



eBook

The Missing MSP Service: Cloud Risk Management

Cloud Detection and Response for client
applications, identities, and configurations





Table of contents

- 01 Client Cloud Risk Management
- 02 Shadow IT and Shadow AI
- 03 Cloud Misconfigurations
- 04 Identity Threats
- 05 Introducing WatchGuard CloudDR
- 06 The CloudDR Advantage
- 07 The MSP Opportunity



Client Cloud Risk Management

Your clients are exposed to unmanaged risks in the cloud. You already own those risks.

A client's cloud applications, identities, and configurations create a dynamic environment that changes every day. Endpoint, firewall, and email security controls offer limited visibility into the cloud. After authentication, most cloud activity evades traditional on-premises security controls.

70%

of breaches now involve data stored in the cloud or hybrid-cloud environments.

IBM Cost of a Data Breach Report 2026

Microsoft 365, Google Workspace, SaaS applications, user identities, file sharing, and AI tools have created an attack surface that MSP security stacks were never designed to monitor. A single client tenant runs dozens of third-party SaaS applications, all with access to client data in the cloud, that most MSPs cannot see.

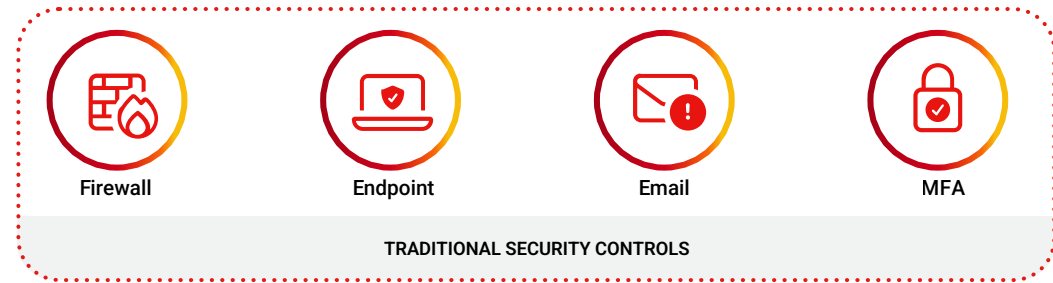
125

average cloud applications discovered during a client's first assessment

WatchGuard CloudDR deployment data

In that visibility gap, a compromised account in the cloud can create mailbox forwarding rules, download files in bulk, grant a malicious app access to the tenant, change permissions, or escalate its own privileges. That activity never generates an alert in the traditional MSP stack. As attackers increasingly use AI to identify exposed applications, weak permissions, and misconfigurations, MSPs need a new approach to build client trust and grow margins.

FOCUS OF TRADITIONAL MSP SECURITY



CLOUD VISIBILITY GAP

Critical activity happens after authentication, outside the visibility of traditional MSP tools.

SHADOW IT AND SHADOW AI

Unapproved SaaS applications

AI tools and copilots

OAuth and third-party access

MISCONFIGURATIONS

Excessive permissions

Insecure sharing settings

Configuration drift

IDENTITY THREATS

Compromised credentials

Post-login account abuse

Privilege escalation

MSPs cannot protect what they cannot see

The Result

Critical cloud activity occurs outside traditional security visibility, creating operational gaps, investigative delays, and business risk. Whether cloud security is formally in scope or not, MSPs already own the risk. Without visibility into cloud applications, identities, and configurations, cloud incidents become an MSP problem long before they are detected.

The Three Cloud Risks MSPs Must Control

While client environments continue to grow in complexity, most cloud incidents can be traced back to three categories of risk:

01

VISIBILITY

Shadow IT and Shadow AI put unmanaged SaaS applications, unknown third-party access, and unmonitored data movement outside MSP visibility.

02

GOVERNANCE

Cloud Misconfigurations erode risk posture through excessive permissions, insecure sharing settings, and configuration drift that breaks compliance controls.

03

EXPOSURE

Identity Threats exploit compromised credentials, weak authentication controls, and account abuse after login, where the speed of detection and response is critical.



WHAT MODERN MSPS NEED

One unified platform to manage cloud risks across Microsoft 365, Google Workspace, 40+ SaaS applications, identities, user activity, and AI tools. We call it:



CloudDR
Cloud Detection
and Response

With CloudDR, you will:

1. See the cloud risks traditional security stacks miss across SaaS applications, identities, misconfigurations, and shadow AI.
2. Simplify cloud security operations by bringing visibility, detection, investigation, and remediation together.
3. Scale security across customers with multi-tenant management, automation, and more efficient remediation.
4. Turn cloud security into a business opportunity with continuous compliance, stronger customer conversations, and a scalable recurring service.

Shadow IT and Shadow AI

Cloud environments are exposing clients to unmanaged risks.

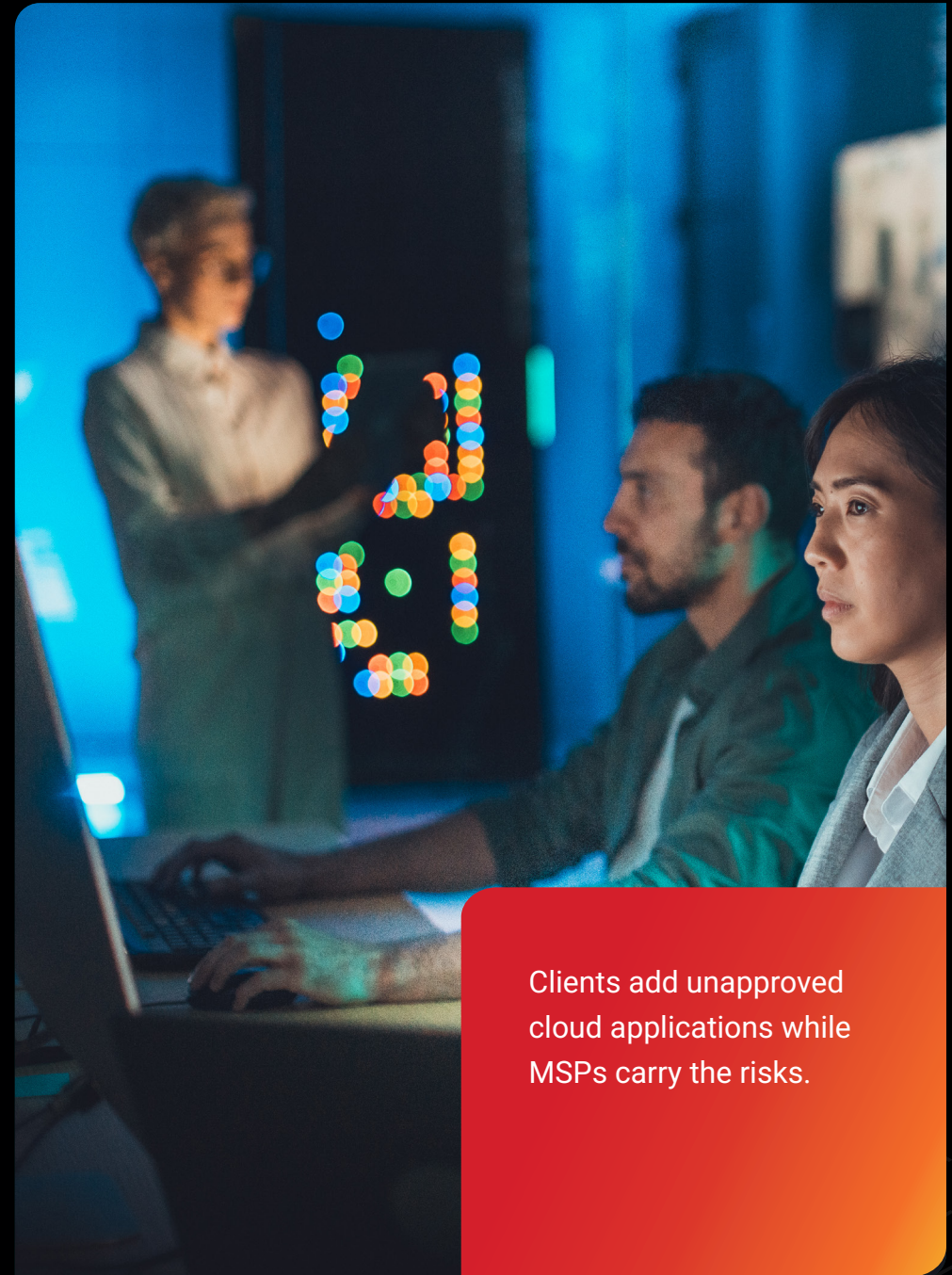
55%

of organizations have employees adopting SaaS applications without security involvement

Cloud Security Alliance, State of SaaS Security Report 2025

File sharing tools, collaboration platforms, browser extensions, AI services, and SaaS applications connect directly to business environments without security review or operational oversight. An employee with a legitimate account establishes the connection. It never reaches a ticket queue.

IT used to request, review, and grant access. Now, a user adds a cloud application in a few clicks. Every unmanaged application widens the attack surface.



Clients add unapproved cloud applications while MSPs carry the risks.



How Shadow IT Happens

MSPs usually learn about a new SaaS or AI application after it causes a problem. A file gets shared externally, an integration breaks, or an investigation turns up an application that was not approved. By then, that application has had access to client data for weeks or months. A periodic review closes the gap only until the next application appears.

Visibility is only the first step. Analysts also need to quickly understand what happened, why it matters, and what action to take. As cloud activity grows across customer environments, reducing the time from discovery to remediation becomes critical to scaling security operations.

COMMON SHADOW IT RISKS

- Sensitive data exposure
- Compliance violations
- Unreviewed OAuth grants into the tenant
- Unapproved file sharing
- Unknown third-party access



The Rise of Shadow AI

64%

of employees use unsanctioned AI tools for work tasks

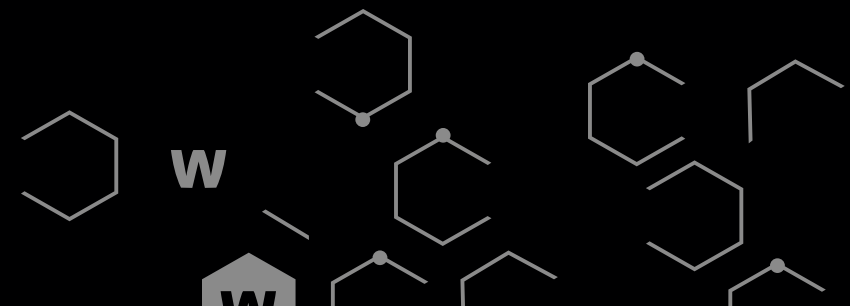
WatchGuard Cybersecurity Hygiene Report 2026

AI has significantly expanded the cloud risks traditionally associated with shadow IT. Employees access unsanctioned AI tools using company resources every day, and each session expands the organization's threat surface without anyone recording it.

Employees routinely use AI platforms for document creation, coding assistance, research, summarization, file analysis, and data processing, often without understanding how the platforms store, retain, share, or govern the information they submit.

COMMON SHADOW AI RISKS

- Uploading sensitive files into public AI tools
- Connecting AI tools directly into SaaS environments
- Sharing customer or financial data with AI platforms
- Employees bypassing approved workflows
- Compliance violations from unauthorized AI usage



Cloud Misconfigurations

Configuration drift starts on day one.

Almost
8
Months

to fix half of all weak-password and permission misconfiguration findings in third-party cloud environments

37%

of organizations had an admin account with MFA disabled on an IaaS platform

Verizon 2026 Data Breach Investigations Report

Modern cloud environments are complex and highly dynamic. A cloud configuration that is secure today will not remain secure over time. Configurations change constantly due to new users, new applications, permission changes, sharing policies, third-party integrations, AI-enabled workflows, and evolving vendor security recommendations.

Most security analysts already understand what a secure cloud configuration should look like. What they often lack is continuous monitoring capable of identifying when a secure configuration drifts into a risky state and validating that cloud configurations remain aligned with current security best practices.

How Misconfigurations Happen

Most MSPs have no mechanism to detect cloud misconfigurations and cannot respond quickly. Misconfigurations persist for months, and many are never fixed at all. Cloud configurations change daily in a multi-tenant environment, and a periodic manual audit only captures a single point in time.

COMMON CLOUD MISCONFIGURATIONS

- Excessive user permissions
- Public or unrestricted file sharing, including shares that were meant to be temporary
- Weak identity policies or inactive MFA
- Unused privileged accounts and local accounts left behind after an SSO migration
- Misconfigured SaaS security settings and vendor defaults that were never changed
- Insecure OAuth application access



Identity Threats

Attackers don't hack in. They log in.

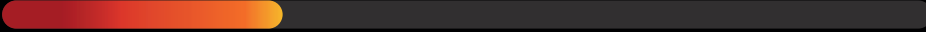
76% of employees reuse passwords across multiple accounts



78% of employees have at least one account without MFA



30% of employees share passwords with others



WatchGuard Cybersecurity Hygiene Report 2026

User identities have become extremely valuable for threat actors targeting cloud applications and services. Once they find a vulnerable target, attackers can gain access to client environments quickly through stolen passwords, reused credentials, and weak identity controls. With the rate of AI-driven attacks accelerating, the time to detect and respond to cloud incidents is more important than ever.

Identity risk now extends across Microsoft 365, SaaS applications, cloud storage, collaboration platforms, AI-enabled tools, and sensitive business data. As organizations adopt more cloud applications, user accounts are spread across multiple platforms, leading to accounts that may be forgotten, unmanaged, or left active after an employee leaves.

Remote workers, distributed locations, and hybrid operations each add identity requirements across every tenant.

How Identity Threats Happen

Identity-driven attacks use legitimate credentials and take place inside a session the platform has already authenticated. They generate little or no malware activity, blend into normal cloud usage patterns, and evade the security tools an MSP already runs.

COMMON IDENTITY EXPOSURES

- Weak passwords and lack of MFA
- External and guest accounts nobody reviews
- Shared and reused credentials
- Unidentified accounts inside the tenant
- Dormant accounts still carrying licenses and access
- Off-boarded users still active in SaaS apps



Introducing WatchGuard CloudDR

Cloud Detection and Response for the Modern MSP

WatchGuard CloudDR gives MSPs visibility into connected applications and AI tools, control over cloud configurations, and detection of identity threats after login. One platform covers all three cloud risks across every tenant an MSP manages.

CloudDR connects through OAuth and API integrations and begins returning findings within 30 minutes of administrator approval. Every finding includes severity, business impact, and recommended remediation, while automation and bulk actions accelerate response across tenants.



Discover Shadow IT and Shadow AI

CloudDR identifies connected applications through the OAuth grants behind them. Where an application never requested OAuth access, CloudDR identifies it from activation, sign-up, and registration emails within the tenant, which surfaces the AI services employees register for using a work address. CloudDR reads only critical metadata and does not scan the private information contained in an employee's message.

From a single view, a security analyst can review which users were granted which permissions and revoke the grant. Automated workflows approve, deny, or revoke application access across tenants without requiring a security analyst to open each one. The Shadow SaaS Inventory and the Discovered Applications Report turn each finding into audit-ready documentation.

SHADOW IT AND SHADOW AI USE CASES

- Shadow SaaS Applications from Risky Vendors
- Accounts from Shadow SaaS Applications marked "Not Approved"
- Shadow Application Accounts with Risky Scope Access
- Dormant Shadow Applications
- AI Shadow Application Accounts

Operational Outcome

MSPs gain visibility into previously unmanaged applications and AI services, enabling faster investigation, stronger governance, and reduced client exposure.

Manage Misconfigurations Continuously

CloudDR monitors configuration states continuously rather than waiting for a manual review or the next audit. Each detection identifies the affected setting, assigns a severity level, and specifies the required change, which removes the investigative work that precedes most fixes.

When the same finding appears across multiple tenants, CloudDR groups those findings and allows security analysts to remediate them in a single, bulk action.

CLOUD MISCONFIGURATIONS DISCOVERED

- Password policy gaps
- Legacy authentication enabled
- External calendar sharing
- Uncontrolled mail forwarding
- Unapplied sensitivity labels
- Overly broad admin roles
- Audit logging disabled

Operational Outcome

MSPs detect configuration drift within minutes, not months, and remediate findings across all affected tenants at once, holding client risk posture steady between audits.

Detect and Respond to Identity Threats

Identity attacks generate no malware and no endpoint alert. They produce a legitimate login followed by illegitimate behavior: a mailbox rule that forwards externally, a bulk download, a new OAuth grant, or a privilege escalation.

CloudDR monitors account behavior across all connected tenants to detect cloud identity abuse. When activity crosses a defined threshold, the security analyst responds from the same console, revoking sessions and tokens, disabling the account, or removing privileged access.

IDENTITY THREATS USE CASES

- Multi-Factor Authentication (MFA)
- Dormant Accounts
- Disabled Accounts
- External Accounts
- Unidentified Accounts
- Partially Off-boarded Accounts
- Unused Licenses

Operational Outcome

MSPs reduce identity risk by identifying dormant accounts, weak identity controls, and account exposures before attackers can exploit them.

Continuous Compliance and Audit Readiness

CloudDR maps client environments to hundreds of preconfigured policies aligned with CIS Controls, NIST, SOC 2, and 30+ compliance frameworks, with additional frameworks being added regularly. Each application receives a posture score. Each framework is measured on the percentage of controls passed. Risk posture and compliance are visible and continuously updated to ensure audit readiness.

The operational effect appears in audits and quarterly business reviews. CloudDR keeps every client's compliance posture current between audits, scored per framework, with the evidence behind each control ready to prove it across every tenant an MSP manages.

67% of organizations need additional support to manage growing compliance requirements

WatchGuard IT Survey 2026

Operational Outcome

Audit readiness stops being a project. MSPs can continuously track compliance posture, automatically collect evidence, and help customers prepare for audits with confidence. One-click PDF reporting delivers audit-ready documentation on demand, making compliance services easier to deliver and scale.



CloudDR tracks evidence as it accumulates and exports section-level reports to PDF on a daily, weekly, or monthly schedule, which replaces the manual assembly that normally precedes each review.

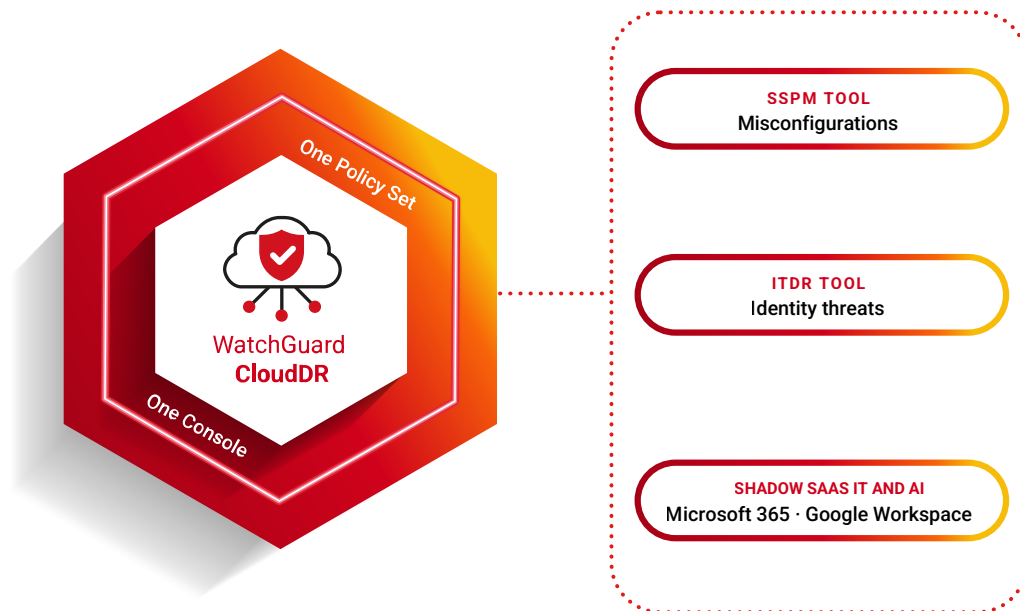


The CloudDR Advantage

Simplify Cloud Security Operations

CloudDR reduces the hours spent securing each client's cloud environment by streamlining investigation and remediation in a single operational platform. Most MSPs assemble cloud coverage from three sources: SSPM tools for misconfigurations, ITDR tools for identity threats, and the automated controls in Microsoft 365 and Google Workspace, which secure the platform but not the way each tenant is configured or used. That means separate licenses, consoles, renewal cycles, and margin absorbed by tool overhead rather than service delivery.

CloudDR consolidates all three. MSPs work from one console, one set of policies, and audit-ready reporting per customer, and can expand recurring cloud security services without the cost and effort of another tool.



Why WatchGuard CloudDR

01

Operate more efficiently. Respond faster. Scale with stronger margins.

CloudDR helps MSPs reduce manual effort, streamline cloud security operations, and grow recurring services without increasing operational overhead.

02

Actionable by design.

Every finding explains what happened, why it matters, and how to remediate it, with automation and bulk remediation built in.

03

MSP-first architecture.

Multi-tenant from the ground up, with ready-to-use workflows built for MSPs to strengthen existing managed security offerings and build new cloud security services.

04

Flexible choices to deploy.

Choose agentless or the FireCloud Agent. The agentless option has no software to install and no end-user impact. The FireCloud Agent is a lightweight endpoint companion that adds an additional layer of cloud activity monitoring where deeper visibility is needed.

Assess Cloud Risks in Minutes

Onboarding a tenant takes one step: an administrator approves the OAuth permissions, and CloudDR connects service-to-service via API. Findings are returned within 30 minutes. There is no agent to deploy, no end-user impact, and no per-tenant professional services engagement required.

Enable Cloud Security Capabilities

Instead of alert fatigue, tool sprawl, and preventable cloud incidents, MSPs get application visibility, risk posture control, and identity threat detection in one multi-tenant platform. Security analysts detect and respond to cloud threats quickly, and client systems, users, and data stay secure and compliant.

Build Trust and Grow Revenue



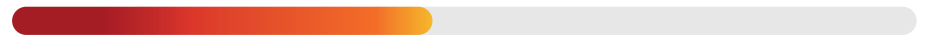
“MSPs are struggling with fragmented tools that only solve pieces of the cloud security problem. There’s a real need for something that brings visibility and response together in one place. WatchGuard CloudDR does exactly that.”

Neil Holme

Founder and CEO of Impact Business Technology

Priced per user per tenant, CloudDR is designed to attach to an existing managed security tier or stand up as a billable cloud security add-on. MSPs can grow recurring revenue without absorbing the cost of another tool.

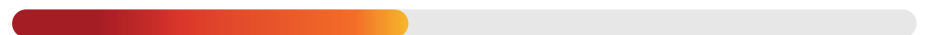
48% of organizations already rely on external providers to supplement internal teams



35% want more identity and access security from their providers



44% are willing to pay more for AI-driven threat detection and automated response



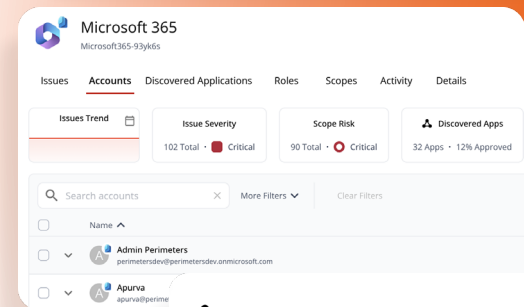
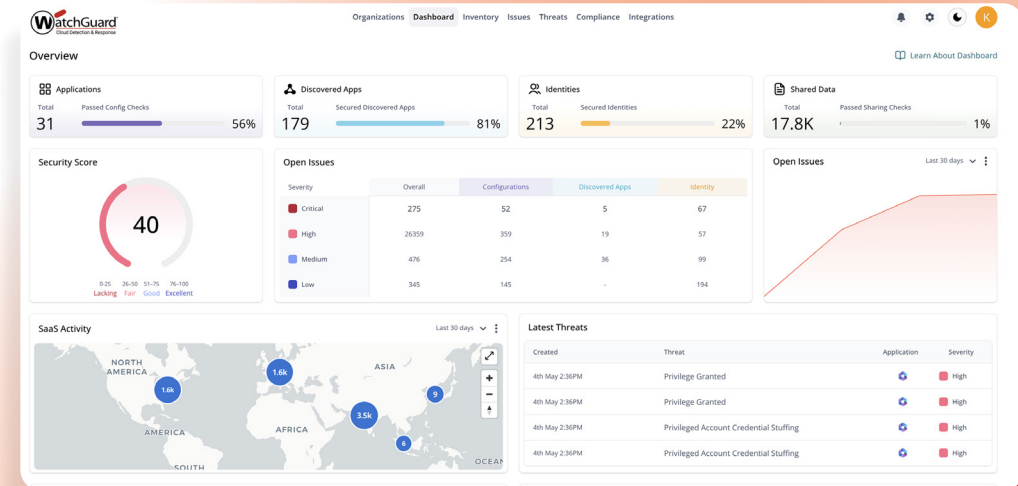
The MSP Opportunity

Start the Cloud Risk Conversation

Client adoption of SaaS and AI is not slowing down. The clients who are already asking for more identity and access security and are willing to pay for AI-driven detection are in your book of business today. MSPs don't have to wait for a cloud security incident to act. Connect CloudDR to a tenant and see what your current stack is missing within 30 minutes, then use those findings to start the cloud risk management conversation.

SUPPORTED APPLICATIONS INCLUDE:

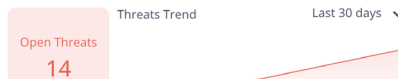
- Atlassian Guard
- Atlassian Jira
- Autotask
- BambooHR
- Bitbucket
- Box
- Confluence
- ConnectWise PSA OnPrem
- Claude
- Datadog
- DocuSign
- Dropbox
- Duo
- Email
- Entra ID
- GitHub
- GitLab
- Google Workspace
- HiBob
- HubSpot
- Jamf
- JumpCloud
- Microsoft 365
- Microsoft Intune
- Microsoft Teams
- monday.com
- MongoDB
- Okta
- OneLogin
- OpenAI
- Salesforce
- Sentry
- ServiceNow
- SharePoint
- Slack
- Trello
- Webhook
- Zendesk
- Zoom



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.



Dormant Accounts: Identify accounts that have not been used for a while and take action by disabling or removing them, along with any remaining privileges if needed.



Unused Licenses: Identify and review unused or inactive licenses to optimize license usage. Remove or reassign licenses that are no longer needed to reduce unnecessary cost and minimize access risk.



External Accounts: Review external accounts to determine their necessity, keep track of needed accounts, and disable or remove those no longer required, along with any remaining privileges if necessary.



Complete Cloud Protection – Without Enterprise Complexity or Cost.

CloudDR connects to Microsoft 365, Google Workspace, and the third-party SaaS applications and AI tools your clients use most. If a specific integration is not yet available, contact your WatchGuard partner manager.



Learn more at www.watchguard.com

Sources

WatchGuard IT Survey, Spring 2026
WatchGuard Cybersecurity Hygiene Report 2026
Verizon 2026 Data Breach Investigations Report
IBM Cost of a Data Breach Report 2026
Cloud Security Alliance, State of SaaS Security Report 2025

About WatchGuard

WatchGuard Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers (MSPs). For more than 30 years, WatchGuard has defined how MSPs 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, enabling MSPs to reduce operational complexity, improve security outcomes, and grow their businesses more efficiently. Trusted by more than 25,000 MSPs protecting over 1.5 million customers worldwide, WatchGuard enables partners to deliver strong, measurable security outcomes for customers across the globe. Learn more at WatchGuard.com

NORTH AMERICA SALES 1.800.734.9905

INTERNATIONAL SALES 1.206.613.0895

WEB www.watchguard.com

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2026 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Unified Security Platform, and AuthPoint are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No.WGCE67967_091626

