6 REQUERIMIENTOS DE SEGURIDAD:
PARA UNA ESTRATEGIA DE PROTECCIÓN EFECTIVA

El AntiVirus tradicional (AV) ha sido la solución por defecto para proteger los Endpoints por décadas. Mientras los AV revisan todos los puntos para auditorías de regulación y cumplimiento proporciona muy poco beneficio a las organizaciones:

A pesar de que las soluciones de Antivirus o Antimalware protegen casi todos los Endpoints y servidores en el mundo, la cantidad de brechas de seguridad que ocurre día a día son alarmantes. Esto se debe en gran parte al hecho de que el AV tradicional es una solución de seguridad reactiva que se centra en detectar y reaccionar a las amenazas conocidas.
Si bien es cierto, los atacantes experimentados son capaces de brincar los Antivirus con herramientas automatizadas en internet que producen innumerables variantes de ataques. En otras palabras, el Antivirus tradicional está resultando inadecuado para proteger los sistemas contra las brechas de seguridad que los atacantes están aprovechando muy bien.

Ante el panorama de amenazas actual una organización debe protegerse contra amenazas cibernéticas conocidas y desconocidas, así como de las fallas de los AV tradicionales, a fin de prevenir y reducir brechas de seguridad. Para lograr esto, debe haber un enfoque en prevención. La prevención es la única manera efectiva, escalable y sostenible para reducir la frecuencia y el impacto de las incidencias de seguridad. Entonces, **¿Qué debería hacer una solución integral de seguridad para tu Endpoint?**

Las secciones siguientes analizan los seis requisitos para una solución completa que proteja los sistemas, usuarios y endpoints contra amenazas conocidas y desconocidas.

TU SOLUCIÓN INTEGRAL DE SEGURIDAD PARA ENDPOINT DEBERÍA . . .

1 Prevenir las brechas de seguridad de los equipos Endpoint al bloquear preventivamente las amenazas conocidas y desconocidas.

Debe haber un cambio al detectar y responder a los incidentes después de que los activos críticos ya han sido comprometidos, esto con el fin de prevenir las brechas de seguridad.
Los endpoints deben estar protegidos contra las amenazas conocidas, desconocidas y los ataques de día cero que llegan a través de malware y exploits, en este sentido no importa si la máquina está conectada a internet o no, o si está conectado a la red de la organización o no.

2 Proteger y permitir que los usuarios realicen actividades diarias sin temor a las amenazas de seguridad.

Una solución de seguridad avanzada para endpoint debe permitir a los usuarios finales llevar a cabo sus actividades diarias sin ningún tipo de pánico, deben ser capaces de utilizar sus aplicaciones móviles y en la nube sin el temor de amenazas desconocidas.
Deben tener la confianza de que están protegidos contra malware o exploits que inadvertidamente se ejecuten y comprometan su sistema.

3 Convertir automáticamente la inteligencia de amenazas en prevención.

La experiencia adquirida sobre amenazas a través de ataques nuevos y únicos, así como la inteligencia de proveedores de servicios de terceros y sitios públicos de inteligencia compartida, debe permitir que los agentes de endpoint se prevengan instantáneamente contra malware conocido, así mismo identifiquen y bloqueen malware desconocido antes de que el equipo sea infectado.

4 Proporcionar protección completa para todas las aplicaciones.

Las aplicaciones son el centro de cualquier organización para que ésta funcione eficazmente. Desafortunadamente, los errores y fallas en las aplicaciones proporcionan a los cibercriminales una gran superficie de ataque en la cual el AV tradicional no logra cumplir con su función de protección.

La infraestructura de seguridad de una organización debe ser capaz de proteger todas las aplicaciones contra vulnerabilidades, incluidas las aplicaciones de terceros y las aplicaciones propietarias.

5 Proporcionar una solución ligera y escalable.

La prevención de las brechas de seguridad nunca debe poner en peligro la productividad de los usuarios. Las soluciones de protección endpoint, y cualquier solución de seguridad para este propósito debería ser escalable, ligera y fácil de usar sin demandar recursos significativos del sistema que invariablemente degradaran la experiencia del usuario y su productividad.

6 Ofrecer soporte para sistemas que no cuentan con parches disponibles.

Las organizaciones podrían optar por no implementar las actualizaciones de sistema y los parches de seguridad inmediatamente, ya sea porque podría interferir con las capacidades operativas críticas, disminuir su operación o peor aún eliminar algo vital para que la organización continúe con su operación.

O bien porque los parches podrían no estar disponibles para sistemas antiguos, o para aquellos que han llegado al final de su vida útil (EoL). Una plataforma endpoint completa debe impedir que se exploten las vulnerabilidades del software, ya sean conocidas o desconocidas, esto independientemente de la disponibilidad o la aplicación de parches de seguridad.

Las empresas de hoy en día deben centrarse en una estrategia de seguridad integral que no solo se enfoque en implementar un antivirus tradicional para la protección a nivel endpoint sino que deben combinar las herramientas, tecnologías y tácticas que brinden un nivel de seguridad importante y que mida la efectividad para cumplir con los seis requisitos anteriores.

Si quieres conocer cómo puedes defenderte de las amenazas protegiendo de forma eficaz tus equipos endpoint, se parte del Entrenamiento de Defensa Integral Hands On con Grupo Smartekh y Palo Alto Networks.

IMPLEMENTAR UNA ESTRATEGIA DE PROTECCIÓN A NIVEL ENDPOINT VALE LA PENA

Para todas las organizaciones. No se trata sólo de detectar riesgos para tu negocio, se trata de reducir la superficie de ataque para que las amenazas se ejecuten en tu negocio.

Grupo Smartekh