

ManageEngine

Ransomware Protection Plus

Descripción del producto





Acercas de

Ransomware Protection Plus es una solución basada en ML que detecta comportamientos anómalos indicativos de actividad de ransomware. Identifica y mitiga el ransomware al tiempo que garantiza la recuperación de datos sin problemas en caso de ataque.

La solución supervisa continuamente el comportamiento del sistema, incluso cuando está desconectado, para identificar y neutralizar las cepas de ransomware sofisticadas y emergentes, con el fin de mantener el estricto cumplimiento de la normativa y la continuidad operativa.

El problema

72% de las empresas afectadas por ransomware en 2023.

El pago promedio por rescate ronda los **1,5 millones** de dólares.

El **60%** de las **pymes** cierran en los 6 meses siguientes a un ataque.

Aumento del 40% de los ataques de ransomware en pymes.

El ransomware causará a sus víctimas pérdidas de alrededor de **265.000 millones de dólares** anuales para el año 2031.



Consecuencias de un ataque de ransomware

Pérdidas económicas: Pago de rescates, costes de recuperación, gastos legales.

Caos operativo: Tiempo de inactividad, pérdida de datos, interrupción de la cadena de suministro.

Daños a la reputación: Pérdida de confianza de los clientes, multas reglamentarias.

El problema de la seguridad tradicional

Las herramientas basadas en firmas no detectan ransomware sofisticado: Las herramientas basadas en firmas se basan en patrones predefinidos para identificar amenazas conocidas. Al centrarse en lo que hace el ransomware y no en lo que parece, la detección de comportamientos ofrece una protección proactiva y adaptable frente a las amenazas en evolución.

Dependencia excesiva de las copias de seguridad: El ransomware de eliminación de copias de seguridad o el ransomware antirrecuperación emplean tácticas para obstaculizar los esfuerzos de restauración, asegurándose de que las víctimas no puedan recuperarse fácilmente sin pagar el rescate. Las herramientas de seguridad tradicionales carecen de mecanismos para contrarrestar esta situación.



Visión general

Defensa proactiva

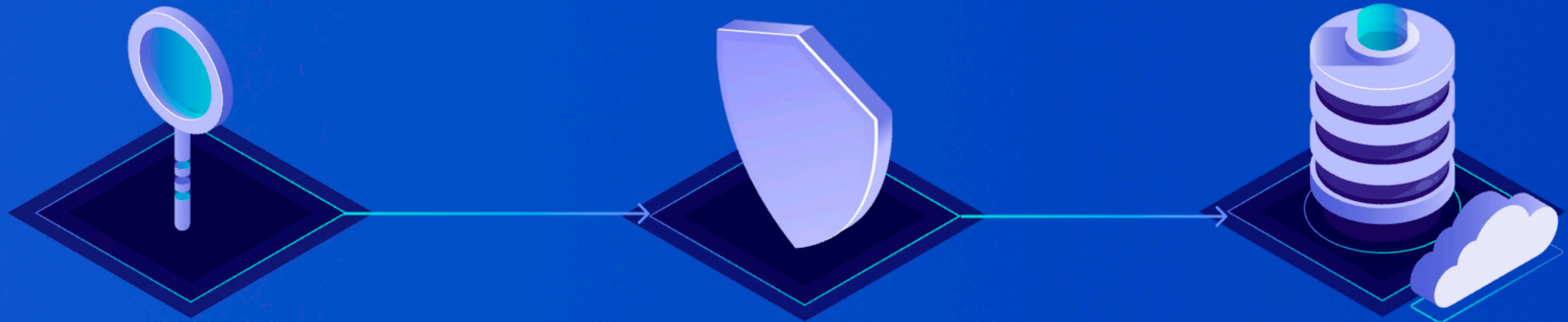
- Detección de ransomware basada en memoria
- Protección contra ransomware fuera de línea
- Mitigación de exploits

Protección activa:

- Análisis del ciclo de vida del ataque
- Mitigación preventiva de incidentes
- Aislamiento de dispositivos en tiempo real
- Bloqueo dinámico de cifrado

Respuesta rápida y recuperación

- Investigaciones forenses
- Recuperación instantánea
- Defensa contra reincidentes
- Kill-switch adaptable



Funciones de Ransomware Protection Plus



Respuesta y recuperación

Copias de seguridad inviolables:

Las copias de seguridad inmutables garantizan que el ransomware no pueda borrar tus datos de recuperación.

Retroceso y recuperación rápidos:

Restaura archivos y sistemas cifrados a su estado anterior al ataque en cuestión de minutos.

Cambia entre los modos auditoría y kill:

Prueba las defensas en modo Auditoría, luego activa el modo Kill para neutralizar las amenazas vivas.

Resiste ataques repetidos:

Los sistemas de autoendurecimiento recuperan los puertos para evitar que los atacantes ataquen dos veces.

¿Por qué Ransomware Protection Plus?



Detecte anomalías de comportamiento con ML: Identifique el ransomware analizando la actividad sospechosa en tiempo real.

Interceptar el ransomware en pleno ataque: Neutralizar el ransomware en seco, evitando el cifrado y minimizando los daños.

Recupere los archivos cifrados por el ransomware: Restaure los archivos cifrados al instante, sin tiempo de inactividad ni pago de rescates.

Protección frente al ransomware de día cero: Defiéndase frente a ataques de ransomware nunca vistos y cepas emergentes.

Diferenciadores únicos

Su guardián silencioso: Funciona de forma invisible sin ralentizar a los usuarios ni los flujos de trabajo, con un rendimiento cero, incluso durante los análisis de todo el sistema.

- **Aprende y crece con usted:** La gestión centralizada se amplía sin esfuerzo desde las nuevas empresas hasta las grandes compañías, adaptándose a los ecosistemas informáticos en crecimiento y a las amenazas en evolución.
- **Despliegue sin esfuerzo:** Implemente la protección en toda la empresa en cuestión de minutos, sin reinicios, tiempos de inactividad ni configuraciones complejas.

Ventaja de ciberseguro y ROI: La reducción del riesgo de ransomware disminuye las primas al tiempo que reduce el presupuesto de seguridad.

- **Defensa adaptable:** Personalice la aplicación con modos -desactivación automática o auditoría forense para adaptarla a su postura de ciberseguridad.

Conozca más

Sitio web

Prueba gratuita de 30 días

Solicite una cotización

Demo personalizada

Cómo empezar

Recursos

