Responder a sus necesidades de seguridad de TI actuales y futuras

Ciberseguridad con un enfoque por etapas

kaspersky

Crear una base de seguridad para su organización mediante la elección del producto o servicio adecuado es solo el primer paso. Desarrollar una estrategia de ciberseguridad corporativa con visión de futuro es clave para el éxito a largo plazo.

La cartera de Kaspersky para empresas refleja las demandas de seguridad de las empresas actuales, y responde a las necesidades de las organizaciones en distintos niveles de madurez con un enfoque por etapas. Este enfoque combina diferentes capas de protección contra todos los tipos de ciberamenazas para detectar los ataques más complejos, responder de manera rápida y adecuada a cualquier incidente y prevenir futuras amenazas.

Tipos de amenazas y qué experiencia se necesita para contrarrestarlas

A medida que los ambientes de TI aumentan en tamaño y complejidad, las empresas se enfrentan a amenazas cada vez más sofisticadas que las obligan a mejorar constantemente su experiencia en ciberseguridad para lograr una defensa eficaz.

Nuestra experiencia y la investigación continua de amenazas nos permiten dividir todas las amenazas disponibles en categorías. La mayoría de las amenazas está en la base de la pirámide. Estas son las amenazas genéricas para las cuales solo se requieren mecanismos defensivos básicos y seguridad de TI. Más arriba en la pirámide, se encuentran las amenazas más avanzadas que evaden la protección preventiva mediante el uso de tácticas, técnicas y procedimientos (TTP) conocidos. Los cibercriminales de esta categoría, por ejemplo, pueden conseguir y reutilizar las herramientas más sofisticadas que sus "colegas" con más recursos ya desarrollaron. La mayoría de las vulneraciones provienen de esta categoría. Por último, en la parte superior, están las amenazas complejas de tipo APT y los ataques que utilizan TTP desconocidos. Los cibercriminales de este nivel tienen recursos ilimitados para desarrollar herramientas y métodos altamente sofisticados con objetivos muy específicos en mente.

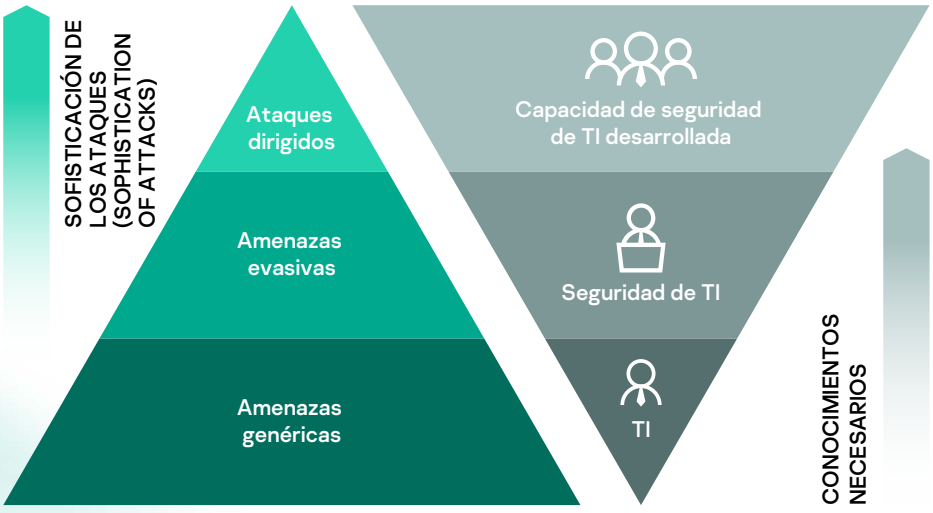

Figura 1. Tipos de amenazas y qué experiencia se necesita para contrarrestarlas

Para impulsar el crecimiento empresarial exitoso y mantener la competitividad, las empresas aumentan continuamente su confianza en las tecnologías de la información. La transformación digital continua amplía la superficie de ataque potencial a través de sistemas cada vez más interconectados. A medida que los ambientes de TI aumentan en tamaño y complejidad, las empresas se enfrentan a amenazas cada vez más sofisticadas que las obligan a mejorar constantemente su experiencia en ciberseguridad para lograr una defensa eficaz.

Ciberseguridad con un enfoque por etapas

Teniendo en cuenta el aumento de la cantidad y la complejidad de las amenazas, el nivel de madurez de la seguridad de TI, las habilidades en materia de ciberseguridad y los presupuestos existentes, existe una clara necesidad de empezar a desarrollar una estrategia de seguridad integral y adaptable.

En consonancia con las amenazas y el grado variable de las funcionalidades de ciberseguridad de nuestros clientes, empleamos una estrategia de lanzar nuestros productos y servicios al mercado a fin de ayudar a las organizaciones a prevenir el 90 % de las amenazas de forma automática y, luego, potenciarlas para agregar nuevas funcionalidades avanzadas de manera sistemática y metódica con el objetivo de contrarrestar las amenazas más sofisticadas a medida que su negocio crece.

En la etapa 1, proporcionamos todos nuestros productos preventivos líderes junto con soporte y servicios profesionales de primera calidad para garantizar que los clientes obtengan el máximo beneficio de nuestras tecnologías. En la etapa 2, a medida que uno asciende en la pirámide, aumenta la necesidad de contrarrestar las amenazas que eluden los mecanismos preventivos existentes. Para respaldar la protección de los recursos contra amenazas avanzadas y evasivas, ofrecemos una solución basada en la nube que complementa las habilidades básicas de ciberseguridad del cliente con detección administrada, priorización y respuesta guiada, junto con un conjunto de herramientas automatizado que ayuda al personal de seguridad a identificar y analizar las amenazas evasivas más peligrosas, y responder a ellas con mayor eficacia. Las organizaciones que se encuentran en el paso 3 tienen más posibilidades de enfrentarse a una APT real y necesitan una defensa eficaz contra los TTP desconocidos. Para satisfacer las necesidades de los equipos de seguridad de TI desarrollados, Kaspersky ofrece una combinación innovadora y equilibrada de tecnologías y servicios para abordar los desafíos de las amenazas y los ataques dirigidos más sofisticados de hoy en día.

La implementación rápida y lista para usar del producto permite una función de seguridad de TI madurada al instante sin necesidad de invertir en personal o experiencia adicionales Al mismo tiempo, permite que los procesos de evaluación de incidentes queden a cargo de Kaspersky para que los equipos de seguridad de TI desarrollados se centren en reaccionar a los resultados críticos obtenidos.

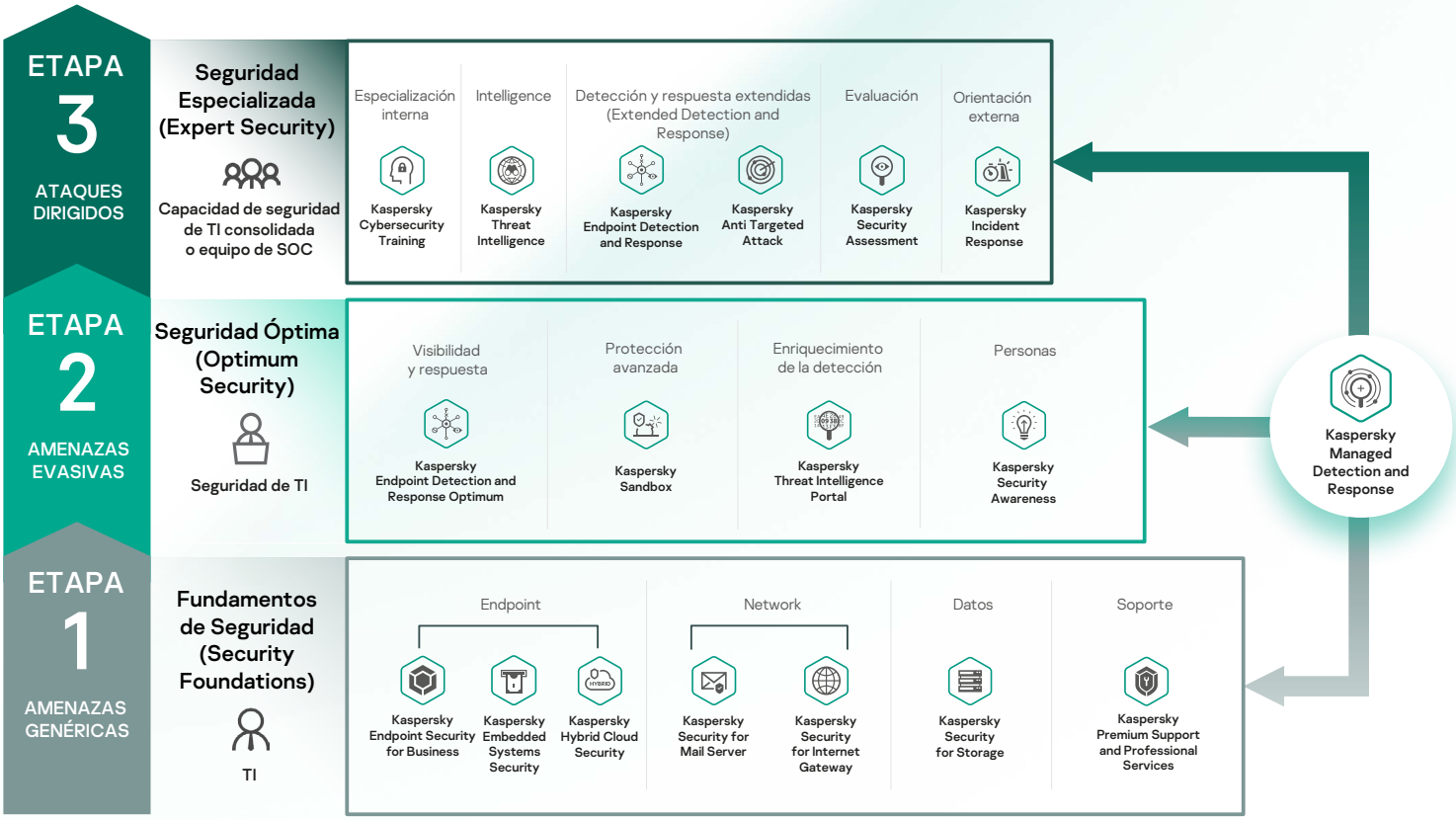

Figura 2. Ciberseguridad con un enfoque por etapas

Fundamentos de Seguridad (Security Foundations)

Bloquee la máxima cantidad de amenazas de forma automática.

La etapa fundamental para organizaciones de cualquier tamaño y complejidad de infraestructura para crear una estrategia de defensa integrada contra amenazas complejas Ofrece prevención automatizada de varios vectores de una gran cantidad de posibles incidentes causados por amenazas a las mercancías. Esta etapa suele ser suficiente para las empresas más pequeñas que solo cuentan con equipos de TI.

Las empresas no pueden saltarse esta etapa y pasar directamente a la implementación de tecnologías avanzadas de detección y respuesta. Esto se debe a que, para la mayoría de esas tecnologías, se necesita la participación de personas, lo que, por supuesto, es costoso y requiere experiencia. El costoso personal de seguridad de TI se ve abrumado por las alertas y la mayoría de las amenazas no se pueden prevenir. En lugar de buscar las amenazas ocultas y responder a los incidentes de manera proactiva, el personal de seguridad de TI pierde tiempo clasificando y priorizando miles de alertas, por lo que deja la mayoría de ellas sin atender.

Figura 3. Características clave de la etapa 1

Seguridad Óptima (Optimum Security)

Centrarse en la detección avanzada y brindar una respuesta rápida a las amenazas que evaden la protección preventiva.

Con el aumento del tamaño y la complejidad de los ambientes de TI que respaldan el desarrollo y el crecimiento empresariales, también crece la superficie de ataque potencial de las organizaciones. Se vuelven objetivos más atractivos para los cibercriminales y corren un mayor riesgo de enfrentarse a amenazas avanzadas que evaden los mecanismos automáticos de prevención.

Debido al aumento de la superficie de ataque potencial, no se puede subestimar la importancia de establecer prácticas básicas de respuesta a incidentes como mínimo. Por lo general, estas empresas comienzan a desarrollar una función de seguridad de TI dentro de su departamento de TI, pero su madurez sigue siendo baja. Los equipos de seguridad de TI pequeños necesitan instrumentos para la detección automatizada de amenazas avanzadas y una respuesta centralizada como base para continuar desarrollando esta función. La capacitación del personal también es esencial para generar conciencia sobre la seguridad en la organización y motivar a todos los empleados a prestar atención a las ciberamenazas y a aprender a manejarlas, incluso si esto no se considera como una parte específica de sus responsabilidades laborales.

A partir de las bases de seguridad, Optimum Security permite a las organizaciones con ambientes de TI más grandes y complejos contrarrestar las amenazas a las mercancías y las amenazas que eluden los mecanismos preventivos existentes. Una solución orientada a los recursos es ideal para pequeños equipos de seguridad de TI que tienen conocimientos básicos. Esta etapa permite a los clientes mejorar sus propias capacidades de detección y respuesta, además de beneficiarse de una protección administrada en todo momento. Al mismo tiempo, una cartera de productos de capacitación lúdica por computadora ayuda a moldear las habilidades de ciberseguridad de los empleados y los motiva a mantener prácticas seguras.

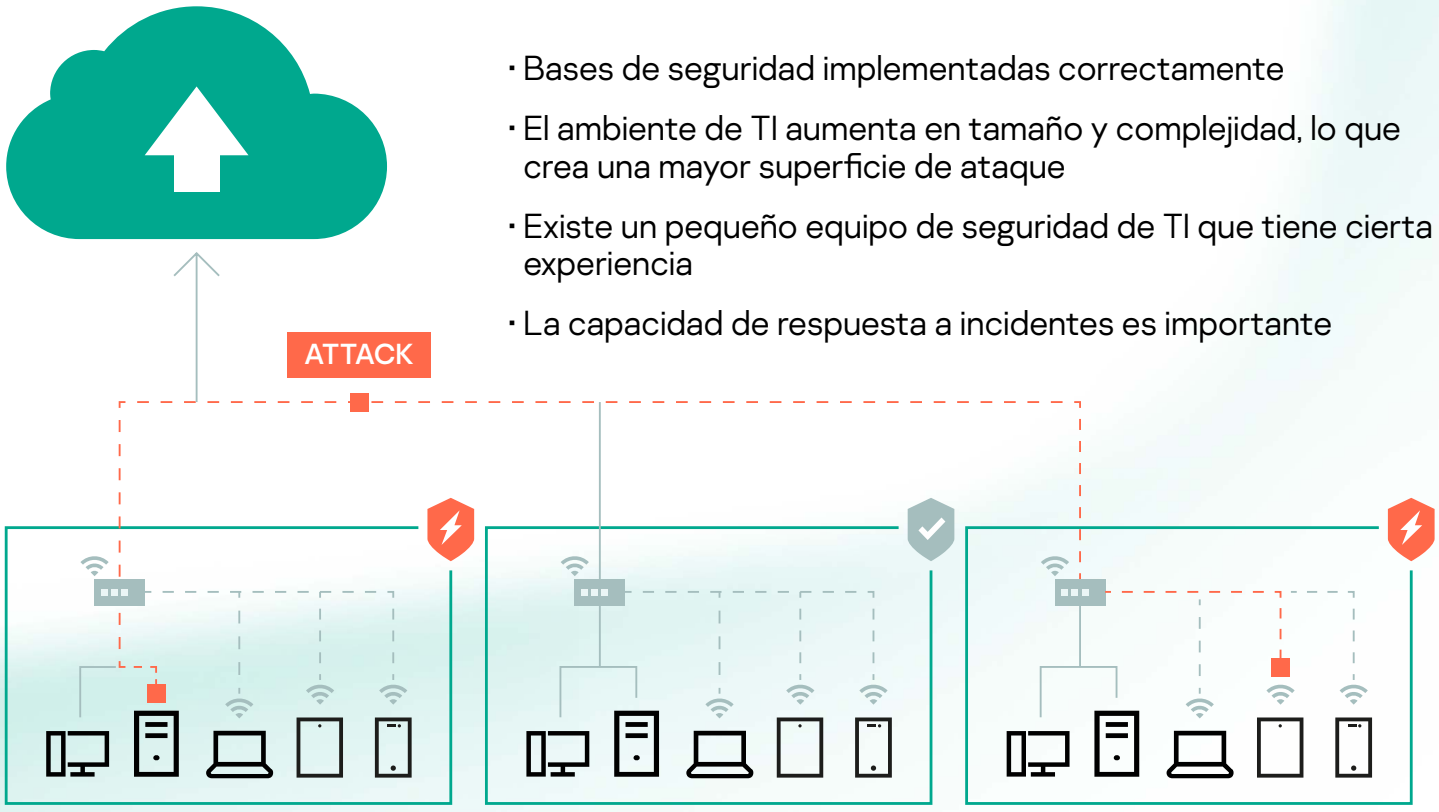

Figura 4. Características clave de la etapa 2

Seguridad especializada

Preparación para repeler ataques complejos y similares a APT

Adoptar prácticas manuales de búsqueda de amenazas y casos de uso avanzados de inteligencia de amenazas, y contar con un equipo completamente capacitado con conocimientos profundos en temas específicos, como análisis forense digital y de malware, será vital para las organizaciones en la etapa 3. Tendrán la ventaja de establecer relaciones de confianza con un socio altamente calificado para complementar rápidamente las capacidades existentes con conjuntos de habilidades más específicas cuando sea necesario. Kaspersky Expert Security ofrece una plataforma ampliada de detección y respuesta junto con orientación, evaluación, inteligencia de amenazas y capacitación en habilidades inigualables, que se combinan para satisfacer las necesidades de seguridad integrales de cualquier empresa, con una función de seguridad de TI desarrollada para enfrentar las amenazas complejas, los ataques dirigidos y los ataques tipo APT actuales.

- Los entornos de TI son complejos y están distribuidos.
- El equipo de seguridad de TI está desarrollado o se estableció un centro de operaciones de seguridad (SOC)
- El apetito de riesgo es bajo debido a los altos costos de los incidentes de seguridad y las filtraciones de datos.
- El cumplimiento de la normativa es una preocupación.

Figura 5. Características clave de la etapa 3

¿Por qué Kaspersky?

Nuestra misión es simple: construir un mundo más seguro. Creemos que la tecnología nos ayudará a construir un mañana mejor. Por eso que lo protegemos, para que cada quien, sin importar de dónde sea, tenga las infinitas oportunidades que nos brinda.

Somos una empresa global, con una visión global y un enfoque en los mercados internacionales. Realizamos negocios en 200 países y territorios, y tenemos 35 oficinas en 31 países. Nuestro equipo está formado por más de 4000 especialistas altamente calificados.

Siempre estamos innovando, para ofrecer protección eficaz, útil y accesible. La profunda inteligencia de amenazas y la experiencia en seguridad de Kaspersky Lab se transforman constantemente en soluciones y servicios de seguridad para proteger empresas, infraestructuras críticas, gobiernos y consumidores de todo el mundo. Nuestra completa cartera de seguridad ofrece soluciones y servicios líderes en protección, detección y respuesta para combatir amenazas digitales sofisticadas y en evolución. Las tecnologías de Kaspersky Lab protegen a más de 400 millones de usuarios y ayudan a 270 000 clientes corporativos a resguardar lo que más les importa.

latam.kaspersky.com