Microsoft Security

## Protección del patrimonio digital:

# Un enfoque integrado para incrementar la eficiencia del SOC

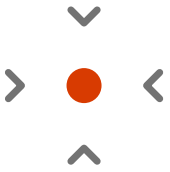
Los complejos entornos de TI de hoy requieren un enfoque más eficiente, optimizado e integrado para el Centro de operaciones de seguridad.

# Contenido

# Aportes claves de este documento

**Un panorama de ataques cada vez más sofisticados y complejos** hace que para los SOC sea más desafiante mantener el ritmo.

**La integración de los sistemas SIEM y XDR** aumenta la eficacia y eficiencia de la seguridad en toda la empresa.



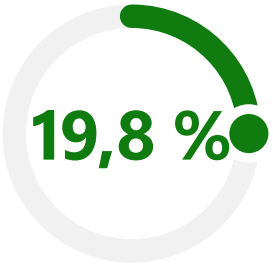
La automatización y la IA son componentes esenciales del kit de herramientas de seguridad, ya que pueden **detectar y corregir proactivamente las amenazas,** liberando así  recursos de operaciones de seguridad.

**Un enfoque de seguridad nativo de la nube** mejora el rendimiento y la escala para los entornos de TI híbridos actuales.

# Introducción

Los equipos de seguridad aún sienten el impacto del cambio repentino al trabajo remoto. De acuerdo con la CIO Pandemic Business Impact Survey, los CEO están exigiendo experiencias de usuario mejoradas que se adapten a las extensas directivas de trabajo desde casa, a la vez que están solicitando a los CISO mejoras en la seguridad de TI para impulsar la resiliencia.

Entretanto, las amenazas evolucionan constantemente. Según el Informe de defensa digital de Microsoft, la sofisticación de los ataques sigue creciendo y a menudo se intensifica en tiempos de crisis.[1] El 2021 Phishing Benchmark Global Report de Terranova Security descubrió que el 19,8 % de los empleados estadounidenses hicieron clic en un vínculo de una simulación de phishing, y el 14,4 % del total de participantes descargó el documento de la página web de la simulación de phishing.[2] Al mismo tiempo, los centros de operaciones de seguridad (SOC) se ven abrumados por la cantidad de señales que tienen que analizar, incluidas muchas señales de baja fidelidad que son difíciles, si no imposibles, de detectar manualmente y mitigar. A medida que las amenazas aumentan, se hace difícil para los equipos de SOC sobrecargados mantenerse al día.




**de los empleados estadounidenses hicieron clic en un vínculo en una simulación de phishing.**

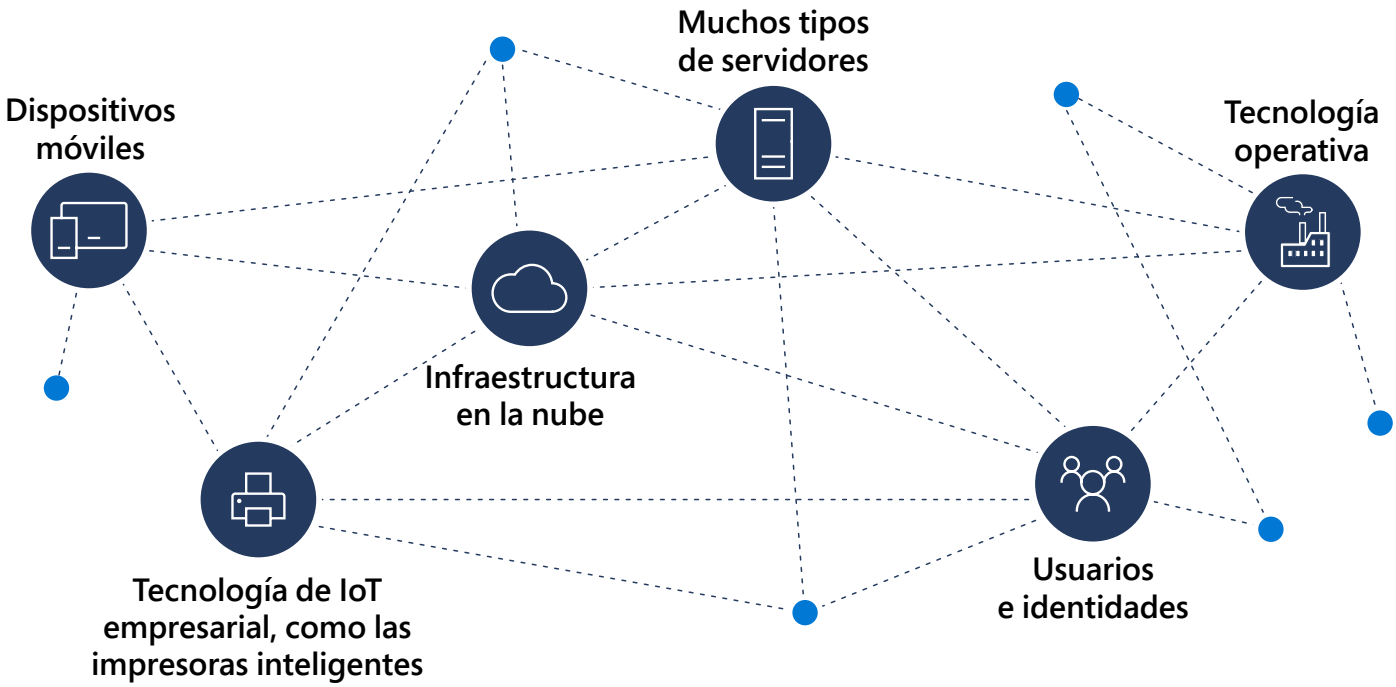

**del total de participantes descargó el documento en la página web de simulación de phishing.**

El mosaico de herramientas de seguridad de hoy proporciona focos de protección, pero hace que sea difícil integrar la amplitud de las señales de seguridad que abarcan la empresa. Como resultado, es difícil para los equipos de operaciones de seguridad obtener una visión de la cadena de ataque completa de toda la empresa, lo que explica por qué las filtraciones pueden tardar meses o más tiempo en descubrirse sin los controles de seguridad adecuados. Una vez que los atacantes están dentro y no se detectan, el daño puede escalar rápidamente. La asignación de más recursos para llenar las brechas no es la respuesta, ya que encontrar suficientes profesionales de seguridad calificados es un desafío constante. Esto deja debilitados a los equipos de seguridad.

[1] "Informe de defensa digital de Microsoft", 2021, Microsoft

[2] "Free Phishing Benchmarking Data to Train Your Cyber Heroes", 2021, Terranova.

## El patrimonio digital en expansión es difícil de administrar y proteger



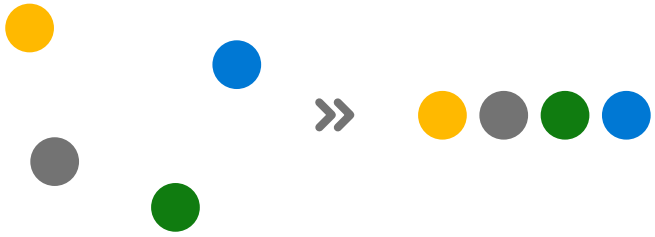

Si bien el alcance de los desafíos de seguridad de hoy a veces puede parecer abrumador, los CISO que buscan mejorar la eficiencia y eficacia de sus operaciones de seguridad tienen motivos para sentirse optimistas. La respuesta radica en un enfoque de la protección contra amenazas integrado de extremo a extremo que ayudará a los SOC a:

- ✓ **Detener los ataques antes de que se produzcan**, al reducir la superficie del ataque y eliminar las amenazas persistentes.
- ✓ **Detectar amenazas en todos los dominios**, al integrar los datos de las amenazas para respuestas rápidas y completas.
- ✓ **Liberar los recursos del equipo de seguridad**, con herramientas que puedan buscar, de manera proactiva, ataques sofisticados en todos los dominios.

Este enfoque se habilita mediante la integración de una solución de detección y respuesta extendida (XDR) con un sistema SIEM nativo de la nube que utiliza capacidades de inteligencia artificial (IA) y automatización que ayudarán al SOC a ser más predictivo, más proactivo y más preventivo frente a los ataques que afecten a toda la empresa.

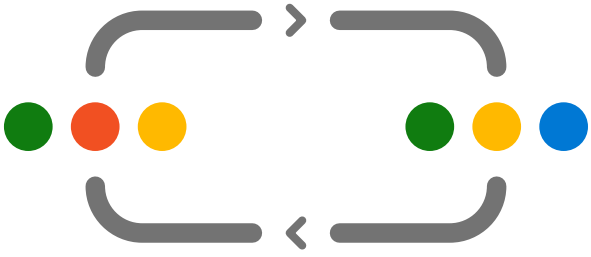
# El cambio a la protección contra amenazas integrada

**Un enfoque integrado puede ayudar a un SOC de tres maneras importantes:**



**Menor complejidad al consolidar las herramientas para ayudar a optimizar la seguridad, a la vez que se refuerza la postura de seguridad.**

**Detección y correlación automatizada de alertas y fragmentos de datos en incidentes administrables.**

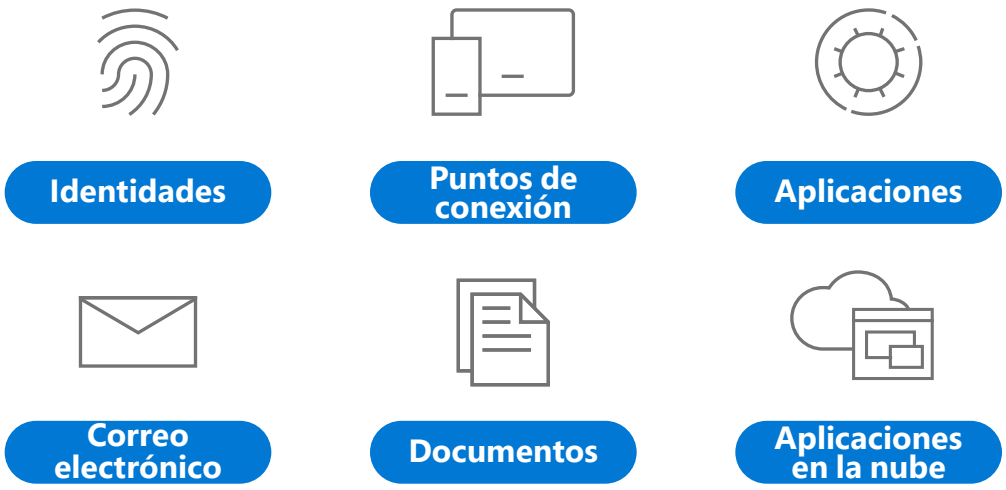


**Capacidades de “recuperación automática” que dan tiempo a los equipos de SOC para la búsqueda de amenazas.**

Un enfoque nativo de la nube para la protección contra amenazas proporciona el rendimiento, la escala y la visibilidad necesarios para abarcar todos los tipos de amenazas: a usuarios, aplicaciones, datos, dispositivos e infraestructura. Aplica capacidades de IA y automatización que ayudan a los equipos de SOC a priorizar las amenazas más importantes. El estudio 2021 Security Priorities de IDG encontró que los líderes de seguridad de TI planifican aumentar el gasto hacia la protección de datos en la nube (30 %), los controles de acceso (29 %), los servicios de ciberseguridad basados en la nube (28 %), y más, lo que indica claramente que la seguridad en la nube y los entornos conectados es lo más importante.[3]

La protección contra amenazas integrada es fundamental porque los malos actores no respetan los perímetros, estos explotarán cualquier vulnerabilidad que puedan encontrar en dispositivos, aplicaciones y usuarios. Cuando descubran o creen una oportunidad, la usarán como punto de partida para desplazarse lateralmente hasta que encuentren su objetivo, a menudo en forma de sistemas o datos confidenciales que pueden tomar como rehenes o exfiltrar.

## Los atacantes buscan vulnerabilidades en toda la organización




Por ejemplo, el actor de estado nación BISMUTH ha logrado pasar desapercibido en gran medida al aprovechar las alertas de prioridad baja provocadas por los mineros de criptomonedas.
Su objetivo: establecer supervisión y espionaje continuos para filtrar información útil.

[3]"IDG Security Priorities Study", 2021, IDG.

Este nivel de sofisticación y complejidad es tan asombroso como alarmante. Es por eso que resulta fundamental alinear SIEM y XDR para correlacionar alertas, priorizar las amenazas más grandes y coordinar la acción en toda la empresa. En última instancia, estas soluciones proporcionan eficiencia a SecOps y reducen el riesgo de que se produzcan costosas filtraciones de datos.

Por ejemplo, la integración de SIEM y XDR ofrece a los equipos de operaciones de seguridad de más contexto que nunca, gracias a las capacidades de IA integradas. Además, la automatización implementa y mejora de manera proactiva las técnicas de prevención, a la vez que permite a los equipos enfocarse en tareas más sofisticadas como la búsqueda de amenazas y la creación de herramientas personalizadas que reducen el tiempo de respuesta.

Considere, por ejemplo, que es posible que una señal de bajo nivel no capte mucha atención de un SIEM tradicional. Sin embargo, con el uso de la IA, un SIEM nativo puede comparar automáticamente esa señal con señales de otros orígenes en toda la organización,  correlacionando varios conjuntos de datos para descubrir ataques de varias etapas.

Luego, el sistema normaliza, analiza y correlaciona los datos, a la vez que se proporciona contexto sobre la manera en que el ataque ingresó a la infraestructura, junto con la cronología de su propagación. Esto permite a los equipos de SOC visualizar la vulneración, desde una sola consola, y abordarla con eficacia.

# Fortalecimiento de la postura de seguridad con protección contra amenazas integrada e inteligente

Las soluciones de protección contra amenazas de Microsoft ofrecen una seguridad integrada y completa con capacidades de automatización e IA incorporadas como parte de una pila completa de SIEM y XDR. Esta estrategia apoya a los equipos de SOC con la funcionalidad correcta para detener incluso los ataques entre dominios más sofisticados en aplicaciones de Microsoft, de terceros y personalizadas.

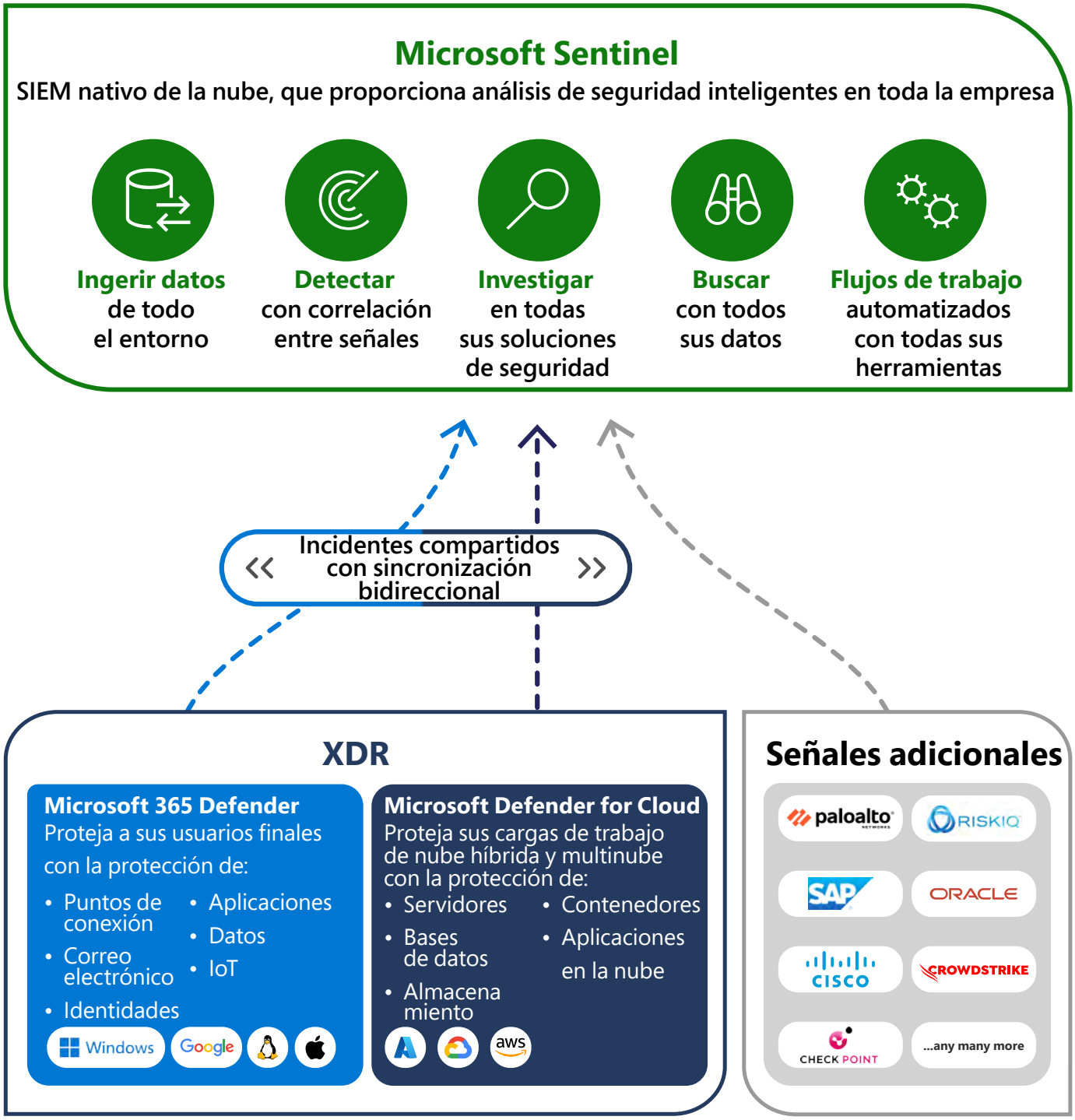
**Microsoft 365 Defender** aborda la seguridad local y del usuario final en el ecosistema de Microsoft 365 mediante la protección de identidades, puntos de conexión, correo electrónico y aplicaciones. Utiliza herramientas de inteligencia artificial para consolidar alertas y corregir ataques simples.

**Microsoft Defender for Cloud** protege los entornos de nube híbrida y multinube a través de bases de datos, máquinas virtuales, contenedores, almacenamiento y más. Encuentra puntos débiles en la configuración de su nube, ayuda a fortalecer la postura general de seguridad de su entorno y puede proteger las cargas de trabajo de las amenazas en evolución.


**Microsoft Sentinel** proporciona una experiencia integral de comando y control de SecOps en toda la empresa. Recopila e integra datos de amenazas de todos los recursos de seguridad de la empresa, incluidos firewalls y herramientas existentes, así como sistemas y plataformas de terceros. También ayuda a reducir el ruido de los eventos legítimos con machine learning integrado y conocimiento basado en el análisis de billones de señales diarias.

Con la integración de estos productos, los equipos SOC están equipados para afrontar los desafíos del trabajo híbrido, las señales abrumadoras y la prevención de infracciones.

# Adelántese a los atacantes con una experiencia de SecOps unificada



# Dé el próximo paso

El panorama de ataques, junto con la necesidad constante de un trabajo remoto seguro, requiere un enfoque moderno e integrado para la protección contra amenazas. La integración de extremo a extremo empodera a los defensores de su organización, al poner las herramientas e inteligencia adecuadas en manos de las personas correctas. Con las soluciones integradas de SIEM y XDR, los defensores están dotados de todo el contexto y la automatización que necesitan para detener incluso los ataques más sofisticados entre dominios.

Como paso siguiente, considere una evaluación para obtener una imagen completa de su postura de seguridad. Microsoft Secure Score ayuda a los CISO a entender el estado actual de su organización. Hace recomendaciones para mejorar la protección contra amenazas y establece indicadores claves de rendimiento para ayudar a las empresas a supervisar su progreso.

**Obtenga más información sobre la protección contra amenazas integrada con SIEM y XDR.**

Microsoft Security