NUVOL

The right people, for the best service

NUVOL

SERVICIOS DE CIBERSEGURIDAD

México, Panamá, Colombia

@cybernuvol.com

SERVICIOS

- Centro de Operaciones SOC as a Service
- Seguridad Microsoft Azure & O365
- Seguridad AWS
- Security Awareness
- Simulación de Intrusión de Ataque
- Análisis de Vulnerabilidades
- Automatización de Cumplimiento
- Pentest & Ethical Hacking
- Pruebas de ingeniería social
- Servicios Red Team
- Protección de Datos Personales
- Auditorías ISO 27001
- Protección de Marca
- Gobierno, Riesgo y Cumplimiento

CONTACTO:

Ciudad de México
M. cfarfan@cybernuvol.com
T. 55 9124 0158 o 442 808 7788
Dirección: Edificio City No 11B, Blvd. Manuel Ávila Camacho No. 3130, Tlalnepantla, C.P. 54020, CDMX.

Panamá
M. jvega@cybernuvol.com
Dirección: Edif. 109, Ciudad del Saber, Panamá.

Colombia
M. info@cybernuvol.co
Dirección: Oficina We Work, Piso 5, Carrera 7 #116-50 Bogotá 110221

NUVOL
The right people, for the best service

PORTAFOLIO DE SERVICIOS

PROFICIO™

Centro de Operaciones SOC as a Service

Proficio es un servicio del tipo "Managed Detection and Response (MDF) de clase mundial, ofrece monitoreo de seguridad y detección de amenazas 24/7 con servicio de respuesta a incidentes automatizados.

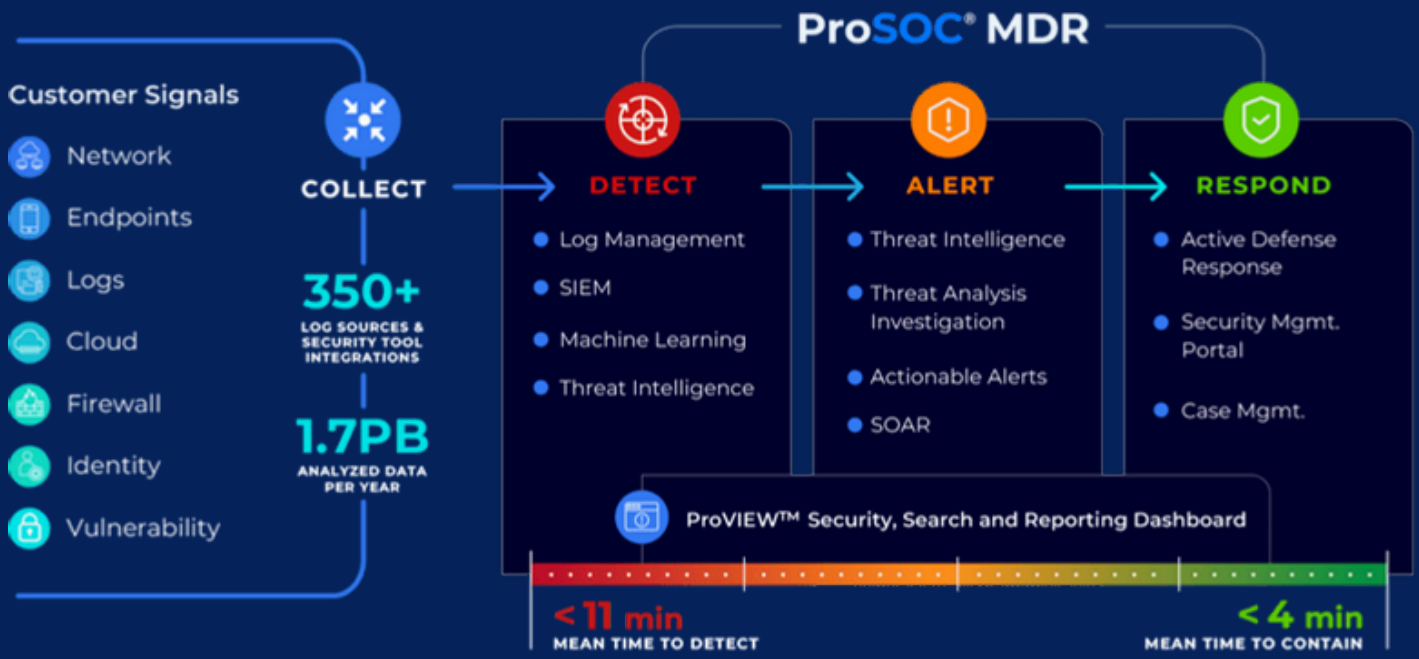
- Expertos 24 × 7 de seguimiento y análisis continúo.
- 3 SOC´s a nivel mundial: Singapur, San Diego y Barcelona, "follow the sun"
- Threat Intelligence
- Threat Hunting e investigación de amenazas
- Defensa activa (SOAR).
- Protección avanzada contra amenazas, internas y perimetrales.
- Experto de seguridad, reunión mensual de seguimiento
- Certificación SOC Tipo II e ISO 27001:2013

Servicios Detección y respuesta gestionadas:

1. **ProSOC MDR:** SOC como servicio 24/7 con tecnología SIEM alojada en Proficio
2. **ProSOC MDR para Microsoft**: Gestión de plataformas y SOC como servicio 24/7 con tecnología de Microsoft Sentinel
3. **ProSOC MDR para endpoint:** Protección contra amenazas en todos sus endpoints
4. **ProSOC MDR para Splunk:** Gestión de plataformas y SOC como servicio 24/7 con tecnología de Splunk
5. **ProSOC XDR:** Potente monitorización 24/7 SOC-as-a-Service impulsado por la plataforma SIEM

Servicio Monitoreo y Detección de Amenazas

El servicio administrado de Nuvol/Proficio proporciona un servicio SOC, llamado ProSOC, completamente gestionado utilizando el conjunto de herramientas más avanzado de la industria, administrado por un equipo de expertos en SIEM y SOC



Especificaciones técnicas del servicio

Servicio PROSOC			
THREAT MANAGEMENT / GESTIÓN DE AMENAZAS			
Threat Monitoring	*	Investigación de analistas de amenazas	*
Caza de amenazas basada en machine Learning	*	Biblioteca de contenido de amenazas	*
Threat Hunting	*	**Notificación de amenazas**	*
THREAT DEFENSE / DEFENSA DE LA AMENAZA			
Threat Intelligence Profiler	*	**Active Defense**	*
Tipos de inteligencia de amenazas	*	Seguridad perimetral	*
Alcance de la amenaza	*	Endpoint Security	*
Fuentes de amenazas principales	*	Matriz de tecnología compatible	*
Puntuación de reputación de amenazas	*		
GESTIÓN DE REGISTROS			
Hot Log Storage (1 año)	*		*
Instancia Dedicada Elastic	*		
SERVICIOS PRINCIPALES			
Portal de clientes		**Gestión del éxito del cliente**	*
ProView	*	**Expert on Call**	*
ITSM	*		
Investigador de Amenazas	*		

En esencia, PROSOC MDR de Proficio es un SOC como servicio gestionado por expertos, con tecnología incluida, que proporciona detección proactiva y respuesta rápida a incidentes de seguridad.

¿Qué se requiere?, requisitos técnicos

Nuvol/Proficio sigue un enfoque minucioso y metódico para implementar servicios para nuevos clientes. El proceso comienza con la comprensión y documentación de la red y las políticas de un cliente y continúa hasta la capacitación y la ejecución del servicio.

PASOS	DESCRIPCIÓN
Event Collection	El cliente configura dispositivos dentro del entorno para transmitir datos a un colector ProSOC y configurarlos para que el recopilador ProSOC recupere datos. Los tipos de recopilación más comunes son la transmisión de syslog, el sondeo de WMI para orígenes de datos de Windows y las conexiones de bases de datos a tipos especiales de productos, como los servidores de antivirus. Las características de dicho colector son: 6 GB RAM, 4 VCPUs, 40 GB HD, Una interfase de red, HyperV o VMWare
Collector Event Processing	Una vez recibido el evento, ProSOC Collector analiza, agrega y normaliza los eventos y luego los transmite a nuestro SIEM a través de una conexión segura.
SIEM Event Processing	El ProSOC/ SIEM recibe los eventos y realiza la gestión de correlación e incidentes a través del SIEM. Es en este momento cuando los eventos están disponibles para revisión y escalamiento.
Analyst Review	Los analistas de Proficio en línea 24x7 realizan varios análisis de datos de alto nivel con paneles, visores de consultas y canales activos para evaluar las tendencias que se deben escalar a los clientes de ProSOC como posibles incidentes de seguridad.
Automated Notifications	Pueden ocurrir varios tipos de incidentes que no requieren revisión adicional por parte de Proficio y necesita ser escalado inmediatamente al cliente. Las notificaciones automáticas se envían al cliente y el caso correspondiente con los eventos que desencadenaron el caso se guardan en el Portal de ProView.
ProSOC Reports	Los informes del SIEM se pueden enviar a petición del cliente. Estos informes pueden ser generados en un horario estándar o ad-hoc por el cliente en el Portal ProView
Analyst Action Notifications	Muchas alertas no se pueden enviar directamente al cliente y requieren una revisión de analistas para evaluar si se ha producido un incidente de seguridad. Para los eventos considerados por el analista como una seguridad potencial, estos casos se derivan al cliente como una notificación.
ProView Portal Access	Los clientes pueden revisar tableros, informes, casos y buscar eventos en el Portal ProView, utilizando tecnología Splunk para un manejo más eficiente de los datos.
ProView Reports	Los clientes recibirán un resumen de los servicios, como un resumen mensual de notificaciones, un informe TIP diario u otros tipos de informes personalizados que detallan un resumen de los servicios.

Proceso de toma del servicio en 6 semanas

Implementación PROSOC	semanas					
	1	2	3	4	5	6
Reunión Inicial - Kick off Revisión de la documentación Recopilación de datos Diagrama de Red Bienes Contacto Escalada Políticas de seguridad						
Implementación VM Collector y acceso a la red Cuenta de servicio de dominio						
Configuración de registros y casos de usos Configurar el dispositivo para la recopilación de registros Habilitar casos de uso y reglas de correlación para fuentes de registro						
Modelado de activos Configurar dispositivos avanzados para la recopilación de registros						
Personalización Personalización del tablero Usar la personalización de casos Personalización de informes						

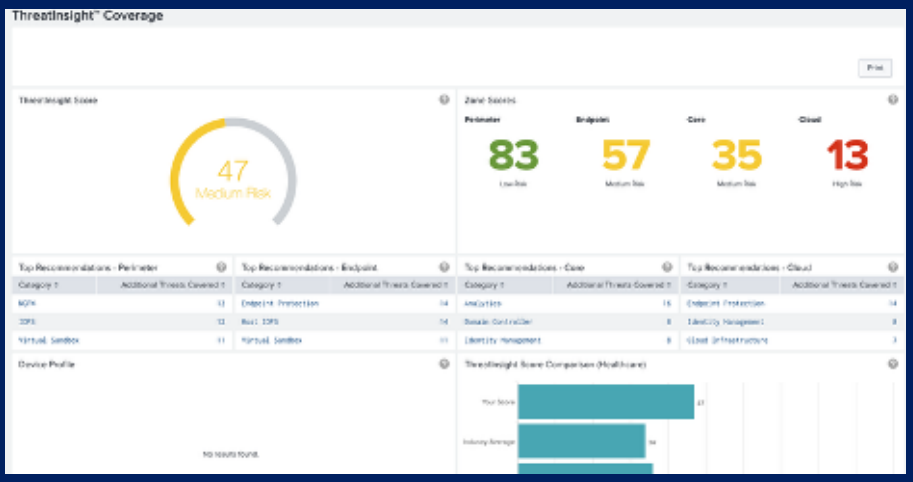
Dashboard e informes

El portal ProView de Nuvol/Proficio se desarrolló para brindar a los equipos de seguridad una visión más profunda de la postura de seguridad de su organización.

El dashboard ejecutivo presenta resúmenes de alto nivel que le permiten ver los detalles, las tendencias y podrá tener una visión completa de su entorno de seguridad. A continuación, se muestran unos ejemplos del portal ejecutivo

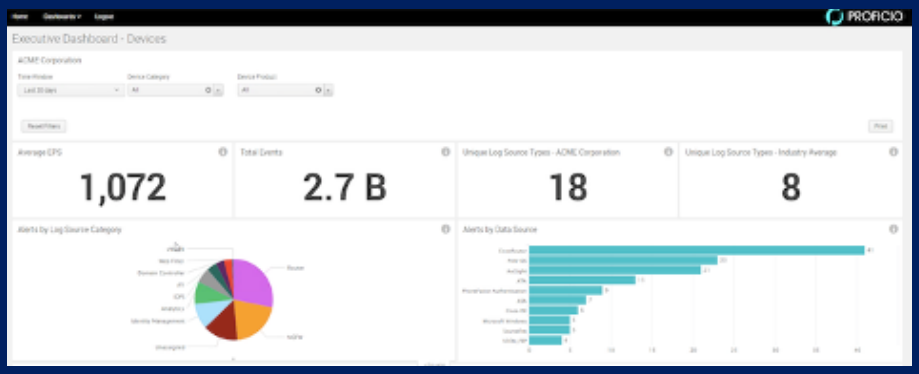
Portal ProView Portal

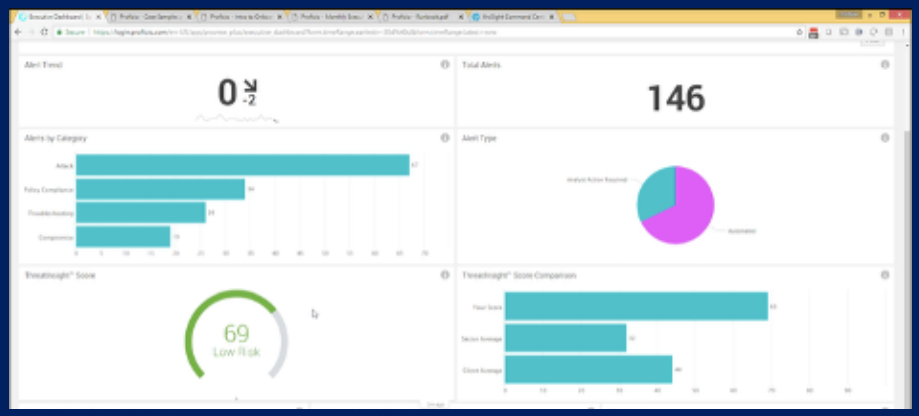
El portal ejecutivo provee un análisis detallado del estado de salud para las diferentes zonas (core, perímetro, end users y cloud), como la tendencia de alertas, casos de uso para análisis de causa- raíz y una calificación del riesgo comparándolo con otros clientes de Proficio o bien, con el promedio de la industria.



Alertas de alta calidad

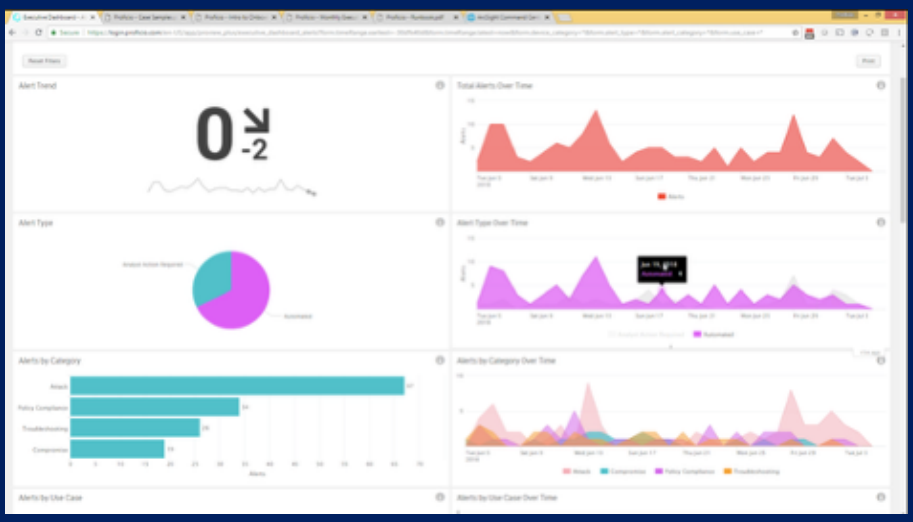
El objetivo de Nuvol/Proficio es proporcionar a los clientes alertas accionables a los pocos minutos de un evento desencadenante. Como se muestra en el ejemplo anterior, las alertas útiles incluyen información suficiente para ayudar al destinatario a comprender el contexto de la alerta y las recomendaciones que permiten una acción inmediata.





Informes predefinidos, parametrizables o a solicitud

Nuvol/Proficio monitorea activamente cada elemento de SIEM en busca de salud y rendimiento, monitorea cada fuente de registro crítica y alerta si una fuente de registro deja de enviar registros durante un período de tiempo específico. Nuvol/Proficio proveerán al cliente un Dashboard con los KPIs y métricas del servicio.



¿Quién es Proficio?

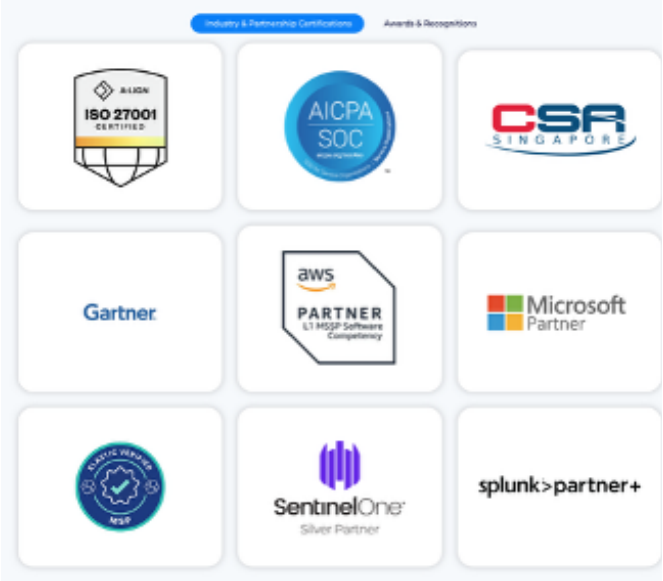
Proficio fue fundado en el año 2010, es un galardonado proveedor de servicios de seguridad administrados (MSSP), que brinda servicios de monitoreo de seguridad y detección y respuesta administrada (MDR) las 24 horas del día, los 7 días de la semana a través de su red global de Centros de operaciones de seguridad modernos, los cuales se encuentran en San Diego, Barcelona y Singapur, monitoreando eventos de seguridad y buscando ataques dirigidos.

@proficio.com

Beneficios

- Presencia global con 3 SOC´s ubicados en Singapur, Barcelona y San Diego en un esquema "Follow the sun", monitoreo 24x7
- Contamos con más de 50 personas certificadas en tecnología SIEM
- Contamos con más de 100 ingenieros certificados en otras tecnologías, desde firewalls, CEH, CISM, CISSP, etc.
- MMSP con certificación SOC 2, así como en el framework NIST e ISO 27001:2013
- Servicio integrado de Threat Intelligence profiles y threat hunting, tanto para los servicios web, dark web y redes sociales.
- Ofrecemos un SLA de notificación y tiempo de respuesta sumamente agresivo: 30 minutos para los incidentes de prioridad 1.
- Nuestro portal web permite al usuario profundizar y pivotar sobre un activo, incidente o usuario para comprender mejor la naturaleza.
- Implementación en 30 días, sin agentes, logs ilimitados.

Cumplimiento y Certificaciones



MICROSOFT ZERO TRUST

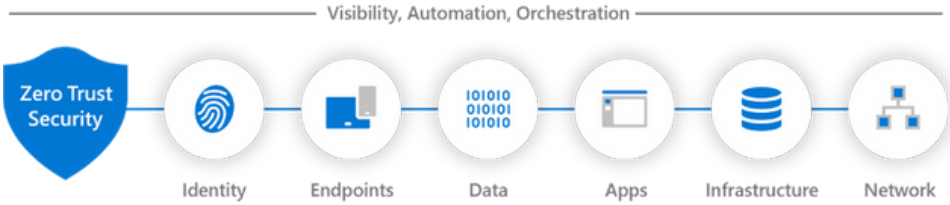
Microsoft

Servicios Administrados Microsoft

Contamos con diferentes modelos de servicios: consultoría, implementación por proyecto o soporte administrado con especialistas certificados en Microsoft. Trabaje con un administrador de cuentas técnico para evaluar, revisar, definir, planificar y entregar su entorno tecnológico de Microsoft deseado, todo alineado a sus objetivos.

Aprovecha las ventajas de tu licenciamiento con una estrategia de seguridad en la nube, a fin de garantizar la mayor protección de información.

Adopción seguridad Zero Trust



Microsoft Defender

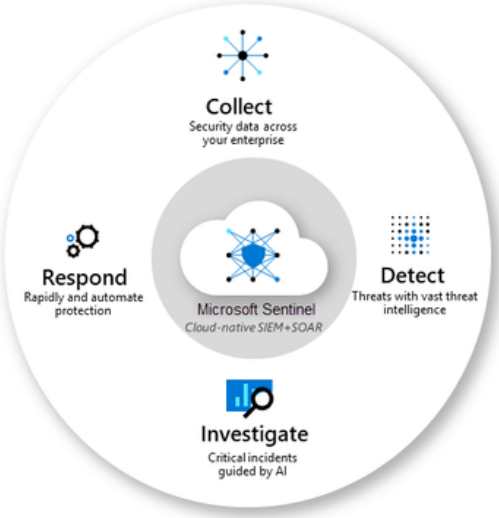
Microsoft Defender es una suite de seguridad unificada que protege contra ransomware, malware y otras ciberamenazas en diversos dispositivos y entornos. Incluye varios componentes especializados:

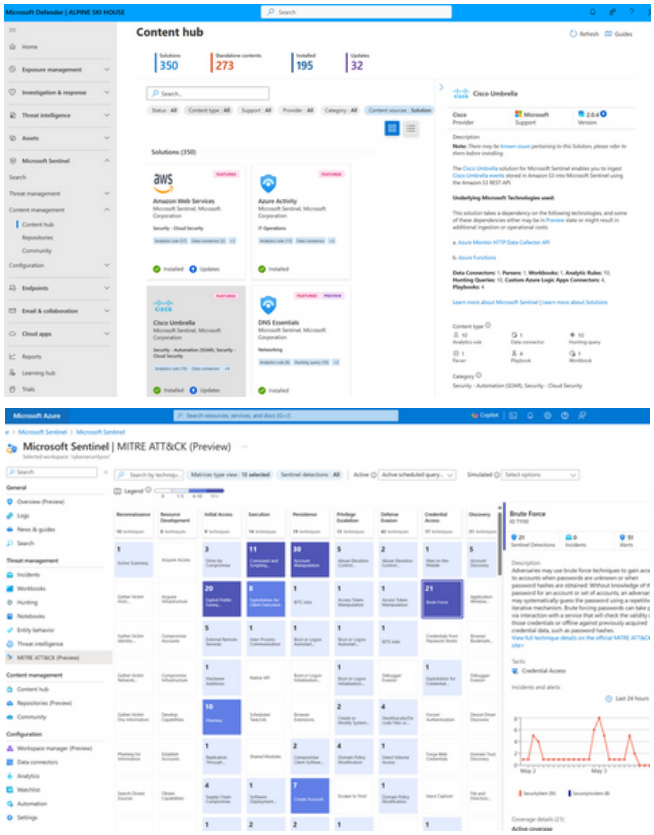
- **Microsoft Defender XDR:** Detección y respuesta extendidas (XDR) que interrumpe automáticamente los ataques más sofisticados.
- **Microsoft Defender para Empresas:** Solución de seguridad de nivel empresarial para pequeñas y medianas empresas (hasta 300 empleados), rentable y fácil de usar.
- **Microsoft Defender para punto de conexión:** Protección completa contra amenazas para dispositivos finales, como PC, Mac y móviles.
- **Microsoft Defender para Office 365**: Protege el correo electrónico, los documentos y otros datos en la suite de Microsoft 365.
- **Microsoft Defender for Cloud:** Protección de la carga de trabajo en la nube (CWPP), gestión de la postura de seguridad (CSPM) y seguridad para aplicaciones nativas (CNAPP) en entornos híbridos y multinube.
- **Microsoft Defender for Identity:** Protección basada en inteligencia contra amenazas avanzadas y actividades maliciosas que afectan las identidades.
- **Microsoft Defender for Cloud Apps:** Un agente de seguridad de acceso a la nube (CASB) que protege las aplicaciones SaaS.

Microsoft Sentinel

Microsoft Sentinel es una solución de seguridad en la nube, nativa de Azure, que unifica la administración de eventos e información de seguridad (SIEM) y la orquestación, automatización y respuesta de seguridad (SOAR) para detectar, investigar y responder a amenazas de ciberseguridad.

- **SIEM en la nube:** Solución de gestión de eventos e información de seguridad (SIEM) nativa de la nube, impulsada por inteligencia artificial (IA), que permite supervisar y analizar datos de seguridad en toda la empresa.
- **Detección de amenazas:** Utiliza IA para identificar amenazas potenciales y actividades sospechosas en entornos complejos.





¿Cómo funciona?

- **Recopilación de Datos:** Se conectan diversas fuentes de datos, como usuarios, dispositivos, aplicaciones e infraestructura, tanto en la nube como en entornos locales.
- **Análisis con IA:** La inteligencia artificial y los análisis de seguridad se aplican a los datos para detectar patrones y anomalías.
- **Detección y Respuesta:** Se generan alertas sobre posibles amenazas, y se pueden activar playbooks (cuadernos de estrategias) para automatizar las acciones de respuesta.

Beneficios

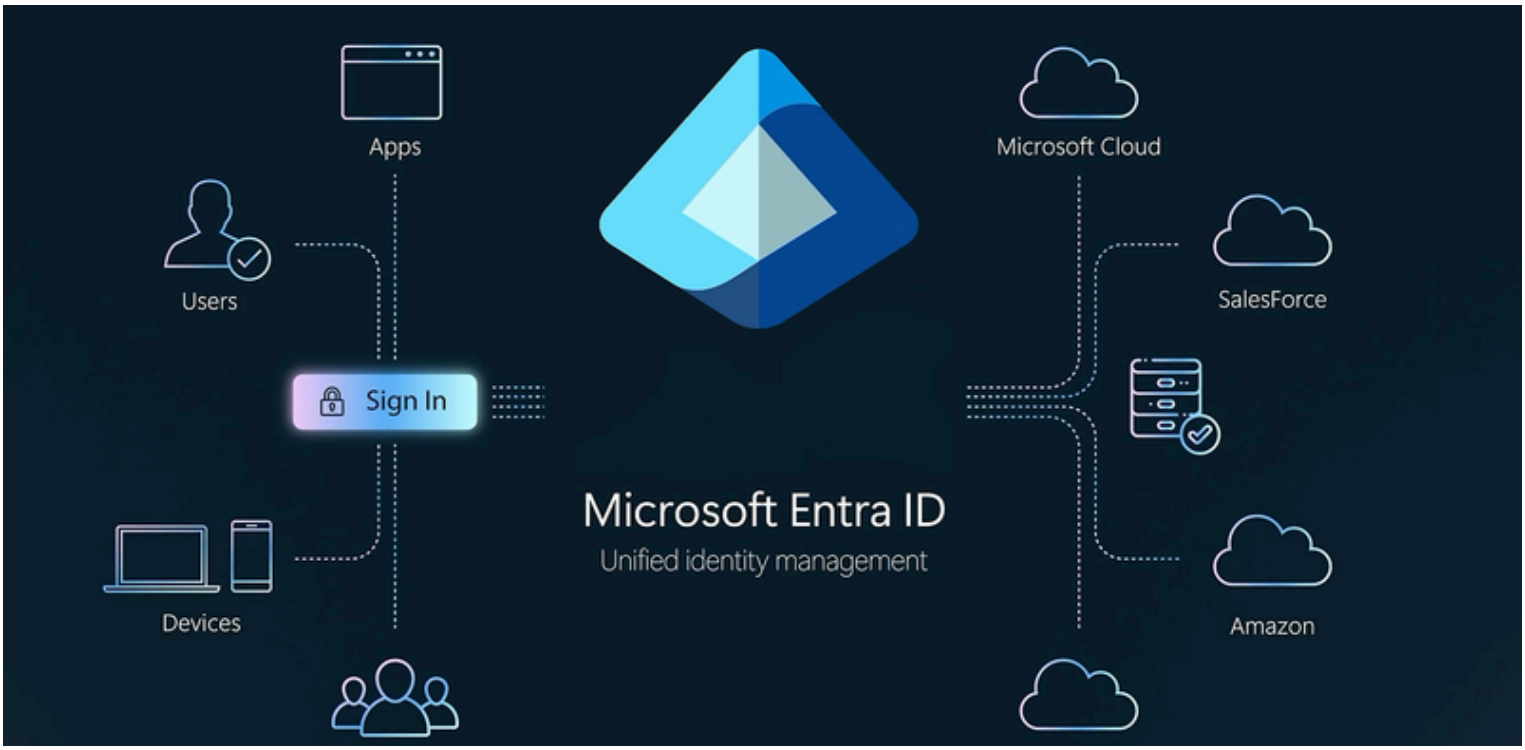
Seguridad Nativa de la Nube: Se integra perfectamente en el entorno de Azure, proporcionando una solución escalable y rentable.
Análisis Inteligente: Aprovecha la inteligencia de amenazas y la IA para ofrecer análisis de seguridad más profundos.
Protección de Múltiples Entornos: Ofrece seguridad unificada para infraestructuras híbridas y multinube

Microsoft Entra

Anteriormente Azure Active Directory

Microsoft Entra es un servicio de seguridad que administra y protege el acceso a aplicaciones y datos para las organizaciones. Esta familia de productos ayuda a las empresas a implementar la identidad y el acceso en entornos de nube y locales, estableciendo un modelo de Zero Trust y asegurando el acceso para empleados, clientes y cargas de trabajo de IA.

- **Microsoft Entra ID:** Administra y protege identidades para garantizar que los usuarios adecuados tengan acceso a las aplicaciones y servicios correctos.
- **Microsoft Entra ID Protection:** Detecta vulnerabilidades y riesgos en la identidad del usuario para prevenir ataques.
- **Microsoft Entra ID Governance:** Garantiza automáticamente que las personas apropiadas tengan el acceso adecuado a las aplicaciones y los servicios necesarios en el momento preciso.



Funciones principales

- **Protección de identidades:** Ayuda a proteger las identidades de empleados y clientes.
- **Acceso a la red:** Permite el acceso seguro a cualquier aplicación, ya sea en la nube o local.
- **Gobernanza de identidades:** Administra los ciclos de vida de las identidades.
- **Verificación de identidades:** Permite la emisión de credenciales verificables.

Ejemplo práctico: Si una empresa necesita gestionar el acceso a sus aplicaciones internas y a servicios en la nube de forma segura, puede utilizar Microsoft Entra para implementar políticas que aseguren que solo los usuarios autorizados puedan acceder a la información, independientemente de dónde estén conectados

Microsoft Purview

Microsoft Purview es una solución de gobernanza, seguridad y cumplimiento de datos que ayuda a las organizaciones a controlar, proteger y administrar toda su información confidencial en entornos multinube y locales. Proporciona visibilidad integral de los datos y permite clasificarlos inteligentemente, aplicar etiquetas de confidencialidad y cifrado, y establecer políticas para prevenir la pérdida y el uso indebido de datos sensibles.

Funcionalidades clave de Microsoft Purview

Gobernanza de datos unificada:
Permite descubrir, entender y administrar el patrimonio de datos de una organización en un portal unificado.

Protección de la información

- **Clasificación inteligente:** Utiliza IA para identificar y clasificar información confidencial en archivos, correos electrónicos y otros datos.
- **Etiquetado de confidencialidad:** Permite aplicar etiquetas con diferentes niveles de seguridad, que pueden restringir el acceso mediante cifrado y agregar marcas de agua a los documentos.
- **Prevención de pérdida de datos (DLP)**: Ayuda a evitar el uso, el intercambio y la transferencia no autorizados de datos confidenciales.

Administración de riesgos:
Ofrece herramientas para gestionar riesgos internos y controlar el acceso a los datos.

Cumplimiento normativo:
Facilita el cumplimiento de regulaciones de privacidad como el RGPD, gracias a la aplicación de políticas de seguridad.

Compatibilidad con IA: Permite bloquear el acceso a aplicaciones de IA no deseadas y controlar la visibilidad y el uso de datos en la era de la inteligencia artificial.

Microsoft Purview es una plataforma integral para la gestión segura y conforme de los datos, diseñada para la complejidad de los entornos modernos.

Microsoft

Microsoft Security Copilot

Microsoft Security Copilot es una solución de seguridad impulsada por inteligencia artificial generativa que potencia a los profesionales de seguridad y TI para detectar, investigar y responder a ciberamenazas a gran escala.

Utiliza el lenguaje natural para interactuar con las herramientas de seguridad de Microsoft y terceros, ayudando en tareas como la búsqueda de amenazas, la gestión de incidentes y la recopilación de inteligencia de amenazas para mejorar la eficacia y la velocidad de los equipos de seguridad.

Al usar complementos como orígenes de punto de datos, los profesionales de seguridad tienen una visibilidad más amplia de las amenazas y obtienen más contexto.

Security Copilot se centra en facilitar la realización de los siguientes casos de uso: Investigación y corrección de amenazas de seguridad, Creación de consultas de KQL o análisis de scripts sospechosos, Descripción de los riesgos y administración de la posición de seguridad de la organización, Solución de problemas de TI más rápido, Definir y administrar directivas de seguridad, Configuración de flujos de trabajo de ciclo de vida seguro, Desarrollar informes para las partes interesadas, Compilar y agregar agentes

Security Copilot procesa y organiza iterativamente estos servicios sofisticados para ayudar a generar resultados relevantes para su organización, ya que se basan contextualmente en los datos de la organización.

Servicios de Nuvol para Zero Trust con tecnología Microsoft

Nuestros servicios administrados le brindan la tranquilidad de que su seguridad está en manos de profesionistas certificados en Seguridad Microsoft. Ofrecemos:

Evaluación y planificación

Analizamos su postura de seguridad actual y diseñamos una estrategia Zero Trust personalizada y gradual, adaptada a sus necesidades y licenciamiento de Microsoft.

Implementación y configuración:

Desplegamos y optimizamos las soluciones de ciberseguridad de Microsoft, como Microsoft Defender, Microsoft Entra ID y Microsoft Purview.

Nuvol + Microsoft
Su camino hacia Zero Trust

Como socio de servicios administrados de Microsoft, Nuvol aprovecha la tecnología líder del mercado para crear una defensa integral para su negocio.

En Nuvol, nuestro mayor activo es nuestro equipo de especialistas altamente certificados, líderes en el soporte de nivel 3 para tecnologías de Microsoft. No solo conocemos la teoría de Zero Trust; la aplicamos con la experiencia de quien domina la suite de ciberseguridad más completa del mercado. Esta profunda experticia en Microsoft nos permite diseñar, implementar y gestionar una estrategia Zero Trust robusta y eficiente, maximizando el potencial de sus licencias y garantizando una protección inigualable para su organización.

Capacitación y concienciación

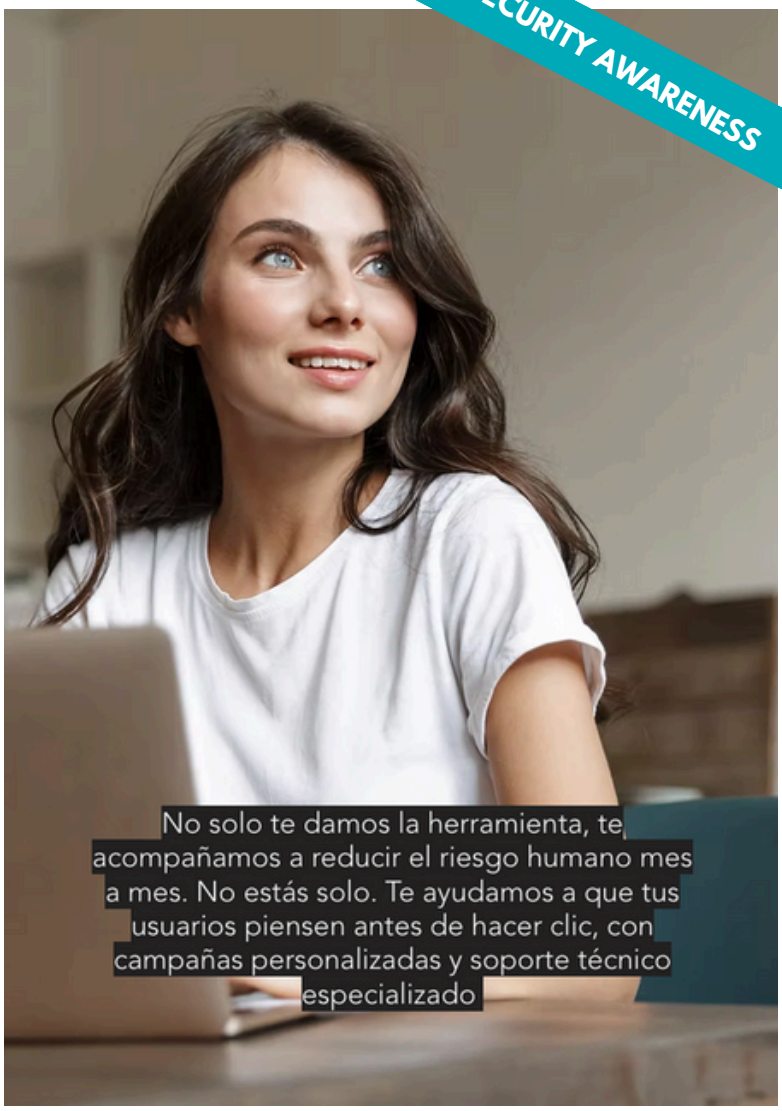
Formamos a su equipo de TI y a sus usuarios finales para que comprendan y adopten las mejores prácticas de Zero Trust, fortaleciendo la cultura de seguridad de su organización.

Plataformas de Security Awareness autogestionadas

¿Cansado de implementar herramientas de concienciación que no generan resultados? **Nuvol se encarga de todo:** desde la configuración hasta el análisis de métricas, con un equipo dedicado a reducir tu riesgo humano.

- Administramos la herramienta por ti: configuraciones, métricas y ajustes según tus objetivos.
- Know-how local: Expertos en LATAM que entienden riesgos regionales
- Soporte proactivo: reuniones mensuales, informes de progreso y mejora continua.
- Entendemos los desafíos de ciberseguridad en LATAM y adaptamos las estrategias a tu cultura organizacional.

Security Awareness no es un software, es un proceso. En Nuvol, lo hacemos realidad contigo



Nuvol es partner de las Principales Plataformas de Security Awareness

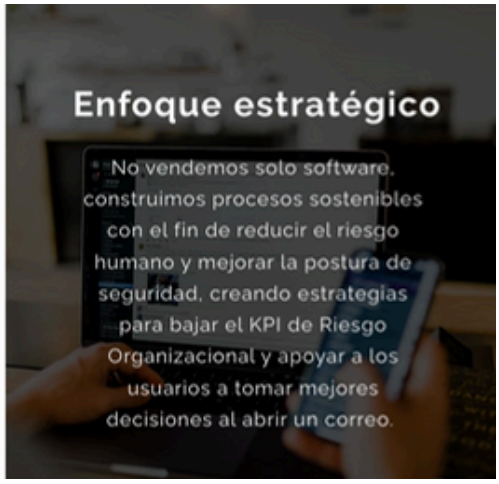
Nuvol es partner de las Principales Plataformas de Security Awareness
Llevamos más de 7 años ayudando a organizaciones en Latinoamérica a fortalecer su Security Awareness con estrategias efectivas y adaptadas a sus necesidades. Con más de 57 clientes en Panamá, México, Colombia y otros países, hemos apoyado a empresas de diversos sectores a reducir su riesgo humano y reforzar su postura de seguridad.

En Nuvol, somos partner oficial de las plataformas líderes en el mercado:

KnowBe4 Human error. Conquered. SMARTFENSE HOXHUNT Abnormal

Nuestra Misión: Reducir el Riesgo Organizacional

Nuestra experiencia con múltiples plataformas nos permite ofrecer soluciones personalizadas, diseñadas para integrarse sin problemas con los objetivos de las áreas de Ciberseguridad y TI. No solo implementamos herramientas, sino que creamos una cultura de seguridad en tus usuarios finales, con métricas claras y resultados medibles.



¿Cuál es la mejor herramienta?

Depende de las necesidades de cada cliente.
Lo más importante es que Nuvol tiene el Know-How para implementarlas correctamente, maximizando su potencial y asegurando resultados.

¿Por Qué Elegir Nuvol para tu Security Awareness?

Acompañamiento Continuo y Proactivo

- Campañas mensuales personalizadas: Diseñamos y ejecutamos simulaciones de phishing adaptadas a tus riesgos reales.
- Optimización constante: Aseguramos que la plataforma elegida (KnowBe4, HoxHunt o Smartfense) rinda al máximo.
- Métricas accionables: Reportes claros que miden progreso y áreas de mejora.

Customer Success Manager (CSM) Dedicado

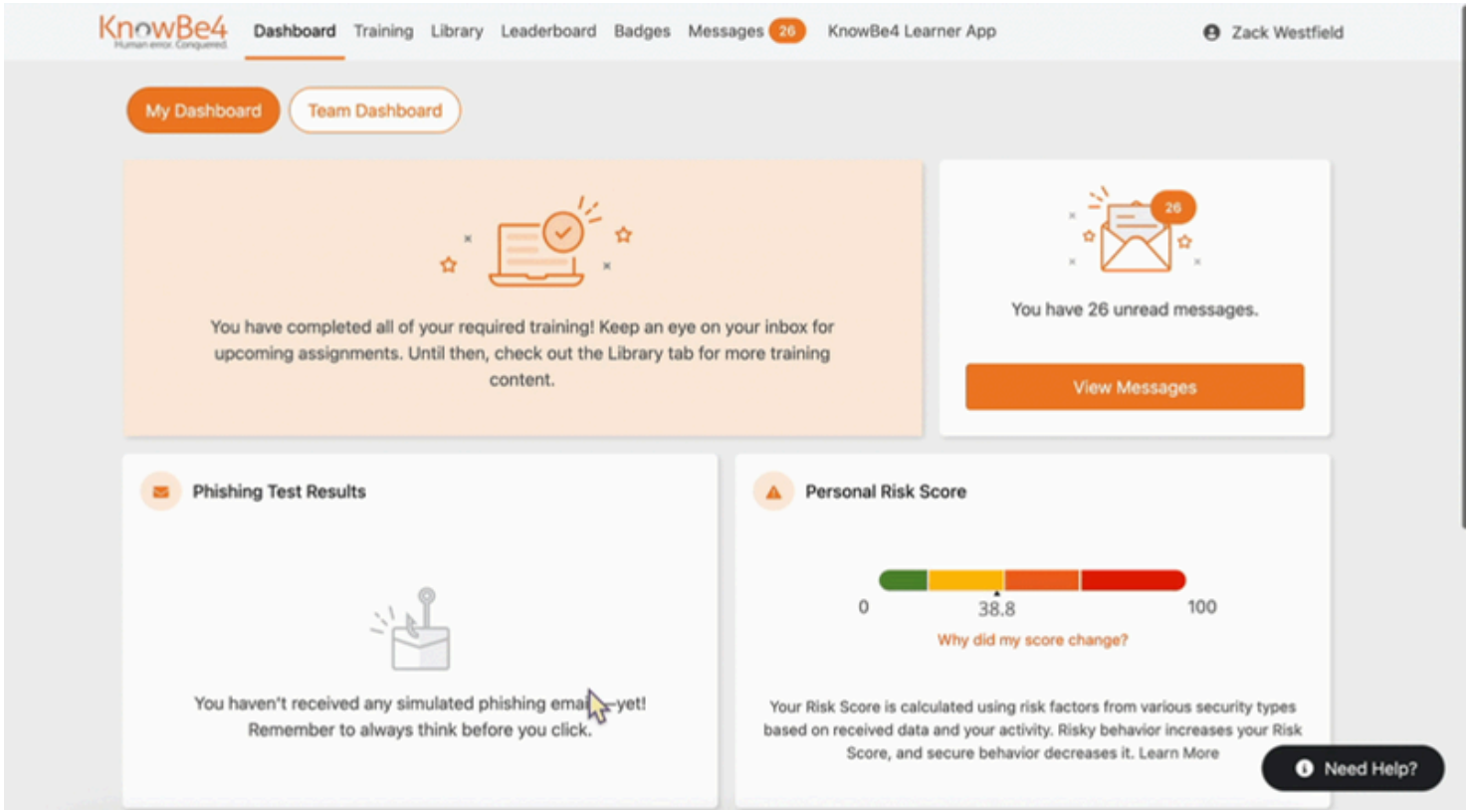
- Un experto asignado a tu cuenta: Garantiza continuidad y alineación con tus objetivos.
- Soporte estratégico: No solo resolvemos dudas, mejoramos tu estrategia internamente.
- Nuestro éxito se mide con el tuyo: Si tus KPIs de riesgo no bajan, nosotros no cumplimos

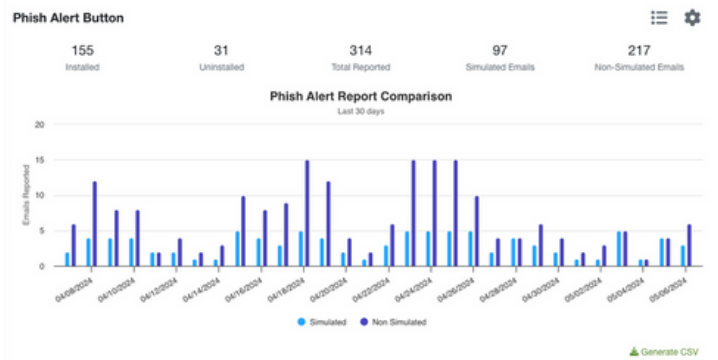
Compromiso Real con los Resultados

- No somos un vendedor más, somos un equipo extendido: Nos sumamos a tus iniciativas internas.
- Enfoque práctico: Combina tecnología + cambio cultural

Uno de los principios de KnowBe4 es continuamente

1. **Entrenar a los usuarios:** KnowBe4 cuenta con la biblioteca más grande de contenido sobre conciencia de seguridad. Contenido en video tipo Netflix, módulos interactivos, videojuegos, carteles, etc. (más adelante hablaremos de el)
2. **Probar a los usuarios con campañas de phishing simulado:** para medir los conocimientos aprendidos de los usuarios se envían pruebas de phishing. vishing simulados totalmente automatizados y con plantillas que se pueden adaptar o regionalizar.
3. **Analizar los resultados:** estadísticas e informes gráficos de alto nivel, incluso tendrá una línea de tiempo por cada usuario, grupo o departamento.



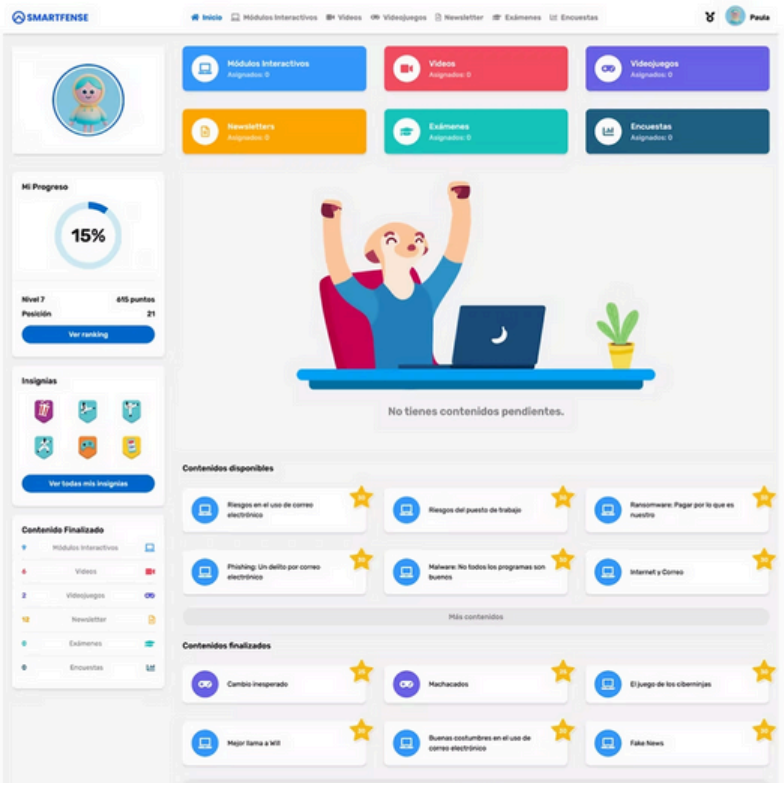


"Seguridad informática que transforma conductas: Más protección, menos riesgos"

Smartfense es la plataforma para brindar al usuario final una experiencia única y entretenida para fortalecer de manera positiva la concienciación en seguridad informática.

Para las áreas de seguridad informática la plataforma nos proporciona todos los Indicadores que necesitamos.

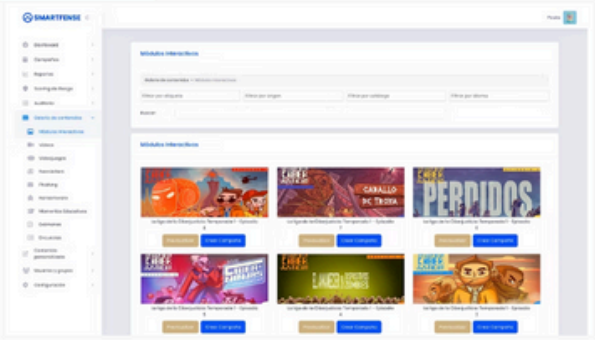
- KPI Riesgo Organizacional
- Reportes de campañas de phishing
- Reporte de campañas de capacitación
- Grado de conocimiento de los usuarios sobre políticas
- Reporte Gamificación
- Mapa de Calor que señala nivel de riesgo



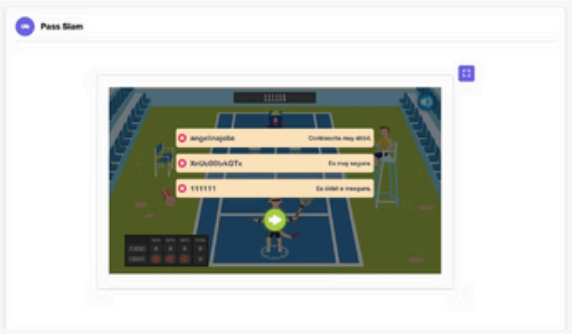
Herramientas de Educación y Refuerzo

Todos los contenidos de la plataforma pueden editarse, utilizarse como plantillas para la creación de otros, o bien crearse nuevos desde cero.

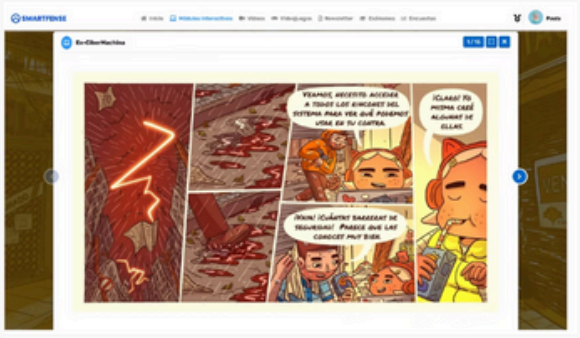
Videos



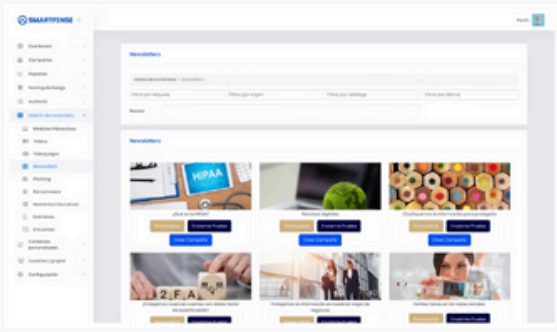
Videojuegos



Módulos Interactivos

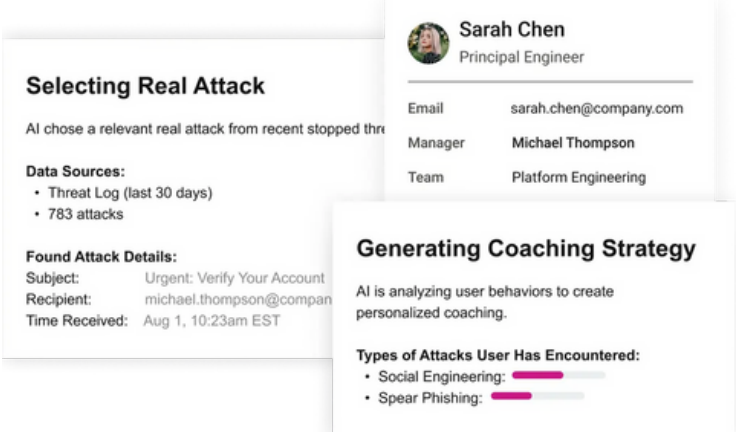


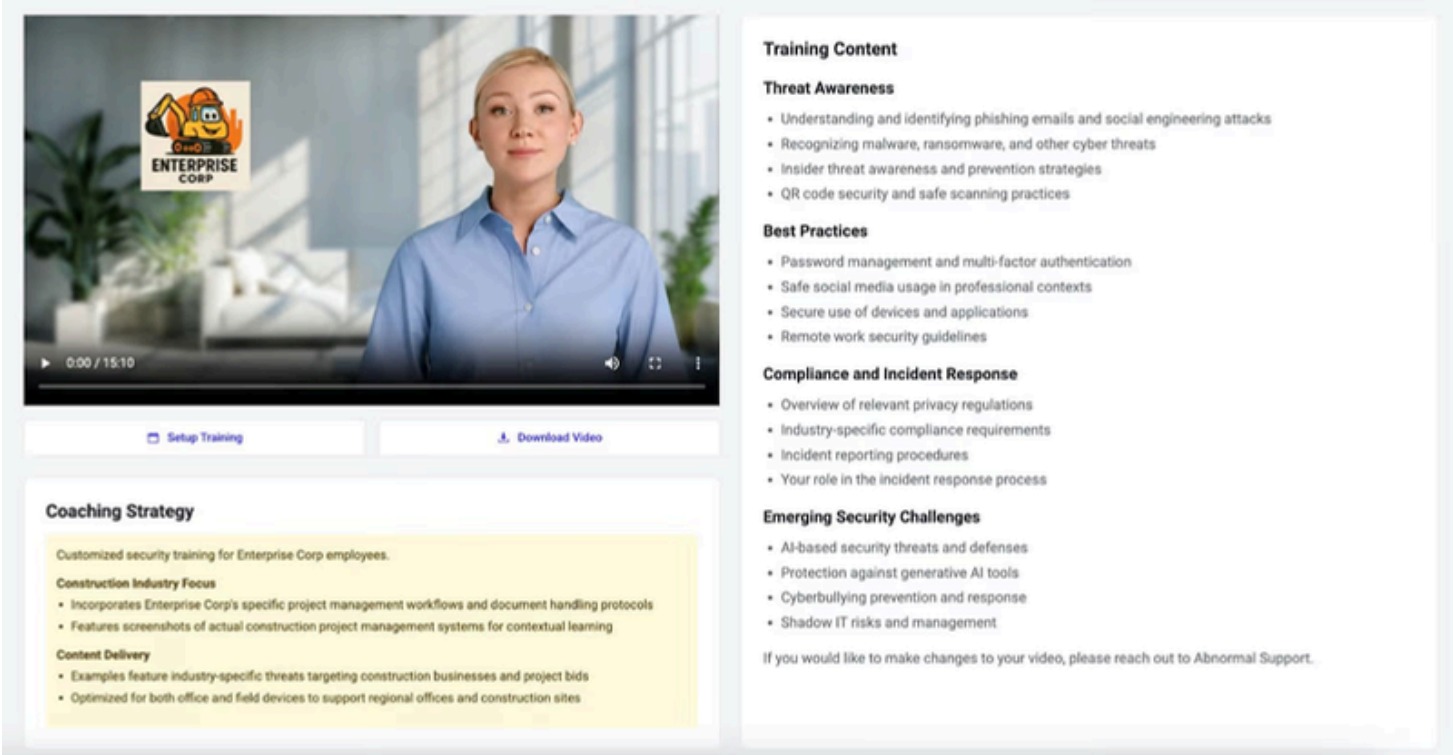
Newsletter



Presentamos AI Phishing Coach: capacitación personalizada y autónoma en concientización sobre seguridad.

Descubra cómo Abnormal transforma la capacitación en seguridad con simulaciones de phishing personalizadas, entrenamiento en tiempo real y gestión de programas totalmente autónoma.





AI Phishing Coach cambia eso con simulaciones de phishing personalizadas basadas en datos de amenazas específicos de los empleados. Gracias a la integración segura de la API de Abnormal AI , AI Phishing Coach aprovecha el contexto organizacional, como la función laboral y los patrones de comunicación habituales, para adaptar mejor la capacitación.

Esto significa que los empleados reciben pruebas y capacitación sobre los tipos de ataques que probablemente verán en la práctica. Esto comienza con el análisis de amenazas reales y remediadas en el Registro de Amenazas. Los ataques se seleccionan y se neutralizan para enviarse a cada empleado como simulaciones basadas en:

- Rol y responsabilidades del empleado
- Los tipos de ataques dirigidos a un empleado y sus pares en roles similares en la organización
- Participación y tendencias de capacitación previa (es decir, sensibilidad específica del rol a las amenazas, resultados de simulaciones previas, cambios de comportamiento observados, etc.)

SIMULACIÓN DE ATAQUES

PICUS

Simulación de Intrusión de ataques

Picus Security BAS (Breach and Attack Simulation) es una plataforma que simula ataques del mundo real para validar y mejorar la eficacia de los controles de seguridad de una organización.

Sirve para probar y medir continuamente las herramientas de detección y prevención de amenazas, identificar brechas de seguridad, visualizar rutas de ataque, validar la efectividad de las reglas de detección, y obtener información procesable para optimizar las inversiones en seguridad y fortalecer la resiliencia cibernética

¿Qué hace Picus BAS?

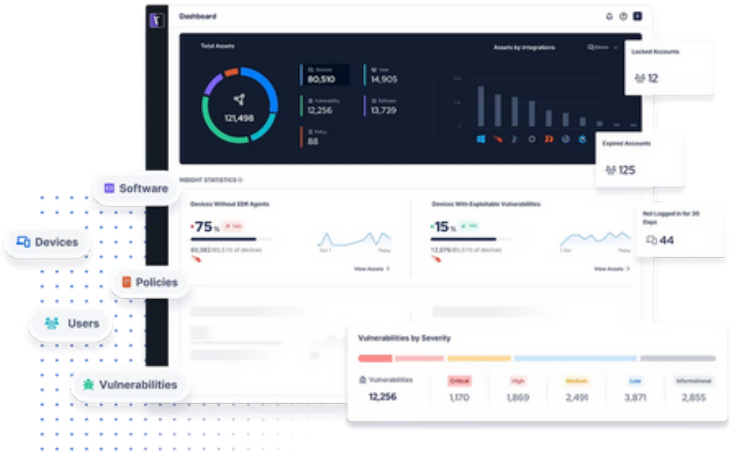
Simula ataques reales: Ejecuta miles de simulaciones de amenazas y técnicas de ataque para verificar si los controles de seguridad funcionan correctamente.

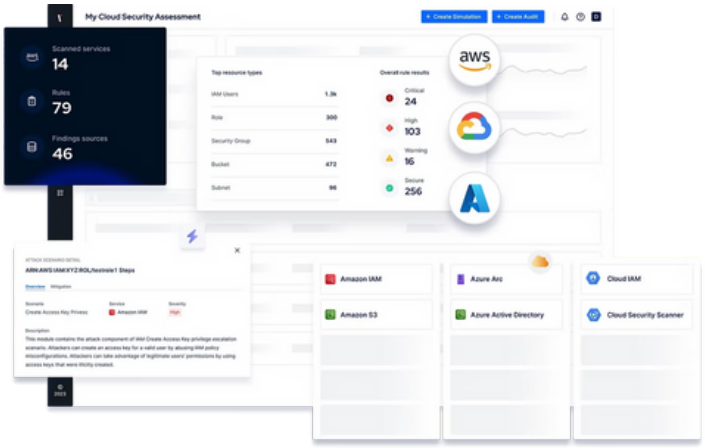
Válida controles de seguridad: Asegura que las herramientas de prevención y detección, como firewalls y sistemas de detección de intrusos, estén bien configuradas y sean efectivas.

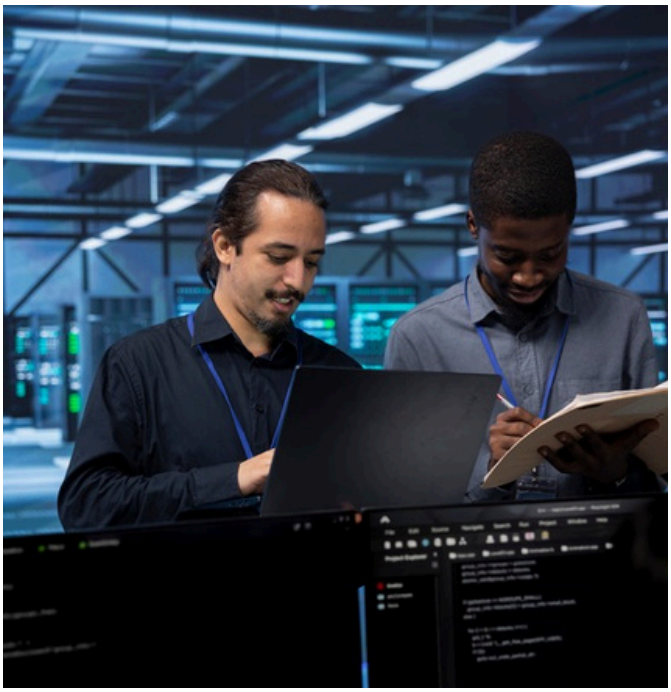
Identifica brechas de seguridad: Permite encontrar vulnerabilidades y configuraciones erróneas en la nube y en el entorno de red antes de que sean explotadas por atacantes.

Valida la efectividad de las reglas de detección: Ayuda a los equipos de seguridad a mantenerse al día con la línea base de sus reglas de detección y automatiza los procesos de ingeniería.

Visualiza rutas de ataque: Muestra los pasos que un atacante podría seguir para comprometer los sistemas, revelando los puntos más críticos para el riesgo







Para qué sirve

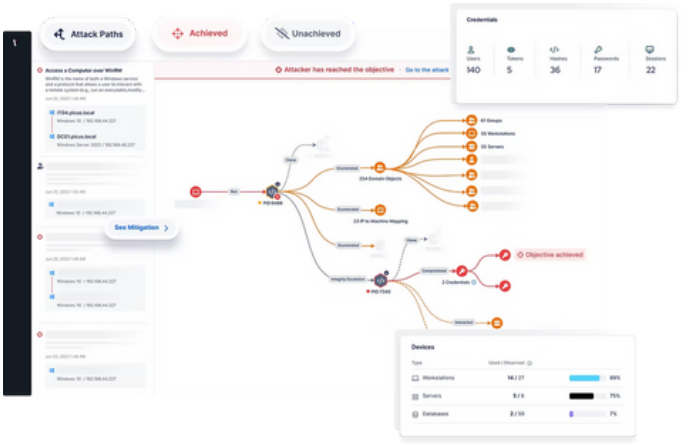
- **Mejora la resiliencia cibernética:** Fortalece la capacidad de una organización para prepararse y recuperarse de ataques cibernéticos.
- **Reduce el riesgo cibernético**: Al identificar y mitigar proactivamente las vulnerabilidades, disminuye la exposición a los atacantes.
- **Optimiza las inversiones en seguridad:** Comprueba el valor de las inversiones realizadas en herramientas de seguridad, asegurando que protegen eficazmente.
- **Aumenta la visibilidad de la postura de seguridad:** Proporciona una visión integral y holística de la seguridad de la organización.
- **Automatiza las pruebas de seguridad**: Libera al personal de la necesidad de realizar pruebas manuales, permitiéndoles enfocarse en brechas críticas y soluciones de alto impacto

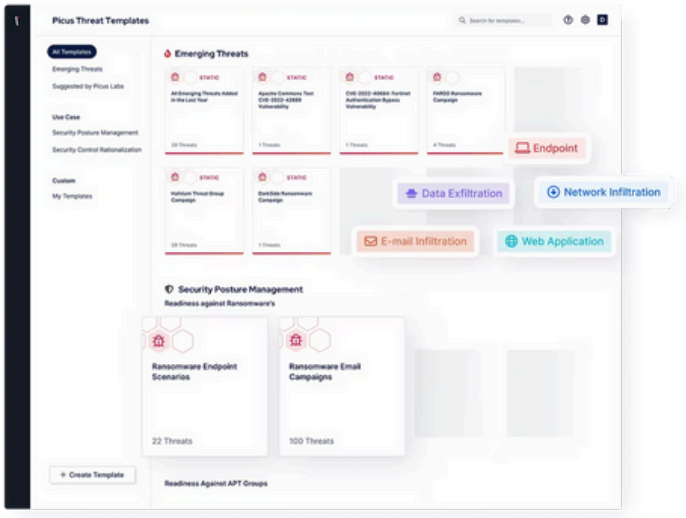
Ejemplo práctico en las empresas

Imagine una empresa de tecnología que ha invertido en varias soluciones de seguridad, incluyendo un firewall de última generación y un sistema de detección y respuesta de puntos finales (EDR). El equipo de seguridad utiliza Picus Security BAS para evaluar la eficacia de estas defensas

1. Simulación de un ataque de ransomware

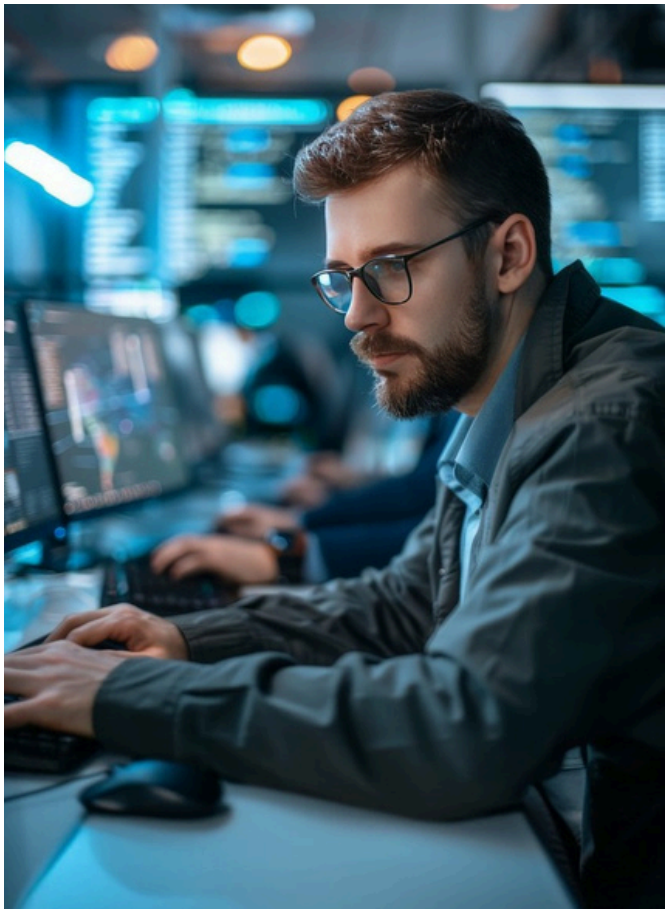
- **Configuración**: El equipo de seguridad de la empresa lanza una simulación de ataque de ransomware a través de la plataforma de Picus. La simulación emula las tácticas que un atacante real utilizaría, como el movimiento lateral, el robo de credenciales y la exfiltración de datos.
- **Ejecución**: Picus despliega pequeños agentes de software (sin riesgo para los sistemas) que actúan como atacantes dentro de la red. Estos agentes intentan evadir las defensas, buscar vulnerabilidades y realizar acciones maliciosas simuladas.
- **Validación de la detección**: El sistema comprueba si el EDR de la empresa detecta los movimientos del atacante simulado y si el SIEM genera alertas apropiadas y oportunas.
- **Validación de la prevención**: Verifica si el firewall bloquea el tráfico malicioso que intenta exfiltrar datos.





2. Análisis de resultados y mitigación

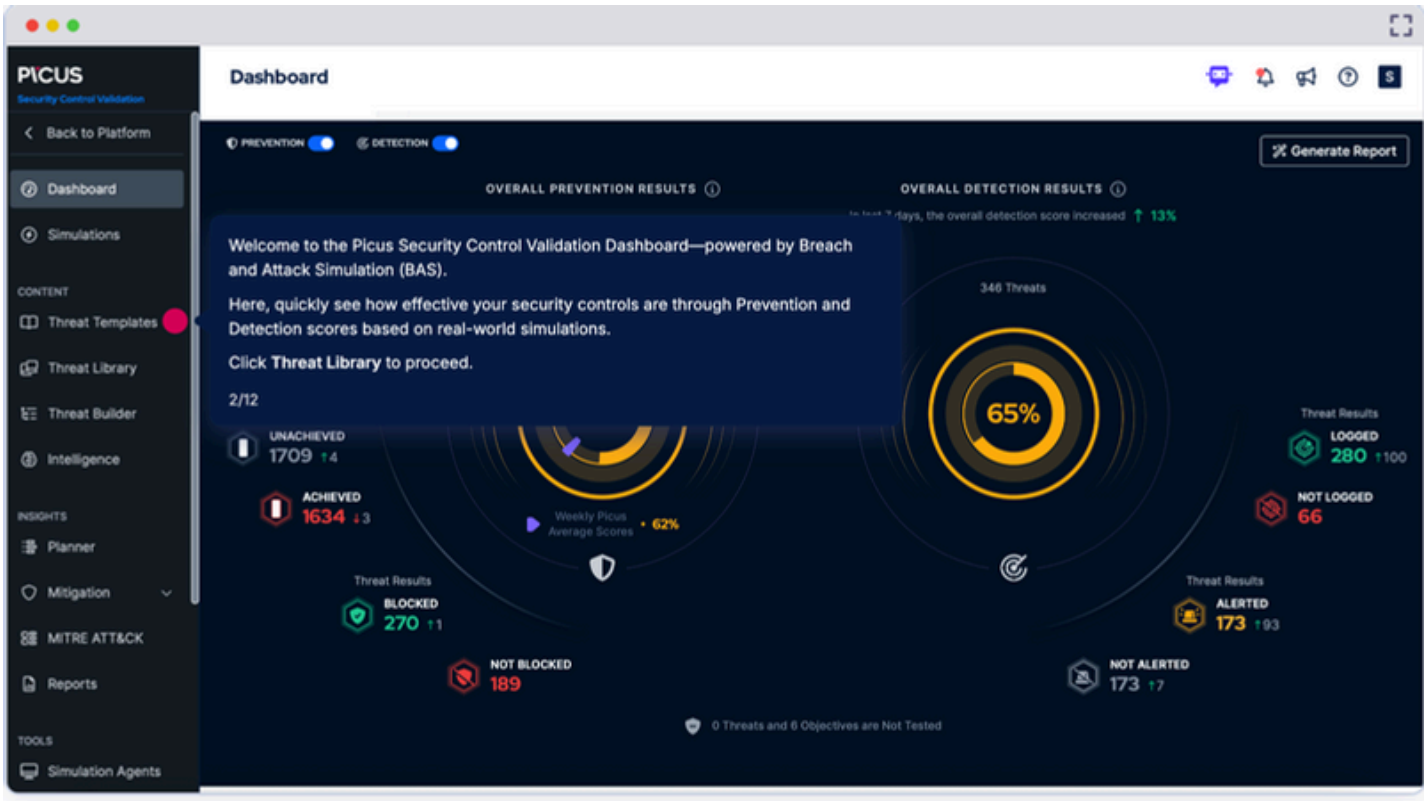
- **Resultados de la simulación**: El informe de Picus revela que, si bien el EDR detectó el ransomware en la fase inicial, no generó una alerta crítica en el SIEM. Además, una configuración incorrecta en el firewall permitió el paso de tráfico de exfiltración simulado.
- **Recomendaciones accionables**: La plataforma proporciona recomendaciones claras, como ajustar la regla de correlación en el SIEM para que las detecciones del EDR generen alertas de alta prioridad. También sugiere corregir la configuración del firewall para bloquear el tráfico de exfiltración



3. Verificación de la mejora

- **Nueva simulación**: Después de implementar las correcciones recomendadas, el equipo ejecuta una nueva simulación de ataque de ransomware.
- **Resultados mejorados:** El informe muestra que, en la segunda prueba, el EDR detectó el ataque, y esta vez el SIEM generó una alerta crítica, lo que permitió al equipo de seguridad responder de manera oportuna. Además, el firewall bloqueó exitosamente el intento de exfiltración de datos

Este ejemplo demuestra cómo Picus BAS permite a las empresas pasar de una postura de seguridad reactiva a una proactiva. En lugar de esperar a ser atacados para descubrir debilidades, las empresas pueden identificarlas y corregirlas de forma continua y automatizada



BlueVoyant

Protección de Marca Digital

Es un servicio de ciberseguridad proactivo que detecta y elimina amenazas externas que imitan la marca de una empresa para estafar a clientes y socios. Utiliza una combinación de inteligencia artificial, datos globales y experiencia humana para proteger la propiedad intelectual y la reputación de la marca, evitando daños financieros y de confianza

Caracteristicas Principales

- **Detección de suplantación de identidad:** Identifica de forma proactiva sitios web y nombres de dominio falsos que imitan a su empresa para realizar ataques de phishing.
- **Neutralización de amenazas**: Ofrece una eliminación rápida e ilimitada de dominios de phishing, aplicaciones móviles fraudulentas y cuentas de redes sociales falsas.
- **Monitorización integral:** Supervisa la web abierta, la web profunda y la dark web, así como más de 300 tiendas de aplicaciones, para detectar actividades fraudulentas.
- **Inteligencia y experiencia combinadas**: Utiliza inteligencia artificial y análisis de datos a gran escala, junto con la investigación de expertos en ciberseguridad, para enriquecer la inteligencia de amenazas y agilizar las contramedidas.
- **Protección de ejecutivos y VIPs:** Detecta ataques dirigidos específicamente a los líderes de la empresa, previniendo daños financieros y a la reputación.
- **Monitorización de comunidades clandestinas:** Explora foros clandestinos para identificar actividades fraudulentas, como la venta de información corporativa o de clientes.
- **Análisis de exposición:** Identifica credenciales de empleados o datos corporativos filtrados debido a configuraciones incorrectas o brechas de seguridad.

El servicio monitoriza continuamente internet para identificar actividades maliciosas antes de que impacten a la organización.

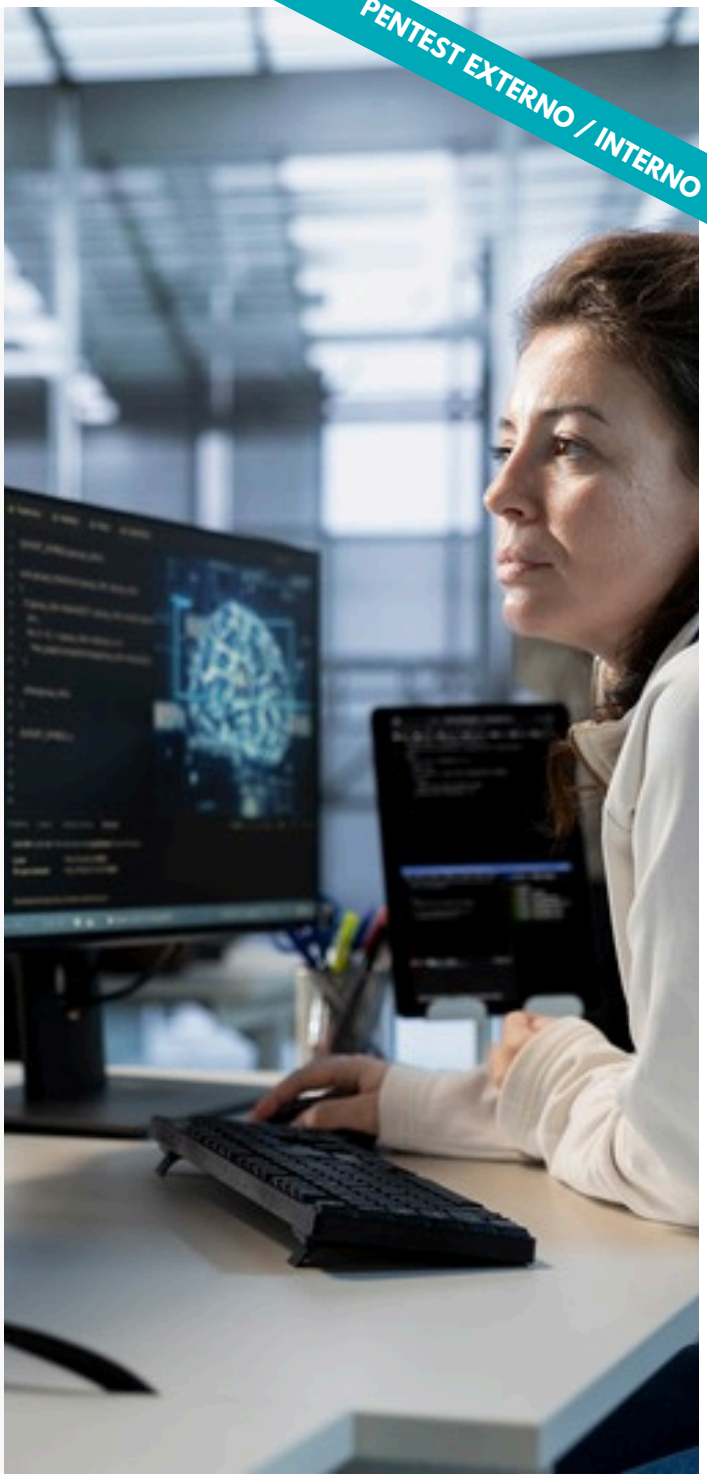
Proporciona una visión integral de la superficie de ataque externa, más allá del perímetro de la red corporativa.

NUVOL
Cybersecurity services

PENTEST EXTERNO / INTERNO

Pentest & Ethical Hacking

Los Servicios de auditoría de seguridad tratan de proporcionar información sobre el grado de la integridad de los sistemas de información con la finalidad de eliminar accesos ilegales, prevenir robos de información y pérdidas de productividad. El proceso de auditoría incluirá distintas pruebas de intrusión con el objetivo de identificar vulnerabilidades a través de una revisión de las técnicas de ataque actuales, realizando un hacking ético de las aplicaciones identificadas y reproduciendo estos ataques mediante un plan de pruebas.



Servicios de prevención de vulnerabilidades

- Pentesting
- Auditoría externa e interna
- Análisis de vulnerabilidades en código fuente
- Ingeniería inversa de malware
- OSINT e inteligencia de amenazas
- Campañas de phishing y malware
- Test de intrusión
- Auditoría aplicación web
- Auditoría wireless
- Auditoría de Redes: VoIP, WiFi, Citrix, accesos remotos.
- Auditoría de Base de Datos: SQL, Oracle
- Auditoría de Código estático y dinámico
- Auditoría de Móviles: aplicaciones y entorno
- Auditorías de Cumplimiento: PCI, ESSI, NIST
- Análisis Forense

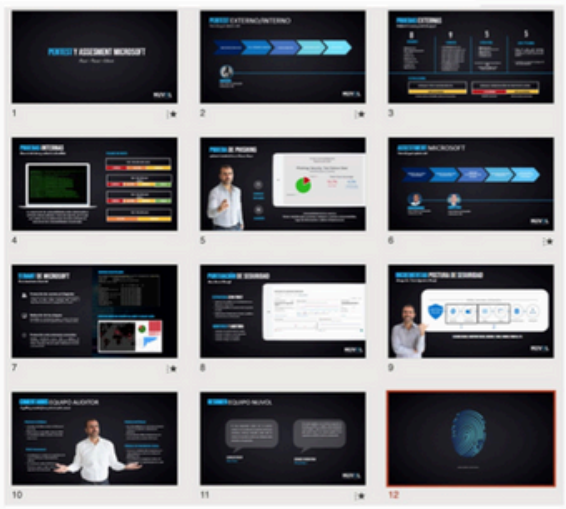
¿Porqué elegirnos?

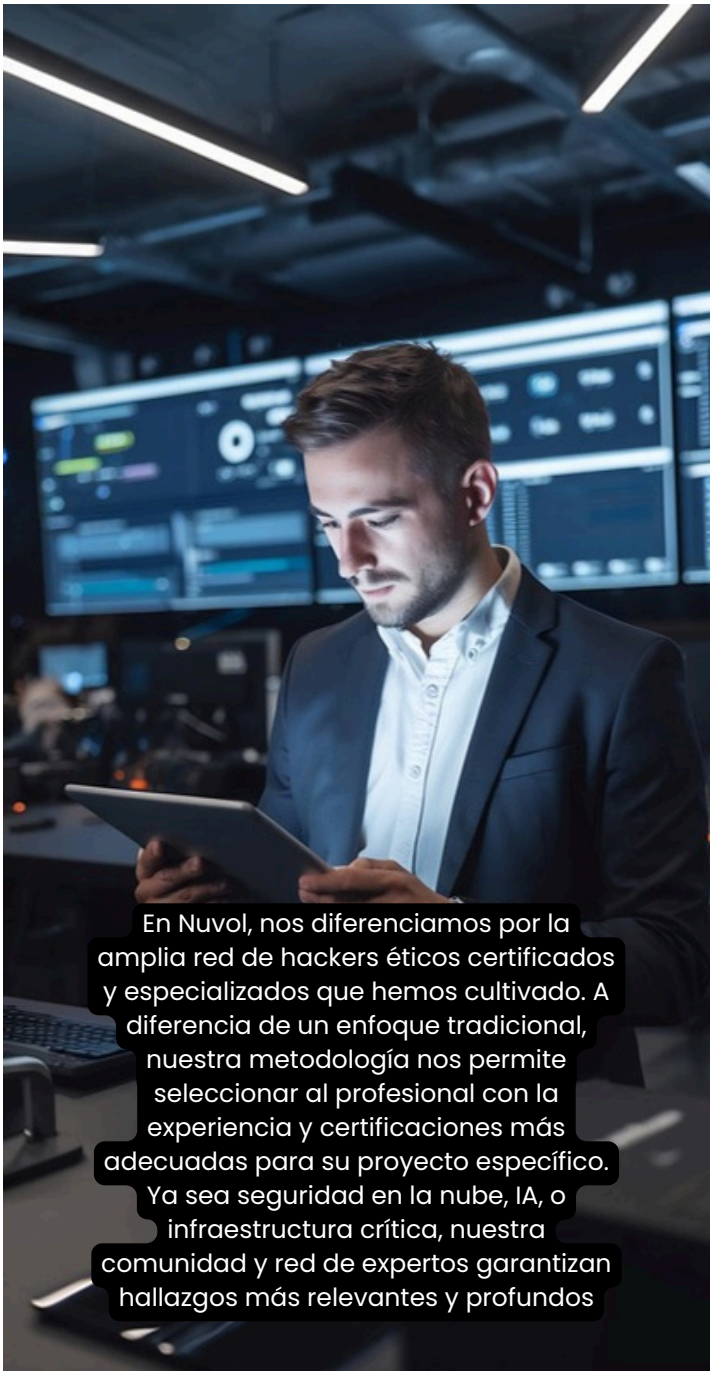
- Auditorias personalizadas al entorno existente
- Mas allá de un escaneo de vulnerabilidades detectamos los riesgos de negocio de acuerdo a los servicios del cliente
- Reportes técnicos y ejecutivos enfocados a la dirección
- Realización de las tareas en sitio y en los horarios que nuestros clientes establezcan
- Siempre cumplimos con los tiempos de proyecto establecidos
- Servicios de ingeniería social incluidos, tanto físicos como por medios electrónicos, personalizados al ambiente de trabajo de los empleados de la organización.

NUVOL
Cybersecurity services

Ejemplo reporte técnico y ejecutivo

Tabla de contenido





Nuestro enfoque se centra en:

- **Impacto Empresarial Real:** Traducimos los hallazgos técnicos en riesgos concretos para el negocio, priorizando las vulnerabilidades críticas y ofreciendo planes de remediación accionables.
- **Adaptación Tecnológica:** Especializamos nuestras pruebas en tecnologías emergentes, como inteligencia artificial (IA), entornos de nube y la seguridad de la cadena de suministro, para protegerlo contra las amenazas más avanzadas.
- **Modelo de Servicio Continuo:** Ofrecemos Pentesting como Servicio (PTaaS) y simulaciones de adversarios (Red Teaming) para una vigilancia constante y una evaluación más precisa de sus defensas.
- **Fortalecimiento Colaborativo:** Trabajamos con sus equipos internos para fortalecer sus capacidades de ciberseguridad, validando sus controles existentes y proporcionando capacitación para cerrar brechas de conocimiento.

Nuestro objetivo es convertir el pentesting en una herramienta estratégica que demuestre un claro retorno de la inversión al mitigar riesgos financieros y operativos.

NUVOL
Cybersecurity services

CUMPLIMIENTO

Cumplimiento normativo y atención de auditorías: Protege tus datos y tu reputación

Asegura la confidencialidad, integridad y disponibilidad de tu información con nuestros servicios especializados en auditoría y cumplimiento de estándares de seguridad como ISO 27001 y PCI DSS.

Evaluación y Cumplimiento ISO 27001

Demuestra tu compromiso con la protección de datos y genera confianza en tus clientes y socios comerciales a través de la certificación ISO 27001. Nuestro servicio te guía paso a paso para establecer, implementar y mantener un SGSI robusto.

Evaluación y Cumplimiento GAP ANÁLISIS PCI DSS

Si tu empresa maneja, procesa o almacena datos de tarjetas de pago, cumplir con el Estándar de Seguridad de Datos PCI (PCI DSS) es obligatorio. Nuestro servicio de Análisis GAP te permite identificar y corregir las deficiencias para lograr y mantener el cumplimiento.

PROFESSIONAL CERTIFICATION
certiprof
I27001LA
ISO 27001 LEAD AUDITOR

¿Porqué elegirnos?

Expertos en cumplimiento, socios en seguridad.

- **Reducir riesgos:** Protegemos tus activos de información más valiosos.
- **Mejorar la eficiencia:** Integramos la seguridad en tus procesos de negocio, no como un obstáculo, sino como un facilitador.
- **Generar confianza:** Te ayudamos a construir una reputación sólida de protección de datos, un factor clave en el mercado actual.
- **Evitar sanciones:** El cumplimiento normativo te protege de multas y consecuencias legales por el manejo inadecuado de datos.

Information Security Management System
ISO
27001
Certified

Cómo trabajamos:

- **Revisión inicial:** Realizamos un diagnóstico para entender el estado actual de tu seguridad y definir el alcance del proyecto.
- **Identificación y clasificación de activos:** Determinamos qué activos de información son críticos para tu negocio y los clasificamos por su nivel de importancia.
- **Análisis de riesgo:** Evaluamos la probabilidad y el impacto de posibles amenazas para identificar los riesgos más relevantes para tu organización.
- **Planes de acción y documentación:** Desarrollamos estrategias concretas para mitigar riesgos, y te ayudamos a documentar las políticas y procedimientos necesarios para el cumplimiento.
- **Informes ejecutivos y detallados:** Te entregamos una visión completa de los riesgos, los planes de mejora y los próximos pasos, en formatos adaptados para la dirección ejecutiva y los equipos técnicos.
- **Programa de mejora continua:** El cumplimiento no es un evento único, sino un proceso constante. Te ayudamos a desarrollar un programa para mantener tu SGSI actualizado y eficaz a largo plazo.

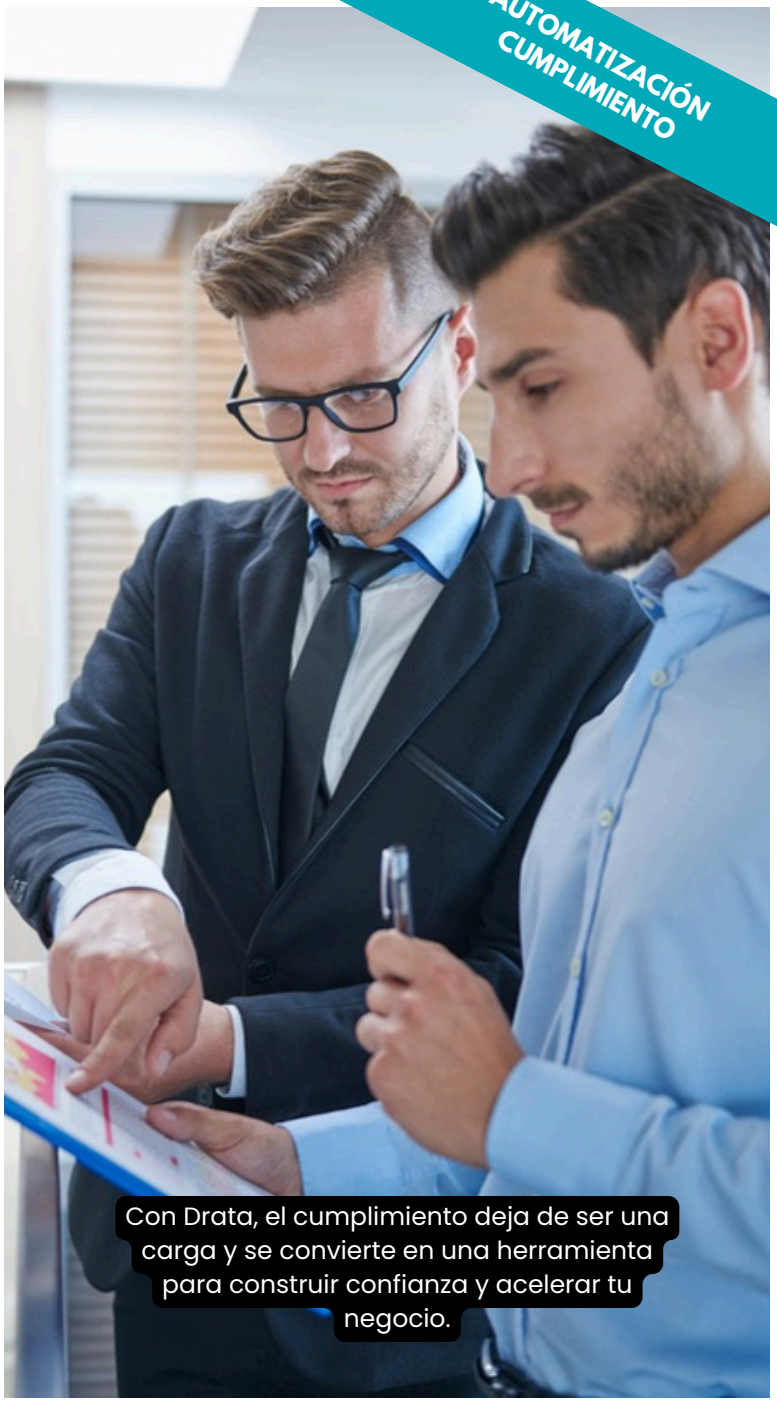
DRATA

Automatiza tu cumplimiento. Construye confianza. Crece más rápido.

Ofrecemos una solución integral para empresas que buscan automatizar la gestión de riesgos y el cumplimiento (GRC). A través de la plataforma Drata, te ayudamos a centralizar, monitorear y gestionar todos los aspectos de tu seguridad y conformidad, desde el inicio hasta la renovación.

Funciones

- **Automatización inteligente:** Integra Drata con tus herramientas existentes para recopilar evidencias de forma automática y continua.
- **Visibilidad en tiempo real:** Obtén una vista completa del estado de tu cumplimiento, identifica brechas y toma decisiones proactivas.
- **Agilidad en auditorías:** Simplifica el proceso de auditoría con informes listos para el auditor, reduciendo tiempo y estrés para tu equipo.
- **Preparación para la ISO 27001:** Nuestros expertos y la plataforma Drata te guían en cada paso de la certificación, desde la documentación inicial hasta la implementación de controles.



¿Cómo ayuda Drata con la ISO 27001?

Drata automatiza la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) de la ISO 27001. Recopila evidencias, supervisa tus controles de seguridad y genera informes detallados, facilitando enormemente el proceso de auditoría.

¿Es Drata solo para empresas grandes?

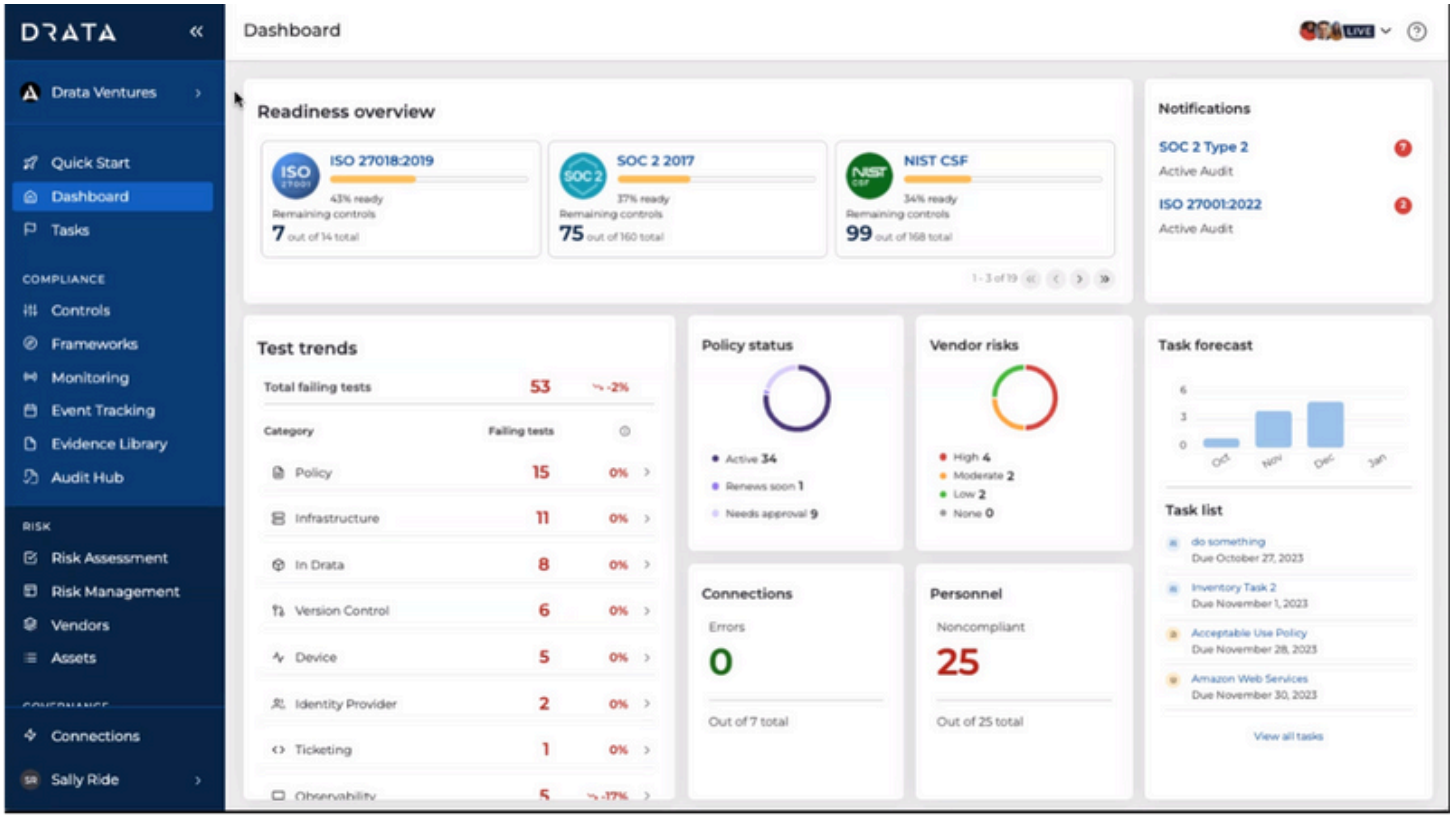
No. Drata es una herramienta escalable que se adapta a las necesidades de empresas de todos los tamaños, desde startups en crecimiento hasta grandes corporaciones. Es especialmente útil para empresas que experimentan un crecimiento rápido y necesitan gestionar el cumplimiento de forma ágil.

¿Cuánto tiempo se tarda en obtener la certificación con Drata?

El tiempo varía según la preparación de cada empresa, pero la automatización de Drata reduce drásticamente el cronograma. Muchas empresas logran su certificación en menos de la mitad del tiempo que les tomaría con métodos manuales.

Drata en el contexto mexicano

Drata es una herramienta poderosa que ayuda a las empresas mexicanas a pasar de un cumplimiento reactivo y manual a un enfoque proactivo y automatizado. Mientras que las regulaciones locales como la LFPDPPP son obligatorias, las certificaciones como la ISO 27001 y otras internacionales son estratégicas. Las que más sirven son aquellas que no solo evitan sanciones, sino que también generan una ventaja competitiva y permiten a la empresa expandirse a nivel global. Drata facilita la gestión de todas ellas desde una sola plataforma.



- **ISO 27001 (Sistema de Gestión de Seguridad de la Información).** Drata automatiza la recolección de evidencia para los controles del SGSI (Sistema de Gestión de Seguridad de la Información) de la ISO 27001, simplificando todo el proceso de auditoría.

- **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).** Drata puede ayudar a organizar y automatizar el cumplimiento de los principios de la ley, como la licitud, consentimiento y responsabilidad.

- **Normas de la CNBV (Comisión Nacional Bancaria y de Valores)** La automatización de Drata facilita la demostración de cumplimiento ante los supervisores, garantizando transparencia y estabilidad

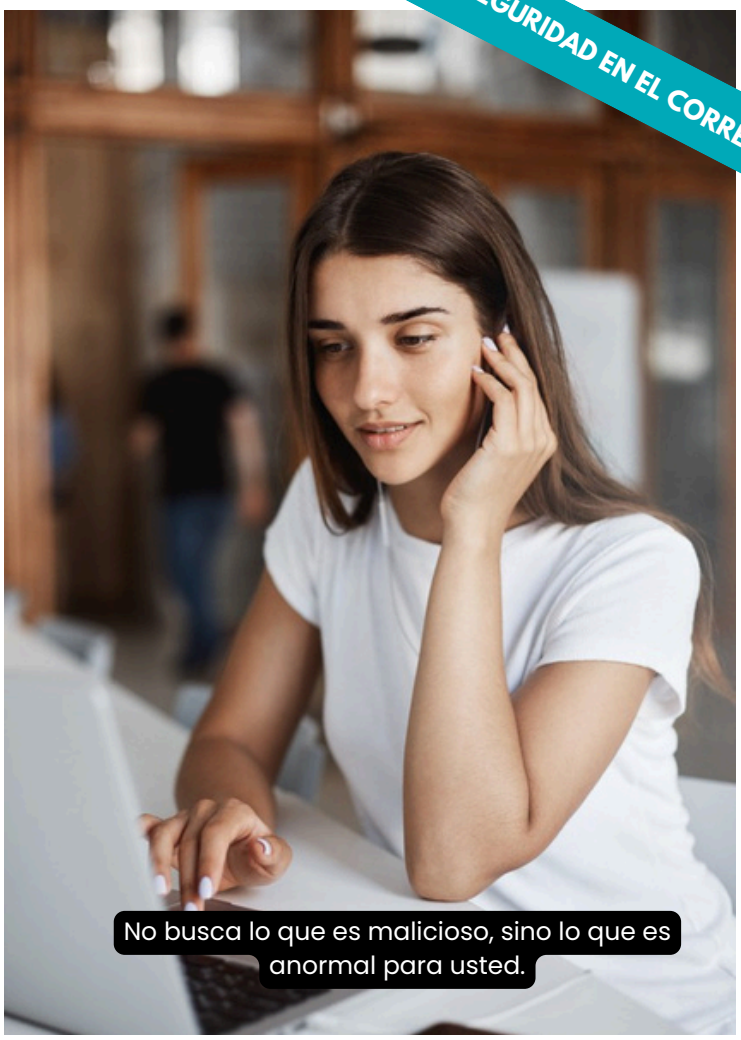
SEGURIDAD EN EL CORREO

Abnormal

Protección del Correo Electrónico Impulsada por Inteligencia Artificial

Abnormal Security es una solución de ciberseguridad que se especializa en la detección automática de ataques de día cero. Mientras las soluciones convencionales se basan en listas negras y firmas conocidas, Abnormal utiliza un enfoque revolucionario:

- **Modelo de Comportamiento Basado en IA**:
  1. Identidad Digital. Crea un modelo único para cada persona en su organización, analizando miles de puntos de datos
  2. Comportamiento normal: Estilo de escritura, patrones de comunicación, horarios, relaciones con colegas y proveedores.
  3. Contexto de la identidad: Jerarquía en la empresa, permisos, departamento, etc.



- **Análisis en Tiempo Real:** Cada email entrante es comparado contra estos modelos de comportamiento. Cualquier desviación o anomalía es detectada instantáneamente, incluso si el ataque es nuevo y nunca antes visto.

- **Protección Integral:** La plataforma identifica y bloquea automáticamente amenazas que otros sistemas pasan por alto, deteniendo el ataque antes de que llegue a la bandeja de entrada.

Abnormal AI Nombrado “Lider” en The Forrester Wave : Enterprise Email Security, Q2 2025

Estadísticas que Demuestran su Eficacia

- +90% de detección de ataques de BEC que otras soluciones pasan por alto.
- Miles de millones de dólares en pérdidas potenciales prevenidas para sus clientes.
- Reducción del >90% en el tiempo de investigación y respuesta a incidentes de correo.
- Minutos para implementar la solución, frente a horas o días de otras plataformas.

Abnormal

¿Cómo Funciona Abnormal AI?

1. Integración API Nativa

- Se conecta directamente a Microsoft 365 o Google Workspace via API
- Sin redirección de correo (sin cambios en MX records)
- Implementación en minutos sin afectar el flujo de email

2. Modelado de Comportamiento Basado en IA

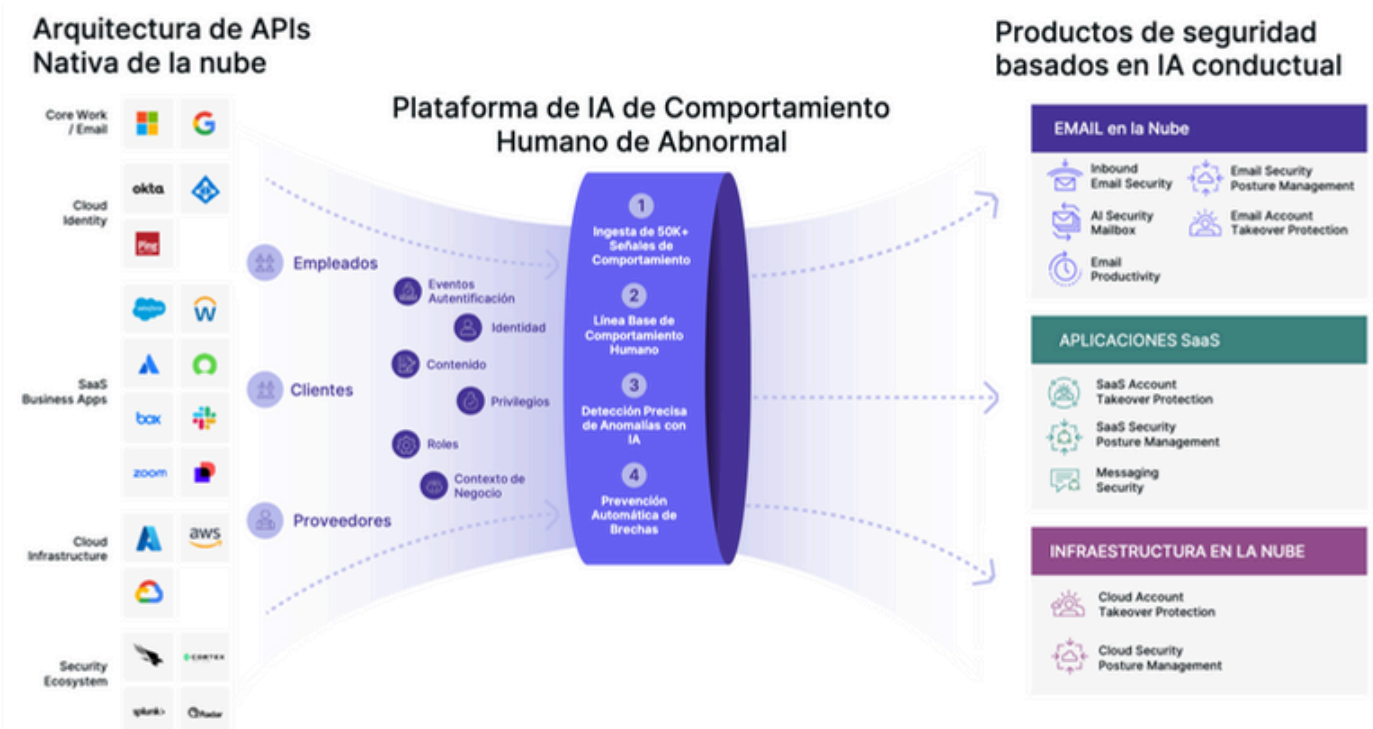
- Analiza +50,000 señales conductuales por usuario
- Crea una "Línea Base Conductual" entre Identidad, Comportamiento y Contexto:
  - Patrones de comunicación normales
  - Relaciones interdepartamentales típicas
  - Comportamiento histórico de correo
  - Dispositivos y ubicaciones habituales

3. Motor de Análisis en Tiempo Real

- Evalúa cada email contra el modelo de comportamiento establecido
- Aplica gráficos de relación entre entidades (empleados, proveedores, dominios)
- Analiza contexto organizacional y patrones transaccionales

4. Detección de Anomalías Multi-Capa

- Análisis de Identidad: Verifica desviaciones en el comportamiento del remitente
- Análisis de Relación: Detecta interacciones fuera de patrones establecidos
- Análisis de Contenido: Evalúa intención y contexto del mensaje
- Análisis de Dispositivo/Ubicación: Identifica acceso desde fuentes no habituales



5. Automatización de Respuesta

- Cuarentena automática de amenazas identificadas
- Recuperación automática de emails comprometidos
- Reversión de transacciones fraudulentas en casos de BEC

6. Plataforma Unificada de Protección

- Prevención de BEC (Business Email Compromise)
- Detección de suplantación de identidad
- Protección contra ataques a la cadena de suministro
- Defensa contra phishing y ransomware

Beneficios Clave en Seguridad de Correo

- **Detecta lo Indetectable:** Detiene ataques de ingeniería social avanzada como el BEC (Business Email Compromise), suplantación de identidad de ejecutivos y ataques de cadena de suministro, que son la principal causa de pérdidas financieras.
- **Disminución de Falsos Positivos:** Al entender el comportamiento normal, prácticamente elimina los bloqueos de correos legítimos, mejorando la productividad y evitando que los equipos de TI pierdan tiempo revisando cuarentenas.
- **Automatización Total:** La IA no solo detecta, sino que responde automáticamente a los incidentes, como revertir transacciones fraudulentas en cuestión de minutos.
- **Protección Sin Configuración Compleja:** Al ser una solución basada en API, se integra en minutos con Microsoft 365 y Google Workspace, sin necesidad de cambiar flujos de correo o hardware.
- **Ahorro de Tiempo y Recursos:** Libera a los equipos de seguridad de la gestión manual de alertas, permitiéndoles enfocarse en estrategias más críticas.

CLOUDFLARE

Red de nube global con servicios avanzados de ciberseguridad

Cloudflare consolida todas las soluciones de red y seguridad en una única plataforma, eliminando la complejidad de gestionar múltiples proveedores. Esto permite implementar políticas de seguridad consistentes en toda la organización y supervisar todas las operaciones desde un panel de control unificado.

Zero Trust Network Access (ZTNA).
Reemplaza VPNs con acceso seguro por aplicación

- Verifica identidad y dispositivo antes de permitir acceso
- Acceso granular a apps específicas, no a toda la red
- Beneficios: Elimina riesgos VPN, acceso remoto seguro, mejor experiencia usuario

Cloud Access Security Broker (CASB)
Protege sus aplicaciones en la nube (SaaS)

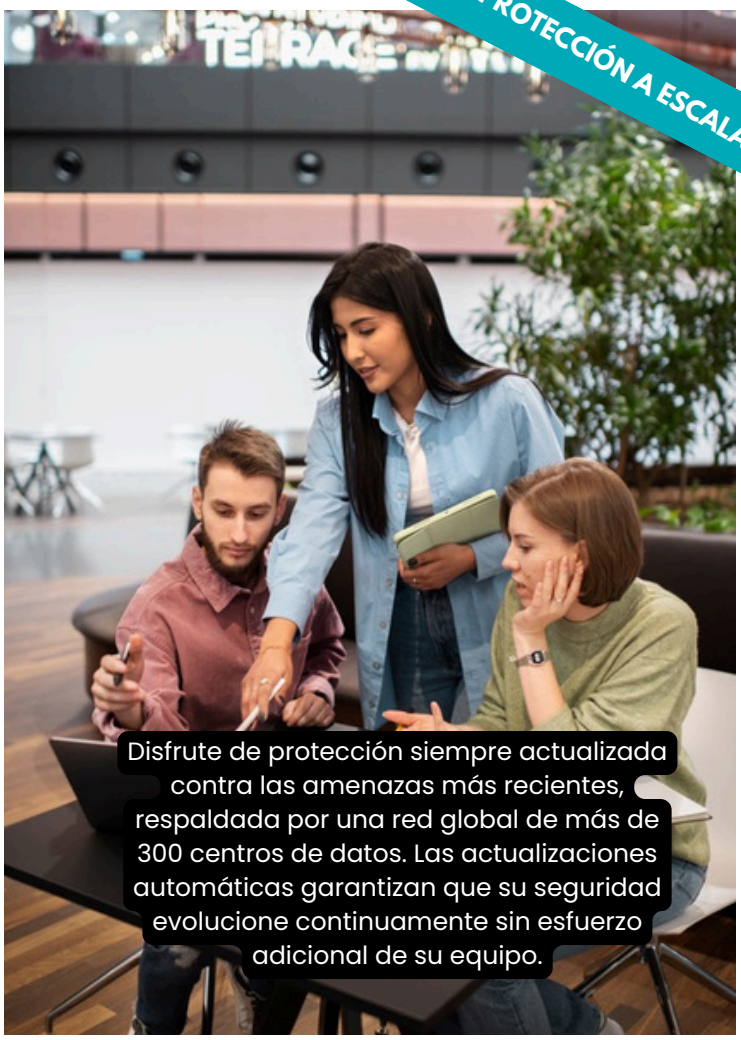
- Detecta shadow IT y aplicaciones no autorizadas
- Escanea Office 365, Salesforce, Google Workspace
- Beneficios: Visibilidad cloud, prevención fugas datos, cumplimiento normativo

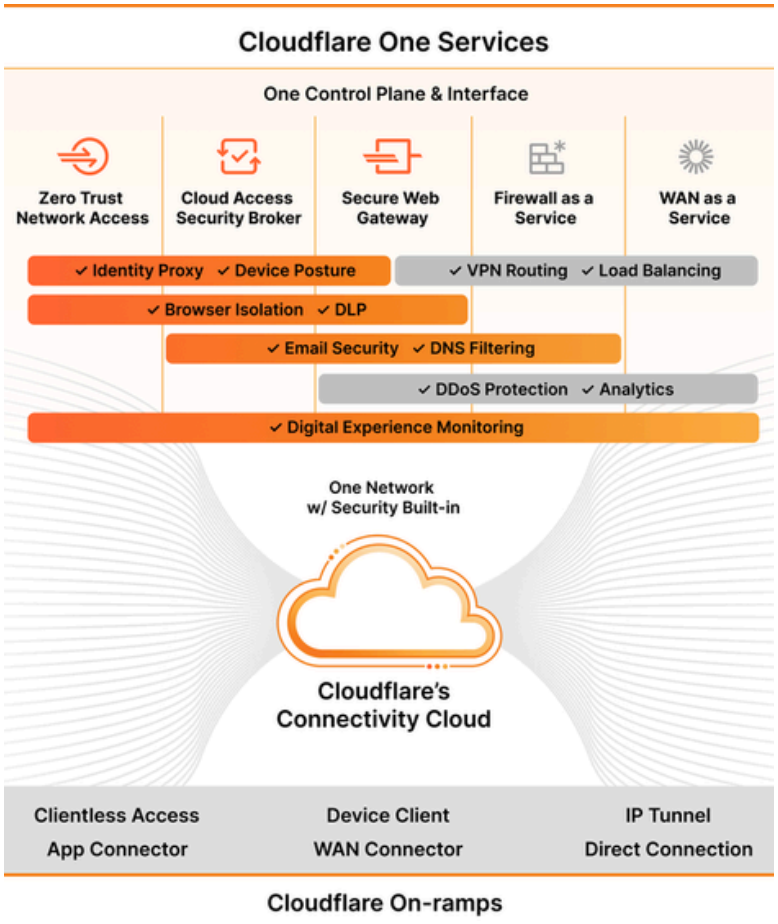
Secure Web Gateway (SWG)
Filtra y protege todo el tráfico web

- Bloquea malware, phishing y sitios maliciosos
- Controla acceso a aplicaciones web
- Beneficios: Protección contra amenazas web, control productividad, políticas uniformes

Firewall as a Service (FWaaS)
Firewall en la nube sin hardware

- Inspecciona todo el tráfico norte-sur y este-oeste
- Políticas centralizadas para todas las ubicaciones
- Beneficios: Sin costos de hardware, escalabilidad ilimitada, actualizaciones automáticas





WAN as a Service (Magic WAN)

Conecta oficinas y centros de datos globalmente

- Reemplaza MPLS tradicional
- Enrutamiento inteligente por la red Cloudflare
- Beneficios: Mejor rendimiento, menor costo que MPLS, implementación rápida

Beneficios Clave de Cloudflare

Seguridad Superior

- Protección DDoS líder del mercado con mitigación en <3 segundos
- WAF avanzado que bloquea automáticamente amenazas OWASP Top 10
- Zero Trust integrado para acceso seguro sin VPN
- SSL/TLS gratuito con cifrado siempre activo

Rendimiento Excepcional

- CDN global con +300 centros de datos worldwide
- Reducción de latencia hasta en 50% con Argo Smart Routing
- Caché inteligente que acelera sitios web hasta 200%
- Optimización automática de imágenes y contenido

Ahorro y ROI Comprobado

- Hasta 70% de ahorro vs soluciones tradicionales
- Elimina costos de hardware y mantenimiento
- Planes gratuitos con funcionalidades empresariales
- Precio predecible sin cargos por sobreuso

Simplicidad Operativa

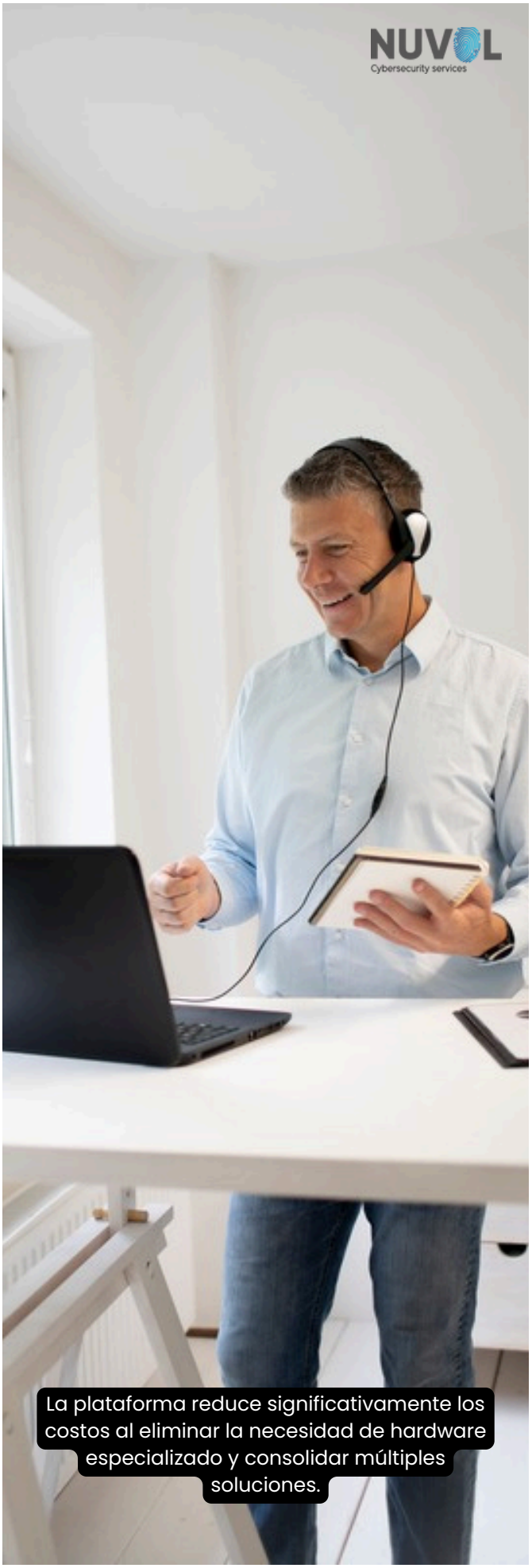
- Configuración en minutos, no en meses
- Dashboard unificado para gestionar todos los servicios
- APIs robustas para automatización completa
- Actualizaciones automáticas sin tiempo de inactividad

Escalabilidad Global

- Infraestructura elástica que maneja tráfico ilimitado
- Crecimiento automático con su negocio
- Red resistente con 100% uptime histórico
- Presencia global sin configuración adicional

Innovación Constante

- Nuevas funciones semanales
- Tecnología Edge Computing con Workers
- Integraciones nativas con principales clouds
- Machine Learning para protección proactiva



La plataforma reduce significativamente los costos al eliminar la necesidad de hardware especializado y consolidar múltiples soluciones.

NUVOL
The right people, for the best service

Gracias

SERVICIOS DE CIBERSEGURIDAD
@CYBERNUVOL

SERVICIOS

- Centro de Operaciones SOC as a Service
- Seguridad Microsoft Azure & O365
- Seguridad AWS
- Security Awareness
- Simulación de Intrusión de Ataque
- Análisis de Vulnerabilidades
- Automatización de Cumplimiento
- Pentest & Ethical Hacking
- Pruebas de ingeniería social
- Servicios Red Team
- Protección de Datos Personales
- Auditorías ISO 27001
- Protección de Marca
- Gobierno, Riesgo y Cumplimiento

CONTACTO:

Ciudad de México
M. info@cybernuvol.com
T. 55 9124 0158 o 442 808 7788
Dirección: Edificio City No 11B, Blvd. Manuel Ávila Camacho No. 3130, Tlalnepantla, C.P. 54020, CDMX.

Panamá
M. info@cybernuvol.com
Dirección: Edif. 109, Ciudad del Saber, Panamá.

Colombia
M. info@cybernuvol.co
Dirección: Oficina We Work, Piso 5, Carrera 7 #116-50 Bogotá 110221