SOLUCIONES DE CIBERSEGURIDAD

Atera

Atera es una plataforma en la nube **todo-en-uno** para proveedores de servicios gestionados y equipos de TI. Centraliza monitoreo, soporte y automatización con IA para resolver problemas rápido, escalar fácil y trabajar con eficiencia; sin importar el número de dispositivos y también ayuda a configurar fácilmente automatizaciones en alertas y parches.

Cómo se licencia/vende:

Se licencia en función de un modelo simple por técnico (no por dispositivo), con dispositivos ilimitados. Suscripción mensual facturada anualmente.

Sweet Spot: Idealmente Proveedores de servicios gestionados en crecimiento y equipos de TI pequeños que buscan eficiencia, visibilidad y automatización sin complejidad

Usuarios objetivo: Proveedores de Servicios Gestionados (MSPs), Equipos internos de TI, Gerentes de TI, Administradores de sistemas, Técnicos de soporte

Sectores verticales: Educación, Hospitales, Organizaciones sin fines de lucro, Servicios profesionales, Bienes Raíces y aspectos Legales.

Principales Competidores

ninjaOne · N-ABLE · Kaseya · CONNECTWISE

Diferenciadores

- **Todo-en-Uno: Monitoreo y Gestión Remota (RMM), Automatización de Servicios Profesionales (PSA), parches, acceso remoto y más en un solo panel.**
- **IA Integrada: Automatiza tareas y resuelve tickets más rápido.**
- **Soporte Remoto Instantáneo: Accede a cualquier dispositivo al instante.**
- **100% en la Nube: Implementación rápida, sin instalaciones.**

Cequence Security

Cequence es una plataforma de Seguridad de API y Gestión de Bots impulsada por inteligencia artificial (IA), diseñada para proteger aplicaciones web, móviles y basadas en API contra ataques automatizados, abusos y fraudes. Ofrece visibilidad, evaluación de riesgos y protección en tiempo real para todo el ecosistema de API.

Cómo se licencia/vende:

Se licencia en función del volumen de tráfico API (solicitudes por mes), y también el módulo Spyder puede cotizarse por dominio.
Con diferentes niveles y opciones de contrato anual o multianual.

Sweet Spot: El punto de partida ideal es de más de 25,000 llamadas API por día. Es especialmente adecuado para empresas con APIs públicas o portales de atención al cliente.

Usuarios objetivo: Equipos de seguridad de aplicaciones, Equipos de DevSecOps, Responsables de seguridad de redes, Empresas con plataformas digitales o aplicaciones para clientes.

Sectores verticales: Servicios financieros, Comercio electrónico y retail, Telecomunicaciones, Salud, Turismo y hospitalidad, Gobierno

Principales Competidores

imperva · SALT · CLOUDFLARE · noname · Akamai

Diferenciadores

- **Plataforma unificada para descubrimiento, protección y mitigación de bots en APIs**
- **Uso de IA y aprendizaje automático (ML) para análisis de comportamiento y detección avanzada de amenazas**
- **Motor de políticas sin código para una respuesta rápida ante nuevas amenazas**
- **Integración fluida con gateways de API y plataformas en la nube existentes**
- **Permite a las organizaciones cumplir con normativas de seguridad de API como NIST y OWASP API Top 10**

Cynet

Cynet ofrece una plataforma de ciberseguridad todo en uno diseñada para MSPs y PYMEs. Proporciona protección contra amenazas en endpoints, redes, usuarios, correo electrónico, dispositivos móviles, SaaS y entornos en la nube. Algunas características clave incluyen: EDR, NGAV, SOAR, UBA, CSPM y MDR.

Cómo se licencia/vende:

Cynet ofrece precios transparentes con paquetes adaptados a las necesidades empresariales. Su modelo de licencia es basado en suscripción, generalmente cobrado por endpoint por mes. Algunos detalles clave incluyen: Paquete Elite y Paquete All-in-One

Sweet Spot: Pequeñas y medianas empresas (PYMEs) que pueden no tener el presupuesto o la experiencia para gestionar múltiples soluciones de seguridad.

Usuarios objetivo: Cynet está dirigido principalmente a PYMEs y grandes empresas que necesitan ciberseguridad completa sin la complejidad de administrar múltiples soluciones de seguridad.

Sectores verticales: Finanzas Y Seguros, Salud, Retail, Gobierno & Educación, Manufactura E Industria.

Principales Competidores

DARKTRACE · SOPHOS · wazuh. · CROWDSTRIKE

Diferenciadores

- **Detección y respuesta automatizada de amenazas**
- **Despliegue rápido – Protege decenas de miles de endpoints en tan solo dos horas.**
- **Correlación cruzada entre redes, usuarios, archivos y endpoints**
- **Capacidades de seguridad integradas**
- **Detección y respuesta gestionada 24/7 (MDR)**
- **Solución rentable**

SOLUCIONES DE CIBERSEGURIDAD

esper

Esper proporciona una plataforma de gestión de dispositivos (**MDM**) diseñada para empresas modernas, ofreciendo automatización, seguridad y personalización para dispositivos Android y iOS. Sus Kits ayudan a integrar las herramientas de Esper en su infraestructura, permitiendo aprovisionamiento remoto, despliegue y depuración.

Cómo se licencia/vende:

Esper ofrece planes de precios flexibles según el número de dispositivos y características requeridas. Sus planes incluyen: Genesis, Bridge y Architect.

Sweet Spot: Ideal para empresas grandes y medianas en crecimiento que necesitan gestión escalable. Es óptimo para empresas que requieren **implementación avanzada** y **geofencing**.

Usuarios objetivo: Administradores de TI, Usuarios en ambientes empresariales, desarrolladores, minoristas proveedores, hostelería, proveedores de atención médica, clinicas, logística y transporte.

Sectores verticales: Proveedores Minoristas, Salud, Logística & Transporte, Educación, Fitness Y Bienestar, y Señalización Digital.

Principales Competidores

Scalefusion · hexnode · jamf · AirDroid · ManageEngine Mobile Device Manager

Diferenciadores

- **Personalización de AOSP Diseñado para dispositivos personalizados (AOSP).**
- **Herramientas avanzadas de DevOps – Pipelines de desarrollo que integran y despliegan continuamente, facilitando la gestión de flotas de Android y iOS.**
- **Aprovisionamiento sin intervención, depuración y control remoto – Ofrece acceso seguro a ADB remoto, monitoreo en tiempo real y herramientas avanzadas.**
- **Propiedad total del ecosistema de dispositivos – Para gestionar completamente su ecosistema de hardware y software, asegurando escalabilidad a largo plazo.**

HORNETSECURITY

Hornet Security es una plataforma en la nube que brinda seguridad avanzada para correo electrónico, respaldo y cumplimiento. Protege entornos de Microsoft 365 frente a phishing, ransomware, pérdida de datos y riesgos regulatorios mediante inteligencia artificial y continuidad automática.

Cómo se licencia/vende:

Licencia mensual por usuario. Se ofrece en paquetes que combinan seguridad, respaldo y cumplimiento. Modelo apto para MSPs con gestión multiempresa.

Sweet Spot: Es una solucion Ideal para empresas con más de 50 usuarios en Microsoft 365 que buscan una solución integral de seguridad y respaldo.

Usuarios objetivo: Todo tipo de administradores de TI, Empresas de gestión de servicios tercerizados (MSPs), equipos de seguridad y oficiales de cumplimiento con enfoque en Microsoft 365.

Sectores verticales: Empresas que trabajan en aspectos legales, Salud, Finanzas, Educación, Manufactura, Gobierno.

Principales Competidores

mimecast · Acronis · veeam · proofpoint · Barracuda

Diferenciadores

- **Plataforma todo-en-uno para seguridad, archivo, respaldo y continuidad**
- **Protección avanzada con filtrado basado en IA**
- **Respaldo completo de Microsoft 365 (Teams, OneDrive, SharePoint, Mail)**
- **Gestión sencilla y reportes listos para auditoría**
- **Consola MSP con visibilidad multicliente y control granular**

Kymatio®

Kymatio es una plataforma innovadora que ayuda a las organizaciones a gestionar el riesgo humano en ciberseguridad. A través de inteligencia artificial y neuropsicología, Kymatio identifica vulnerabilidades, entrena a los empleados y fortalece toda la seguridad organizacional.

Cómo se licencia/vende:

Kymatio es un SaaS modular y se vende por usuario activo al año, con precios escalables según el volumen. Incluye módulos como A&A para evaluacion y sensibilización, ABS para evaluar cuentas comprometidas y TRICKSTER para ejecutar campañas de concientización.

Sweet Spot: Pequeñas y medianas empresas (PYMEs) Empresas de alto volumen de empleados, que buscan fortalecer la seguridad de su información en sus compañias.

Usuarios objetivo: PYMEs y grandes empresas que necesitan educar y medir en aspectos de ciberseguridad a sus empleados ademas de cumplir con niveles de normativas importantes para su industria.

Sectores verticales: Organizaciones de sectores sensibles a los ataques (finanzas, salud, tecnología y equipos de ciberseguridad).

Principales Competidores

sosafe · HOXHUNT · CYBSAFE · KnowBe4

Diferenciadores

- **Firewalls Humanos: Capacita a los empleados para ser la primera línea de defensa contra amenazas.**
- **Métricas en Tiempo Real: Enfoca la evaluacion del riesgo antes de que se materialice con base en indicadores psicosociales y de comportamiento.**
- **Concienciación Personalizada: Formación adaptada y personalizada para cada usuario con una mayor efectividad.**

SOLUCIONES DE CIBERSEGURIDAD

miniOrange

MiniOrange es una plataforma integral de gestión de identidades y accesos (IAM) que permite la autenticación segura de usuarios, el inicio de sesión único (SSO), la autenticación multifactor (MFA) y la gobernanza de identidades en aplicaciones en la nube y locales. Proporciona una integración perfecta con más de 5.000 aplicaciones.

Cómo se licencia/vende:

Licencia por usuario o por aplicación, con opciones de suscripción anual o mensual. Disponible en despliegues alojados en la nube, locales o híbridos.

Sweet Spot: Organizaciones de todos los tamaños, en particular las que necesitan gestionar el acceso a múltiples aplicaciones en la nube y garantizar una autenticación segura con cumplimientos normativos.

Usuarios objetivo: Administradores de TI, CISO, equipos de IAM, ingenieros de DevOps/seguridad, responsables de cumplimiento y MSP.

Sectores verticales: Principalmente todos los ambitos relacionados a la Educación, Hospitales, Finanzas, administración pública, tecnología, comercio minorista y fabricación.

Principales Competidores

PingIdentity. onelogin DUO Microsoft Entra ID okta

Diferenciadores

- **Amplia biblioteca de integración para aplicaciones en la nube/on-prem**
- **Opciones MFA altamente personalizables y políticas de acceso condicional**
- **Compatibilidad perfecta con SSO a través de SAML, OAuth, OIDC y LDAP**
- **Precios asequibles y flexibles para PYMES y grandes empresas**
- **Opciones de marca blanca para MSP y revendedores**
- **Servicio de atención al cliente y asistencia para la implantación**

Miradore

Miradore es una solución de gestión de dispositivos móviles (MDM) basada en la nube, permite administrar, asegurar y monitorear dispositivos de forma centralizada. Permite a las organizaciones aplicar políticas, cifrar datos, controlar accesos y automatizar configuraciones de forma remota, desde una interfaz intuitiva.

Cómo se licencia/vende:

Licencia por dispositivo, con opciones de suscripción mensual o anual. Disponible en modalidad 100% en la nube. Cuenta con un plan gratuito limitado y versiones premium escalables.

Sweet Spot: PYMEs con entornos multiplataforma (BYOD o corporativos), especialmente aquellas con entre 25 y 500 dispositivos que requieren una administración simplificada y eficiente.

Usuarios objetivo: Equipos de TI, administradores de sistemas, responsables de seguridad y soporte técnico que necesitan una solución simple y efectiva para gestionar dispositivos de forma remota.

Sectores verticales: Educación, organizaciones sin fines de lucro, empresas de tecnología, salud, comercio minorista y logística.

Principales Competidores

hexnode jamf kandji Intune ManageEngine Mobile Device Manager

Diferenciadores

- **Interfaz intuitiva y configuración rápida sin experiencia técnica avanzada**
- **Plan gratuito disponible hasta 50 dispositivos**
- **Soporte multiplataforma completo (Windows, macOS, Android, iOS)**
- **Automatización de políticas y despliegue de apps a distancia**
- **Cumplimiento normativo con cifrado y control de accesos**
- **Ideal para empresas con estrategias BYOD**
- **Reportes en tiempo real y alertas de seguridad integradas**

netwrix

Netwrix es una plataforma de visibilidad y seguridad de datos que ayuda a las organizaciones a identificar y mitigar los riesgos informáticos, proteger los datos confidenciales y garantizar el cumplimiento de la normativa. Ofrece soluciones de auditoría, clasificación de datos, control de acceso y detección de amenazas.

Cómo se licencia/vende:

Licencia por número de usuarios o activos (según el módulo), con opciones perpetua y por suscripción. Las ofertas de productos modulares permiten la personalización en función de los casos de uso para cada cliente en especifico.

Sweet Spot: Organizaciones medianas y grandes que requieren auditorías detalladas, cumplimiento de normativas y visibilidad del comportamiento de los usuarios y del acceso a los datos en entornos informáticos complejos.

Usuarios objetivo: Personal de TI, analistas de seguridad, CISO y equipos de gobernanza, riesgo y cumplimiento (GRC).

Sectores verticales: Servicios financieros, sanidad, administración pública, educación, asesoría jurídica, industria y energía.

Principales Competidores

VARONIS jumpcloud. zluri splunk> Quest

Diferenciadores

- **Visibilidad unificada de entornos de TI híbridos (AD, Azure AD, Exchange, SharePoint, VMware, etc.) Auditoría de archivos y acceso basada en riesgos**
- **Informes de cumplimiento listos para usar (HIPAA, GDPR, SOX, PCI-DSS)**
- **Clasificación de datos y descubrimiento de datos confidenciales en archivos compartidos y en la nube**
- **Alertas y detección de anomalías de comportamiento para prevenir amenazas internas específicas.**

SOLUCIONES DE CIBERSEGURIDAD

phishingbox

PhishingBox es una plataforma de simulación de ataques y formación en concienciación de seguridad que permite a las organizaciones identificar, capacitar y evaluar a sus empleados frente a amenazas de ingeniería social. Ofrece campañas personalizables de phishing, pruebas automatizadas y módulos de capacitación en línea.

Cómo se licencia/vende:

Licencia por usuario con opciones de suscripción anual. Disponible como solución SaaS, hospedada en la nube, con escalabilidad flexible según el número de usuarios y campañas activas.

Sweet Spot: Organizaciones que buscan medir y mejorar la resiliencia de su personal ante ataques de phishing y otras amenazas basadas en el comportamiento del usuario, especialmente en sectores regulados o con alto riesgo de ciberataques.

Usuarios objetivo: Responsables de seguridad informática, equipos de TI, oficiales de cumplimiento, CISO, formadores de personal y MSPs que buscan fortalecer el factor humano en la seguridad.

Sectores verticales: Educación, salud, banca, seguros, servicios legales, tecnología, administración pública, y cualquier organización con políticas de cumplimiento o auditorías de ciberseguridad.

Principales Competidores

HOXHUNT · KnowBe4 · Terranova Security · COFENSE

Diferenciadores

- **Editor de plantillas de phishing altamente personalizable**
- **Plataforma multitenant ideal para MSPs y socios de canal**
- **Módulos de formación interactivos y adaptativos**
- **Evaluaciones automatizadas con retroalimentación inmediata**
- **Reportes detallados con métricas clave para auditorías**
- **Soporte técnico con enfoque en personalización y escalabilidad**
- **Integración con herramientas de terceros vía API**

TitanHQ

TitanHQ es una solución integral de ciberseguridad en la nube enfocada en proteger el correo electrónico corporativo, la navegación web y simulaciones de phishing y entrenamiento en concienciación al usuario final frente a amenazas digitales. Destaca por su facilidad de implementación, su enfoque en cumplimiento normativo.

Cómo se licencia/vende:

Licencia por usuario o dispositivo, con suscripción anual. Su enfoque modular permite contratar productos por separado, adaptándose a las necesidades de empresas o MSPs.

Sweet Spot: Organizaciones que buscan consolidar la protección del correo electrónico, navegación segura y formación del usuario en una sola plataforma, sin complicaciones técnicas ni costos elevados.

Usuarios objetivo: Equipos de TI, responsables de ciberseguridad, administradores de correo y MSPs que requieren una solución ágil, escalable y fácil de gestionar desde la nube.

Sectores verticales: Educación, salud, manufactura, tecnología, finanzas, comercio y entornos con trabajadores remotos o híbridos.

Principales Competidores

mimecast · proofpoint · veeam · cisco Umbrella · Barracuda

Diferenciadores

- **PhishTitan: Protección avanzada contra phishing con inteligencia en tiempo real**
- **WebTitan: Filtrado DNS para navegación segura y control de contenido**
- **SpamTitan: Filtro antispam de alta precisión para proteger el correo**
- **EncryptTitan: Cifrado automático de correos con cumplimiento integrado**
- **ArcTitan: Archivado seguro y accesible para auditorías o recuperación**
- **TitanHQ SAT: Simulación de ataques y formación en concienciación continua**
- **Consola unificada, multitenant y soporte técnico con rápida puesta en marcha**

vicarius

Vicarius es una plataforma de gestión proactiva de vulnerabilidades diseñada para ayudar a las organizaciones a priorizar, mitigar y remediar riesgos de ciberseguridad antes de que sean explotados. Ofrece visibilidad completa del entorno, análisis basado en contexto y ejecución de parches desde una interfaz intuitiva.

Cómo se licencia/vende:

Licencia anual por dispositivo, con precios escalables según volumen. Ofrecido como solución SaaS, con opciones on-premise disponibles bajo demanda. Modelo flexible y orientado a empresas y MSPs.

Sweet Spot: Empresas que buscan automatizar la gestión de vulnerabilidades, eliminar la dependencia de parches tradicionales y reducir la superficie de ataque de forma proactiva y contextualizada.

Usuarios objetivo: Equipos de ciberseguridad, administradores de sistemas, responsables de cumplimiento, CISO y proveedores de servicios gestionados que desean consolidar la evaluación y remediación de vulnerabilidades en un solo flujo.

Sectores verticales: Finanzas, salud, tecnología, sector público y cualquier entorno con infraestructura crítica o cumplimiento regulatorio.

Principales Competidores

RAPID7 · tenable · SECPOD · ManageEngine Mobile Device Manager · Qualys.

Diferenciadores

- **Tecnología de parcheo sin agente para mitigar sin esperar actualizaciones**
- **Motor de priorización contextual (Topia) basado en riesgo real y exposición**
- **Consola unificada para evaluación, priorización y remediación**
- **Capacidades de ejecución de scripts y automatización de flujos de trabajo**
- **Visibilidad en tiempo real de activos, vulnerabilidades y estado de mitigación**
- **Integración sencilla con entornos existentes (AD, SIEM, ticketing, etc.)**
- **Reduce el “tiempo a parche” y cierra brechas antes de que sean explotadas**