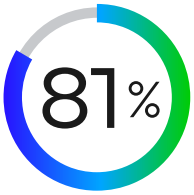
Trellix

INFORME EJECUTIVO

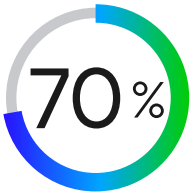
Da vida a tu ciberseguridad con Trellix

Cómo un ecosistema XDR en constante evolución puede dinamizar tu organización

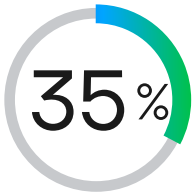
El estado de la ciberseguridad en números



En una encuesta a directores de seguridad de la información, el 81 % de los encuestados respondió que anticiparse a los atacantes es una preocupación constante.[1]



El 70 % de las partes interesadas en seguridad de TI informan de más del doble del volumen de alertas de seguridad en los últimos cinco años.[2]



El 35 % de los analistas de ciberseguridad ignoran las alertas cuando tienen demasiadas incidencias en la cola.[3]

El tiempo promedio para identificar y contener una filtración de datos es 287 días.[4]

El tiempo promedio para responder a un incidente global es 20,9 horas.[5]

El mundo actual está repleto de amenazas dinámicas que se vuelven más complejas cada día.

Esto supone un desafío importante para las organizaciones. Con un enfoque estático y aislado de la ciberseguridad, a menudo estas empresas descubren que no pueden controlar la naturaleza en constante cambio del entorno de amenazas actual.

Para seguir el ritmo a los ataques dinámicos y garantizar una mayor tranquilidad, las organizaciones buscan una visibilidad más centralizada y una resolución rápida de sus problemas de ciberseguridad.

XDR, por sus siglas en inglés, significa detección y respuesta extendidas:

- **Extendida** hace referencia a que la solución se extiende a través de varios vectores de ciberseguridad, incluidos puntos finales, la red, la nube y el correo electrónico, y otros productos de seguridad de terceros.
- **Detección** proviene de la capacidad de detectar amenazas a través de los vectores en el momento en que se producen.
- **Respuesta** permite a tu organización estar mejor preparada para responder de manera efectiva a los ataques en tiempo real.

Con un ecosistema XDR inteligente y adaptable, puedes proteger tu empresa con la próxima evolución de la ciberseguridad.

1. State of Cybersecurity Resilience 2021, Accenture, 2021 | 2. 2020 State of SecOps and Automation, Dimensional Research, 2020 | 3. The Voice of the Analysts, IDC, 2021 | 4. Cost of a Data Breach, IBM, 2021. 5. Voice of SecOps, Deep Instinct, 2021

Por qué las soluciones actuales de ciberseguridad no pueden abordar amenazas futuras

Considerando la creciente sofisticación de las amenazas, es fácil entender por qué tantas empresas son vulnerables a los ataques. Sin embargo, la razón principal por la que siguen estando en peligro es porque sus soluciones de ciberseguridad existentes no satisfacen sus necesidades.

1. Están demasiado centradas en resolver la última amenaza de ciberseguridad, no la próxima

A pesar de la proactividad y el nivel de actualización que muestran muchas organizaciones frente a las amenazas actuales, son las amenazas futuras las que realmente deberían preocuparles. Desafortunadamente, muchas empresas carecen de la experiencia y el personal que necesitan para monitorizar los ataques recibidos y resolver las amenazas. Más importante aún, carecen de las herramientas avanzadas necesarias para controlar futuros ataques. Con la ayuda de aprendizaje automático e inteligencia artificial, obtienen la información que necesitan para identificar ataques prioritarios, mejorar la toma de decisiones y resolver sus problemas.

2. Dependen demasiado de procesos manuales propensos a errores, no de la automatización

Incluso con una solución adecuada, muchos equipos de TI se ven obligados a depender de procesos manuales para gestionar su infraestructura de ciberseguridad, lo que genera a las organizaciones una serie de problemas, concretamente, ineficiencia. Si un miembro de un equipo de TI recibe una alerta de seguridad, debe saber que es legítima. De lo contrario, una empresa podría dedicar tiempo y recursos valiosos a revisar un problema que en realidad no existe en absoluto.

3. Los equipos de ciberseguridad carecen de amplitud para cubrir todos los vectores y productos puntuales

Muchas organizaciones creen que ahorran dinero al desarrollar soluciones de ciberseguridad internas o "hechas en casa", pero lo cierto es que estas soluciones a menudo cuestan más que las soluciones listas para usar. Debido a que el equipo de seguridad no puede cubrir la amplitud de cada vector de amenaza ni responder de forma dinámica, estas soluciones internas, en general, están plagadas de problemas, lo que las hace menos seguras y más onerosas que una solución establecida y confiable.

Cómo Trellix está reescribiendo la historia de la ciberseguridad

Trellix está a la vanguardia de la revolución XDR liderando una nueva forma de unir la detección, la respuesta y la resolución en una única solución de ciberseguridad en constante evolución. Nuestro innovador ecosistema XDR:

- Te capacita para analizar datos al instante y predecir y prevenir ataques con una solución que aprende y se adapta constantemente
- Te permite crear asociaciones abiertas y conexiones nativas para automatizar la organización de políticas de ciberseguridad
- Te apoya con herramientas integradas y conocimientos de expertos para reducir las complejidades y aumentar la eficiencia

Experimenta un enfoque nuevo y unificado a XDR

Trellix XDR se integra a la perfección con nuestra amplia cartera de puntos finales, correo electrónico, red, nube y otros productos de ciberseguridad. Además, se conecta fácilmente con aplicaciones de seguridad de terceros. Esta conectividad dota a tu empresa de detección de amenazas, análisis y respuesta automatizada inteligentes.

Con una experiencia más unificada, tienes la capacidad de:

Detectar ataques avanzados en todos los vectores

Trellix XDR te permite detectar incidentes de seguridad con confianza. Descubre los conocimientos de la telemetría multivectorial en múltiples activos, en toda tu organización, y aplica esa información para frustrar los ataques a escala.

Pasar de la detección de ataques a la prevención de amenazas

Trellix XDR bloquea ataques enviados a través del correo electrónico entrante, la red y los puntos finales. Con un ecosistema inteligente y adaptable, puedes predecir y prevenir amenazas emergentes, identificar las causas principales y responder en tiempo real.

Integrar ciberseguridad de última generación en tus operaciones

Trellix XDR proporciona flujos de trabajo de investigación guiados. Confiriendo una mayor inteligencia al centro de tus operaciones, obtienes la capacidad de automatizar procesos y priorizar tus preocupaciones de ciberseguridad más críticas.

Dinamiza tu empresa con Trellix

Para avanzar hacia el futuro, es crucial proteger el presente. Esto significa asegurarte de que tus equipos puedan ser proactivos, no solo reactivos, de que tu empresa tenga libertad para aprovechar las oportunidades y de que finalmente tengas ventaja sobre las amenazas.

Trellix XDR combina tecnología innovadora con el potencial de la experiencia humana para:

- Crear un mundo digital más resiliente al adaptarse rápidamente a la situación de amenazas globales en constante cambio
- Transformar las amenazas actuales en ventajas futuras al correlacionar eventos dispares de múltiples herramientas en información procesable
- Emprender un futuro empresarial más brillante al reducir los riesgos empresariales a través de la detección y respuesta automatizadas de amenazas

¿Estás preparado/a para dinamizar tu empresa con XDR? Visita trellix.com para empezar ya o habla con unos de nuestros expertos en XDR para descubrir cómo Trellix puede ayudarte a impulsar tu empresa.

Trellix

Copyright © 2022 Trellix US LLC