cloudscout.one what's next CW 39

Product: Microsoft Information Protection

This report contains items, where the 'check before' dates are in the current month and items with upcoming 'check before' dates for the next two months. This is an update-report containing only new or changed items during CW 39.

What's next to do Major Items

(Updated) Microsoft Information Protection: Exact Data Match will add support for salt		**MC220037**

	check before:	**08/14/2020**
Updated September 24, 2020: We are pleased to announce that this is available for all Standard organizations as applicable. We are in the progress of rolling this out for Government customers. Please see the updated timeline below. Thank you for your patience.	Status:	**Rolling out**
	Created:	08/08/2020
	Product:	Microsoft Information Protection
Soon, "https://techcommunity.microsoft.com/t5/microsoft-security-and/new-exact-data-match-edm-classification-helps-you-better-detect/ba-p/793526" Exact Data Match (EDM) will support salt in the data hashing process to improve data security.	Platform:	Web, World tenant, Online
Key points	Scope:	Compliance, Security, User, Administration
Microsoft 365 Roadmap ID: "https://www.microsoft.com/microsoft-365/roadmap?filters=featureid=65207" 65207	Ring:	General Availability
Timing:Standard - Complete		
Government - Complete by early October		
Action: review and assess		

	Type:	Admin impact, New feature, Updated message	Tenant:

Links	65207
Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support
Linked Item Details	65207 Title : Microsoft Information Protection: Exact Data Match will support SALT in the data hashing process to improve data security 65207 Description: Exact Data Match will support SALT in the data hashing process to improve data security. Adding a random string, known as a SALT, to each data value prior to hashing can make it much more challenging for an attacker to reverse engineer the original values.

MS Preperations	Once the feature is available, "https://docs.microsoft.com/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification#set-up-the-edm-upload-agent" download and install the appropriate updated EDM Upload Agent (Commercial/GCC, GCC-High, or DoD). Updated Upload Agents will be available when the feature reaches GA.
	If you had previously hashed, indexed, and uploaded data to the EDM service and are already using EDM and would like to add salt to that hashed data, you will need to re-hash and re-upload that data using the instructions provided on the EDM page.
	Learn more:
	"https://techcommunity.microsoft.com/t5/microsoft-security-and/exact-data-match-upcoming-news/ba-p/1492842" Exact Data Match Upcoming News
	     "https://techcommunity.microsoft.com/t5/microsoft-security-and/implementing-microsoft-exact-data-match-edm-part-1/ba-p/1345360" Implementing Microsoft Exact Data Match
	     "https://techcommunity.microsoft.com/t5/microsoft-security-and/microsoft-information-protection-and-compliance-webinar-page/ba-p/1184481" Webinar: Exact Data Match (EDM) classification ("https://aka.ms/MIPC/Video-EDMwebinar" video | "https://aka.ms/MIPC/Blog-EDMWebinar" deck/FAQ)

MS How does it affect me	Adding a random string, known as a salt, to each data value prior to hashing can make it much more challenging for an attacker to reverse engineer the original values. Customers can choose to use a custom salt or a random salt that is generated by Microsoft. The data hashed and uploaded for EDM will be more secure through the addition of the salt to the hashing process.

Microsoft Information Protection: Double Key Encryption **64646**

Currently available in preview to Commercial tenants, Double Key Encryption from Microsoft allows you to protect your highly sensitive data while maintaining full control of your key. You can protect your data with two keys - your Azure key and your key in the Double Key Encryption service.	check before:	**08/31/2020**
	Status:	**In development**
	Created:	07/21/2020
	Product:	Microsoft Information Protection
	Platform:	Online, World tenant
	Scope:	Compliance, Security, Administration
	Ring:	General Availability
	Type: New feature, Admin impact	Tenant:

Docu to check	Service Description, Automation / Scripts, Working instructions for IT Support, User Knowledge base

Microsoft Information Protection: Data loss prevention for Microsoft Teams

65383

Data loss prevention (DLP) capabilities in Microsoft 365 government clouds will be extended to include Microsoft Teams chat and channel messages, including private channel messages. If your organization has DLP, you can now define policies that prevent people from sharing sensitive information in a Microsoft Teams channel or chat session.

check before:	**10/31/2020**
Status:	**In development**
Created:	06/27/2020
Product:	Microsoft Information Protection, Teams
Platform:	US Instances, World tenant, Online
Scope:	Compliance, Security, Administration
Ring:	General Availability
Type:	Tenant:

Docu to check Service Description, Working instructions for IT Support, User Knowledge base

More Info URL https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide

●●●

What's next to do normal Items

●●●

What's next to do minor Items

Microsoft Information Protection: Auto-classification with sensitivity labels in SPO, EXO, OneDrive for gov clouds

67125

Auto-classification with sensitivity labels in OneDrive, SharePoint Online, and Exchange Online will soon be available in GCC and GCC-High environments. Sensitivity labels are central to Microsoft Information Protection, enabling you to label important content to associate it with protection policies and actions like encryption and visual marking. With this release, you can start using sensitivity labels at scale for documents stored on OneDrive and SharePoint Online, and for emails in transit in Exchange Online automatically without manual user input.

check before:	**09/30/2020**
Status:	**In development**
Created:	09/16/2020
Product:	Exchange, Information Protection - Office 365, Microsoft Information Protection, OneDrive, SharePoint
Platform:	Online, US Instances
Scope:	Compliance, Security, User
Ring:	General Availability
Type:	New feature, Admin impact
	Tenant:

Docu to check Service Description, Automation / Scripts, User Knowledge base

More Info URL https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#how-to-configure-auto-labeling-policies-for-sharepoint-onedrive-and-exchange