

Cloud Detection and Response



Stop Cloud Risk Where It Starts — Before It Becomes an Incident.

Most breaches don't come from hackers breaking in. They come from things you don't know exist, settings you never meant to leave open, and trusted accounts that are stolen or abused. Microsoft 365, Google Workspace, Salesforce, and dozens of AI and SaaS applications are now the primary target for credential theft, misconfiguration exploitation, and shadow IT abuse. Traditional endpoint and network security tools lack visibility into what happens within these environments after access is granted.

With WatchGuard CloudDR, we continuously discover hidden Cloud apps, lock down risky configurations, and stop identity misuse so attackers lose their easiest path to an attack. With an AI-native, agentless platform that delivers continuous visibility, detection, and automated response across SaaS and Cloud environments — built for customers and the end users they protect.

PROTECT AGAINST

Identity Threats

Stolen credentials, session token abuse, MFA bypass, and dormant over-privileged accounts turn legitimate access into a breach.

Misconfigurations

Default settings, overly permissive sharing, and configuration drift create easy entry points that attackers exploit without sophisticated hacking.

Shadow IT & AI

Employees connect unauthorized apps and AI tools, creating data exposure and supply chain risk that IT cannot see.

HOW IT WORKS

Visibility + Detection + Response — In One Unified Platform

WatchGuard CloudDR™ integrates directly with SaaS platforms using deep, agentless API connections. There is no software to install, no agent to deploy, and no performance impact on end-user devices. Once connected, CloudDR continuously evaluates configurations, monitors activity, and enforces security best practices — automatically.

Shadow IT Discovery

Discovers all Cloud applications and OAuth-connected integrations across the organization — including AI tools. Identifies which apps carry risk and enforces application use policies.

Compliance Visibility

Hundreds of pre-configured policies map to CIS Controls, NIST CSF, and SOC 2. Built-in reporting delivers audit-ready evidence without manual assembly.

Identity Threat Detection & Response (ITDR)

Monitors user and account behavior across SaaS platforms. Detects compromised accounts, MFA bypass, impossible travel, and suspicious activity. Automatically revokes access or enforces controls in real time.

Automated Remediation Built-in

Bulk remediation across all environments eliminates manual review cycles. Issues are fixed continuously, not discovered weeks later during a periodic audit.

SaaS Posture Management

Continuously monitors Cloud application configurations against security best practices. Detects risky settings, over-permissive sharing, and configuration drift — and remediates automatically.

Why WatchGuard CloudDR?

01

Unified Coverage

Other solutions only solve one piece of the problem. WatchGuard CloudDR covers shadow IT, misconfigurations, and identity threats together — eliminating the tool sprawl, disconnected views, and operational complexity.

02

Actionable by Design

Not just alerts. WatchGuard CloudDR delivers clear, actionable insights: what's wrong, why it matters, and how to fix it — with built-in bulk remediation and automation.

03

Modern Architecture

Ready to use workflows that are not retrofitted from an enterprise product. Easily managed with other WatchGuard security services for a comprehensive, affordable solution.

04

Agentless Deployment

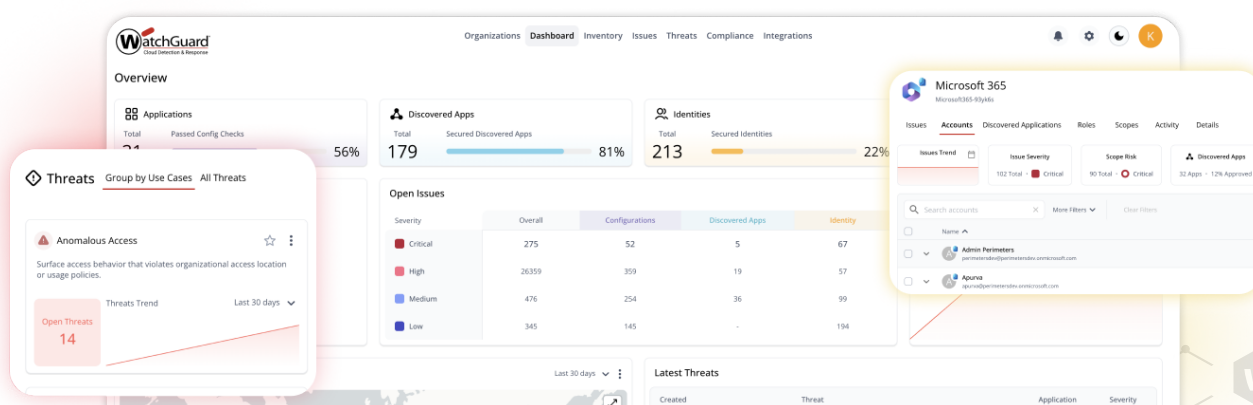
No software to install. No performance impact. WatchGuard CloudDR connects directly to SaaS APIs for immediate time-to-value; typically deployed across a customer environment in minutes.

Supported Cloud Applications

WatchGuard CloudDR supports 40+ applications, with new integrations added continuously to track the evolving Cloud app landscape.

Supported applications include:

- Atlassian Guard
- Atlassian Jira
- BambooHR
- Bitbucket
- Box
- Confluence
- Datadog
- Docusign
- Dropbox
- Duo
- Email
- EntraID
- Github
- Gitlab
- Google Workspace
- HiBob (Coming Soon)
- Hubspot
- Jamf
- Jumpcloud
- Microsoft 365
- Microsoft Intune
- Monday.com
- MongoDB
- Okta
- OneLogin
- OpenAI
- Salesforce
- Sentry
- Service Now
- SharePoint
- Slack
- Teams
- Trello
- Webhook
- Zendesk
- Zoom



Complete Cloud Protection – Without Enterprise Complexity or Cost.

Learn more at www.watchguard.com/wgrd-products/sase/cloud-detection-response

About WatchGuard

WatchGuard Technologies is a global leader in unified cybersecurity. For more than 30 years, WatchGuard has defined how to deliver security at scale, continuously innovating to stay ahead of every major shift in the threat landscape. WatchGuard's AI-powered Unified Security Platform® delivers zero trust-aligned network, endpoint, and identity protection in a single, integrated platform, to reduce operational complexity, improve security outcomes, and grow their businesses more efficiently. Trusted by over 1.5 million customers worldwide.

To learn more, visit WatchGuard.com