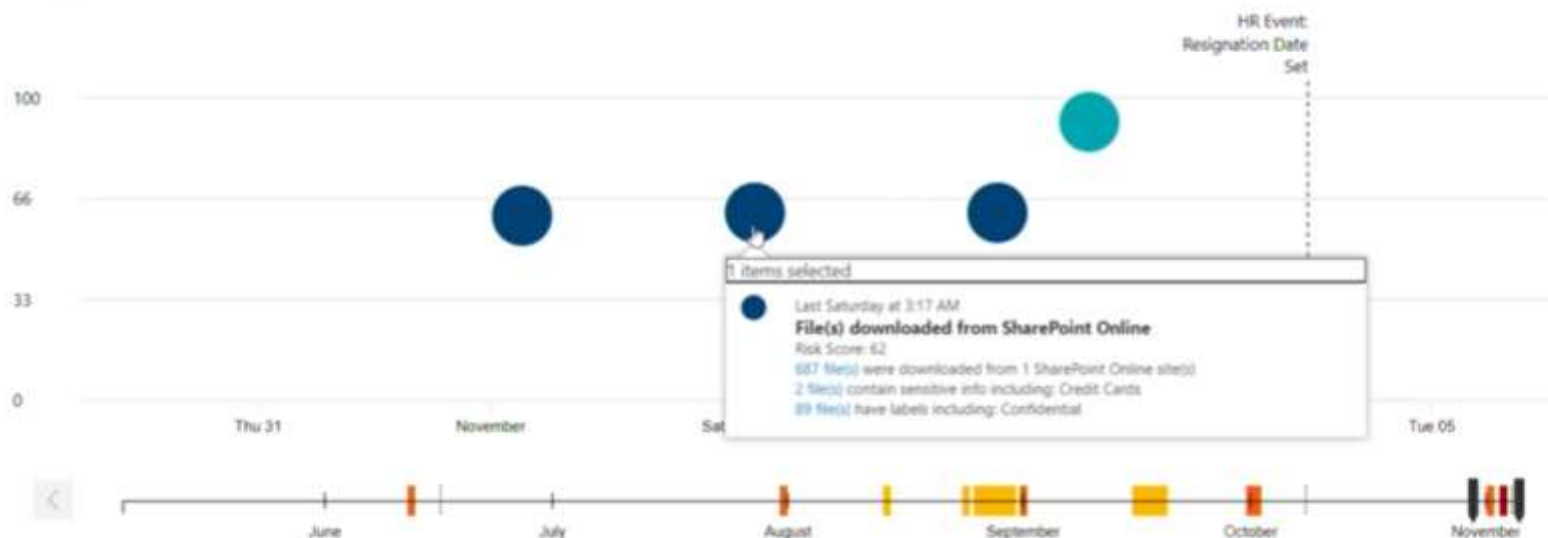
Content at risk
Sensitivity type & labels
Credit Cards
Confidential

Insider risk management > Case > Case 884: (RO) Potential IP theft

Case overview Alerts **User activity** Content explorer Social graph Case notes Contributors

Export

05/05/2019 - 11/05/2019 5 risky activities Filter



SharePoint Online (Download, Sharing) File(s) copied File(s) printed Email(s) sent externally Security tampering or harmful software
Offensive language detected Others Compound

Yesterday at 11:17 AM
HR Event: Resignation Date Set
Resignation date set for: 11/15/2019

Last Sunday at 12:46 PM
File(s) copied to USB device

Case details User details

About this case

Case name
Case 884: (RO) Potential IP theft

Case status
Active

Current risk level



Alerts confirmed
Alert: Confidentiality obligation during departure

Content at risk
Sensitivity type & labels
Credit Cards
Confidential

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

Insider risk management > Case > Case 884: (RO) Potential IP theft

Pseudonymize ☐ On ☒ Open investigation

Case overview Alerts User activity **Content explorer** Social graph Case notes Contributors

>	Subject/Title	Date	Sender/Author	File class	Bcc	Cc	Recipients	ID
	Item			Document				13d4551ae207fa...
	Project Moonshot Spec 5977.docx	10/17/2019, 11:58:00 PM	Tahuh Mir	Document				17988abe14dbf4...
	Project Moonshot Spec 5977 - draft 1.docx	10/17/2019, 11:58:00 PM	Tahuh Mir	Document				1e77a887f340331...
	Project Moonshot 2018 Jan Plan - d2.pub			Document				1f79588c074d88...
	Project Moonshot 2019 Feb Plan - draft 1.pub			Document				1b7e7d8ab14055...
	Project Moonshot 2019 Sep Plan.pub			Document				226f29cd473ca0...
	Project Moonshot Spec 5234 - draft 2.docx	10/17/2019, 11:58:00 PM	Tahuh Mir	Document				244338a512e0a5...
	Project Moonshot Spec 5234.docx	10/17/2019, 11:58:00 PM	Tahuh Mir	Document				263d59a037e494...
	Project Moonshot 2019 Mar Plan.pub			Document				2a6241ca880926...
<input type="radio"/>	CONFIDENTIAL - Project Moonshot One Pager...	10/24/2019, 11:02:30 AM	Tahuh Mir	Document				2c91b1e223bc5e...
	Project Moonshot Spec K4fd - draft 2.docx	10/17/2019, 11:58:00 PM	Tahuh Mir	Document				3069f18c3c6d86...
	Project Moonshot Spec 3435 - draft 1.docx	10/17/2019, 11:58:00 PM	Tahuh Mir	Document				34250980aa45a3...
	CONFIDENTIAL - Project Moonshot One Pager...			Document				36cea37c085151...
	Project Moonshot 2019 Oct Plan.pub			Document				36ebccab108b5d...
	Project Moonshot Spec 34f3 - draft 1.docx	10/17/2019, 11:58:00 PM	Tahuh Mir	Document				3e6ec280561033...
	Project Moonshot 2020 Jan Plan - draft 1.pub			Document				3e92436126f568...

0 items selected. 75 items total.

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

Create insider risk policy

- ☒ Assign policy name
- ☐ Review

Create insider risk policy

Enter a name and description. Give this policy a friendly name so you can easily find it again later

Name *

Description

Select playbook *

- ☐ Departing employee data theft
- ☐ Data leaks
- ☐ Security violation on Laptop/PC
- ☐ Offensive language in communication

Next

Cancel

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

Create insider risk policy

- Assign policy name
- Users
- Content priority
- Indicators
- Monitoring window
- Review

Users

Choose users within your organization who will be subject to this policy. The number of users may be restricted based on your license and selection.

☐ All users

Add user or group

Name

Email

Back

Next

Cancel

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management
 - Communication compliance
- More resources
- Customize navigation
- Show less

Create insider risk policy

- Assign policy name
- Users
- Content priority
- Indicators
- Monitoring window
- Review

Assign content priority

Add Teams group Add SharePoint site Add sensitive type Add label

Microsoft Teams

Name

SharePoint sites

Name

Sensitive type

Name

Label

Name

Back

Next

Cancel

Create insider risk policy

- Assign policy name
- Users
- Content priority
- Indicators
- Monitoring window
- Review

Choose alert indicators

Choose alert signals and assign how heavily you would like the system to weigh each type of trigger when generating an alert.

- ☐ HR Events (Termination date)
- ☐ Sharing files from SharePoint Online
- ☐ Sharing folders from SharePoint Online
- ☐ Sharing SharePoint Online sites
- ☐ Downloading content from SharePoint Online
- ☐ Emailing outside the organization
- ☐ Copying sensitive or classified files to USB
- ☐ Copying sensitive or classified files to cloud
- ☐ Printing sensitive or classified documents
- ☐ Past policy violations
- ☐ Measure anomalous activity

Back

Next

Cancel

- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Information protection
 - Data loss prevention
 - Records management
 - Information governance
 - Data subject requests
 - Content search
 - Audit
 - eDiscovery
 - Insider risk management**
 - Communication compliance
- More resources
- Customize navigation
- Show less

Create insider risk policy

- Assign policy name**
- Users
- Content priority
- Indicators
- Monitoring window
- Review

Select monitoring window

Choose the timeframes to which you would like to apply this policy. This will be used to determine the duration of monitoring once installed.

In-scope timespan (1 to 30 days) 21 days

Historic timespan (0 to 180 days) 90 days

Future termination window (5 to 45 days) 30 days

Past termination window (5 to 45 days) 10 days

☐ Check for activity post termination

Back

Next

Cancel

Communication Compliance

Available today

Quickly identify and remediate communications risks

- Corporate policies – comply with ethical and other corporate standards
- Risk management – Identify and manage legal and corporate risk
- Regulatory compliance – SEC, FINRA require communications oversight

Communication compliance (preview)

🗑️ Remove from navigation

Overview Alerts Policies Notice templates

Monitor for offensive language

Add a policy that uses Microsoft's machine learning model for abusive and offensive language to find and prevent instances of harassment in your organization.

Get started

Monitor for sensitive info

Add a policy that monitors communications containing sensitive information to help prevent unauthorized leaks.

Get started

Monitor for regulatory compliance

Add a policy that monitors communications containing insider information.

Get started

Alerts

Alert	Policy	Severity	Detected
Unusual number of policy matches	MSFT Teams only	Medium	11-04-2019
Unusual number of policy matches	Bribery via Instant Bloomberg	Medium	11-04-2019
Unusual number of policy matches	Confidential project	Medium	11-02-2019

[View all alerts](#)

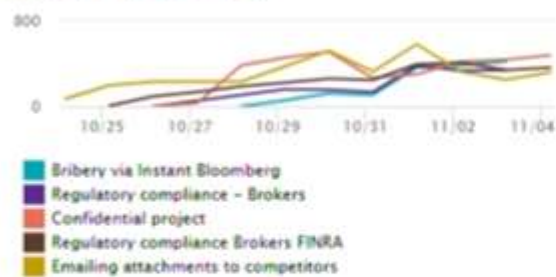
Policies with most matches

Updated 10:38 am today

Policy	Total matches
Confidential project	477

Recent policy matches

Last 30 days, updated 10:38 am today



Resolved items by policy

Last 30 days, updated 10:38 am today



Users with most policy matches

Last 30 days, updated 10:38 am today

Display name	Matches
Lee@scignite19.onmicrosoft.com	110

Escalations by policy

Last 30 days, updated 10:38 am today

Policy	Escalations
Code of conduct	3

Communication compliance (preview) > Policies > Offensive language at Contoso

Overview Pending (73) Resolved (0)

Filter Save the query Filters

☒ Resolve
 ☐ Tag as
 ☒ Notify
 ☐ Escalate
 ☐ False positive
 ...

	Subject	Sender	Recipients	Date
	yes	Lee Gu <Lee...	Nestor Wilke ...	Mon, 04 Nov 201...
	h	Lee Gu <Lee...	Nestor Wilke ...	Mon, 04 Nov 201...
<input checked="" type="checkbox"/>		Lee Gu <Lee...	Nestor Wilke ...	Mon, 04 Nov 201...
		Nestor Wilke ...	Lee Gu <Lee...	Mon, 04 Nov 201...
		Lee Gu <Lee...	Nestor Wilke ...	Mon, 04 Nov 201...
		Lee Gu <Lee...	Megan Bowen...	Sun, 03 Nov 201...
		Lee Gu <Lee...	Megan Bowen...	Sun, 03 Nov 201...
		Lee Gu <Lee...	Nestor Wilke ...	Sun, 03 Nov 201...
		Lee Gu <Lee...	Nestor Wilke ...	Sun, 03 Nov 201...
		Nestor Wilke ...	Lee Gu <Lee...	Sun, 03 Nov 201...
		Nestor Wilke ...	Lee Gu <Lee...	Sun, 03 Nov 201...
		Lee Gu <Lee...	Megan Bowen...	Sun, 03 Nov 201...
		Lee Gu <Lee...	Nestor Wilke ...	Sun, 03 Nov 201...

1 item selected. 73 items total.

Summary Text view Annotate view User history (0)

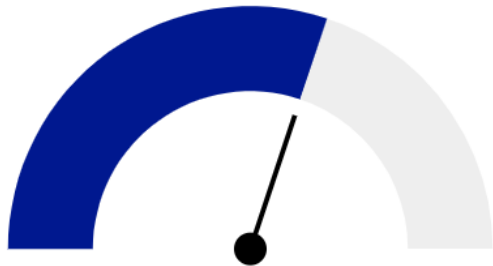
- Lee Gu** November 4, 2019, 5:55 AM
 you pathetic and dumb
- Nestor Wilke** November 4, 2019, 5:55 AM
 WTF
- Lee Gu** November 4, 2019, 5:56 AM
 I don't like you == I will hurt you 🤬

Microsoft Compliance Score

Public preview

Overall compliance score

Your compliance score:
75%



12051/16081 points achieved

Customer-managed points achieved ⓘ
0/4030

Microsoft-managed points achieved ⓘ
12051/12051

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how Compliance Score is calculated](#)

Key improvement actions

Not completed 280 Completed 0 Not in scope 0

Improvement action	Impact	Test status	Group
Conceal Information with Lock Screen	+27 points	• None	Default Group
Require Mobile Devices to Lock Upon Inactivity	+27 points	• None	Default Group
Require Systems to Lock Upon Inactivity	+27 points	• None	Default Group
Use Encrypted Connections for Cloud Services	+27 points	• None	Default Group
Route Traffic Through Managed Network Access Points	+27 points	• None	Default Group
Protect Wireless Access	+27 points	• None	Default Group
Block Jail Broken and Rooted Mobile Devices	+27 points	• None	Default Group
Create a Compliance Policy for Android Devices	+27 points	• None	Default Group
Create a Compliance Policy for Android Enterprise Devi...	+27 points	• None	Default Group

[View all improvement actions](#)

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution
Audit	0/70 points
Azure Active Directory	0/416 points
Azure Information Protection	0/27 points

[View all solutions](#)

DEMO



More news

- Protected PDF support in Edge Chromium (public preview)
- Data protection in Power BI (public preview)
 - Classify and label sensitive data
 - Integration with Cloud App Security
- Microsoft Defender ATP for Mac with endpoint detection and response (EDR) (public preview)
- Microsoft Cloud App Security connectors for AWS (GA) and Google Cloud (public preview)
- Azure MFA part of Azure AD free plan



That's all Folks!