Verstehen der allgemeinen Verfügbarkeit von IDM

Inhalt

[Einleitung](#)

[Überblick](#)

- [Wie unterscheidet sich IDM von EDM?](#)
- [Was sind die gängigsten Anwendungsfälle für IDM?](#)
- [Generiert IDM Fingerprints auf Basis der Datei oder ihres Textinhalts?](#)
- [Wie benutzt man IDM?](#)
- [Kann das SvD-Indexertool so konfiguriert werden, dass regelmäßig Fingerabdrücke von neuen Daten erstellt werden?](#)
- [Wo kann ich auf IDM zugreifen und das DLP-Indexer-Tool herunterladen?](#)
- [Welche Dateitypen sind mit IDM kompatibel?](#)
- [Welche Einschränkungen müssen bei der Verwendung von IDM beachtet werden?](#)
- [Wo finde ich weitere Informationen?](#)

Einleitung

In diesem Dokument wird die allgemeine Verfügbarkeit von IDM (Index Document Match) beschrieben.

Überblick

Das IDM ist eine fortschrittliche DLP-Datenklassifizierungstechnik, die die Fähigkeit der Organisation, Dokumente mit vertraulichen Daten effektiv zu schützen, erheblich verbessert.

Mit IDM können Organisationen den Inhalt von Dokumenten, die ihre vertraulichen Daten enthalten, indexieren und per Fingerabdruck erfassen. Durch die Erstellung eines Fingerabdruck-Repositorys für diese Daten kann unser Data Loss Prevention (DLP)-Produkt während der Inhaltsauswertung vollständige oder teilweise übereinstimmende Dokumente effizient identifizieren.

Der Vorteil von IDM gegenüber herkömmlichem Mustervergleich mit regulären Ausdrücken und Schlüsselwörtern ist beträchtlich. Anstatt einen Abgleich mit Daten vorzunehmen, die vertraulichen Daten ähneln können, können Sie mit IDM einen Abgleich mit Ihren tatsächlichen vertraulichen Daten vornehmen. Durch diesen zielgerichteten Ansatz wird die Anzahl von DLP-Vorfällen mit geringer Bedeutung reduziert, und Organisationen können ihre Sicherheitsverfahren und -ressourcen auf wichtige Untersuchungen konzentrieren.

Wie unterscheidet sich IDM von EDM?

IDM (Indexed Document Match) und EDM (Exact Document Match) unterscheiden sich hinsichtlich der Art der Daten, die sie abnehmen.

EDM konzentriert sich speziell auf das Fingerprinting tabellarischer Daten, bei denen es sich um strukturierte Daten in einem Tabellenformat handelt. Das bedeutet, dass EDM für die Verarbeitung von Daten mit einer bestimmten Struktur wie Datenbanken oder Tabellenkalkulationen konzipiert ist. Ein Unternehmen kann beispielsweise mithilfe von EDM einen Fingerabdruck einer Kreditkartentabelle eines Unternehmens erstellen und so sicherstellen, dass nur diese Firmenkreditkarten überwacht und geschützt werden.

IDM wird dagegen für die Indizierung und das Abnehmen von Fingerabdrücken von Freihanddokumenten verwendet, bei denen es sich um unstrukturierte Daten handelt, die kein bestimmtes Format verwenden. IDM ist in der Lage, Dokumente zu verarbeiten und per Fingerabdruck zu erfassen, die nicht in einer tabellenähnlichen Struktur organisiert sind, wie z. B. Textdateien, PDF-Dateien oder Word-Dokumente.

Zusammenfassend lässt sich sagen, dass IDM für den unstrukturierten Daten-Fingerprinting verwendet wird, während EDM für den strukturierten Daten-Fingerprinting verwendet wird.

Was sind die gängigsten Anwendungsfälle für IDM?

Zu den gängigen Szenarien gehören Fingerabdrücke und der Schutz geistigen Eigentums, z. B. Quellcode-Repositorys, Patentanmeldungen oder sensible Unternehmensdaten wie Personalarbeitsformulare, Unternehmensdokumente und Rechtsdokumente.

Generiert IDM Fingerprints auf Basis der Datei oder ihres Textinhalts?

IDM indiziert und druckt den Textinhalt des Dokuments per Fingerabdruck und nicht die Datei selbst. Dadurch kann IDM teilweise mit ausgewertetem Inhalt übereinstimmen, selbst wenn einige der sensiblen Daten kopiert und in eine neue Datei eingefügt werden. Sie können flexibel festlegen, wie viele Übereinstimmungen erforderlich sind, um eine Verletzung auszulösen. Dazu können Sie aus einer vordefinierten Liste von Optionen auswählen (20 %, 60 %, 80 %).

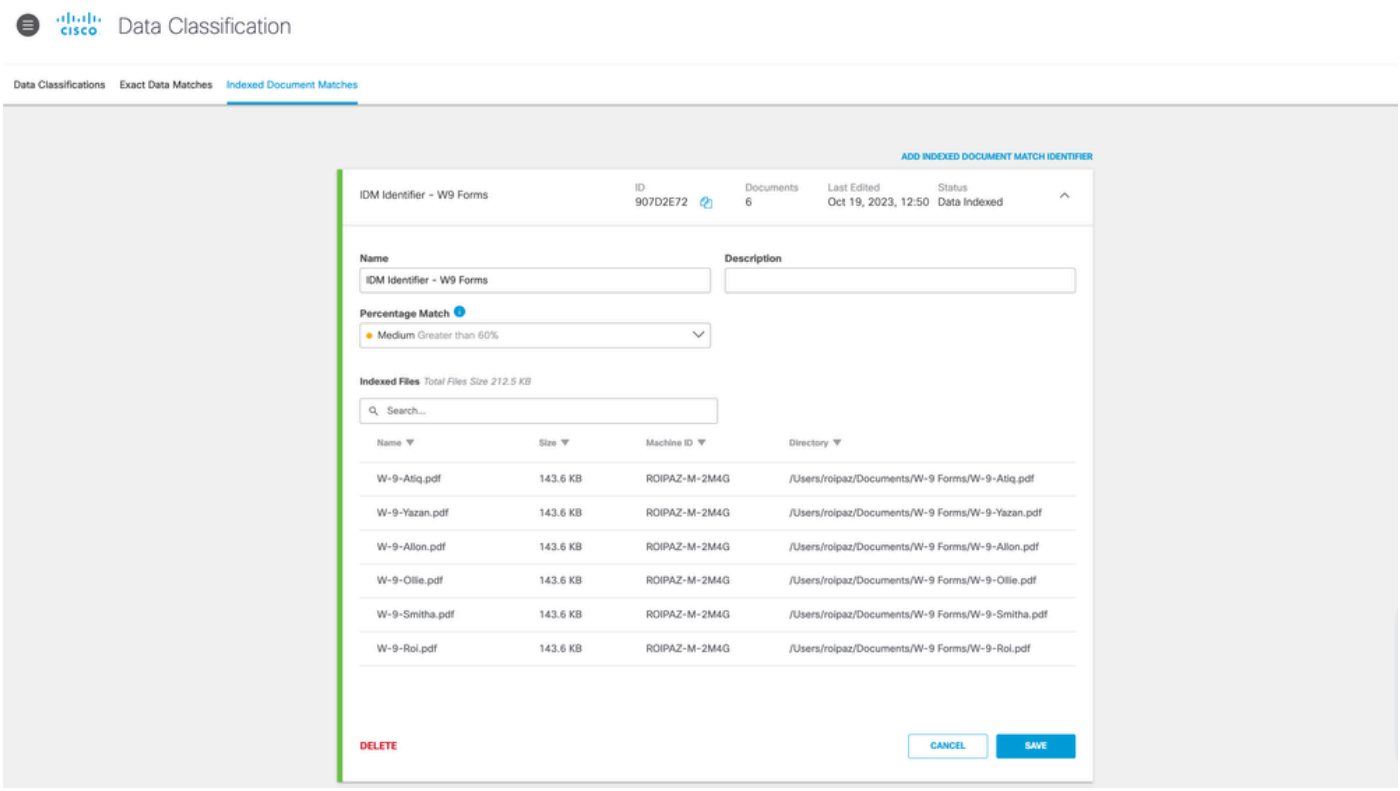
Wie benutzt man IDM?

IDM (Indexed Document Match) in Umbrella erzeugt Hash-Fingerprints des extrahierten Texts aus sensiblen Dokumenten. Diese Fingerprints werden dann von den verschiedenen Scans von Multi-Mode-DLP verwendet, um den Inhalt der Dokumente vollständig oder teilweise zu identifizieren. Um diese Fingerabdrücke zu generieren, müssen Sie das DLP-Indexer-Tool von Cisco lokal herunterladen und verwenden.

Der Indexer, eine Befehlszeilenschnittstelle, extrahiert Text aus den Dokumenten, führt Fingerprinting- und Indexierungsvorgänge aus und hasht den indizierten Text. Anschließend lädt das Tool die gehashten Fingerabdrücke zu Umbrella oder Secure Access hoch.

Die Ausgabe des Indexertools ist ein neuer IDM-Datenbezeichnertyp, der in der benutzerdefinierten Datenklassifizierung verwendet wird. Diese Klassifizierungen werden mit

Echtzeit-DLP-Regeln und SaaS-API-DLP-Regeln angewendet, um sowohl ruhende Daten als auch Daten bei der Übertragung wirksam zu schützen.



20327456127636

Kann das SvD-Indexertool so konfiguriert werden, dass regelmäßig Fingerabdrücke von neuen Daten erstellt werden?

Das Indexer-Tool kann im Überwachungsmodus als Hintergrundprozess ausgeführt werden. In diesem Modus kann der DLP-Indexer in regelmäßigen Abständen automatisch neu indiziert werden. So wird sichergestellt, dass die Quelldaten in Umbrella regelmäßig aktualisiert werden, ohne dass eine manuelle Operation erforderlich ist.

Wo kann ich auf IDM zugreifen und das DLP-Indexer-Tool herunterladen?

1. Melden Sie sich beim Umbrella Dashboard an.
2. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Datenklassifizierung > Datenklassifizierung.
3. Klicken Sie auf die Registerkarte Indexierte Dokumentzuordnung.
4. In diesem Abschnitt können Sie IDM-Bezeichner erstellen und den SvD-Indexer herunterladen.

Welche Dateitypen sind mit IDM kompatibel?

IDM unterstützt alle Dateitypen, die von DLP unterstützt werden. Eine umfassende Liste der unterstützten Dateitypen finden Sie in der Dokumentation. Erwähnenswert ist, dass IDM auch Unicode-Zeichen unterstützt.

Welche Einschränkungen müssen bei der Verwendung von IDM beachtet werden?

Die Gesamtmenge des indizierten Texts für alle IDM-Datenbezeichner in einer Organisation darf 1 GB nicht überschreiten. Auf der Registerkarte "Indexierte Dokumentzuordnungen" auf der Seite "Datenklassifizierung" werden Warnungen angezeigt, wenn das zugewiesene Kontingent erreicht wird.

Wo finde ich weitere Informationen?

Umbrella-Dokumentation

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.