

WatchGuard CloudDR für Microsoft 365 E5

Verbinden Sie CloudDR, um Ihre MSFT 365 E5-Sicherheitsfunktionen zu erweitern.

E5 findet heraus, was in Ihrer Microsoft-Umgebung nicht stimmt. CloudDR wandelt jede dieser Feststellungen in eine Änderung um, die in jedem Mandanten eigenständig umgesetzt wird und in allen Cloud-Anwendungen außerhalb von Microsoft denselben Standard gewährleistet.

Der Vorteil von CloudDR+ E5

1. CloudDR wendet den Fix an. Für über 100 Microsoft 365-Regeln gibt es einen Autofix.
2. Jede Einstellung wird täglich anhand von Hunderten von integrierten Regeln überprüft.
3. Eine einfache agentenlose Integration dauert nur wenige Minuten. Erste Ergebnisse in 30 Minuten.
4. Über 40 Cloud-Apps außerhalb von Microsoft nach den gleichen Regeln.
5. Eine Konsole, ein Standard, eine Punktzahl für jeden Mandanten.

CloudDR nimmt die Änderung für Sie vor. Für über 100 Regeln zu Fehlkonfigurationen in Microsoft 365 gibt es einen Autofix. Einmal einrichten, und CloudDR wendet die Einstellung auf jedes passende Ergebnis in jedem von Ihnen verwalteten Mandanten an – mit automatischen Benachrichtigungen und einer schrittweisen Fehlerbehebung, die nur für die Fälle vorgesehen ist, in denen ein Mensch eingreifen muss.

Es bleibt unverändert. Eine Konfigurationsabweichung ist der Grund dafür, dass das nächste Audit fehlschlägt. CloudDR führt jeden Tag Hunderte von Cross-Checks für jede Einstellung durch, berichtet jedes Ergebnis mit seinem Schweregrad und der erforderlichen Änderung und bewertet die Ergebnisse anhand der führenden Compliance-Frameworks.

Ihr aktuelles Team führt es aus. Eine einzige, einfache, agentenlose Integration verbindet einen Mandanten, und die ersten Ergebnisse liegen bereits nach 30 Minuten vor. Ein IT-Administrator mit breit gefächertem Fachwissen betreibt das System von dort aus auf der Infrastruktur, die Sie bereits nutzen.

Jede App, bei der sich Ihre Mitarbeiter anmelden. Über 40 Cloud-Anwendungen nach den gleichen Regeln und Aktionen, einschließlich mehrerer Instanzen einer App. Google Workspace, Dropbox, Salesforce, Slack und Okta fallen alle unter den Standard, den Sie bereits festgelegt haben.

Auditnachweise stehen auf Anforderung bereit. Mehrere wichtige Frameworks, einschließlich NIST CSF 2.0, SOC 2, HIPAA, PCI DSS, DSGVO, ISO 27001 und weitere, werden zusammen mit der vollständigen Zuordnung zu Microsoft Defender kontinuierlich bewertet und nach einem Zeitplan in PDF exportiert. Weitere Frameworks werden folgen.

DER VORTEIL VON WATCHGUARD

CloudDR ist Teil der WatchGuard-Plattform. Es nutzt Daten aus Ihrem gesamten WatchGuard-Stack, läuft eigenständig und arbeitet mit den Tools zusammen, die Sie bereits besitzen, sodass Sie Ihren bestehenden Stack beibehalten können. Es ist auch anbieterneutral: Microsoft bewertet seine eigene Konfiguration und CloudDR überprüft sie von außen.

E5 allein

E5-Fähigkeiten	E5-Einschränkungen
Erkennung von Schatten-IT und KI	Erfasst Drittanbieter- und Schattenanwendungen anhand der im Mandanten gespeicherten OAuth-Zugriffsberechtigungen und identifiziert 1.200 bekannte generative KI-Dienste. Eine Application, für die nie eine Zugriffsberechtigung registriert wurde, wird nicht entdeckt. Nicht verwaltete Geräte und BYOD-Geräte werden erst bis zu drei Stunden später im Rahmen von Batch-Protokoll-Uploads und Sperrvorgängen über Defender for Endpoint auf verwalteten Windows-Systemen angezeigt.
Informationen zu Schatten-Apps	Das Risiko wird bewertet. Der Anbieter hinter der Application ist nicht benannt.
OAuth-App-Governance	Deckt Entra ID, Google Workspace und Salesforce seit Juni 2023 ohne zusätzliche Kosten ab. Standardmäßig ausgeschaltet, manuell pro Mandant eingeschaltet und in mehreren Abrechnungsregionen nicht verfügbar.
SaaS-Sicherheitsmanagement	Geschützt durch Konnektoren. Ist nur für Applications mit einem API-Konnektor verfügbar, und der Regelsatz führt insgesamt 460 Prüfungen über alle Konnektoren hinweg durch. Ein Mandant, der 200 SaaS-Anwendungen betreibt, erhält einen Überblick über etwa acht.
Extern freigegebene Dateien und Ordner	Nicht abgedeckt. Benutzereigene Dateien und Ordner, die außerhalb des Unternehmens freigegeben werden, fallen nicht unter die Berichterstattung von Defender.
Sicherheitsbewertung	Ein Mandant nach dem anderen, nur Konfigurationshygiene. Jede Änderung wird in der Konsole und unter der Rolle vorgenommen, die für die Einstellung verantwortlich ist. Punkte werden in etwa 24 Stunden aktualisiert.
Privileged Identity Management	Deckt Entra- und Azure-Rollen ab. Die Zugriffsrechte innerhalb von Salesforce, Dropbox, Atlassian und den übrigen SaaS-Anwendungen gelten außerhalb dieser Applications nicht.
Mandantenfähige Verwaltung	Bis zu 100 Mandanten werden untersucht. Konfigurations-Baselines gelten ausschließlich für Partner die Cloud-Lösungen anbieten, und nur für Mandanten mit bis zu 2.500 lizenzierten Benutzern.

E5 mit CloudDR

CloudDR-Fähigkeiten	E5 + CloudDR
Autofix	Mit der Regel verknüpft. Mehr als sieben Regeln für Fehlkonfigurationen in Microsoft 365 enthalten eine solche. Eine einmalige Konfiguration pro Organisation reicht, dass die Regel bei jedem neuen Problem angewendet wird, auf das sie zutrifft.
Governance von OAuth-Einwilligungen	Vom ersten Tag an aktiviert, ohne Mandantenwechsel. Einwilligungen sind in allen verwalteten Organisationen korreliert.
Erkennung über OAuth-Zugriffsberechtigungen hinaus	Applications, für die nie eine Zugriffsberechtigung registriert wurde, werden ebenfalls gefunden, einschließlich der browserbasierten KI-Tools, bei denen sich Mitarbeiter mit einer geschäftlichen E-Mail-Adresse anmelden.
Anbieterinformationen pro App	Der Anbieter hinter jeder entdeckten Application mit Zertifizierungen, Vorfallhistorie und den bekannten Schwachstellen bei den eigenen Lieferanten dieses Anbieters. Weitere Details werden kontinuierlich hinzugefügt.
Zugriff bei der Gewährung widerrufen	Das Beenden der Einwilligung einer Application funktioniert auf einem verwalteten Laptop, einem persönlichen Gerät oder einem nicht verwalteten Gerät genauso.
1.200 Sicherheitsprüfungen	Etwa 1.200 Prüfungen über alle Konnektoren hinweg, im Vergleich zu 460 bei Defender. Einige Prüfungen sind spezifisch für einen Konnektor, und die meisten werden über mehrere verteilt.
Extern freigegebene Dateien und Ordner	Benutzereigene Dateien und Ordner, die außerhalb des Unternehmens freigegeben werden, werden pro Unternehmen angezeigt und mit einem einzigen Klick kann die Freigabe widerrufen werden.
Bibliothek mit einer Regel	Ein Schweregradsmodell und ein Sicherheitswert, der über alle verwalteten Organisationen hinweg ermittelt wird. Keine CSP-Registrierung und keine Benutzeranzahlbergrenze.
Agentenlose Einrichtung	Eine einzige OAuth-Einwilligung verbindet einen Mandanten, und die ersten Ergebnisse kommen in 30 Minuten zurück. Die Konfiguration wird alle 24 Stunden synchronisiert, bis zu 48 für einige Applications.

CloudDR-Fähigkeiten	E5 + CloudDR
Compliance-Frameworks	CIS-Kontrollen, SOC 2, HIPAA, DSGVO, ISO 27001:2022, NIST SP 800-53, NIST CSF, CSA STAR und PCI DSS, die als insgesamt bestandene Prüfungen bewertet wurden, wobei die Nachweise auf Abschnittebene in PDF exportiert wurden. Weitere Frameworks sind auf der Roadmap.
Dauerhaft vergebene SaaS-Berechtigung	Administratorkonten, ruhende zugriffsberechtigte Konten und ungenutzter Zugriff auf Salesforce, Dropbox, Atlassian und den Rest der Umgebung. PIM erreicht diese nicht.
Risiko mit einem Fälligkeitsdatum wird akzeptiert	Ein Ergebnis, das der Kunde akzeptiert, wird als „akzeptiert“ gekennzeichnet und nach Ablauf des Datums erneut zur Prüfung freigegeben.

Wo CloudDR und Microsoft 365 E5 sich überschneiden

Beide erkennen Fehlkonfigurationen in Microsoft 365, decken riskante OAuth-Zugriffsberechtigungen auf, bewerten die Sicherheitslage und melden Compliance-Frameworks. Auf einer Umgebung, auf der diese E5-Funktionen bereits ausgeführt werden, werden CloudDR-Ergebnisse zurückgegeben, die erkannt werden. Die Überlappung endet am Aktionspunkt, bei der Anzahl der Mandanten und außerhalb von Microsoft.

Nur CloudDR wendet den Fix automatisch an, identifiziert Applications, für die noch nie eine OAuth-Berechtigung registriert wurde, nennt den jeweiligen Anbieter, ermittelt eine einheitliche Bewertung über alle Mandanten hinweg – ohne Beschränkung hinsichtlich der CSP-Registrierung oder der Nutzerzahl –, bewertet eine Vielzahl von Compliance-Frameworks, meldet und widerruft den Zugriff auf extern freigegebene Benutzerdateien und -ordner, meldet dauerhafte Berechtigungen innerhalb der SaaS-Anwendungen selbst und schließt ein Ergebnis mit einem Fälligkeitsdatum ab, an dem es zur Prüfung erneut geöffnet wird.

Die Angaben zu den Microsoft-Kompetenzen stammen aus der Microsoft Learn-Dokumentation und den Microsoft-Sicherheitsblogs. Die Angaben zu WatchGuard CloudDR stammen aus dem WatchGuard-Produktmanagement und dem WatchGuard-Hilfecenter. Die Funktionen können je nach Ebene, Konfiguration und Region variieren.



Sehen Sie, was Angreifer sehen

Entdecken Sie, wie WatchGuard CloudDR das, was Ihre Sicherheitstools melden, in Änderungen umwandelt, die tatsächlich in jedem von Ihnen verwalteten Unternehmen angewendet werden.

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit des Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von über 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter [watchguard.de](https://www.watchguard.de).