DATENBLATT

# Cloud Detection and Response

## Stoppen Sie das Cloud-Risiko dort, wo es beginnt – bevor es zu einem Sicherheitsvorfall wird.

Die meisten Sicherheitsverletzungen stammen nicht von Hackern, die von außen eindringen. Sie stammen von Dingen, von denen Sie gar nicht wissen, dass sie existieren, von Einstellungen, die Sie nie offen lassen wollten, und von vertrauenswürdigen Konten, die gestohlen oder missbräuchlich verwendet werden. Microsoft 365, Google Workspace, Salesforce und Dutzende von KI- und SaaS-Anwendungen sind jetzt das primäre Ziel für den Diebstahl von Anmeldedaten, Missbrauch von Fehlkonfigurationen und Missbrauch von Schatten-IT. Herkömmlichen Endpoint- und Netzwerksicherheitstools mangelt es an Einblick darin, was in diesen Umgebungen passiert, nachdem der Zugriff gewährt wurde.

Mit WatchGuard CloudDR entdecken wir kontinuierlich versteckte Cloud-Anwendungen, sperren riskante Konfigurationen und stoppen Identitätsmissbrauch, sodass Angreifer ihre einfachste Angriffsmöglichkeit verlieren. Mit einer KI-nativen, agentenlosen Plattform, die kontinuierliche Transparenz, Erkennung und automatisierte Reaktion über SaaS- und Cloud-Umgebungen hinweg bietet – speziell für MSPs und die von ihnen geschützten Kunden entwickelt.

## SCHUTZ VOR

### Identitätsdiebstahl

Gestohlene Anmeldedaten, Missbrauch von Sitzungs-Tokens, MFA-Umgehung und ruhende Konten mit zu vielen Berechtigungen machen den legitimen Zugriff zu einem Verstoß.

### Fehlkonfigurationen

Standardeinstellungen, übermäßig freizügiges Teilen und Konfiguration Drift schaffen einfache Einstiegspunkte, die Angreifer ohne ausgeklügeltes Hacking ausnutzen können.

### Schatten-IT und KI

Mitarbeiter verbinden nicht autorisierte Apps und KI-Tools, was zu einem Datenrisiko und einem Lieferkettenrisiko führt, das die IT nicht sehen kann.

## FUNKTIONSWEISE

### Transparenz + Erkennung + Reaktion – In einer einheitlichen Plattform

WatchGuard CloudDR™ lässt sich über umfassende, agentenlose API-Verbindungen direkt in SaaS-Plattformen integrieren. Es muss keine Software installiert und kein Agent bereitgestellt werden und die Leistung der Geräte von Endanwendern wird nicht beeinträchtigt. Nach der Verbindung bewertet CloudDR kontinuierlich Konfigurationen, überwacht Aktivitäten und setzt Best Practices für die Sicherheit durch – automatisch.

#### Erkennung von Schatten-IT

Erkennt alle Cloud-Anwendungen und OAuth-verbundenen Integrationen im gesamten Unternehmen – einschließlich KI-Tools. Identifiziert, welche Apps mit Risiken behaftet sind, und setzt Richtlinien zur Anwendungsnutzung durch.

#### Compliance-Sichtbarkeit

Hunderte von vorkonfigurierten Richtlinien sind auf CIS Controls, NIST CSF und SOC 2 abgestimmt. Integrierte Berichte liefern für Audits geeignete Nachweise ohne manuelle Arbeit.

#### Identity Threat Detection & Response (ITDR)

Überwacht das Anwender- und Kontoverhalten über SaaS-Plattformen hinweg. Erkennt kompromittierte Konten, MFA-Umgehung, unmögliche Ortswechsel und verdächtige Aktivitäten. Widerruft automatisch den Zugriff oder erzwingt Kontrollen in Echtzeit.

#### Integrierte, automatisierte Abhilfemaßnahmen

Durch die Massenbehebung von Fehlern in allen Umgebungen werden manuelle Überprüfungszyklen überflüssig. Probleme werden kontinuierlich behoben und nicht erst Wochen später während eines regelmäßigen Audits entdeckt.

#### SaaS-Sicherheitsmanagement

Überwacht kontinuierlich Cloud-Anwendungskonfigurationen anhand von Best Practices für die Sicherheit. Erkennt riskante Einstellungen, übermäßige Freigabe und Konfigurationsabweichungen – und behebt diese automatisch.

#### Mandantenfähige MSP-Konsole

Eine zentrale Oberfläche für alle Kundenumgebungen. Speziell für Skalierung, Standardisierung von Richtlinien, Überwachung von Risiken und Nachweis der Sicherheit für jeden Kunden von einer Plattform aus.

# Warum WatchGuard CloudDR?

### 01 Einheitliche Abdeckung

Andere Lösungen beheben nur einen Teil des Problems. WatchGuard CloudDR deckt Schatten-IT, Fehlkonfigurationen und Identitätsbedrohungen zusammen ab und beseitigt die Ausbreitung von Tools, fragmentierte Ansichten und betriebliche Komplexität.

### 02 Direkt umsetzbar

Nicht nur Warnmeldungen. WatchGuard CloudDR liefert klare, umsetzbare Erkenntnisse: was falsch ist, warum es wichtig ist und wie man das Problem beheben kann – mit integrierter Massenfunktion zur Fehlerbehebung und Automatisierung.

### 03 MSP-First-Architektur

Direkt Mandantenfähig. Einsatzbereite Workflows für die MSP-Skalierung, die nicht durch ein Unternehmensprodukt nachgerüstet werden. Passt einfach in bestehende oder neue Servicepakete für eine umfassende, erschwingliche, verwaltete Lösung.

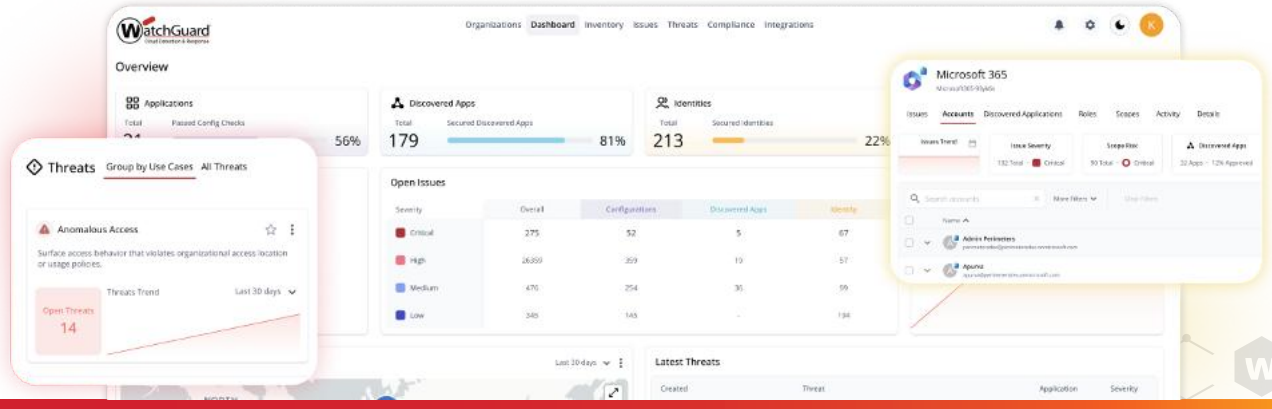
### 04 Agentenlose Bereitstellung

Ohne Installation von Software. Keine Auswirkungen auf die Leistung. WatchGuard CloudDR stellt eine direkte Verbindung zu SaaS-APIs her, um sofortig Mehrwert zu erzielen. Die Bereitstellung erfolgt normalerweise in einer Kundenumgebung innerhalb von wenigen Minuten.

## Unterstützte Cloud-Anwendungen

WatchGuard CloudDR unterstützt mehr als 40 Anwendungen, wobei neue Integrationen kontinuierlich hinzugefügt werden, um die sich entwickelnde Cloud-App-Landschaft zu verfolgen. **Zu den unterstützten Anwendungen gehören:**

- Atlassian Guard
- Atlassian Jira
- BambooHR
- Bitbucket
- Box
- Confluence
- Datadog
- Docusign
- DropBox
- Duo
- E-Mail
- EntraID
- GitHub
- GitLab
- Google Workspace
- HiBob (in Kürze verfügbar)
- HubSpot
- Jamf
- JumpCloud
- Microsoft 365
- Microsoft Intune
- Monday.com
- MongoDB
- Okta
- OneLogin
- OpenAI
- Salesforce
- Sentry
- Service Now
- SharePoint
- Slack
- Teams
- Trello
- Webhook
- Zendesk
- Zoom




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

**Weitere Informationen erhalten Sie unter: www.watchguard.com/wgrd-products/sase/cloud-detection-response**

## 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 WatchGuard Technologies, Inc.