Cyber-T | Servicio Administrado

Powered by WatchGuard technology

HOJA TÉCNICA

Servicio de Detección y Respuesta Cloud

Detección, visibilidad y respuesta para riesgos en SaaS, identidad y colaboración empresarial

Detén el riesgo en la nube desde donde inicia, antes de que se convierta en un incidente.

La mayoría de las brechas no ocurren porque los hackers “entren por la fuerza”. Ocurren por elementos que no sabes que existen, configuraciones que nunca debieron quedar abiertas y cuentas confiables que son robadas o utilizadas indebidamente.

El Servicio de Detección y Respuesta Cloud de Cyber-T ayuda a las organizaciones a identificar, priorizar y responder ante riesgos en plataformas cloud y SaaS como Microsoft 365, Google Workspace, Teams, SharePoint, OneDrive y otras aplicaciones empresariales.

A diferencia de una protección enfocada solamente en endpoint o firewall, este servicio amplía la visibilidad hacia aplicaciones conectadas, permisos OAuth, actividad de usuarios, configuraciones inseguras, accesos anómalos y señales de compromiso que pueden derivar en fraude, fuga de información o interrupciones operativas.

Con WatchGuard CloudDR, descubrimos continuamente aplicaciones cloud ocultas, reforzamos configuraciones riesgosas y detenemos el uso indebido de identidades para que los atacantes pierdan su camino más fácil hacia un ataque.

PROTEGE CONTRA

Amenazas de identidad	Configuraciones riesgosas	Shadow IT e IA
Cuentas comprometidas, accesos anómalos, abuso de tokens de sesión, permisos excesivos y actividad sospechosa dentro de aplicaciones SaaS.	Ajustes inseguros, exposición de archivos, colaboración no controlada y desviaciones de configuración que incrementan la superficie de ataque.	Aplicaciones no autorizadas, herramientas de IA, integraciones externas y permisos OAuth que TI no siempre puede ver ni controlar.

CÓMO FUNCIONA

Visibilidad + Detección + Respuesta — en un solo servicio

Cyber-T integra tecnología WatchGuard CloudDR con nuestro modelo de servicio administrado con Mesa de Servicio para seguimiento de eventos, reportes ejecutivos y acompañamiento técnico para convertir señales de riesgo en acciones de mejora y remediación. Se integra directamente con sus plataformas SaaS mediante conexiones API profundas y sin agentes.
No hay software que instalar, ningún agente que desplegar y no genera impacto en el rendimiento de los dispositivos de los usuarios finales.
Una vez conectado, el servicio de CloudDR evalúa continuamente las configuraciones, monitorea la actividad y aplica automáticamente las mejores prácticas de seguridad.

Descubrimiento de Shadow IT

Identifica apps cloud, conexiones OAuth, IA y servicios externos con acceso a datos.
Identifica qué aplicaciones representan un riesgo y aplica políticas de uso de aplicaciones.

Detección de amenazas de identidad (ITDR)

Monitorea usuarios, accesos inusuales y posibles señales de compromiso SaaS. Detecta cuentas comprometidas, evasión de MFA, viajes imposibles y actividad sospechosa. Revoca automáticamente el acceso o aplica controles en tiempo real.

Postura de seguridad SaaS

Revisa continuamente configuraciones, permisos y exposición de información para reducir riesgos mediante mejores prácticas de seguridad. Detecta configuraciones riesgosas, uso compartido con permisos excesivos y desviaciones de configuración, y las remedia automáticamente.

Visibilidad de cumplimiento

Apoya gobierno, auditoría e ISO 27001 con evidencia, hallazgos y reportes. Con políticas preconfiguradas se alinean con controles CIS, NIST CSF y SOC2. Los reportes integrados entregan evidencia lista para auditoría, sin necesidad de prepararla manualmente.

Seguimiento por Mesa de Servicio

Remediación masiva en todos los entornos elimina los ciclos de revisión manual. Los problemas se corrigen de forma continua, en lugar de descubrirse semanas después durante una auditoría periódica. Documenta y atiende eventos mediante el canal formal Cyber-T con trazabilidad.

Remediación asistida

Orienta acciones correctivas: revocar permisos, revisar accesos y ajustar configuración. Servicio escalable que permite estandarizar políticas, monitorear riesgos y demostrar el valor de seguridad de todo el ambiente de nube.

CYBER-T 55-5929-0715 | froldan@cybert.com.mx | cybert.com.mx

¿Por qué necesito Detección y Respuesta Cloud?

HOJA TÉCNICA

01

Cobertura integral

Integra visibilidad de SaaS, identidad, permisos, aplicaciones conectadas y colaboración, complementando endpoint, correo, MFA y firewall.

02

Acción operativa

No solo muestra alertas: Cyber-T ayuda a clasificarlas, documentarlas, dar seguimiento y convertirlas en acciones de remediación.

03

Modelo MSP administrado

Servicio diseñado para operar con Mesa de Servicio, reportes, evidencia, responsables, seguimiento y mejora continua para clientes empresariales.

04

Implementación sin agentes

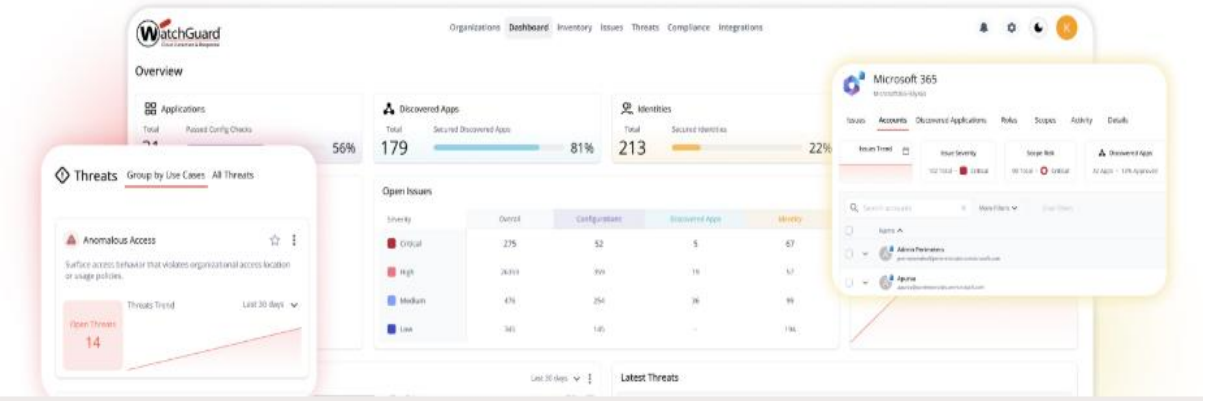
Conexión mediante integraciones API a plataformas SaaS compatibles, sin instalar software en los equipos de usuario y sin impacto de rendimiento.

Ambientes cloud y SaaS que puede cubrir el servicio

El servicio puede monitorear aplicaciones empresariales compatibles con WatchGuard CloudDR y otras soluciones del portafolio, con más de 40 integraciones que evolucionan conforme al ecosistema cloud del cliente.

Aplicaciones y servicios de referencia:

- 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



Protección Cloud administrada — Sin el costo y complejidad empresarial innecesaria.

Evaluación, monitoreo, seguimiento y respuesta con Mesa de Servicio Cyber-T

Acerca del Servicio y de WatchGuard

El Servicio de Detección y Respuesta Cloud de Cyber-T utiliza tecnología de WatchGuard, fabricante global de ciberseguridad durante más de 30 años, reconocido por su enfoque en protección simplificada, visibilidad centralizada y servicios integrados.

Dentro del portafolio Cyber-T, WatchGuard permite complementar este servicio con CloudDR, AuthPoint MFA, Email Protection, Endpoint Security, Firebox con Total Security, ThreatSync/XDR y visibilidad cloud a traves de su Plataforma de Seguridad Unificada® impulsada por IA, asi se cubre identidad, correo, endpoint, red, aplicaciones SaaS y operación administrada.

Con la confianza de más de 25,000 MSPs que protegen a más de 1.5 millones de clientes en el mundo, WatchGuard permite a sus socios GOLD como Cyber-T integrar estas capacidades con Mesa de Servicio, reportes ejecutivos, soporte especializado y acompañamiento de mejora continua.

CONTACTO 55-5929-0715 | froldan@cybert.com.mx | cybert.com.mx