



E-Book

Der fehlende Service für MSPs: cloudbasiertes Risikomanagement

Cloud Detection and Response für Kundenanwendungen, -identitäten und -konfigurationen



I

- 01 Cloudbasiertes Risikomanagement für Kunden
- 02 Schatten-IT und Schatten-KI
- 03 Cloud-Fehlkonfigurationen
- 04 Identitätsdiebstahl
- 05 Neu: WatchGuard CloudDR
- 06 Vorteile von CloudDR
- 07 Chancen für MSPs



Cloudbasiertes Risikomanagement für Kunden

Ihre Kunden sind in der Cloud nicht gemanagten Risiken ausgesetzt. Sie sind für diese Risiken bereits zuständig.

Die Cloud-Anwendungen, Identitäten und Konfigurationen von Kunden schaffen eine dynamische Umgebung, die sich täglich verändert. Die Schutzmechanismen für Endpunkte, Firewalls und E-Mails lassen sich nicht auf die Cloud übertragen. Nach der Authentifizierung in der Cloud sind die meisten traditionellen Sicherheitsmaßnahmen nicht mehr anwendbar.

70%

der Datenlecks beziehen sich mittlerweile auf Informationen, die in der Cloud oder in Hybrid-Umgebungen gespeichert sind.

IBM Cost of a Data Breach Report 2026

Durch Microsoft 365, Google Workspace, SaaS-Anwendungen Anwenderidentitäten, Dateifreigabe und KI-Tools wurde eine Angriffsfläche geschaffen, für die MSP-Sicherheitsmaßnahmen nie gewappnet waren. Ein einzelner Client-Mandant führt Dutzende von SaaS-Anwendungen von Drittanbietern aus, die alle Zugriff auf Kundendaten in der Cloud haben, die die meisten MSPs nicht sehen können.

125

Cloud-Anwendungen werden bei der ersten Beurteilung eines Kunden im Durchschnitt entdeckt.

Bereitstellungsdaten von WatchGuard CloudDR

Durch diese Sichtbarkeitslücke kann ein kompromittiertes Konto in der Cloud Weiterleitungsregeln erstellen, Dateien gesammelt herunterladen, einer schädlichen Anwendung Zugriff zum Mandanten gewähren, Berechtigungen ändern oder die eigenen Berechtigungen ausweiten. Keine dieser Aktivitäten wird von traditioneller MSP-Sicherheitssoftware als verdächtig eingestuft. Da Angreifer bei der Suche nach angreifbaren Anwendungen, schwachen Berechtigungen und Fehlkonfigurationen vermehrt KI einsetzen, benötigen MSPs eine neue Herangehensweise, um Vertrauen aufzubauen und Umsätze zu steigern.

EINFLUSSBEREICH TRADITIONELLER MSP-SICHERHEIT



TRANSPARENZLÜCKEN IN DER CLOUD

Kritische Aktivitäten finden nach der Authentifizierung statt, außerhalb der Transparenz traditioneller MSP-Tools.

SCHATTEN-IT UND SCHATTEN-KI

Nicht genehmigte
SaaS-Anwendungen
KI-Tools und Hilfsmittel
OAuth und Zugriff durch Dritte

FEHLKONFIGURATIONEN

Zu viele Berechtigungen
Nicht sichere
Freigabeeinstellungen
Konfigurationsänderungen

IDENTITÄTSDIEBSTAHL

Kompromittierte Anmeldedaten
Kontomissbrauch
nach Anmeldung
Rechteauserweiterung

MSPs können nur das schützen, was sie auch sehen

Das Ergebnis

Kritische Aktivitäten in der Cloud entziehen sich der Sichtbarkeit traditioneller Sicherheitsmaßnahmen. Das verursacht Lücken, Verzögerungen bei Untersuchungen und Geschäftsrisiken. Unabhängig davon, ob Cloud-Sicherheit formal im Geltungsbereich ist oder nicht, sind MSPs bereits für die Risiken zuständig. Ohne Einsicht in Cloud-Anwendungen, Identitäten und Konfigurationen werden Cloud-Vorfälle zu einem MSP-Problem, lange bevor sie erkannt werden.

Drei Cloud-Risiken, die MSPs eindämmen müssen

Trotz der zunehmenden Komplexität von Client-Umgebungen können die meisten Cloud-Vorfälle einer der folgenden drei Risikokategorien zugeschrieben werden:

TRANSPARENZ

Schatten-IT und Schatten-KI sorgen dafür, dass MSPs nicht verwaltete SaaS-Anwendungen, unbekannte Zugriffe Dritter und unbeaufsichtigte Datenbewegungen nicht überwachen können.

ERKENNUNG

Cloud-Fehlkonfigurationen schwächen Sicherheitsmaßnahmen durch zu viele Berechtigungen, unsichere Freigabeeinstellungen und Konfigurationsänderungen, die der Compliance entgegenstehen.

BEWERTUNG

Identitätsdiebe nutzen kompromittierte Anmeldedaten, schwache Authentifizierungskontrollen und missbrauchen Konten nach dem Anmelden. Hier kommt es auf schnelle Erkennung und Reaktion an.



WAS MODERNE MSPS BRAUCHEN

Eine einheitliche Plattform zum Umgang mit Cloud-Risiken durch Microsoft 365, Google Workspace, über 40 SaaS-Anwendungen, Identitäten, Benutzeraktivitäten und KI-Tools. Wir nennen das:



CloudDR

Cloud Detection and Response

Mit CloudDR können Sie:

Bei SaaS-Anwendungen, Identitäten, Fehlkonfigurationen und Schatten-KI die Cloud-Risiken aufdecken, die traditionellen Sicherheitssystemen entgehen.

Die Sicherheit in der Cloud durch Zusammenführen von Transparenz, Erkennung, Untersuchung und Behebung vereinfachen.

Sicherheitsmaßnahmen mit mandantenfähiger Verwaltung, Automatisierung und effizienterer Behebung auf mehrere Kunden ausweiten.

Cloud-Sicherheit dank kontinuierlicher Compliance, aussagekräftigeren Kundengesprächen und einem skalierbaren, konstanten Service in eine Umsatzchance verwandeln.

Schatten-IT und Schatten-KI

Cloud-Umgebungen setzen Kunden nicht verwalteten Risiken aus.

55%

der Unternehmen haben Mitarbeiter, die SaaS-Anwendungen ohne Sicherheitsbeteiligung einsetzen

Cloud Security Alliance, State of SaaS Security Report 2025

Dateifreigabetools, Kollaborationsplattformen, Browsererweiterungen, KI-Dienste und SaaS-Anwendungen verbinden sich direkt mit Geschäftsumgebungen ohne Sicherheitsüberprüfung oder Betriebsüberwachung. Ein Mitarbeiter mit einem legitimen Konto stellt die Verbindung her. Die Anfrage wird nie an eine Ticket-Warteschlange weitergeleitet.

Früher musste die IT Zugriff anfordern, Anfragen prüfen und den Zugriff gewähren. Heute können Anwender eine Cloud-Anwendung mit wenigen Klicks einbinden. Jede nicht verwaltete Anwendung erweitert die Angriffsfläche.



Kunden binden nicht genehmigte Cloud-Anwendungen ein und MSPs tragen die Risiken.



Wie eine Schatten-IT entsteht

In der Regel erfahren MSPs von einer neuen SaaS- oder KI-Anwendung, nachdem sie ein Problem verursacht hat. Eine Datei wird extern freigegeben, eine Integration wird unterbrochen oder bei einer Untersuchung wird eine nicht genehmigte Anwendung entdeckt. Zu diesem Zeitpunkt konnte die Anwendung bereits wochen- oder monatelang auf Kundendaten zugreifen. Auch regelmäßige Überprüfungen helfen nur, bis die nächste Anwendung erscheint.

Transparenz ist nur der erste Schritt. Analysten müssen zudem schnell ermitteln können, was passiert ist, warum das wichtig ist und welche Maßnahmen zu ergreifen sind. Da die Cloud-Aktivität in allen Kundenumgebungen zunimmt, wird die Zeit von der Erkennung bis zur Behebung für die Skalierung des Sicherheitsbetriebs zum entscheidenden Faktor.

HÄUFIGE RISIKEN DURCH DIE SCHATTEN-IT

- O D
- C
- N OA
für Mandanten
- N D
- U Z D



Der Aufstieg der Schatten-KI

64%

der Mitarbeiter verwenden nicht genehmigte KI-Tools für berufliche Aufgaben

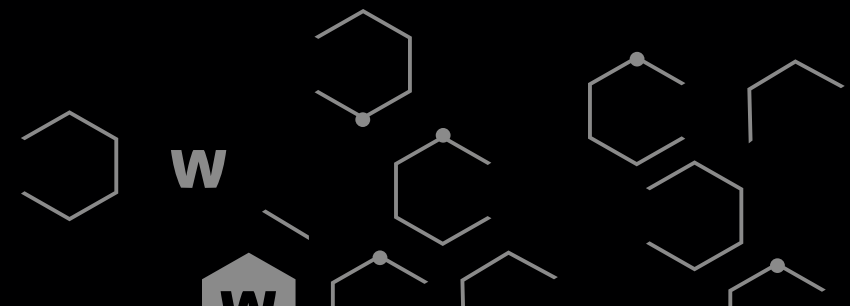
WatchGuard Bericht zur Cybersicherheitshygiene 2026

Die KI hat die Cloud-Risiken, die traditionell mit der Schatten-IT verbunden sind, erheblich erweitert. Mitarbeiter greifen täglich mit Unternehmensressourcen auf nicht genehmigte KI-Tools zu, wobei jede Sitzung das potenzielle Risiko des Unternehmens unbemerkt vergrößert.

Mitarbeiter nutzen KI-Plattformen routinemäßig für die Erstellung von Dokumenten, die Unterstützung bei der Programmierung, die Recherche, die Zusammenfassung, die Dateianalyse und die Datenverarbeitung, oft ohne zu wissen, wie die Plattformen die von ihnen übermittelten Informationen speichern, aufbewahren, weitergeben oder schützen.

HÄUFIGE RISIKEN DURCH DIE SCHATTEN-KI

- ☒ H D KI T ☒ U Workflows durch Mitarbeiter
- ☒ D S S U KI T ☒ C N KI
- ☒ E K KI P



Cloud-Fehlkonfigurationen

Die Konfigurationsänderungen beginnen mit dem ersten Tag.

Fast
8
Monate

zum Beheben aller Fehlkonfigurationen durch schwache Passwörter und Berechtigungen für externe Cloud-Umgebungen

37%

der Unternehmen besaßen ein Administratorkonto auf einer IaaS-Plattform, bei dem die MFA deaktiviert war

Data Breach Investigations Report 2026 von Verizon

Moderne Cloud-Umgebungen sind komplex und äußerst dynamisch. Eine Cloud-Konfiguration, die heute sicher ist, muss dies nicht im Laufe der Zeit bleiben. Aufgrund neuer Anwender, neuer Anwendungen, Berechtigungsänderungen, Freigaberichtlinien, Integrationen von Drittanbietern, KI-fähiger Workflows und sich entwickelnder Sicherheitsempfehlungen von Anbietern sind Konfigurationen ständigen Änderungen unterworfen.

Die meisten Sicherheitsanalysten wissen bereits, wie eine sichere Cloud-Konfiguration aussehen sollte. Ihnen fehlt jedoch häufig eine kontinuierliche Überwachung, mit deren Hilfe sie erkennen können, wann eine ursprünglich sichere Konfiguration zum Risiko wird, und überprüfen können, ob Cloud-Konfigurationen mit den aktuellen Best Practices für Sicherheit in Einklang stehen.

Wie Fehlkonfigurationen entstehen

Den meisten MSPs fehlt ein Mechanismus, mit dem sie Cloud-Fehlkonfigurationen erkennen und schnell darauf reagieren können. Fehlkonfigurationen bleiben monatelang bestehen und werden häufig überhaupt nicht behoben. Cloud-Konfigurationen ändern sich in einer mandantenfähigen Umgebung täglich – und eine regelmäßige manuelle Überprüfung bildet nur einen einzigen Zeitpunkt ab.

HÄUFIGE CLOUD-FEHLKONFIGURATIONEN

❑ Z
für Anwender

❑ D
sein sollten

❑ U I
oder inaktive MFA

❑ Nicht verwendete Konten mit K
einer SSO-Migration vergessen wurden

❑ Falsch konfigurierte SaaS
S A
die nie geändert wurden

❑ Unsicherer OAuth-Zugriff auf Anwendungen



Identitätsdiebstahl

Angreifer müssen Sie nicht hacken.
Sie brauchen sich nur anzumelden.

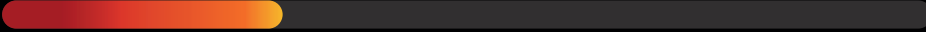
76% der Mitarbeiter verwenden dieselben Passwörter für mehrere Konten



78% der Mitarbeiter nutzen mindestens ein Konto ohne MFA



30% der Mitarbeiter geben Passwörter an andere weiter



WatchGuard Bericht zur Cybersicherheitshygiene 2026

Identitäten von Anwendern sind für Bedrohungsakteure, die Cloud-Anwendungen und -Dienste ins Visier nehmen, äußerst wertvoll geworden. Sobald sie ein anfälliges Ziel gefunden haben, können Angreifer durch gestohlene Passwörter, wiederverwendete Anmeldeinformationen und schwache Identitätskontrollen schnell auf Kundenumgebungen zugreifen. Angesichts der zunehmenden Zahl der KI-gesteuerten Angriffe ist die Zeit bis zur Erkennung und Reaktion auf Cloud-Vorfälle wichtiger denn je.

Das Identitätsrisiko erstreckt sich nun auf Microsoft 365, SaaS-Anwendungen, Cloud-Speicher, Kollaborationsplattformen, KI-fähige Tools und vertrauliche Geschäftsdaten. Wenn Unternehmen weitere Cloud-Anwendungen einführen, werden Benutzerkonten über mehrere Plattformen verteilt. Das führt zu Konten, die nach dem Ausscheiden eines Mitarbeiters vergessen, nicht verwaltet oder aktiv bleiben können.

Remote-Mitarbeiter, dezentrale Standorte und hybride Tätigkeiten bringen weitere, ganz eigene Identitätsanforderungen für jeden Mandanten mit sich.

Wie es zum Identitätsdiebstahl kommt

Identitätsgesteuerte Angriffe verwenden legitime Anmeldeinformationen und finden innerhalb einer Sitzung statt, die die Plattform bereits authentifiziert hat. Sie generieren wenig oder keine Malware-Aktivität, fügen sich in normale Cloud-Nutzungsmuster ein und umgehen die Sicherheitstools, die ein MSP bereits ausführt.

HÄUFIGE EINFALLSTORE FÜR IDENTITÄTSDIEBSTAHL

☒ Schwache Passwörter und fehlende MFA

☒ I K L
Z

☒ Ausgeschiedene Mitarbeiter, die in SaaS-Anwendungen aktiviert

☒ N K
und Gästekonten

☒ Weitergegebene und wiederverwendete A

☒ Nicht identifizierte Konten innerhalb des Mandanten



Neu: WatchGuard CloudDR

Cloud Detection and Response für moderne MSPs

Mit WatchGuard CloudDR erhalten MSPs Einblicke in verbundene Anwendungen und KI-Tools, Kontrolle über Cloud-Konfigurationen und Erkenntnisse zum Identitätsdiebstahl nach dem Anmelden. Eine Plattform deckt alle drei Cloud-Risiken für jeden Mandanten ab, den ein MSP verwaltet.

CloudDR verbindet sich über OAuth- und API-Integrationen und beginnt mit der Rückgabe von Ergebnissen innerhalb von 30 Minuten nach Genehmigung durch den Administrator. Jedes Ergebnis umfasst den Schweregrad, die Auswirkungen auf das Geschäft und die empfohlene Behebung, wobei Automatisierung und gesammelte Aktionen die Reaktion über die Mandanten hinweg beschleunigen.



Schatten-IT und Schatten-KI aufdecken

CloudDR identifiziert verbundene Anwendungen durch die dahinter stehenden OAuth-Genehmigungen. Wenn eine Anwendung nie OAuth-Zugriff angefordert hat, identifiziert CloudDR sie anhand Aktivierungs-, Anmelde- und Registrierungs-E-Mails innerhalb des Mandanten, die die KI-Dienstmitarbeiter für die Verwendung einer beruflichen Adresse registrieren. CloudDR liest nur kritische Metadaten aus und scannt nicht die privaten Informationen, die in der Nachricht eines Mitarbeiters enthalten sind.

Ein Sicherheitsanalyst kann in einer zentralen Ansicht überprüfen, welchen Benutzern welche Berechtigungen erteilt wurden, und die Erteilung widerrufen. Automatisierte Workflows genehmigen, verweigern oder widerrufen den Anwendungszugriff mandantenübergreifend, ohne dass ein Sicherheitsanalyst jeden einzeln öffnen muss. Mit dem Schatten-SaaS-Inventar und dem Bericht über entdeckte Anwendungen wird jedes Ergebnis in eine zur Überprüfung vorbereitete Dokumentation umgewandelt.

ANWENDUNGSFÄLLE FÜR SCHATTEN-IT UND SCHATTEN-KI

- ☒ Schatten-SaaS-Anwendungen A
- ☒ Schattenanwendungskonten mit
- ☒ K Schattenanwendungen
- ☒ N K Schatten-SaaS-Anwendungen
- ☒ Ruhende Schattenanwendungen
- ☒ KI Schattenanwendungen

Operatives Ergebnis

Durch Einblicke in zuvor nicht verwaltete Anwendungen und KI-Dienste, können MSPs Vorfälle schneller untersuchen, die Governance verstärken und Kunden besser schützen.

Fehlkonfigurationen lückenlos verwalten

CloudDR überwacht die Konfigurationszustände kontinuierlich, anstatt auf eine manuelle Überprüfung oder das nächste Audit zu warten. Bei jeder Erkennung wird die betroffene Einstellung identifiziert, mit Schweregrad versehen und die empfohlene Einstellung angegeben. Dadurch entfällt die Detektivarbeit, die den meisten Korrekturen vorausgeht.

Wenn dasselbe Ergebnis über mehrere Mandanten hinweg angezeigt wird, gruppiert CloudDR diese Ergebnisse und ermöglicht es Sicherheitsanalysten, sie mit einer einzigen Aktion gesammelt zu beheben.

ENTDECKTE CLOUD-FEHLKONFIGURATIONEN

- ☒ Lücken in der Passwortrichtlinie
- ☒ A L Authentifizierung
- ☒ Nicht angewendete
- ☒ E K
- ☒ Zu weit gefasste Admin-Rollen
- ☒ Nicht kontrollierte E-Mail-
- ☒ D P P

Operatives Ergebnis

MSPs erkennen Konfigurationsabweichungen innerhalb von Minuten, nicht Monaten, und beheben die Ergebnisse aller betroffenen Mandanten gleichzeitig, wodurch der Schutz des Kunden zwischen Überprüfungen gewahrt bleibt.

Identitätsbedrohungen erkennen und darauf reagieren

Angriffe auf Identitäten fallen durch das Raster der Malware- und Endpunktsicherheit. Sie erzeugen eine legitime Anmeldung, gefolgt von unrechtmäßigem Verhalten: eine Regel für externe Weiterleitungen im Postfach, einen Massen-Download, eine neue OAuth-Erteilung oder eine Berechtigungseskalation.

CloudDR überwacht das Kontoverhalten aller verbundenen Mandanten, um den Missbrauch der Cloud-Identität zu erkennen. Wenn die Aktivität einen definierten Schwellenwert überschreitet, antwortet der Sicherheitsanalyst von derselben Konsole aus und widerruft Sitzungen und Token, deaktiviert das Konto oder entfernt Zugriffsberechtigungen.

ANWENDUNGSFÄLLE IM ZUSAMMENHANG MIT IDENTITÄTSDIEBSTAHL

- ☒ Multifaktor-Authentifizierung (MFA)
- ☒ Nicht identifizierte Konten
- ☒ R K
- ☒ Teilweise deaktivierte Konten
- ☒ D K
- ☒ N L
- ☒ E K

Operatives Ergebnis

MSPs reduzieren das Identitätsrisiko, indem sie ruhende Konten, schwache Identitätskontrollen und Kontorisiken identifizieren, bevor Angreifer sie ausnutzen können.

Kontinuierliche Compliance und Bereitschaft für Prüfungen

CloudDR ordnet Kundenumgebungen Hunderten von vorkonfigurierten Richtlinien zu, die auf CIS-Controls, NIST, SOC 2 und mehr als 30 Compliance-Frameworks ausgerichtet sind, wobei regelmäßig Frameworks hinzukommen. Jeder Anwendung wird eine Risikobewertung zugewiesen. Jedes Framework wird anhand des Prozentsatzes der bestandenen Kontrollen gemessen. Risikoklasse und Compliance sind sichtbar und werden kontinuierlich aktualisiert, um die Bereitschaft für Prüfungen zu gewährleisten.

Der operative Effekt zeigt sich in Prüfungen und vierteljährlichen Berichten zur Geschäftsentwicklung. CloudDR behält den Compliance-Stand jedes Kunden zwischen den Audits im Blick, nach Framework bewertet, wobei alle Maßnahmen für jeden von einem MSP verwalteten Mandanten durch Belege nachzuvollziehen sind.

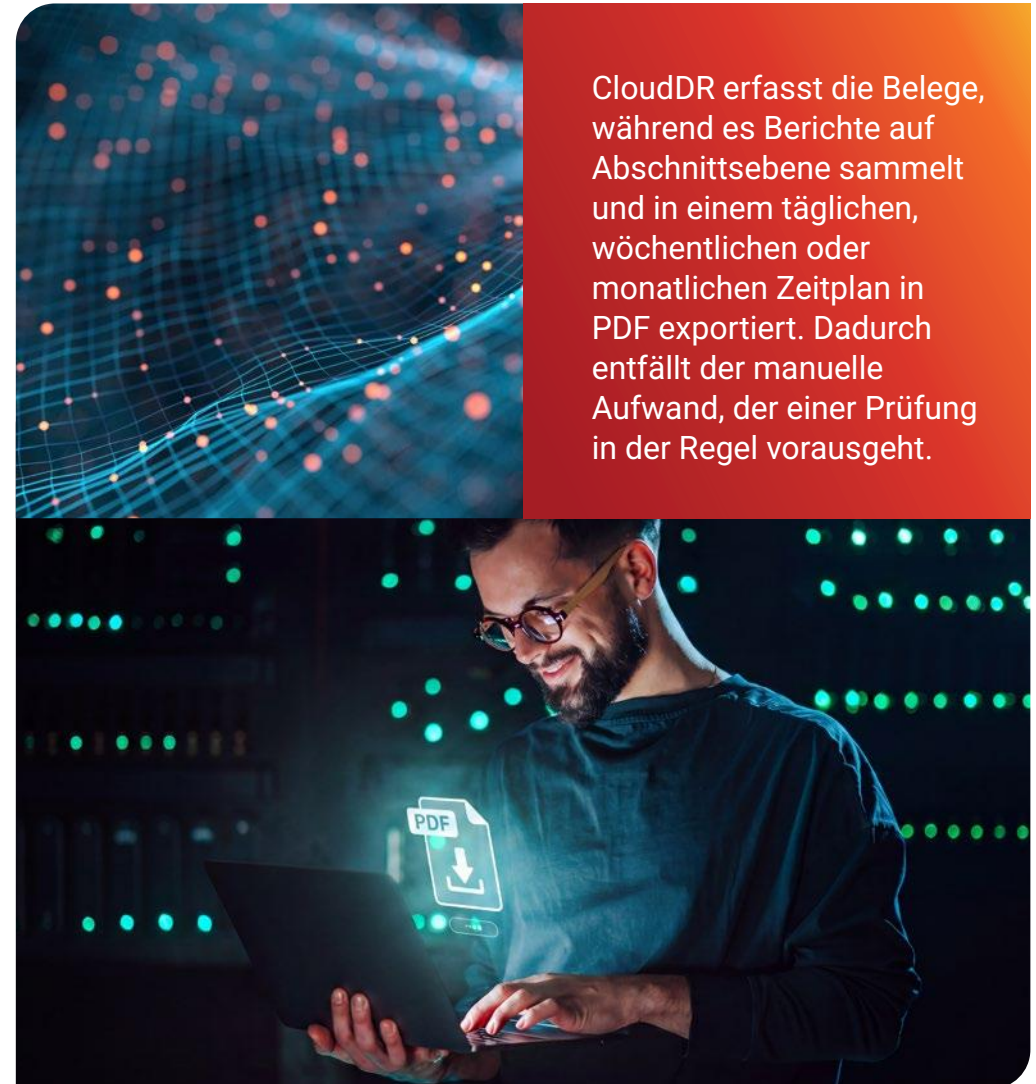
67%

der Unternehmen benötigen zusätzliche Unterstützung bei der Bewältigung wachsender Compliance-Anforderungen

WatchGuard IT-Umfrage 2026

Operatives Ergebnis

Die Bereitschaft für Prüfungen ist mehr als nur ein Projekt. MSPs können den Stand der Compliance kontinuierlich nachverfolgen, automatisch Belege sammeln und Kunden dabei unterstützen, sich überzeugt auf Prüfungen vorzubereiten. Die PDF-Berichte per Mausklick liefern bei Bedarf Dokumentation, die jeder Überprüfung standhält. Dadurch sind Compliance-Services einfacher bereitzustellen und zu skalieren.



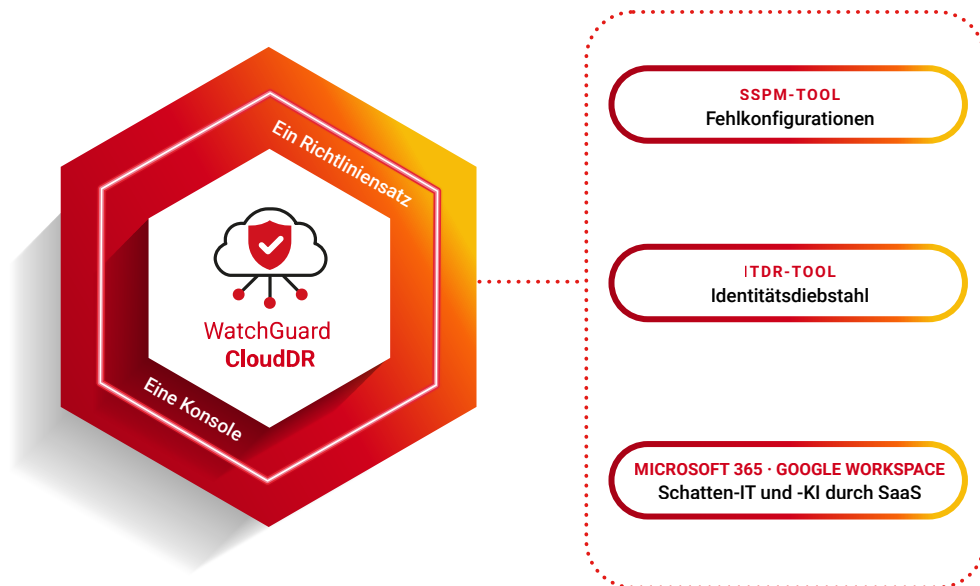
CloudDR erfasst die Belege, während es Berichte auf Abschnittsebene sammelt und in einem täglichen, wöchentlichen oder monatlichen Zeitplan in PDF exportiert. Dadurch entfällt der manuelle Aufwand, der einer Prüfung in der Regel vorausgeht.

Vorteile von CloudDR

Cloud-Sicherheit vereinfachen

CloudDR reduziert den Zeitaufwand für die Sicherung der Cloud-Umgebung jedes Kunden, indem es Untersuchungen und Korrekturen in einer einzigen Plattform zusammenfasst. Die meisten MSPs stellen die Cloud-Abdeckung aus drei Quellen zusammen: SSPM-Tools für Fehlkonfigurationen, ITDR-Tools für Identitätsbedrohungen und die automatisierten Kontrollen in Microsoft 365 und Google Workspace, die zwar die Plattform, aber nicht die Art und Weise sichern, wie jeder Mandant konfiguriert oder verwendet wird. Separate Lizenzen, Konsolen, Verlängerungszyklen und Margen werden dadurch häufig durch den Tool-Overhead und nicht durch die Servicebereitstellung absorbiert.

CloudDR bringt alle drei Quellen zusammen. MSPs arbeiten mit einer Konsole, einem Satz von Richtlinien und prüfungsbereiten Berichten pro Kunde und können ihre Cloud-Sicherheitsdienste konstant ohne die Kosten und den Aufwand eines anderen Tools erweitern.



Warum WatchGuard CloudDR?

01

Effizienter arbeiten. Schneller reagieren. Mit besseren Margen skalieren.

CloudDR hilft MSPs, den manuellen Aufwand
C S D
ohne den Betriebsaufwand zu erhöhen.

02

D

Bei jedem Ergebnis wird erklärt, was passiert ist, warum das wichtig ist und wie es behoben werden kann, wobei Automatisierung und

03

MSP-First-Architektur.

Mandantenfähig von Grund auf, mit einsatzbereiten Workflows, die für MSPs entwickelt wurden, um bestehende verwaltete S Cloud-Sicherheitsangebote zu entwickeln.

04

Wählen Sie zwischen „Agentlos“ oder dem
C A O A
gibt es keine zu installierende Software und
keine Auswirkungen auf den Endnutzer. Der
C A
E
Ebene der Cloud-Aktivitätsüberwachung, wenn
T

Cloud-Risiken minutenschnell beurteilen

Das Onboarding eines Mandanten erfolgt in einem Schritt: Ein Administrator genehmigt die OAuth-Berechtigungen, und CloudDR verbindet die Dienste über eine API. Die Ergebnisse werden innerhalb von 30 Minuten ausgegeben. Es gibt keinen bereitzustellenden Agenten, keine Auswirkungen auf den Endbenutzer und kein Engagement für professionelle Services pro Mandant.

Sicherheit für die Cloud aktivieren

Statt zu vieler Warnmeldungen, Tool-Flut und vermeidbarer Cloud-Vorfälle erhalten MSPs Anwendungstransparenz, Risikokontrolle und Identitätsbedrohungserkennung in einer mandantenfähigen Plattform. Sicherheitsanalysten können Cloud-Bedrohungen schnell erkennen und darauf reagieren und die Systeme, Anwender und Daten von Kunden bleiben sicher und konform.

Vertrauen aufbauen und Umsätze steigern



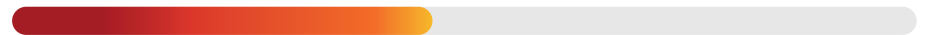
„MSPs haben zunehmend Probleme mit fragmentierten Tools, die nur einen Teil des Cloud-Sicherheitsproblems lösen. Es besteht akuter Bedarf an Lösungen, die Transparenz und Reaktion an einem Ort vereinen. WatchGuard CloudDR ist genau dazu in der Lage.“

Neil Holme

Gründer und CEO von Impact Business Technology

CloudDR ist so konzipiert, dass es an eine vorhandene verwaltete Sicherheitsebene angehängt oder als kostenpflichtiges Cloud-Sicherheits-Add-on bereitgestellt werden kann. Als Kostengrundlage dienen Anwender pro Mandant. MSPs können ohne den Kostenaufwand für ein weiteres Tool wiederkehrende Umsätze steigern.

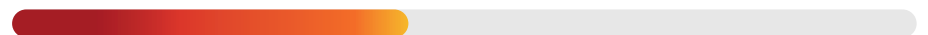
48% der Unternehmen ergänzen ihre internen Ressourcen bereits durch externe Anbieter



35% wünschen sich von ihren Anbietern mehr Identitäts- und Zugriffssicherheit



44% sind bereit, mehr für KI-gestützte Bedrohungserkennung und automatisierte Reaktion zu bezahlen



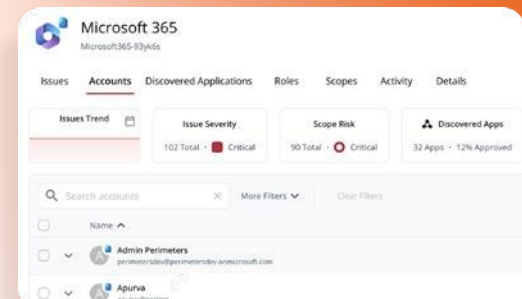
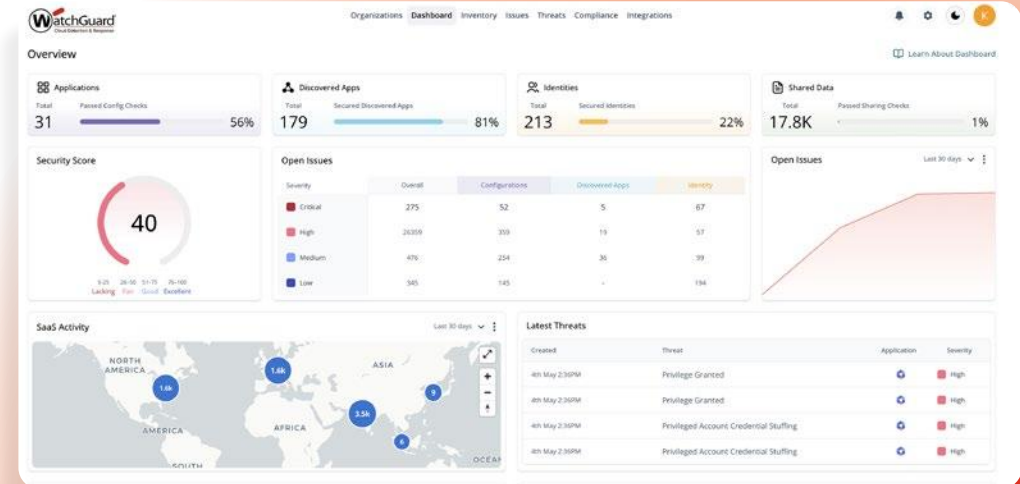
Chancen für MSPs

Kunden auf die Cloud-Risiken ansprechen

Kunden setzen zunehmend auf SaaS und KI. Sie sollten die Kunden ansprechen, die sich bereits jetzt mehr Identitäts- und Zugangssicherheit wünschen und bereit sind, für die KI-gesteuerte Erkennung zu bezahlen. MSPs müssen nicht warten, bis ein Cloud-Sicherheitsvorfall eintritt. Verbinden Sie CloudDR mit einem Mandanten und gewinnen Sie innerhalb von 30 Minuten Erkenntnisse, die Ihnen aktuell entgehen. Nutzen Sie diese Ergebnisse dann zum Anlass für ein Gespräch über das Cloud-Risikomanagement.

ZU DEN UNTERSTÜTZTEN ANWENDUNGEN GEHÖREN:

☒ A		☒ C
☒ A		
☒ A		☒ Microsoft 365
☒ HR		☒ Microsoft Intune
☒		☒ Microsoft Teams
☒		☒
☒ Confluence		☒ MongoDB
☒ C	PSA O P	☒ O
☒ C		☒ O L
☒ D		☒ O AI
☒ D S		☒ S
☒ D		☒ S
☒ D		☒ ServiceNow
☒ E-Mail		☒ S P
☒ E ID		☒ S
☒ H		☒ T
☒ L		☒
☒		☒ Z
☒ H		☒ Z
☒ H S		



Threats Group by Use Cases All Threats

Anomalous Access

Surface access behavior that violates organizational access location or usage policies.



Use Case Hub

All Use Cases Misconfigurations Discovered Apps Identity Data

System Integrity

Monitor system integrity signals, such as unusual admin counts or unmanaged accounts. Investigate and correct configurations that may indicate mismanagement or increased risk.

Open Issues: 75

Issues Trend (Last 30 days)

Open Issues: 70

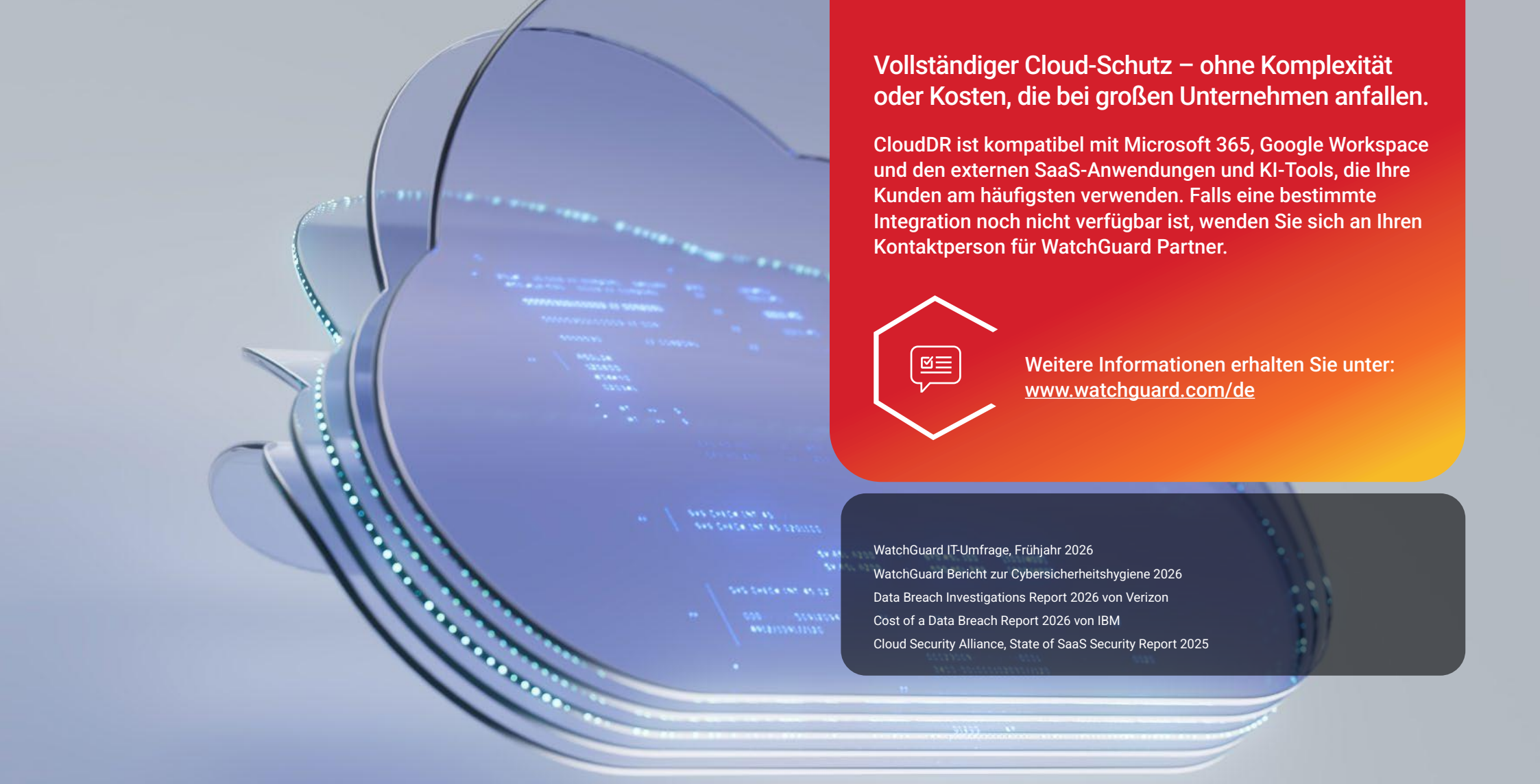
Issues Trend (Last 30 days)

Open Issues: 49

Issues Trend (Last 30 days)

Open Issues: 48

Issues Trend (Last 30 days)



Vollständiger Cloud-Schutz – ohne Komplexität oder Kosten, die bei großen Unternehmen anfallen.

CloudDR ist kompatibel mit Microsoft 365, Google Workspace und den externen SaaS-Anwendungen und KI-Tools, die Ihre Kunden am häufigsten verwenden. Falls eine bestimmte Integration noch nicht verfügbar ist, wenden Sie sich an Ihren Kontaktperson für WatchGuard Partner.



Weitere Informationen erhalten Sie unter:
www.watchguard.com/de

WatchGuard IT-Umfrage, Frühjahr 2026
WatchGuard Bericht zur Cybersicherheitshygiene 2026
Data Breach Investigations Report 2026 von Verizon
Cost of a Data Breach Report 2026 von IBM
Cloud Security Alliance, State of SaaS Security Report 2025

Informationen zu WatchGuard

WatchGuard Technologies ist ein weltweit führendes Unternehmen für einheitliche Cybersicherheit, das speziell für Managed Service Provider (MSPs) entwickelt wurde. Seit mehr als 30 Jahren definiert WatchGuard, wie MSPs Sicherheit in großem Maßstab bereitstellen, und entwickelt kontinuierlich Innovationen, um jeder größeren Veränderung in der Bedrohungslandschaft einen Schritt voraus zu sein. Die KI-gestützte Unified Security Platform® von WatchGuard bietet an Zero-Trust-Prinzipien ausgerichteten Netzwerk-, Endpoint- und Identitätsschutz in einer einzigen, integrierten Plattform, die es MSPs ermöglicht, die betriebliche Komplexität zu reduzieren, Sicherheitsergebnisse zu verbessern und ihr Geschäft effizienter auszubauen. WatchGuard genießt das Vertrauen von mehr als 25.000 MSPs, die weltweit über 1,5 Millionen Kunden schützen, und ermöglicht es Partnern, starke, messbare Sicherheitsergebnisse für Kunden auf der ganzen Welt zu liefern. Weitere Informationen finden Sie unter WatchGuard.com/de.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49-206-596-1001

INTERNATIONALER VERTRIEB: +1-206-613-0895

WEB www.watchguard.com/de

Mit diesem Dokument werden keine ausdrücklichen oder stillschweigenden Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2026 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Unified Security Platform und AuthPoint sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilnr. WGCE67967_091626

