Konfiguration des DLP-Verhaltens bei "Fail-Closed", um Benutzeraktionen während des Cloud-Verbindungsverlusts zu blockieren

Inhalt

Problem

Bei einem Benutzer mit installiertem Endpunkt-DLP-Modul (EDLP) wurde das Drucken und Kopieren in Netzwerkdateifreigaben blockiert, obwohl er nicht in konfigurierten EDLP-Regeln enthalten war. Alle vorhandenen EDLP-Regeln wurden im MONITOR-Modus konfiguriert, wobei nur drei spezifische Benutzer in diese Regeln einbezogen wurden. Der betroffene Benutzer hat unerwartete Blockierungsaktionen für Druckvorgänge und Dateifreigabekopiervorgänge festgestellt, obwohl sie nicht der EDLP-Durchsetzung unterliegen sollten.

Bei der Fehlerbehebung wurde festgestellt, dass die EDLP-Cloud blockiert wurde, wenn keine EDLP-Cloud-Verbindung verfügbar war, sodass das System das Fail-Close-Verhalten als Fallback-Mechanismus anwendet. In Zeiträumen, in denen der EDLP-Client keine Verbindung zum Cloud-Service herstellte, um die Einhaltung von Richtlinien zu überprüfen, kam es zu einer Verweigerung des Druckens und des Zugriffs auf Netzwerkfreigaben.

Umwelt

- Cisco Endpoint DLP-Modul, Version 1.5.0.292
- Cisco Secure Access/Secure/Data Loss Prevention-Portalverwaltung
- Mehrere EDLP-Regeln im MONITOR-Modus konfiguriert
- Netzwerkfreigabekanal konfiguriert mit Fail-Closed-Verhalten
- DNS-Auflösungsänderungen wirken sich auf die Client-Netzwerkverbindung aus

Auflösung

Die Entschließung umfasste das Verständnis und die Erläuterung des Fail-Closed-Verhaltens von EDLP und seiner Anwendung während eines Cloud-Verbindungsverlusts:

Ursachenanalyse

Eine Analyse des DART-Pakets und der EDLP-Protokolle hat ergeben, dass EDLP einen Fallback "Verweigern" angewendet hat, da der Netzwerkfreigabekanal als "Fail-Closed" konfiguriert wurde. Zum Zeitpunkt der Blockierungsvorfälle war die EDLP-Cloud-Verbindung aufgrund von DNS-Auflösungsänderungen im Client-Netzwerk nicht verfügbar, sodass das System keine Richtlinienbewertungen vom Cloud-Service erhalten konnte.

Erläuterung des Verhaltens bei einem Ausfall

Die Fail-Closed-Richtlinie wurde auf das System des Benutzers angewendet, da das EDLP-Modul installiert wurde, unabhängig davon, ob die Identität des Benutzers in einer bestimmten EDLP-Regel enthalten war. Der Status "Fail-Open/Fail-Close" ist eine globale Einstellung, die in der SvD-Policy-Konfiguration bereitgestellt wird. Die Channel-Konfiguration wird auf Basis dieser globalen Einstellung angewendet.

Verbindungswiederherstellung

Das Problem wurde automatisch behoben, nachdem die DNS-Stabilität im Client-Netzwerk wiederhergestellt wurde, sodass der EDLP-Client die Verbindung zum Cloud-Service wiederherstellen konnte. Es war kein manueller Eingriff erforderlich, nachdem das zugrunde liegende Problem der Netzwerkverbindung behoben war.

Bedingungen, die zu einem Fail-Closed-Verhalten führen

Diese Bedingungen können das Fail-Close-Verhalten von EDLP auslösen:

- DNS-Auflösungsprobleme
- Netzwerkausfälle
- Switching zwischen Netzwerken
- Alle Bedingungen, die eine End-to-End-Verbindung zwischen Client und Cloud-Service verhindern

Ursache

Das Blockierungsverhalten wurde durch die Fail-Closed-Konfiguration von EDLP für den Netzwerkfreigabekanal verursacht. Wenn die Verbindung des EDLP-Clients zum Cloud-Service aufgrund von DNS-Auflösungsänderungen unterbrochen wurde, kann er keine Richtlinienergebnisse abrufen und hat daher das konfigurierte Fail-Closed-Verhalten als Fallback-Sicherheitsmechanismus durchgesetzt. Dies geschah unabhängig davon, ob der Benutzer explizit in EDLP-Regeln enthalten war, da die Fail-Closed-Einstellung global für alle Systeme gilt, auf denen das EDLP-Modul installiert ist, wenn keine Cloud-Verbindung verfügbar ist.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

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.