

STORMSHIELD

Cómo elegir una solución de Protección de Endpoint

Entre EDR e HIPS: ¿cúal es la mejor estrategia para bloquear de forma eficaz ciberataques sofisticados?

LIBRO BLANCO



Mientras el tema de la ciberseguridad sigue estando en el punto de mira, los ciberdelincuentes intentan pasar desapercibidos. Este objetivo les lleva a evolucionar constantemente sus técnicas de ataque. Y debido a que saben cómo funcionan las cosas, buscan desarrollar herramientas maliciosas para engañar a las soluciones de ciberseguridad presentes en las estaciones de trabajo de los empleados.

En la actualidad, las aplicaciones antivirus convencionales y otros sistemas de detección, especialmente los basados exclusivamente en firmas, parecen verse superados por técnicas complejas, como el secuestro de aplicaciones legítimas y la elevación de privilegios, así como por el malware sigiloso. Por lo tanto, las soluciones que se centran en la detección y prevención de los ataques conocidos están resultando insuficientes para hacer frente a esta nueva generación de ciberataques sofisticados y desconocidos.

Es fundamental que las organizaciones implementen ***soluciones que analicen con gran detalle el comportamiento de los procesos que se están ejecutando para identificar las posibles amenazas presentes en la máquina****. Por tanto, la solución elegida debe ser capaz de detectarlas y bloquearlas de forma proactiva, automática y en tiempo real para que la continuidad del negocio sea lo más fluida posible.*

Este libro blanco describe los distintos mecanismos que debe tener un sistema de protección para estaciones de trabajo y servidores para cumplir satisfactoriamente su función de detección de amenazas y protección de terminales*.*

Dirigido a los responsables de la seguridad de los sistemas de información, le proporcionará los elementos necesarios para apoyarle mejor en su toma de decisiones en función de sus necesidades.

Contenidos

1

Ciberataques: ¿cómo funcionan?

2

Soluciones de análisis de comportamiento

3

Detección y respuesta frente a amenazas en endpoint

¿Un ideal de seguridad?

4

Las distintas técnicas de protección HIPS

4.1 Enfoque basado en reglas

4.2 Enfoque contextual

4.3 Fortalecimiento

5

Stormshield Endpoint Security Evolution

La solución de protección para estaciones de trabajo

01

Ciberataques: ¿cómo funcionan?

Según la ANSSI, entre 2019 y 2020, el número de víctimas de ciberataques se ha multiplicado por cuatro. Tal y como indica un informe del Senado francés[2], los ciberdelincuentes se han aprovechado de ello, lo que se traduce en un aumento del 667% de los ataques de phishing registrados entre el 1 y el 23 de marzo de 2020.

Además, aunque la concienciación de los usuarios ha mejorado gradualmente, ningún sistema o infraestructura puede ser 100% seguro. Por ello, los ciberatacantes siempre encuentran nuevos trucos para penetrar en los sistemas de información de empresas de todos los tamaños de forma cada vez más dirigida.

91%

de los ataques dirigidos se llevan a cabo empleando spear phishing

Su objetivo: exfiltrar datos sensibles (médicos, bancarios, industriales, etc.), cifrarlos para pedir un rescate o publicarlos, o incluso dañar la productividad de la empresa objetivo (emplazamiento comercial, líneas de producción, etc.). Para ello, los ciberatacantes tratan de burlar los sistemas de seguridad existentes para acceder aprovechando, por ejemplo, las vulnerabilidades de los programas o dispositivos instalados.

Para entender mejor cómo funciona un ciberataque, nos centraremos en las tres fases más decisivas que permiten a un atacante alcanzar su objetivo final. La fase inicial consistirá en comprometer una máquina o servicio de usuario expuesto, proporcionando un acceso inicial sin privilegios al sistema. En la fase dos, el ciberatacante busca entonces penetrar en el sistema de información obteniendo acceso a una cuenta privilegiada o infectando otras máquinas. En la tercera fase, el atacante puede proceder al desencadenamiento de la acción maliciosa como tal: cifrado, exfiltración, etc.

Vamos a hablar de estas tres fases con más detalle.

[2] http://www.senat.fr/rap/r20-678/r20-678_mono.html

En primer lugar, los ciberdelincuentes hacen indagaciones para identificar a las víctimas dentro de la empresa objetivo. El atacante busca implementar vectores de ataque que pueden ser humanos y/o tecnológicos.

A nivel humano, el atacante utiliza técnicas de ingeniería social (LinkedIn, Facebook, etc.) para recopilar información que se utilizará para desviar la atención de la persona o personas que ha elegido para lanzar la infección principal.

FASE 1

DISCUBRIMIENTO E INFECCIÓN PRIMARIA



Intenta engañar al destinatario para que abra un archivo adjunto o haga clic en un enlace web malicioso. Una técnica conocida por su eficacia: el 91% de los ataques dirigidos[2] se realizan con este método de spear phishing.

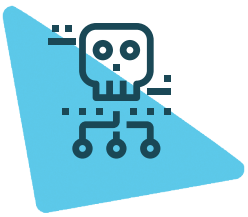
El descuido puede consistir, por ejemplo, en que el ciberatacante se haga pasar por un remitente (entidad financiera, proveedor, etc.) conocido por la persona objetivo.

En el plano tecnológico, el ciberdelincuente busca explotar los fallos del sistema de protección. Se aprovecha de los sistemas que no están debidamente protegidos, como los servidores RDP accesibles desde Internet. También puede intentar aprovechar los puntos débiles de las aplicaciones vulnerables y no actualizadas. Por ejemplo, el Centro Canadiense de Ciberseguridad[3] emitió una alerta en marzo de 2021 recomendando varias actualizaciones contra la explotación activa de vulnerabilidades relacionadas con Microsoft Exchange.

El objetivo: ejecutar un código malicioso para instalar un programa en la máquina objetivo que permita al ciberatacante infiltrarse en ella.

[2] http://www.itpronews.fr/3648/2012/12/spear-phishing-plus-de-90-des-attaques-ciblees.html

[3] https://cyber.gc.ca/en/alerts/active-exploitation-microsoft-exchange-vulnerabilities



FASE 2

MOVIMIENTO LATERAL Y EXPANSIÓN

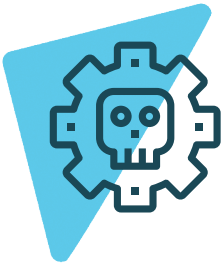
Una vez terminada la fase de infección primaria, el atacante intenta escanear la red para conocerla mejor. En esta fase de movimiento lateral, quiere penetrar más profundamente en el sistema de información para identificar las máquinas y las cuentas de usuario o de administrador que utilizará para alcanzar sus objetivos.

Por lo tanto, al principio navegará y pivotará por diferentes sistemas y cuentas. También puede instalar remotamente sus propias herramientas para intentar explotar las vulnerabilidades del sistema y extraer las credenciales de acceso.

El objetivo: penetrar profundamente en la infraestructura para encontrar las máquinas objetivo donde el ataque tendrá el mayor impacto.

A continuación, trata de penetrar profundamente en el sistema, lo que constituye la fase de expansión. A menudo se hace pasar por un usuario autorizado, lo que resulta muy difícil de detectar. Para ello, puede realizar una elevación de privilegios para hacerse pasar por un administrador local o hacerse con una cuenta de usuario que tenga acceso a un determinado software. También combina varios vectores de ataque en un intento de comprometer otras máquinas vulnerables.

Los enfoques más comunes consisten en explotar los puntos débiles, las malas configuraciones de la infraestructura o las vulnerabilidades existentes. Por ejemplo, una mala segmentación dentro de la red de la empresa que permita el acceso a las máquinas que le interesan, por ejemplo, un servidor con datos sensibles.



FASE 3

IMPACTO

Esta tercera fase es la culminación del ataque, donde el ciberdelincuente realiza acciones acordes con su objetivo. Si el ciberataque se activa, puede permitir la **exfiltración/robo de datos, la modificación de procesos operativos o al apagado de un servidor vital** para el buen funcionamiento de la organización.

En esta fase, el atacante también puede procurar mantenerse sigiloso para volver a explotar la máquina más adelante o lanzar un ataque (más o menos virulento) como el que sufrió TV5 Monde[4] en 2015.

Cabe señalar que, en algunos casos, se encargan de eliminar las distintas copias de seguridad y los rastros de actividad maliciosa.

El objetivo: socavar la infraestructura para bloquear un elemento necesario para la producción de la empresa. También, exfiltrar datos para revenderlos y/o publicarlos (como los datos sanitarios en la dark web) o cifrarlos para obtener un rescate de la organización objetivo.

[4] https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html

02

Soluciones de análisis de comportamiento

En particular, los ciberdelincuentes utilizan técnicas de ataque para pasar desapercibidos y evitar la detección de sus códigos maliciosos por las distintas soluciones de seguridad. Por lo tanto, l**a detección de comportamientos sospechosos y la suspensión preventiva de actividades potencialmente peligrosas son esenciales**.

Por ello, el sistema de prevención de intrusiones en host (HIPS) ayuda a proteger las estaciones de trabajo y los servidores contra el malware, bloqueando las actividades sospechosas que puedan afectar a los sistemas de la infraestructura.

"Algunos sistemas de prevención de intrusiones permiten a los usuarios enviar registros de actividad maliciosa y fragmentos de código sospechosos directamente al proveedor para su análisis y posible identificación."

Stephen J. Bigelow

Editor senior de tecnología

Fuente: Techtarget

A continuación, analizaremos los principales aspectos de los diferentes tipos de HIPS para satisfacer mejor las necesidades de cada organización.

HIPS **basado en firmas**

Se basan en el **conocimiento de las vulnerabilidades de una aplicación y de las amenazas conocidas** y bloquean su uso. Funcionan con una base de datos que debe ser actualizada regularmente.

Identifican los ataques conocidos. Sin embargo, **no pueden detectar** ataques desconocidos o de día cero. **No se adaptan bien a las situaciones en las que la estación de trabajo debe estar desconectada** de su servidor de actualización.

Hay **pocas opciones** en el software.

HIPS **con análisis de comportamiento**

Bloqueo en **tiempo real de ataques conocidos y de día cero**: detección de actividades sospechosas en aplicaciones y procesos legítimos sin necesidad de utilizar bases de datos de firmas o de anomalías en las aplicaciones.

Algunos HIPS combinan métodos de **análisis de comportamiento y heurísticos, la protección de la memoria o el fortalecimiento del sistema operativo** (SO) para ofrecer una mejor protección frente a las amenazas.

Alto nivel de parametrización de listas o reglas y filtros para adaptarse a las diferentes organizaciones.

"Una solución HIPS de análisis de comportamiento reconoce y bloquea las técnicas de ataque comunes y **sofisticadas**, *como la explotación de las vulnerabilidades de las aplicaciones, para garantizar una protección eficaz de la estación de trabajo del usuario."*

Edouard Simpère

Responsable de la división de seguridad de Stormshield

Omnipresentes en el léxico del mundo de la ciberseguridad en los últimos años, las aplicaciones EDR o detección y respuesta frente a amenazas en endpoint[5] son programas informáticos capaces de detectar y bloquear las amenazas conocidas y desconocidas sin esperar parches o actualizaciones. Suelen ser agentes desplegados en los distintos puntos finales de una red, especialmente en las estaciones de trabajo, los teléfonos móviles o los distintos servidores de la infraestructura.

Una característica general de los EDR es que realizan una **supervisión continua de los puntos finales**. Además, algunas soluciones incorporan componentes EPP para proporcionar protección en tiempo real. Esto proporciona una primera barrera de protección eficaz contra la mayoría de las amenazas conocidas y algunas desconocidas.

Detección y respuesta frente a amenazas en endpoint: ¿El ideal de seguridad?

Como subraya la ANSSI[6] , estas soluciones, que gestionan una gran cantidad de datos, ofrecen generalmente capacidades de **detección** (comportamiento sospechoso de aplicaciones legítimas, *ataques sin archivos*[7]), **investigación** (visualización completa del ataque detectado) y **reparación** (restauración de archivos, etc.).

De este modo, los EDR complementan hoy en día las soluciones tradicionales basadas principalmente en firmas. Proporcionan una visibilidad global y generalmente detectan comportamientos anormales en procesos legítimos. Tras esta detección, la solución implementa una respuesta para interrumpir el ataque deteniendo el proceso malicioso. De forma más o menos automatizada, permite informar al administrador. Entonces, o bien aplica una respuesta, o bien el EDR es capaz de proporcionarla automáticamente y casi en tiempo real (esto dependerá de la solución utilizada). De este modo, el ransomware y los ataques polimórficos pueden detectarse y bloquearse con estas herramientas.

[5] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[6] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[7] https://www.riskinsight-wavestone.com/2018/10/fileless-attack-le-retour-a-la-terre/

En el aspecto de gestión, pueden integrarse en el SIEM de la organización para proporcionar los registros de log necesarios que ayuden a los analistas del SOC a optimizar la eficacia en la búsqueda de ataques.

Además, la mayoría de las soluciones EDR del mercado optan hoy en día por un enfoque "*cloud-only*" o "*cloud-first* "[8] para centralizar la recogida de datos y analizar las señales precursoras o de compromiso que indican un ataque. En efecto, la nube se presta a esta recopilación y análisis masivos de grandes cantidades de datos que hay que procesar.

Sin embargo, en determinados casos de uso, no se puede contemplar esta posibilidad debido a la sensibilidad de los datos a procesar. Por ello, **el modo local puede ser una opción eficaz en un entorno sensible** (defensa, ministerios, industria, etc.). Además, es importante distinguir entre el nivel de protección establecido por el servidor o por el cliente instalado en la estación de trabajo.

Veremos las principales diferencias entre ambos enfoques:

Protección centrada **en el servidor**

En este enfoque, el agente ligero instalado en la estación de trabajo **envía toda la información al servidor**. No dispone de amplias funcionalidades.

El servidor, ya sea local o en la nube, analiza los registros de log enviados por el agente en busca de comportamientos maliciosos, anomalías presentes en un determinado puesto de trabajo, etc.

El agente ligero necesita una c**onexión permanente para retroalimentar la información**. Puede haber cierta latencia en la respuesta obtenida.

Protección centrada **en el agente**

El agente en la estación de trabajo es **autónomo para tomar decisiones** y proteger la estación de trabajo sin necesidad de acceder a su servidor.

El servidor tiene menos visibilidad global debido a las **capacidades ampliadas del agente** para gestionar la máquina contra el malware.

El agente puede trabajar de **forma independiente bloqueando** comportamientos maliciosos en **tiempo real.**

Por lo tanto, para garantizar la mejor protección en todo momento, **se debe dar preferencia a las soluciones que pueden detectar el malware sin necesidad de una conexión de red para garantizar una protección fiable y en tiempo real de la estación de trabajo**.

[8] https://www.pcpresse.com/wp-content/uploads/2020/10/LINFO-CR01_MD.pdf

04 Las distintas técnicas de protección HIPS

Los ciberdelincuentes son conscientes de que sus ataques no deben llamar la atención para pasar desapercibidos (fase 2: movimiento lateral y expansión). Para ello, se esfuerzan constantemente en desarrollar nuevas habilidades desplegando nuevas tácticas y técnicas de ataque con el fin de eludir las protecciones tradicionales.

Vamos a hablar de las principales técnicas utilizadas y de cómo el atacante las utilizará para intentar frustrar las distintas protecciones de seguridad.

255%

Esta cifra se corresponde con el aumento de las denuncias de ransomware en 2020, según un estudio de la ANSSI

En la tabla siguiente, hemos observado diferentes técnicas de ataque en las tres fases de un ciberataque. Como recordatorio, en la tercera fase, el atacante ya ha tomado el control y comienza la fase de impacto, como la exfiltración o el robo de datos. Hay que tener en cuenta que estas extracciones suelen ser complicadas de detectar porque los atacantes utilizan herramientas e identificadores *a priori* legítimos.

Fase	Técnicas	¿Cómo lo utiliza el atacante?	Impacto
Fase 1: Descubrimiento e infección primaria	Desbordamiento de búfer. Ejemplo: - Stack Pivot	El atacante utiliza un desbordamiento de búfer proporcionando datos de entrada mal formateados para hacer que la aplicación objetivo escriba datos en la memoria más allá del límite normal. Esto sobrescribe los datos correctos y permite al atacante tomar el control del flujo de ejecución de la aplicación.	El código que el atacante ha insertado en la aplicación objetivo le permite obtener acceso remoto y/o descargar y ejecutar otros archivos maliciosos (carga útil).
Fase 1: Descubrimiento e infección primaria	Empaquetado de malware	Esta técnica consiste en impedir el análisis del archivo malicioso por parte de las soluciones de seguridad mediante la carga dinámica de todas las funciones.	Los empaquetadores dificultan la identificación del malware por parte de los departamentos de seguridad y aumentan el tiempo de análisis. Además, empaquetar un archivo permite eludir las soluciones basadas en firmas.
Fase 1: Descubrimiento e infección primaria	Vaciado de procesos. Ejemplos: - RunPE - Doppelgänging	El principio es hacer que el sistema ejecute código malicioso camuflándolo bajo la identidad de un proceso legítimo. Por un lado, la técnica RunPE abusa de las debilidades del sistema de carga de código ejecutable. Por otro lado, la técnica Doppelgänging utiliza el mecanismo de transacciones NTFS.	El vaciado de procesos permite al atacante evitar la detección de las soluciones de seguridad que generalmente ignoran los procesos legítimos del sistema por los que se hace pasar.
Fase 2: Movimiento lateral y expansión	Elevación de privilegios Ejemplos: - Secuestro de DLL - Manipulación de tokens de acceso	El atacante intenta obtener acceso de más alto nivel a una estación de trabajo o sistema para lograr sus objetivos. Por un lado, para la técnica de secuestro de DLL, el atacante manipula una aplicación con privilegios elevados haciendo que cargue una DLL maliciosa. Por otro lado, la manipulación de tokens de acceso. El atacante puede robar o duplicar los tokens de acceso para modificar el contexto de ejecución de la aplicación objetivo, permitiéndole concederse permisos adicionales.	Después de obtener privilegios avanzados (permisos de administrador o de sistema), el atacante se vuelve difícil de detener porque tiene una fuerte huella en la máquina objetivo. Estos derechos avanzados facilitan el movimiento lateral del ataque. Esto puede ser posible en algunos casos sin privilegios avanzados.
Fase 2: Movimiento lateral y expansión	Pasar el hash	El atacante roba un hash utilizado para identificar una cuenta más privilegiada potencialmente utilizada para conectarse a otras máquinas.	Esta técnica permite al atacante autenticarse en otros ordenadores utilizando esta identidad robada. El objetivo es infectar nuevas máquinas.
Fase 2: Movimiento lateral y expansión	Descubrimiento de la red desde la línea de comandos	El atacante utiliza comandos (como netdiscover) para detectar estaciones de trabajo en la misma red.	El atacante puede tener una visión completa de las diferentes redes existentes.
Fase 3: Impacto	Cifrado de datos	El atacante cifra los datos almacenados en las máquinas (estaciones de trabajo y servidores) para hacerlos inaccesibles a la víctima. Generalmente utiliza técnicas criptográficas legítimas relacionadas con las API de Windows.	Esta técnica se utiliza en los ataques de ransomware en los que el ciberdelincuente exige un rescate para recuperar los datos.

4.1

El enfoque basado en reglas: un método eficaz

Hay una serie de soluciones que utilizan reglas para realizar la detección en las estaciones de trabajo. Sin embargo, en algunos casos los administradores no pueden acceder a ellas. Es cierto que la implementación de estas reglas es bastante sencilla, pero no pueden adaptarse a diferentes usos para el negocio con entornos de seguridad específicos.

En otras soluciones, sin embargo, es posible encontrar un cierto nivel de parametrización para que se adapte mejor a las organizaciones donde se despliega la solución. Así, además de las reglas proporcionadas por el proveedor de seguridad, el usuario puede incluir reglas en función del cargo, la empresa, etc.

Algunos sistemas HIPS combinan varias técnicas de protección en forma de parámetros o reglas que forman lo que se denomina "política de seguridad de la solución". Esto permite al administrador adaptarla en función del proceso de negocio que se desea proteger. En algunas soluciones, los distintos parámetros o reglas pueden personalizarse, lo que ofrece una mejor adaptación y protección para la organización.

¿Sabía que?

Las reglas de comportamiento aplicadas en el lado del agente ofrecen una protección inmediata de la estación de trabajo para limitar el impacto de un ataque

La granularidad de las soluciones de protección empleadas

Algunas soluciones ofrecen listas de reglas predefinidas que pueden ser ampliadas por el administrador para neutralizar el malware.

Como hemos visto anteriormente, hay que dar preferencia a las soluciones HIPS que ofrecen conjuntos de **reglas configurables y muy granulares para controlar cualquier acción realizada en las estaciones de trabajo**, como la supervisión de los procesos en ejecución, los archivos y las claves del registro, la elevación de privilegios, etc.

Esta granularidad permite a los administradores de la organización un alto grado de personalización y, en general, la posibilidad de implementar una política de seguridad lo más cercana posible a las necesidades y requisitos de la organización.

Como norma general, una estación de trabajo o servidor debe considerarse en función de su contexto (por ejemplo, fuera o dentro de la red de la empresa) y de su nivel de exposición a las amenazas.

4.2 El enfoque contextual: cómo entender mejor el entorno

Como cada organización tiene una configuración única con necesidades específicas, la solución de protección debe ser capaz de adaptarse a los diferentes casos de uso dentro de la organización. En consecuencia, la protección de las estaciones de de trabajo y servidores elegida **debe adaptarse al contexto de uso de cada persona y tener en cuenta los diferentes escenarios de movilidad**. Por ejemplo, para controlar qué redes Wi-Fi están permitidas y desactivarlas cuando una conexión LAN está activa. O para bloquear cualquier conexión que no sea la VPN cuando esté activa para evitar los *bounce attacks*.

Por lo tanto, la implementación y el uso de una solución de protección de estaciones de trabajo debe tener una política de seguridad que sea capaz de ser dinámica. Es decir, debe **saber dónde se encuentra el puesto en cuestión y adaptar su seguridad al entorno concreto**.

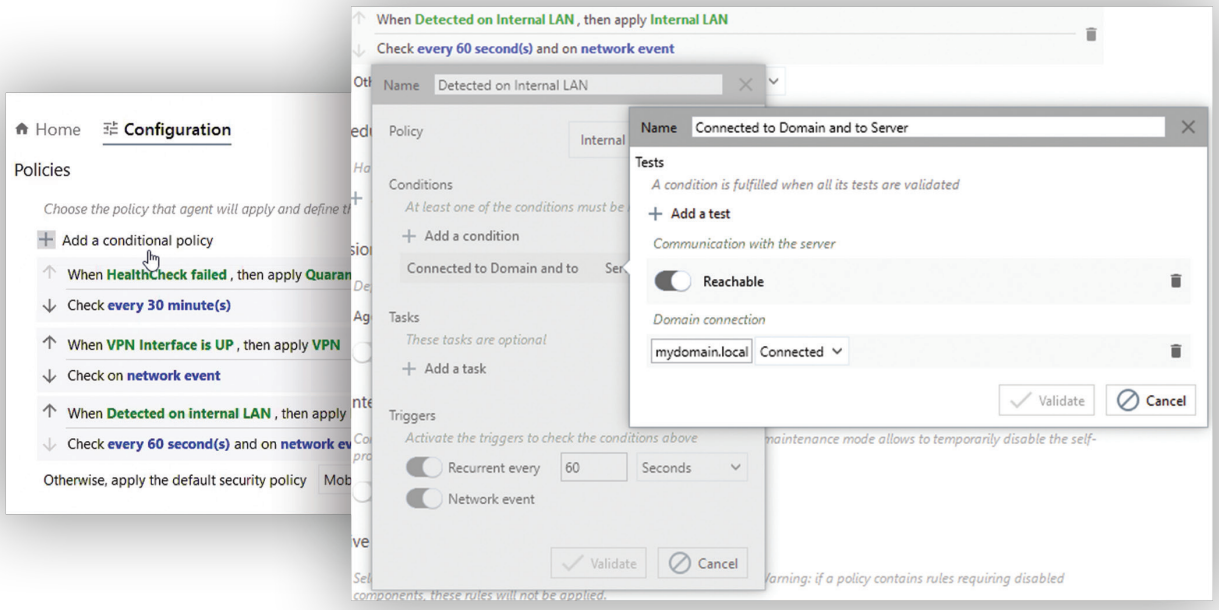


Figura 1

Solución para la seguridad del Endpoint con distintas políticas de seguridad

4.3
"Fortalecimiento" para la protección del propio sistema

Las soluciones de seguridad son un objetivo de ataque para los ciberdelincuentes. Estos buscan desactivar la protección o aprovechar los derechos privilegiados de estas soluciones haciendo un mal uso de las mismas. Por otra parte, como señala la ANSSI[9], hay que comprobar el software (y el hardware) de una infraestructura y fortalecer su configuración antes de utilizarla.

Además, hay que tener en cuenta la superficie de ataque. Los expertos coinciden en que cada nuevo componente (hardware y software) que se añade a la infraestructura aumenta el riesgo de que haya un error o una vulnerabilidad relacionada con ese componente, que permita ser explotado por un ciberatacante.

Para limitar la superficie de ataque y reforzar la protección de las estaciones de trabajo, algunas soluciones de protección de estaciones de trabajo integran en su desarrollo el *enfoque de seguridad por diseño*[10]. Es decir, soluciones en las que la seguridad y los riesgos asociados se integran y estudian desde la fase de diseño del producto.

Ciberataque en Mitsubishi Electric[11]

El fabricante de automóviles japonés ha reconocido que sufrió un ciberataque en junio de 2019. Según una investigación realizada durante varios meses, los atacantes accedieron a la red interna de la empresa y robaron 200 MB de archivos sensibles de miles de empleados e información técnica confidencial.

¿Cómo tuvo lugar?

Un grupo de ciberdelincuentes con sede en China habría explotado una vulnerabilidad de día 0 en el software antivirus de la organización para instalar archivos maliciosos. Según el fabricante del software hackeado, los delincuentes aprovecharon una vulnerabilidad de salto de directorio para extraer archivos de un archivo zip arbitrario a una carpeta específica del servidor del antivirus. Esto aparentemente causó la *ejecución remota de código*.

9 https://www.ssi.gouv.fr/uploads/2020/08/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.1.pdf

10 https://www.securecontrolsframework.com/security-privacy-design-principles

11 https://www.zdnet.fr/actualites/une-faille-0day-de-l-antivirus-trend-micro-utilisee-dans-le-piratage-de-mitsubishi-electric-39898077.htm

Para ello, la arquitectura general de este tipo de soluciones debe desarrollarse según las reglas de programación defensiva de software en torno a una arquitectura de microservicios segura. Aquí es precisamente donde se aplica el principio del mínimo privilegio.

Esto permite dividir la solución en **varios servicios independientes** que garanticen la máxima seguridad, cada uno con un papel específico y privilegios limitados. Así, por ejemplo, el módulo que gestiona la conexión con el servidor de configuración no debe ser el encargado de interpretar estos datos. O el servicio que gestiona los registros de log se encarga exclusivamente de esta tarea y no puede acceder a la política establecida de seguridad para los ciberdelincuentes.



Figura 2
Solución de seguridad dividida en varios servicios independientes

Para lograr un alto nivel de robustez, los procesos de construcción de software de seguridad también deben definir reglas de codificación estrictas y prever el uso de diversas opciones de compilación y ejecución. Estas opciones permiten limitar el riesgo de explotación en caso de errores y también limitar el número de errores aumentando las comprobaciones antes y durante la ejecución.

En resumen, las **soluciones fortalecidas o robustas basadas en estos principios proporcionan una mejor protección contra los ciberataques**.

Stormshield Endpoint Security Evolution: la solución de protección de estaciones de trabajo

Stormshield Endpoint Security Evolution **protege entornos sensibles** bloqueando ataques en su etapa más temprana, antes de que impacten en sus infraestructuras



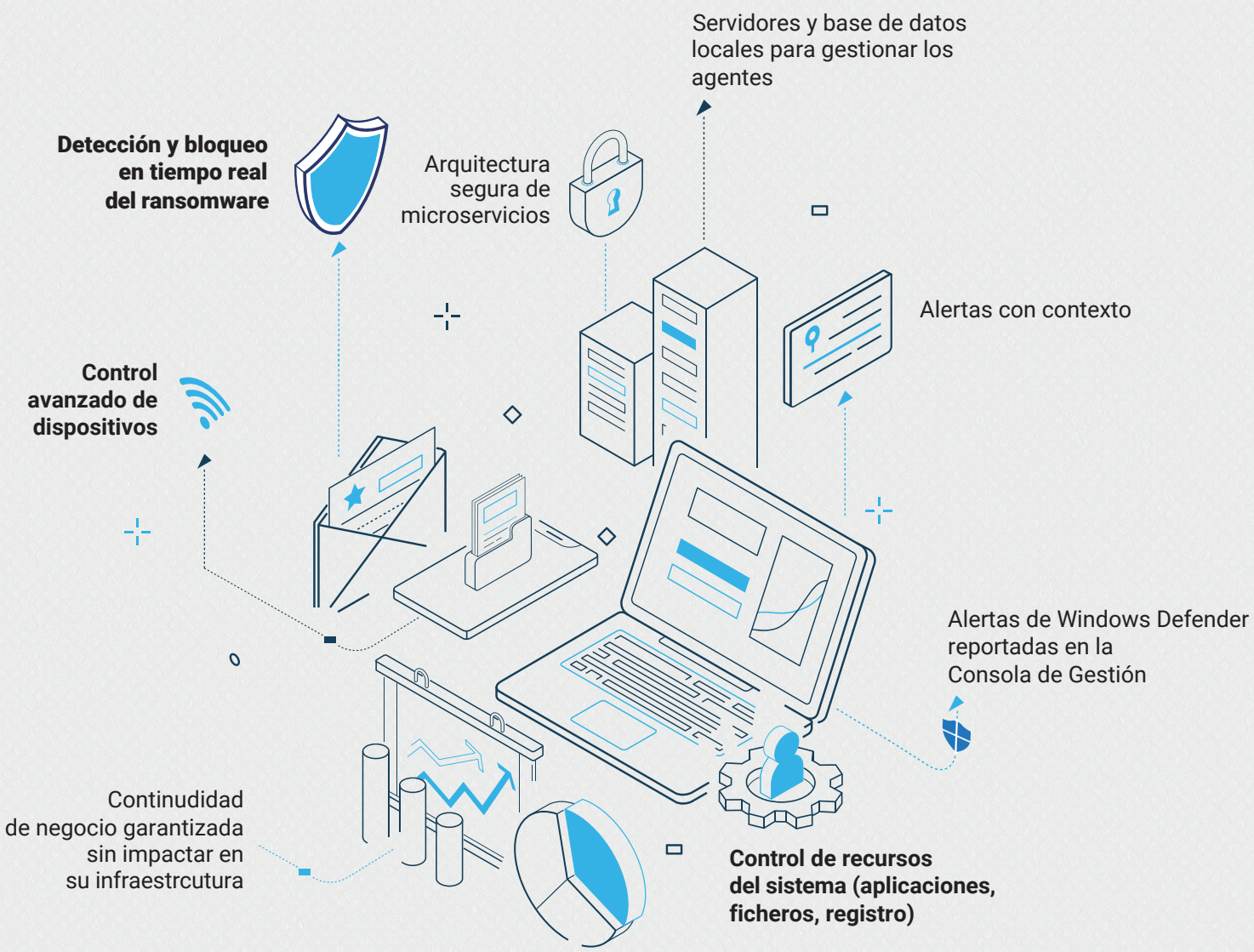
Análisis avanzado de comportamiento capaz de bloquear amenazas desconocidas, ataques de día cero y ataques sin archivos.



Solución autónoma que no requiere conexión de red para funcionar y mantener la seguridad del endpoint.



Control avanzado de dispositvos. Amplia gama de control de dispositivos: comprobación de redes Wi-Fi y llaves USB, accesos a volúmenes de disco o conexiones de red.



El

91%

de los ataques dirigidos se llevan a cabo empleando spear phishing

El

40%

de las infecciones primarias usan la técnica de vaciado de procesos

El

255%

de incremento en los casos de ransomware (segùn un estudio de la ANSSI)

ALGUNOS EJEMPLOS DE ATAQUES

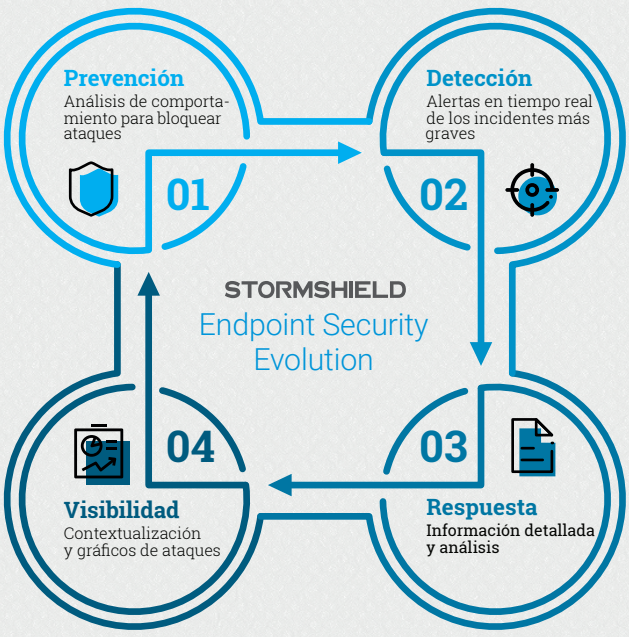
- GUSANO DE ORDENADOR
- MALWARE DE CORREO ELECTRÓNICO
- DISPOSITIVOS INFECTADOS
- ROBO DE CONTRASEÑAS
- ESCANEO DEL SISTEMA
- ATAQUE SIN FICHEROS
- PHISHING
- HACKER
- TROYANO
- PÉRDIDA DE DATOS
- VULNERABILIDADES DEL SOFTWARE
- ...

ALGUNOS CONSEJOS ESENCIALES

Tenga cudidado con los correos con adjuntos o sitios web dudosos.

Haga copias de seguridad con **regularidad**

Actualice sus aplicaciones, complementros y sistemas operativos.



LA **OPCIÓN EUROPEA DE CIBERSEGURIDAD**

www.stormshield.com

Queda prohibida toda distribución, reproducción o representación, incluso parcial, de este libro blanco, para cualquier fin que no sea el uso privado, independientemente del soporte, y puede comprometer la responsabilidad civil y penal de cualquier persona que incumpla esta prohibición.

Copyright © 2022 Stormshield