Vectra CDR para M365 | Detección y respuesta en la nube basadas en IA

Vea y detenga las amenazas dirigidas a las aplicaciones y los datos de Microsoft 365

Microsoft 365 (M365) es la suite de productividad en la que confían cientos de millones de usuarios empresariales para que sus equipos se conecten, colaboren y realicen su trabajo cada día. Sin embargo, con un gran número de usuarios a bordo, la plataforma es también un objetivo principal de los ciberatacantes para robar credenciales, hacerse con cuentas, acceder a sistemas críticos o lanzar campañas maliciosas. Sin visibilidad, una visión adecuada y una amplia cobertura a través de M365, sigue siendo difícil discernir un compromiso de forma rápida y eficaz. A medida que se conectan más empleados, la seguridad debe ser una preocupación primordial, ya que los controles nativos pueden dejar las aplicaciones expuestas a los atacantes, que pueden ejecutar ataques de extremo a extremo sin necesidad de herramientas externas. Vectra puede ayudar.

Principales retos

- Visibilidad limitada del SOC en M365
- Puesta en peligro de cuentas y actividad inadvertida de usuarios y entidades
- Visibilidad unificada para M365
- Comprensión clara de los ataques

Sepa cuándo su entorno de Microsoft 365 está en peligro

Vectra Cloud Detection and Response (CDR) para M365 es la defensa contra ataques basada en IA más avanzada del sector para identificar y detener amenazas y ataques en todo su entorno M365. Vectra CDR para M365 aprovecha Security AI-driven Attack Signal Intelligence™ para ir más allá de la simple detección de anomalías y analizar y comprender el comportamiento de los atacantes. Esto garantiza la detección temprana con claridad, precisión y contexto para borrar incógnitas y sacar a la superficie amenazas, ataques y actividades maliciosas a través de una cadena completa de eventos sospechosos. Con Vectra, las organizaciones ven, comprenden y responden eficazmente a las amenazas y ataques que otras soluciones pasan por alto, de modo que los equipos de seguridad pasan menos tiempo ajustando, buscando e investigando, y pueden responder antes a los ataques.

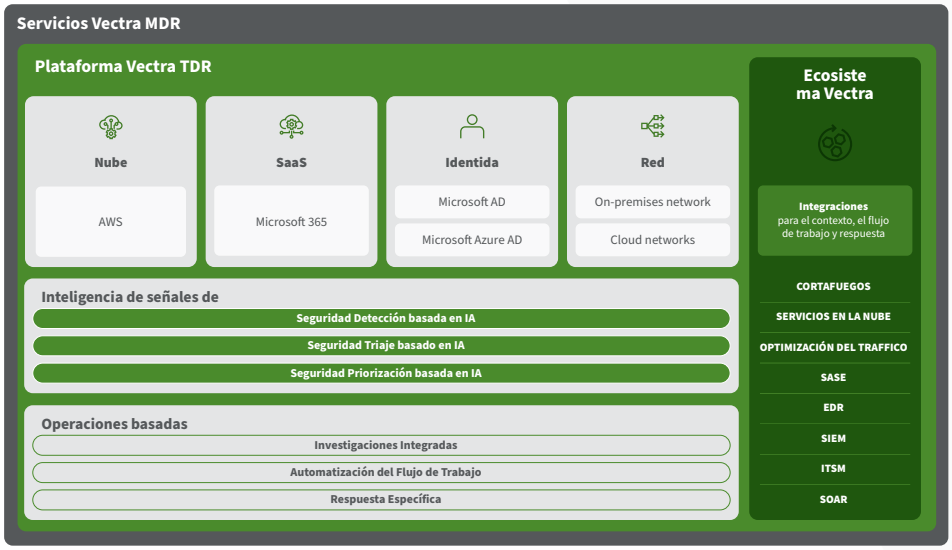
Principales funciones del producto

- **Detección basada en IA**
  Aprovechando la Inteligencia de Señales de Ataque basada en IA de Seguridad, Vectra va más allá de las firmas y la simple detección de anomalías para exponer la narrativa completa de los ataques a los que se enfrentan las aplicaciones M365. Los modelos de detección predefinidos detectan y correlacionan con precisión la actividad de los atacantes, automatizando el complejo análisis de los datos M365 para revelar más del 90% de las técnicas maliciosas en el marco MITRE ATT&CK.
- **Triaje basado en IA**
  Aprovechando la Inteligencia de Señales de Ataque basada en IA de Seguridad, Vectra comprende las amenazas previamente priorizadas y la actividad sospechosa de M365. Vectra analiza continuamente los incidentes de M365 y distingue los eventos maliciosos de los incidentes benignos y automatiza las tareas manuales con la perspectiva de un experto analista, por lo que las puntuaciones de riesgo asociadas, el contexto y los elementos comunes se clasifican como detecciones "verdaderas".
- **Priorización basada en IA**
  Aprovechando la Inteligencia de Señales de Ataque basada en IA de seguridad, Vectra correlaciona, puntúa y clasifica automáticamente detecciones múltiples y concurrentes cuando se desarrollan los eventos. Los análisis de IA evalúan automáticamente los incidentes en comparación con los eventos existentes al nivel de un analista de seguridad altamente experimentado, revelando al instante los niveles de exposición al riesgo y la priorización relacionada para que SecOps pueda dedicar más tiempo a impulsar planes de acción.
- **Investigación avanzada**
  Vectra simplifica la investigación en profundidad y pone las respuestas al alcance de los analistas, reduciendo el esfuerzo y el tiempo necesarios para ejecutar consultas complejas e interpretar los resultados. Para M365, Vectra CDR conserva de forma única grandes volúmenes de datos de origen detrás de cada detección y, a continuación, aprovecha la IA para obtener más significado y sacar a la luz información en cuestión de minutos. Los investigadores comprenden rápidamente los detalles de "quién", "qué", "cuándo" y "cómo" detrás de las amenazas, junto con los efectos de largo alcance que tendrán en las aplicaciones y los datos de M365.
- **Flujos de trabajo automatizados**
  Elimine las tareas que requieren mucho tiempo para supervisar y evaluar adecuadamente los registros de la nube, investigar las detecciones, iniciar las amenazas respuesta y llegar a la atribución con las amenazas. Vectra hace el trabajo en minutos, de modo que los analistas pueden ver las cuentas comprometidas, las aplicaciones infractoras y cómo acceden los usuarios a los inquilinos.
- **Respuesta específica**
  Con un contexto de amenazas más profundo que el de las herramientas nativas de Microsoft, los equipos de seguridad adquieren amplias capacidades para responder, contener, investigar, comunicar y abordar los sistemas comprometidos en menos tiempo. La aplicación de la normativa por parte de los analistas pone a los humanos en control de la respuesta con un enfoque flexible que permite flujos de trabajo automatizados o mediante acciones activadas por los analistas en la interfaz de usuario. Los controles de respuesta "listos para usar" incluyen herramientas y libros de jugadas que ya están en todo ello infundiendo confianza en todo el equipo, reduciendo el agotamiento y minimizando los costes.

Explore la plataforma Vectra

La plataforma Vectra Threat Detection and Response (TDR) combina una completa cobertura de la superficie de ataque en la nube pública, SaaS, identidad y red. Aprovechar la seguridad Señal de ataque basada en IA Intelligence™, obtén una claridad de señal inigualable que te permite tener el control mientras defiendes contra los ciberatacantes modernos, evasivos y avanzados.

- **Cobertura de ataques:** elimine las amenazas desconocidas en 4 de sus 5 superficies de ataque: nube, SaaS, identidad y redes.
- **Claridad de las señales:** aproveche la inteligencia de las señales de ataque para detectar, clasificar y priorizar automáticamente las amenazas desconocidas.
- **Control inteligente:** arme la inteligencia humana para cazar, investigar y responder a amenazas desconocidas.



Por qué las empresas eligen Vectra para M365

- **Attack Signal Intelligence** proporciona señales enriquecidas que los analistas pueden utilizar para automatizar las tareas manuales relacionadas con la detección, el triaje y la priorización de amenazas.
- **Cobertura sin agentes que se despliega en minutos** y activa la detección sin firmas, escuchas virtuales ni políticas estáticas.
- **Detecte amenazas a través de las tácticas de MITRE** que otras soluciones no pueden ver.
- **Investigación y respuesta integradas** que aceleran la detección de amenazas y amplían la cobertura para reducir significativamente el tiempo medio de respuesta (MTTR).
- **Elimina montañas de falsos positivos** para que los analistas dispongan de más tiempo para la investigación proactiva y estratégica.
- **Vista única de la actividad que vincula las detecciones** originadas en M365, on-premises, AWS y AzureAD

Acerca de Vectra

Solo Vectra optimiza la IA de seguridad para comprender los comportamientos de los atacantes en la nube pública, la identidad, las aplicaciones SaaS y los centros de datos. Aprovechando la IA de seguridad, Vectra se compromete a capacitar a los equipos de seguridad para pasar a la ofensiva y evitar que los ciberataques se conviertan en brechas. Vectra proporciona la cobertura de amenazas, la claridad y los controles que los equipos de operaciones de seguridad necesitan para crear estrategias de seguridad más eficaces, eficientes y resistentes. Organizaciones de todo el mundo confían en la plataforma y los servicios gestionados de Vectra para obtener una mayor resistencia frente al ransomware, la cadena de suministro, el compromiso de cuentas y las amenazas internas. Más información en www.vectra.ai.

Si desea más información, póngase en contacto con nosotros:
Correo electrónico: info@vectra.ai | vectra.ai