Allgemeine Verfügbarkeit von Umbrella DLP

Inhalt

Einleitung

Hintergrundinformationen

Definieren und Steuern

Erkennen und Durchsetzen

Überwachung und Berichterstellung

Einleitung

Dieses Dokument beschreibt die allgemeine Verfügbarkeit von Umbrella Data Loss Prevention (DLP).

Hintergrundinformationen

Cisco Umbrella ist eine der Kernkomponenten der SASE-Architektur von Cisco. Es integriert mehrere Komponenten, die zuvor eigenständige Sicherheitsservices und -anwendungen waren, in einer einzigen, Cloud-nativen Lösung.

Wir freuen uns, Ihnen heute die allgemeine Verfügbarkeit von Umbrella DLP bekannt geben zu können. Das Konzept des Datenschutzes ist sicherlich nicht neu, aber es ist komplexer geworden, da Benutzer sich direkt mit dem Internet und den Cloud-Anwendungen verbinden und herkömmliche Sicherheitsfunktionen vor Ort umgehen. Cisco Umbrella Data Loss Prevention hilft, diese Komplexität zu vereinfachen. Die Lösung ist in einer Reihe angeordnet und überprüft den Internetverkehr, sodass Sie vertrauliche Daten in Echtzeit mit flexiblen Kontrollmechanismen überwachen und blockieren können.

Definieren und Steuern

- Nutzung von mehr als 80 vordefinierten Daten-IDs, die Inhalte wie personenbezogene Daten (PII), Finanzdetails und personenbezogene Gesundheitsdaten (PHI) abdecken. Diese können so angepasst werden, dass sie auf bestimmte Inhalte zugeschnitten werden und Fehlalarme reduzieren.
- Erstellen benutzerdefinierter Wörterbücher mit benutzerdefinierten Schlüsselwörtern, z. B. Projektcodenamen
- Erstellen flexibler Richtlinien für eine präzise Kontrolle - Anwendung unternehmensspezifischer Daten-IDs auf bestimmte Benutzer, Gruppen, Standorte, Cloud-Anwendungen und Ziele

Erkennen und Durchsetzen

- Gleichzeitige Analyse vertraulicher Daten mit hohem Durchsatz, geringer Latenz und flexibler Skalierung
- Nutzung des Umbrella SWG-Proxys für skalierbare SSL-Verschlüsselung
- Analyse vertraulicher Datenflüsse zur Auswahl von Cloud-Anwendungen und Datei-Uploads an beliebige Ziele
- Erkennung und Blockierung sensibler Daten, die an unerwünschte Ziele übertragen werden, sowie potenzielle Gefährdung sensibler Daten in genehmigten Anwendungen, um Datendiebstahl zu verhindern

Überwachung und Berichterstellung

Detaillierte Berichte mit Angaben zu Identität, Dateiname, Ziel, Klassifizierung, Mustervergleich, Auszug, ausgelöster Regel usw.

Ausführliche Informationen finden Sie in der Umbrella-Dokumentation:

- Datenklassifizierungen verwalten
- Verwalten der Richtlinie zum Schutz vor Datenverlust
- Bericht zum Schutz vor Datenverlust

Mit der in Ihr Umbrella-Abonnement integrierten Cloud-nativen DLP-Funktion können Sie Ihre Compliance-Ziele erreichen, Ihren Security-Stack vereinfachen und den nächsten Schritt in Richtung SASE wagen.

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.