Check Point®
SOFTWARE TECHNOLOGIES LTD.

ARQUITECTURA CHECK POINT INFINITY

LA ARQUITECTURA DE CIBERSEGURIDAD DEL FUTURO

ÍNDICE

INTRODUCCIÓN

Prácticamente todas las organizaciones de TI buscan mejorar su capacidad para mitigar riesgos con un nivel de inversión razonable y sostenible. Pero hay tres retos que lo hacen extremadamente difícil:

1. Un panorama de amenazas agresivo y en continuo cambio
2. La enorme cantidad y diversidad de datos, aplicaciones e infraestructuras de la organización que deben ser protegidos (datos móviles, entornos cloud/SaaS, outsourcing de terceros... son sólo tres ejemplos).
3. Encontrar y retener personal de seguridad que pueda convertir los objetivos de negocio en estrategias técnicas efectivas y sostenibles en el tiempo.

Ante estos desafíos, algunos en la industria han llegado a la conclusión de que es imposible alcanzar una verdadera protección y que, por tanto, hay que centrarse en detectar y mitigar las amenazas una vez que éstas han penetrado las defensas. Pero ésta es una estrategia muy arriesgada. Lo que realmente se necesita es una arquitectura de seguridad que se adapte a las demandas empresariales actuales, cada vez más dinámicas, y que se centre en la prevención para garantizar que todos los activos clave están completamente protegidos.

Check Point lnfinity es la única arquitectura consolidada de ciberseguridad que puede poner "a prueba de futuro" su negocio y su infraestructura de TI, incluyendo redes, entornos de nube y dispositivos móviles. Infinity aprovecha tres ventajas clave para resolver los desafíos a los que se enfrenta la seguridad de TI:

1. **Prevención avanzada de amenazas:** La suite de capacidades de protección líder en la industria, desplegadas a través de redes, entornos de nube y dispositivos móviles
2. **Plataforma de inteligencia de amenazas:** Check Point ThreatCloud aglutina y distribuye inteligencia de amenazas y actualizaciones de protección en tiempo real.
3. **Gestión de amenazas consolidada:** Una interfaz de gestión unificada que permite utilizar políticas de riesgos orientadas al negocio y convertirlas en protecciones de seguridad, con APIs para proyectos de integración con otras aplicaciones e infraestructuras de TI.

Check Point lnfinity proporciona una protección completa ante ataques conocidos y de día cero en todo el entorno, incluyendo aplicaciones cloud y dispositivos móviles. Su interfaz de gestión, sencilla y orientada al negocio, reduce la complejidad, facilitando la implementación de la seguridad y su ajuste aun presupuesto y un nivel de personal moderados. lnfinity ayuda a las organizaciones a ofrecer unas TI ágiles y seguras, que se podrán ir adaptando a medida que vayan cambiando los requisitos del negocio. A través de la prevención avanzada de amenazas, la gestión de políticas orientadas al negocio y una inteligencia de amenazas basada en la nube, lnfinity aporta una base sólida para una estrategia de gestión de riesgos sostenible y efectiva.

SITUACIÓN DE PARTIDA

La rápida transformación digital de las empresas implica cada vez mayores exigencias de seguridad. Las organizaciones convergen aplicaciones y datos en redes IP, desplegando y actualizando aplicaciones cada semana, o incluso a diario. Los equipos desktop de la compañía están siendo progresivamente reemplazados por PCs portátiles, tabletas y dispositivos de los empleados (BYOD), en tanto que las aplicaciones se van moviendo desde el data center o CPD hacia nubes híbridas, alimentadas por dispositivos loT o externalizadas completamente bajo modelos de software como servicio (SaaS). Y, por si fuera poco, regulaciones como GDPR han generado nuevos requisitos de control de datos difíciles de implementar en estos entornos.

Desgraciadamente, mientras los productos de seguridad proliferan, las arquitecturas de seguridad realmente efectivas son mucho menos frecuentes. El despliegue de productos de prevención tradicionales ha dado como resultado una gran cantidad de datos de registro y alertas, la mayoría de los cuales han sido ignorados. Esto ha llevado a la conclusión de que "entrarán sí o sí" y que, por tanto, la respuesta debe pasar por implementar estrategias de detección y mitigación, invirtiendo en soluciones de prevención tradicional. Este enfoque ha traído más complejidad, con múltiples productos y sistemas de gestión independientes, que no comparten inteligencia de políticas y amenazas, y que dejan entre sí importantes carencias defensivas. En definitiva, estos modelos han desembocado en infraestructuras de seguridad más complejas y costosas, pero que no mejoran la protección, como queda demostrado por el flujo continuo de ataques exitosos que vemos a diario en la prensa.

Por último, la cantidad y la tipología de las amenazas se están acelerando. La amplia superficie de ataque de los entornos de nube híbrida, la movilidad y las redes de loT suponen un gran número de nuevos puntos de ataque por aprovechar. Mientras tanto, las organizaciones criminales, actores a nivel de estado e incluso la filtración de "ciberarmas" por parte de agencias como la NSA, han generado una tecnología de ciberataque cada vez más potente, disponible para unos adversarios cada vez en mayor número y bien organizados.

Está claro que se necesita un enfoque completamente nuevo: una verdadera arquitectura de seguridad, que debe combinar una tecnología de prevención efectiva, una política de seguridad unificada y un modelo operacional cuya implementación esté acorde con los entornos de TI actuales, con una dotación de personal y un presupuesto razonables. Ese nuevo enfoque es Check Point lnfinity.

PRESENTAMOS CHECK POINT INFINITY

Check Point Infinity es la única arquitectura de seguridad que proporciona el mayor nivel de prevención de amenazas de la industria a lo largo de redes, entornos de nube y dispositivos móviles. Infinity aporta la ciberseguridad más avanzada para las infraestructuras de TI actuales, combinando una solución de prevención de amenazas multi-capa junto con una gestión consolidada y consistentes APIs.

La arquitectura Infinity está basada en tres elementos principales: en primer lugar, Infinity está centrada en entregar la mejor prevención de amenazas de la industria. Desde su nacimiento, Check Point ha estado centrada siempre en ofrecer la mejor seguridad posible, y como tal, estamos totalmente enfocados en la creación de tecnologías y productos innovadores para PREVENIR los ataques. Nuestras tecnologías de prevención están diseñadas para detener tanto ataques conocidos como desconocidos (de día cero) en todas las áreas de la infraestructura de TI, incluyendo entornos cloud y de movilidad. Y, si el atacante penetra el perímetro, bloquearemos sus canales de Comando y Control rompiendo la "cadena mortal" (kill chain) del ciberataque antes de que pueda extraer datos.

En segundo lugar, Infinity ofrece esta protección desde una plataforma unificada. Todos los componentes de Infinity se basan en una misma plataforma de software común, controlada y monitorizada por un mismo sistema de gestión, y comparten la misma inteligencia de amenazas. Esto significa que las políticas, la monitorización y la prevención se actualizan y se aplican de manera uniforme en toda la infraestructura de TI. Y, si bien Infinity proporciona una base, sabemos que cualquier infraestructura de seguridad probablemente requerirá productos y fuentes de datos adicionales. Para atender a este reto, Infinity proporciona un amplio conjunto de APIs para integrar herramientas de seguridad de terceros como parte de infraestructuras más amplias, y que permiten la integración y la orquestación en la nube para implantar servicios y crear políticas de una manera dinámica. Infinity es la arquitectura sobre la cual la infraestructura de seguridad opera como un único muro cohesivo de protección

¿Qué tiene de especial Check Point Infinity?

Check Point Infinity es una arquitectura diseñada para gestionar desde un solo sistema políticas cohesionadas de seguridad, inteligencia, prevención y gestión, desde la monitorización hasta la respuesta en todas las redes, entornos de nube y dispositivos móviles. Además, usted podrá contar con productos de terceros como parte de su infraestructura de seguridad, ya que Check Point Infinity permite integrar estos productos para garantizar un sistema de seguridad verdaderamente cohesionado. Esto contrasta con otras muchas infraestructuras, donde los productos de seguridad operan en sus propias "islas" y no comparten prestaciones de políticas, inteligencia o gestión. Check Point Infinity le permitirá construir una única posición de seguridad cohesiva, al tiempo que hará que su equipo de seguridad sea más efectivo y eficiente en sus operaciones.

Pero, si bien esta plataforma de prevención de amenazas es fundamental, incluso las mejores soluciones de seguridad pierden su valor si no se gestionan adecuadamente. Check Point cuenta con una larga trayectoria proporcionando la mejor gestión de la seguridad. Y es que una administración efectiva es absolutamente esencial para unas operaciones de seguridad precisas y eficientes. El modelo de gestión de Infinity es una base idónea para garantizar unas operaciones de seguridad, monitorización y respuesta unificadas y coherentes, a lo largo de todas las redes, entornos de nube y dispositivos móviles. Por ejemplo, este modelo de gestión permite a las organizaciones escribir una única política y aplicarla en toda la infraestructura de TI, lo que permite la flexibilidad de múltiples nubes sin comprometer la seguridad. Esta política, además, permite construir ricas implantaciones basadas en atributos como identidad, inteligencia de aplicaciones, ubicación o política de prevención de amenazas, entre otros muchos. Gestión unificada de eventos de seguridad y delegación de gestión basada en roles completan la solución de seguridad más completa disponible en la actualidad. El modelo de gestión de Infinity permite a los equipos de seguridad proteger realmente las operaciones de TI, ya sea en pequeñas empresas, grandes organizaciones o para proveedores de servicios gestionados.

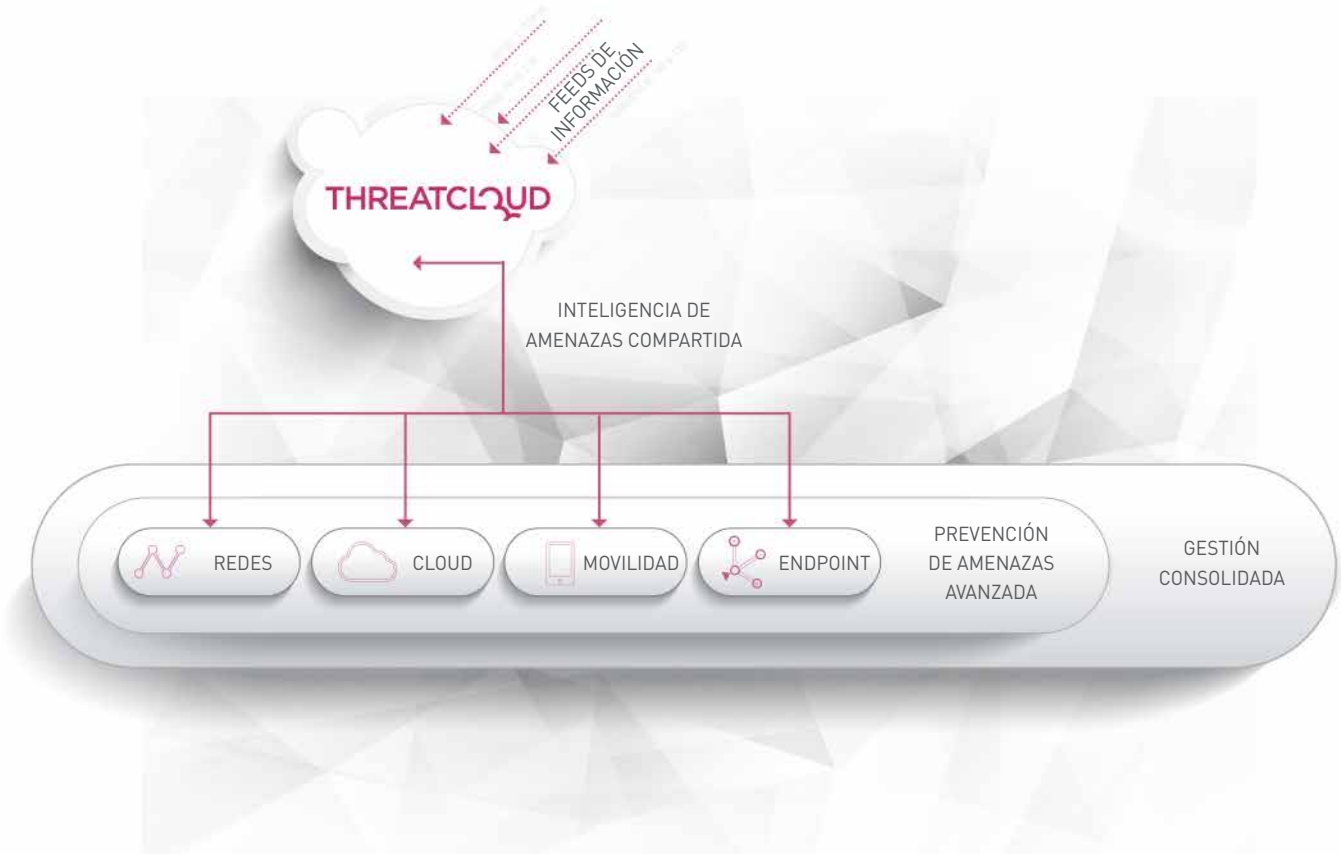
El diferenciador clave de Infinity, comparado con otros enfoques, es la integración de la mejor prevención y gestión de amenazas en toda la arquitectura. Ningún otro proveedor cuenta con el nivel de liderazgo de Check Point en ambas áreas. Por eso, somos el único proveedor que aparece en la sección superior derecha del Cuadrante Mágico 2017 de Gartner para firewalls de nueva generación y gestión unificada de amenazas. Mientras otros proveedores asumen que los atacantes entrarán sí o sí, y se centran en la detección y la respuesta, nuestro enfoque sigue siendo el mismo: detener los ataques antes de que tengan éxito. Un enfoque que se demuestra en capacidades como:

- Prevención con sandboxing con CPU-Level que bloquea los ataques antes de que éstos puedan iniciar sus técnicas de evasión
- Threat Extraction, que entrega a los usuarios ficheros seguros y limpios, protegiéndoles de posibles infecciones.
- Anti-Phishing, que detecta y bloquea los ataques de phishing antes de que pueda infectar a los usuarios.
- Anti-Ransomware, que detecta y bloquea ataques de ransomware y restaura cualquier fichero inicialmente cifrado.

La incorporación de inteligencia de amenazas a lo largo de toda la arquitectura es el elemento que completa la imagen, asegurando que toda la superficie de ataque esté protegida de manera consistente. Finalmente, a través de APIs abiertas, lnfinity se integra en las infraestructuras de TI más amplias permitiendo el intercambio de información sobre políticas, identidades y eventos. Esta integración es crucial para implementar una protección de amenazas orientada al negocio de una manera viable a nivel operativo, con total separación de los controles de tareas, logging y cumplimiento.

CHECK POINT INFINITY, EN DETALLE

A continuación analizamos en detalle la arquitectura Infinity, para mostrar de qué modo ofrece prevención de amenazas y aplicación de políticas. Infinity se compone de tres capas, como se muestra a continuación.



Las capas trabajan juntas para definir las políticas, traducir estas políticas en reglas de aplicación y luego llevar esas reglas a los puntos de aplicación a lo largo de todo el entorno. Finalmente, los eventos y la inteligencia de amenazas producidos por la capa de cumplimiento se consolidan y se presentan al equipo de Operaciones de Seguridad, ya analizados para asegurar el control del cumplimiento, y se introducen en ThreatCloud para actualizar en tiempo real la información sobre prevención de amenazas para todos los clientes de Check Point.

GESTIÓN DE POLÍTICAS DE SEGURIDAD CON CHECK POINT

La administración de políticas de Check Point está diseñada para extrapolar los objetivos del negocio a las políticas de seguridad. No importa cuán buena sea la tecnología de seguridad si las políticas requeridas por la empresa no pueden expresarse en su sistema de gestión. Ya no es suficiente con escribir simples reglas estáticas basadas en red que no se pueden aplicare sobre lo que la empresa realmente intenta hacer o proteger. Además, los gestores deberán consolidar estas políticas a lo largo la red, en la nube y en los entornos de movilidad, en lugar de depender del departamento de Operaciones de Seguridad para alinear manualmente las políticas a través de múltiples soluciones puntuales.

Check Point es consciente desde hace tiempo de que esta necesidad existe, tanto para una efectiva prevención de amenazas y el control de accesos como para minimizar el exceso de personal de administración. A fin de ofrecer el portfolio de seguridad más completo de la industria, el componente de gestión de lnfinity soporta, entre otras muchas, las siguientes dimensiones orientadas al negocio:

ELEMENTO	EJEMPLOS
Usuario o Grupo	Joe, Dpto. de Marketing, Summer Interns
Aplicación	Twitter, Instagram
Datos y contenido	Número de tarjeta bancaria, ruta ABA Bank
Para aplicar sobre	Amazon AWS, VMware Cluster, entornos móviles

Name	Source	Destination	Services & Applications	Data	Action	Install On
Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
Social media for marketing	marketing_role John	Internet	Twitter LinkedIn Instagram	Any	Accept	SG15600
Developers upload	developer_role	Internet	Dropbox Box	Any Direction Source Code - JAVA	Accept	SG15600 CapsuleCloud
Access Sensitive Servers	Any	Any	Any	Any	SensitiveServers	Policy Targets
Mobile Access	Mobile Devices	MailUS	MailServer	Any	Accept	Mobile
Access to Web Server	Any	WebServer	https	Any	Accept	AWS VMWare

Unificación de políticas en R80.x: gestión de la seguridad basada en políticas orientadas al negocio y no a la construcción de TI

DELEGACIÓN DE GESTIÓN. AUDITORÍA

La capa de gestión admite delegación de autoridad, con una total auditoría sobre la administración. Esto permite distribuir responsabilidad sobre las políticas de seguridad entre las personas que están en mejores condiciones para juzgar lo que debería permitirse, haciendo que la seguridad responda mejor a las necesidades del negocio. El sistema de gestión de Check Point incluye flujos de trabajo y aprobaciones para todos los cambios de política, una capacidad que es fundamental para garantizar que se aplican las políticas adecuadas, que se evitan errores disruptivos y que se implementan controles de cumplimiento sobre de la actividad de administración.

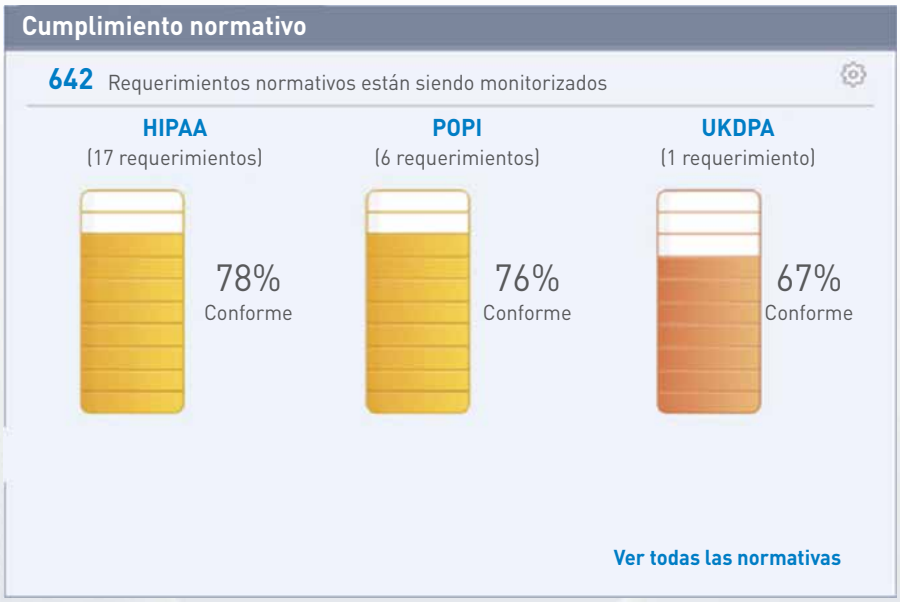
La administración modular permite definir por un lado las políticas de acceso y control de datos y, por otro, la activación del sistema de prevención de amenazas. Las políticas de prevención de amenazas podrán entonces aplicarse automáticamente al tráfico permitido por las políticas de acceso y control de datos, o bien ser gestionadas por diferentes personas, e incluso por parte de personal subcontratado.

Ejemplo: Gestión de delegación de políticas

El equipo de Marketing necesita constantemente acceder a nuevas aplicaciones SaaS, y tendrá que intercambiar información con una lista cambiante de subcontratas y agencias de servicios, lo que va a suponer decenas de tickets para el Help Desk. Estos tickets, a su vez, se irán retrasando a la espera de que se clarifique cuáles son las necesidades exactas de cada uno y las aprobaciones de soporte necesarias para dar respuesta.

Con Check Point Infinity, el equipo de Marketing podría responsabilizarse de sus propias políticas de seguridad. Podrían nominar a uno de los empleados como policy manager, para ocuparse de actualizar las políticas para el equipo de Marketing y sus datos, pero no para el resto de la organización. Toda esta actividad sería auditada por el departamento de Seguridad y Cumplimiento para su validación, mientras que el equipo de Seguridad podría dedicar su esfuerzo a aplicar las principales protecciones ante amenazas, tales como mitigación de malware o prevención de pérdidas de datos.

GESTIÓN DE APLICACIÓN DE LA POLÍTICA



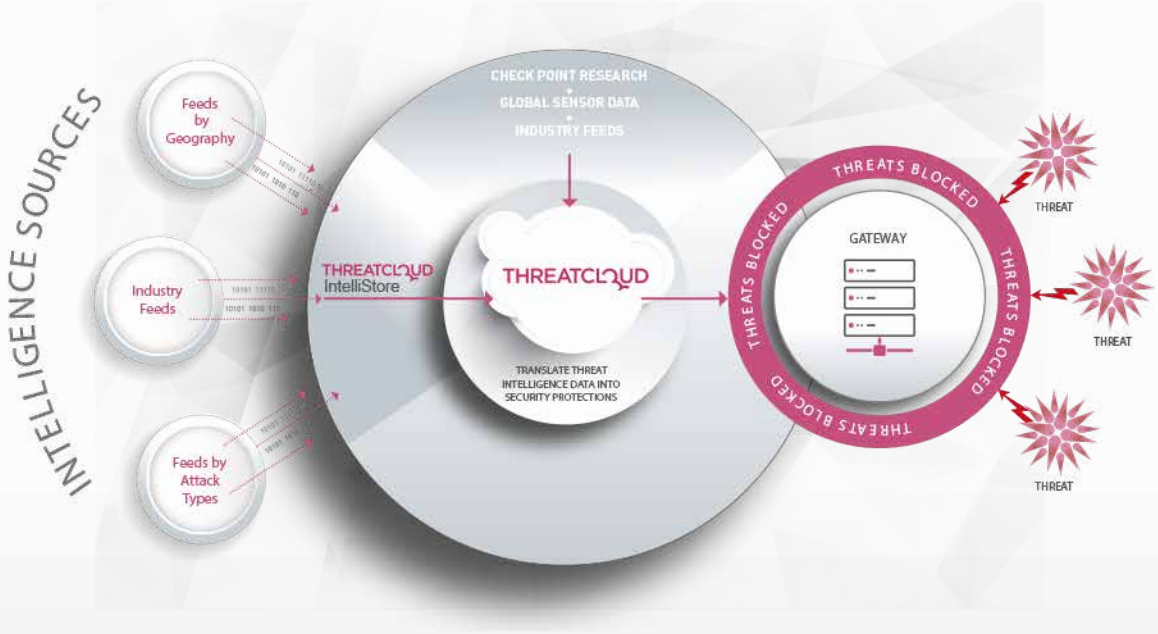
Dashboard de niveles de cumplimiento (general)

El modelo de gestión de Check Point incluye un componente opcional para validar configuraciones de seguridad a lo largo de la arquitectura Infinity. El Software Blade de Cumplimiento opera sobre una base de datos con miles de reglas basadas en buenas prácticas de configuración y cumplimiento, y las aplica sobre la infraestructura. Las violaciones serán marcadas de forma instantánea y se recomendarán las acciones más adecuadas para su remediación. Un panel de control (dashboard) normativo y el manejo de informes de apoyo convierten la validación del cumplimiento y las auditorías para estándares como PCI, ISO 27001, PCI DSS y GDPR en tareas sencillas.

CONTROL. INTELIGENCIA DE AMENAZAS

Dos funciones principales de la arquitectura Infinity son la distribución de las políticas configuradas en la capa de gestión a los puntos de aplicación, y derivar y distribuir automáticamente inteligencia sobre amenazas y actualizaciones sobre prevención. La arquitectura incorpora una diferencia esencial, que es su capacidad de distribuir políticas a través de redes, dispositivos móviles y entornos *cloud*, desplegando un perfil de protección unificado para todos los activos de la empresa.

lnfinity derriba los silos de seguridad consolidando una inteligencia completa y a tiempo a lo largo de la infraestructura completa. Check Point ThreatCloud almacena toda la inteligencia de amenazas, proveniente de una amplia gama de fuentes: investigaciones de Check Point, análisis de sandboxing, sistemas de Respuesta ante lncidentes, appliances de seguridad, equipos de emergencia (CERTs) y de respuesta (CSIRTs), fabricantes de productos de seguridad y otras organizaciones dentro de la comunidad de seguridad.



ThreatCloud contiene un registro con más de 11 millones de firmas de malware, más de 2,7 millones de sitios web infectados con malware y más de 5.500 patrones diferentes de redes bot*. ThreatCloud se actualiza constantemente con nueva información sobre amenazas, proveniente de una red mundial de sensores, sistemas de terceros, investigaciones de Check Point, organizaciones del sector y gateways de la propia Check Point

*Datos del 3º trimestre de 2017.

ThreatCloud combina y analiza todas estas fuentes de información, extrae nuevos modelos de prevención de amenazas y las envía dinámicamente en los puntos de aplicación para su activación inmediata. En este proceso colaborativo, si una empresa sufre un ataque de malware, la información relevante sobre el ataque será compartida al instante en ThreatCloud, y se añadirá una nueva firma para el ataque en la base de datos para ser aprovechada al instante por todos los demás clientes de Check Point. Este nuevo enfoque, colaborativo, dinámico y automatizado, es la única vía realista para mantenerse un paso por delante en el cambiante panorama actual de las ciberamenazas.

ThreatCloud en acción

El ataque: Una empresa recibe un email malicioso a través de una cuenta de Office365, pero es bloqueado por Sandblast Cloud

Inteligencia: ThreatCloud recibe la notificación IOC (Incident of Compromise) correspondiente al ataque y lo extiende a otros IOCs

Distribución automatizada: ThreatCloud envía las actualizaciones a lo largo de la arquitectura lnfinity

Protección: Otros ataques similares, que llegan vía SMS y desde sitios web infectados, son también bloqueados

PREVENCIÓN DE AMENAZAS - EVITANDO ATAQUES ANTES DE QUE SUCEDAN

Uno de los mayores desafíos a que se enfrentan los profesionales de la seguridad es la combinación entre una variedad de ataques cada vez más amplia y una superficie de ataque cada vez mayor. Una protección reamente completa requerirá un enfoque orquestado que evite los ataques antes de que sucedan. El objetivo es vencer a todos los ataques, en todos los vectores posibles. Una arquitectura de seguridad que facilite una infraestructura de protección cohesionada e integrada aportará una protección más completa y más rápida que una infraestructura compuesta de piezas que no trabajan juntas. Esto es lo que ofrece Check Point Infinity: una arquitectura de seguridad para prevenir ataques antes de que ocurran. Analicemos en detalle las capacidades de prevención de amenazas de esta arquitectura.

1. Amenazas conocidas

La mayoría de los ataques que su red podría estar sufriendo ahora mismo son ataques conocidos, es decir, ataques conocidos que han sido detectados y analizados con anterioridad, y a los que se ha asignado ya un conjunto de indicadores de ataque y detalles asociados. La prevención de ataques conocidos es esencial para cualquier plan de seguridad de TI. Infinity proporciona la base y las capacidades necesarias para protegerse contra ataques conocidos, a través de una prevención de amenazas basada en red en cada gateway de seguridad, apoyada por la inteligencia sobre ataques que aporta Check Point ThreatCloud. El modelo de prevención contra ataques conocidos de Check Point Infinity cuenta con las mejores tecnologías de prevención de intrusiones para evitar exploits conocidos contra vulnerabilidades conocidas; antivirus para evitar archivos y URLs maliciosas conocidas, y capacidades post-infección para bloquear conexiones de redes bot a servidores de Comando y Control conocidos. En algún punto, todos los ataques intentarán atravesar su red; la protección de redes de Check Point Infinity los bloqueará en diversos puntos de la cadena mortal (*kill-chain*).

2. Amenazas avanzadas y desconocidas

Mucho menos numerosos, pero mucho más preocupantes, son los ataques desconocidos, especialmente los ataques personalizados concretamente para apuntar a su negocio. Las amenazas desconocidas normalmente pasan desapercibidas por más tiempo, causando más daño. Aquí es donde muchas infraestructuras de seguridad "internas" fallan, ya que aplican sistemas de protección puntuales, con buena tecnología pero que operan de forma autónoma, contra los ataques desconocidos y avanzados. Para combatir este tipo de amenazas es esencial poder compartir en tiempo real inteligencia sobre ataques dirigidos y de día cero anteriormente desconocidos con el resto de la infraestructura de seguridad. Check Point Infinity evita amenazas avanzadas y ataques dirigidos y desconocidos como parte integrada de su arquitectura de seguridad global. Con una amplia familia de productos, SandBlast proporciona un conjunto avanzado de soluciones de protección que incluye más de 30 innovaciones tecnológicas para detectar y evitar ataques desconocidos, dirigidos y de día cero en todas las áreas de la infraestructura de TI. Y, de nuevo, poder compartir al instante indicadores de ataques recién detectados con el resto de la infraestructura de seguridad será esencial para prevenir los ataques antes de que ocurran. Eso es exactamente lo que hace Check Point.

3. Protección preventiva

Si pudiera usted proteger preventivamente su empresa de los ciberataques sin afectar a la operativa diaria ¿no lo haría? Las capacidades innovadoras en Check Point Infinity le permiten precisamente eso: protección preventiva contra ciberataques sin afectar a las operaciones. Por ejemplo, SandBlast Threat Extraction desinfecta de malware todos los archivos que los usuarios finales descargan de Internet y reciben por correo electrónico, antes de que éstos los abran, y sean infectados. Imagine por un momento el valor de esta capacidad... todos los ficheros, descargados de Internet y recibidos por email por todos sus usuarios, entregados limpios, y sin que ello impacte en las operaciones.

Dashboard de niveles de cumplimiento (general)

4. Puestos de trabajo (endpoints)

Todos sabemos que los *puestos de trabajo (endpoints)* son un repositorio de valiosa información corporativa, y por ello son, al mismo tiempo, el objetivo más común para las ciberamenazas. A pesar de ello, la evolución natural de la tecnología de seguridad ha aislado la protección de los puestos de trabajo de la protección de la red. Durante muchos años, ese muro artificial impidió el avance de una seguridad y respuesta de TI más unificada y cohesionada... hasta ahora. Check Point Infinity no sólo protege los puestos de trabajo sino que también permite compartir inteligencia y análisis forense con datos e información que solo pueden provenir del propio puesto de trabajo. Concretamente, las innovadoras capacidades preventivas mencionadas anteriormente en Check Point SandBlast Agent evitan los ataques de archivos y URLs maliciosos y aportan además prevención anti-bot post-infección y análisis de tipo sandboxing para bloquear ataques desconocidos y de día cero, además de anti-ransomware. Esta capacidad única e innovadora es tan oportuna como efectiva para detectar y bloquear actividad de ransomware y restaurar los archivos afectados. Recientemente, la tecnología Anti-Ransomware de Check Point evitaba dos de los últimos ataques de ransomware: WannaCry y NotPetya. A través de ThreatCloud, toda la inteligencia de amenazas se comparte instantáneamente desde y hacia SandBlast Agent para evitar ataques antes que ocurran, tanto en los endpoints como en el resto de la infraestructura de seguridad.

5. Dispositivos móviles

Los dispositivos móviles son ya parte del tejido de TI y de las operaciones de negocio en todas partes. Todos podemos conectarnos a la red de nuestra empresa y acceder a todo tipo de aplicaciones e información "propietaria" desde nuestros dispositivos mientras estamos en cualquier parte del mundo. Una regla básica de seguridad es desplegar el nivel de protección de acuerdo al valor del activo que se está protegiendo. Desgraciadamente, en la mayoría de las empresas los dispositivos móviles no están protegidos, ni mucho menos, de forma proporcional al valor de los activos a los que se puede acceder a través de ellos, y sin embargo, ése es sin duda un vector de amenaza del que preocuparse. De nuevo, como arquitectura de seguridad, Check Point Infinity amplía sus capacidades core de prevención de amenazas al mundo móvil para prevenir ataques antes de que sucedan. En concreto, Check Point SandBlast Mobile proporciona prevención de amenazas avanzada para evitar todo tipo de ataques en dispositivos iOS y Android: a nivel de sistema operativo, aplicaciones maliciosas, ataques dirigidos a apps y técnicas basadas en red como ataques "man-in the-middle" (MiTM). Al igual que el resto de componentes de Check Point Infinity, SandBlast Mobile recibe y comparte inteligencia de amenazas a través de ThreatCloud para garantizar la seguridad más completa y oportuna en toda su infraestructura de TI.

6. Entornos de nube

No es ningún secreto que una de las tecnologías más impactante en los negocios de la actualidad es la nube. Atractivas en muchos aspectos -en particular, flexibilidad operativa y ahorro de costes-, las implementaciones en la nube, ya sean remotas, privadas o híbridas, han de estar protegidas contra las mismas amenazas y con los mismos medios que se han detallado hasta ahora. Esta es otra de las fortalezas y beneficios de la arquitectura Infinity de Check Point. Con vSEC, usted podrá respaldar sus activos y operaciones de TI con independencia del proveedor y del modelo de nube que elija. Por su parte, Check Point SandBlast ofrece protección para entornos Microsoft Office365. Ambos amplían las capacidades de Check Point Infinity para prevenir ataques antes de que ocurran, como parte de la estructura global, integrada y cohesiva que se necesita para obtener la mejor protección.

7. A prueba de futuro

Para entender en su totalidad el valor de Check Point Infinity, ahora y en el futuro, es importante entender que Check Point está totalmente enfocado a construir productos que prevengan los ataques antes de que ocurran. Como muestra este documento, Check Point Infinity se compone de un conjunto de tecnologías de prevención innovadoras y líderes, intercambio de inteligencia y gestión a lo largo de todas las plataformas de TI utilizadas en la actualidad. Y ampliaremos estas mismas capacidades a cualquier nueva plataforma de TI o tecnologías que se desarrollen mañana, para seguir previniendo los ataques antes de que ocurran.

El futuro con Check Point Infinity

Para entender en su totalidad el valor de Check Point Infinity, ahora y de cara al futuro, es importante entender que Check Point está totalmente enfocado a construir productos que prevengan los ataques antes de que ocurran.

GESTIÓN DE EVENTOS

La gestión de la seguridad es un proceso que no acaba nunca, es un proceso continuo de implementación, monitorización y actualización de políticas. La mayoría de las organizaciones tienen dificultades para monitorizar la multitud de soluciones específicas con que cuentan, o para implementar actualizaciones de políticas basadas en eventos. Check Point Infinity combina la potencia su modelo de gestión con las ventajas de una plataforma unificada, ofreciendo un ciclo de vida de seguridad continuo.

El punto de partida del proceso de monitorización es la recolección de eventos. A diferencia de otros productos de seguridad, que simplemente transfieren eventos a un SIEM y esperan que algo bueno pueda extraerse, la arquitectura de Check Point incluye el componente SmartEvent, que realiza correlación de eventos en tiempo real y análisis Big Data, recopilando, consolidando y correlacionando eventos desde los puntos de aplicación desplegados en la red. Asimismo, ofrece una visión de incidentes consolidada y correlacionada, basada en múltiples fuentes de información, que ayuda al personal de Respuesta ante Incidentes a identificar las acciones que deben tomarse, así como una visualización en tiempo real de la cadena de eventos que permitirá identificar los vectores de ataque iniciales y los hosts y datos comprometidos.

El cuadro de mando de R80.x, SmartEvent, consolida los eventos de seguridad y acelera la respuesta ante incidentes

SmartEvent va más allá y automatiza las actualizaciones sobre prevención de amenazas. Cada proceso de investigación generará nuevos indicadores de amenaza, patrones de comportamiento y direcciones de red asociadas a cada ataque identificado. Tras ello, estos indicadores se enviarán, también automáticamente, a la plataforma ThreatCloud, y desde allí de distribuirán a la capa de aplicación para proteger a la organización con bloqueo en tiempo real.

Este modelo de "bucle cerrado" de Infinity es una ventaja esencial, ya que elimina la necesidad de que el equipo de Seguridad tenga que medir y administrar lo que debería ser un proceso unificado y automatizado. Esto mejora la posición de seguridad y libera recursos para dedicarlos a tareas de mayor valor, como la respuesta ante incidentes o la supervisión de políticas.

INTEGRACIÓN TECNOLÓGICA. APIs

La arquitectura Infinity no existe en el vacío. Ha de soportar integración automatizada con los entornos más amplios de la organización, por diferentes razones:

- **Rapidez y agilidad:** Los departamentos de TI están bajo una continua presión para ser más ágiles y sensibles ante las necesidades del negocio, incluyendo la seguridad. Pasando de los tickets de incidencias y las actividades manuales a un modelo de procesos automatizados, los servicios y políticas de seguridad podrán ser aplicados rápidamente allá donde sea necesario, eliminando los cuellos de botella en la implementación de aplicaciones o el acceso a las mismas.

- **Respuesta mejorada ante amenazas e incidentes:** La seguridad abarca inevitablemente múltiples sistemas y fuentes de información (*repositorios de identidades*, inventarios de activos, sistemas de gestión de eventos, etc.) que deben trabajar juntos para ofrecer una correcta protección ante amenazas. En el caso de la respuesta ante incidentes, los analistas deben recopilar información de múltiples fuentes de la manera más eficiente posible para determinar la respuesta adecuada. Cuantas más interacciones se automaticen, más oportunas serán las actualizaciones para la prevención de amenazas.

- **Políticas adecuadas:** Muy a menudo, las brechas de seguridad ocurren porque un proceso manual se ejecutó incorrectamente, o no se ejecutó. La automatización reemplaza los pasos manuales, poco fiables, mejorando la precisión de las políticas. La automatización de los controles de cumplimiento, además, reduce los esfuerzos para responder ante auditorías y reduce las posibilidades de hallazgos durante las mismas.

- **Delegación:** Tanto para las empresas como para los proveedores de servicios, hay cierto nivel de control de políticas que debe delegarse a aquéllos que se encuentran en la mejor posición para tomar las decisiones. Por ejemplo, un proveedor de servicios puede querer delegar las decisiones diarias sobre control de acceso en el personal técnico de su cliente, y éstos, a su vez, pueden querer delegar parte de estas decisiones en las diferentes divisiones de negocio. Las integraciones basadas en APIs permiten esta capacidad, al tiempo que conservan trazas de auditoría completas de la actividad.

Infinity incluye un rico conjunto de APIs que dan soporte a estos objetivos, y que son utilizadas por los partners tecnológicos de Check Point para desarrollar soluciones integradas. Tanto las APIs RESTful como el acceso a líneas de comando están disponibles, posibilitando un amplio rango de aplicaciones, como las siguientes:

- **Entornos de nube y virtualizados:** A medida que las aplicaciones se desarrollan cada vez más utilizando automatización y metodologías DevOps, la seguridad debe ser también automatizada para evitar que sea un cuello de botella. Para hacer esto posible, las APIs de Check Point permiten desplegar gateways de software e implementar políticas de forma automática, incluyendo aprovisionamiento *zerotouch* para Openstack, Amazon AWS y VMware NSX, entre otros. Además, está integrado también con Office365, lo que permite aplicar de forma efectiva prevención de amenazas en emails entrantes.

Check Point Infinity en los centros de datos definidos por software

La naturaleza dinámica de los centros de datos definidos por software hace obsoletos los métodos tradicionales de gestión de seguridad basados en reglas estáticas. Para superar este desafío, Check Point se ha asociado con VMware para integrar Infinity con su plataforma para centros de datos definidos por software [SDDC]. Esta integración automatiza la seguridad de forma que los servidores virtuales están protegidos dinámicamente en función de políticas predefinidas, permitiendo a las empresas proteger sus centros de datos sin renunciar a la agilidad que exige su negocio.

La integración de Check Point con VMware SDDC y NSX soporta la instalación de los gateways y de las políticas de seguridad aplicadas a ellos. De este modo, por ejemplo, si el equipo de VMware agrega un servidor a un clúster e implementa aplicaciones virtuales sobre él, Infinity activará automáticamente un nuevo gateway virtual [vSEC] en dicho servidor. Luego, aplicará políticas de seguridad en el gateway para proteger las aplicaciones migradas. Esta estrategia de "microsegmentación" inserta una seguridad adyacente a los activos protegidos, maximizando la efectividad. Infinity puede, incluso, alertar a NSX cuando un servidor parece infectado, de forma que el equipo de VMware pueda implementar acciones de remediación manuales o automáticas.

- **Actualización de objetos y de la tabla de reglas:** Las tareas administrativas más comunes son cambios en la membresía de grupos de objetos o cambios en la tabla de reglas. Automatizar estas tareas, por una parte, libera mucho tiempo de personal y, por otra, disminuye la posibilidad de incidencias debidas a errores humanos.

- **Prevención de amenazas:** Aplicación de protecciones ante amenazas basadas en sistemas de respuesta ante incidentes o en políticas de terceros. Esto implica compartir información de identidades con la infraestructura para soportar políticas basadas en identidades, por ejemplo con Cisco ISE, ACI o TrustSec.

- **Self-Service:** Aprovisionamiento de portales especializados para delegar acciones a personal cualificado que será informado y autorizado para tomar decisiones sobre seguridad para su organización.

- **Mejora en la respuesta a tickets:** El sistema de data mining de Check Point busca entradas correspondientes a una persona o sistema de interés para automatizar la investigación y respuesta de incidentes..

Para respaldar el esfuerzo de nuestros clientes por utilizar nuestras APIs, Check Point ofrece Checkmates, nuestra comunidad de usuarios. Los miembros de la comunidad pueden hacer preguntas, interactuar con sus colegas, compartir código y colaborar con el departamento de I+D de Check Point. Para más información, visite la sección dedicada a desarrolladores haciendo clic aquí.

El objetivo de Check Point es garantizar que toda actividad o manejo de datos en Infinity que se pueda realizar manualmente, también podrá realizarse de forma programada a través de APIs fiables y auditadas. Este compromiso con la automatización hace que Infinity sea mucho más que una simple infraestructura de seguridad: es un habilitador de negocio que se mantiene efectivo y viable a medida que las aplicaciones pasan a operar en arquitecturas dinámicas, nativas de nube.

PRIMEROS PASOS CON LA ARQUITECTURA CHECK POINT INFINITY

Para implementar cualquier arquitectura, será necesario utilizar una metodología que tenga en cuenta las realidades tanto de la operación como de los objetivos de negocio de la organización. A continuación se muestra cómo Infinity puede aplicarse en la práctica con un enfoque por fases que acelera el tiempo de adquisición de valor, al tiempo que minimiza los riesgos.

1. Evaluación de riesgos

El objetivo esencial de la seguridad de TI es reducir los riesgos del negocio. Por tanto, cualquier nueva iniciativa de seguridad debería comenzar con una evaluación de riesgos. Es un proceso en dos pasos:

a. ¿Qué riesgos estamos tratando de minimizar? tiempo de inactividad de la producción, pérdida de propiedad intelectual, daño a la reputación, incumplimiento de los requisitos normativos... ¿Qué ponderación le asignamos a cada uno? Son decisiones difíciles que deben involucrar a la dirección, quienes no siempre querrán "salir al aire" al tomar estas decisiones. Pero lo cierto es que ésta es una discusión puramente orientada al negocio; de hecho, en esta fase no debería introducirse ningún componente de tecnología. El resultado debe incluir, al menos, una lista de riesgos, una ponderación relativa de su importancia y una discusión del proceso y la gente que habrá de utilizarse para llegar a la meta, para evitar dudas.

b. ¿Cuál es nuestro nivel de exposición a cada uno de los tipos de riesgo identificados? Esto se puede abordar identificando primero los activos de TI y de datos a los que afecta cada tipo de riesgo, y luego evaluando cómo podrían verse comprometidos.

2. Conociendo la posición general de seguridad

El siguiente paso es evaluar los sistemas y procesos de seguridad con los que cuenta la organización. Esto implica una evaluación realista de lo que está instalado, algo que suena simple pero que en la práctica puede ser todo un desafío. Un error común que debe evitarse es confiar al 100 por cien en el personal de seguridad a la hora de realizar la evaluación. Sencillamente, porque el equipo de Seguridad puede no ser capaz de proporcionar una visión objetiva de cómo se ha construido la postura de seguridad. Puede que no quieran revelar sus deficiencias, o al menos minimizarán los niveles de exposición. También pueden intentar "barrer para casa", y reclamar esos sistemas que tanto desean pero nunca se incluyen en el presupuesto, o criticar a personas o equipos en los que no confían o con los que no tienen una buena comunicación. Por último, puede que no estén en la mejor posición para evaluar el factor humano: ¿Cuál es el impacto del comportamiento de los usuarios finales y de los administradores de TI en la posición general de seguridad? Sean cuales sean las razones, es importante involucrar en el proceso a personas ajenas a la seguridad, a fin de mantener dicho proceso lo más objetivo y amplio posible.

3. Comprendiendo los objetivos de negocio y de TI

El tercer paso es mirar hacia adelante: ¿Cuáles son los proyectos, estrategias y restricciones de ejecución que pueden afectar en un futuro a la arquitectura de seguridad? ¿Es probable que se produzcan adquisiciones? ¿Se abrirán nuevas oficinas, o el camino a seguir es la consolidación? Llevar a cabo proyectos de este tipo, ¿puede crear nuevos riesgos de disponibilidad de la producción que no existen en la actualidad? ¿Vamos a seguir sujetos a regulaciones de privacidad de datos como GDPR? Y ¿cuál es la actitud ante la posible migración a la nube y la externalización (MSP / MSSP)? Estas decisiones, que son críticas para la planificación, normalmente se toman a nivel de negocio, no técnico.

4. Definiendo y construyendo la arquitectura de seguridad del futuro

Solo después de que se hayan dado los primeros tres pasos, la organización podrá emprender la tarea de construir la arquitectura. Sugerimos proceder en dos vertientes: estratégica y táctica. A nivel estratégico, es importante ser realista: ¿qué soluciones se pueden implementar de manera realista teniendo en cuenta la dotación de personal, el presupuesto y la actitud de la dirección sobre riesgos? ¿Podrá usted conseguir el tiempo, el apoyo y la paciencia necesarios para poner en marcha estrategias que pueden tardar hasta dos años en implementarse por completo? Sea cual sea el caso, no se centre en exceso en la estrategia, ya que puede haber riesgos clave identificados que necesitan una solución más rápida. Busque victorias tácticas rápidas que le ayudarán a justificar y validar todo el esfuerzo.

También es importante aprovechar los estándares existentes al establecer objetivos de mejora de la posición de seguridad. Ejemplos como NIST, PCI y SANS establecen sólidos marcos de controles iniciales que se pueden utilizar en función de los riesgos establecidos en los pasos anteriores, y son, además, una excelente forma de reducir el riesgo de que los fallos de organización difuminen el esfuerzo.

RESUMEN

Dependiendo del punto de vista, las operaciones de TI y la seguridad están actualmente en medio de un gran período disruptivo, o bien en medio de un gran renacimiento. Independientemente de cómo lo vea usted, es seguro que, como profesional de seguridad, se encuentra bajo una tremenda presión para aumentar la eficiencia de las operaciones. Probablemente esté usted intentando resolver problemas de gestión de riesgos relacionados con la expansión de la tecnología y la diversidad de las infraestructuras, mientras intenta satisfacer la demanda de servicios ágiles y flexibles tanto para los clientes como para los usuarios finales. Y, además, debe entregar esos servicios de forma segura y a escala. Un plan reflexivo basado en una arquitectura que pueda cumplir con estas demandas a la vez que proporciona un control cohesionado, elasticidad del servicio y escalabilidad para satisfacer las necesidades futuras puede generar renacimiento, en lugar de disrupción, para su negocio.

Check Point Infinity es la arquitectura sobre la cual usted podrá construir un nuevo sistema de seguridad de TI. Infinity es la primera solución de seguridad consolidada para redes, entornos de nube y dispositivos móviles, que proporciona el más alto nivel de prevención de amenazas contra ataques conocidos y desconocidos para mantener su negocio protegido ahora y en el futuro. Es importante entender que Infinity no es simplemente un reclamo de marketing; es la culminación de nuestra visión general para construir una arquitectura de seguridad que aúne la mejor seguridad, la mejor inteligencia y la mejor gestión en todas sus redes, en la nube y en los entornos de movilidad. Check Point R80 es la "versión producto", que reúne las capacidades de seguridad, inteligencia y administración para cumplir con las múltiples demandas de seguridad de TI de la actualidad. Y, si R80 es la "versión producto", el conjunto completo de capacidades es mucho más que un producto, ya que establece las bases para diseñar e implementar una infraestructura de seguridad cohesiva, un sistema único, que cumplirá con sus requisitos de seguridad ahora, pero que también será extensible para satisfacer sus requisitos cambiantes en el futuro. En conjunto, estas capacidades forman una arquitectura, y esa arquitectura tiene un nombre: Check Point Infinity.

1. Protección

Check Point cree en una estrategia de protección ante amenazas preventiva, centrada en evitar los ataques, y no sólo en su detección. Nuestro objetivo es bloquear los ataques antes de que tengan éxito. Check Point Infinity extiende nuestras múltiples capas de seguridad, desde la detección basada en firmas hasta las capacidades avanzadas de prevención de la familia de productos SandBlast, en toda su infraestructura de redes, aplicaciones en la nube y dispositivos móviles, para una prevención de problemas constante y efectiva..

2. Inteligencia

Para prevenir los ataques antes de que ocurran, será esencial contar con una inteligencia de amenazas integral siempre actualizada, que se entregue simultáneamente a todos los puntos de cumplimiento. Check Point Infinity ofrece esa inteligencia de amenazas integral y actualizada. A través de Check Point ThreatCloud, todos los puntos de aplicación de su red, entornos de nube y dispositivos móviles estarán equipados con inteligencia de amenazas derivada de múltiples fuentes externas, investigaciones internas e indicadores provenientes de nuestros clientes en todo el mundo, incluidos indicadores sobre ataques desconocidos y de día cero detectados a través de los análisis sandbox de Check Point SandBlast.

3. Gestión

Check Point es el líder reconocido en gestión de seguridad. Sabemos que una mejor administración significa una mejor seguridad. La arquitectura Infinity consolida la gestión de múltiples capas de seguridad en función de sus políticas de seguridad orientadas al negocio, y ofrece a su equipo una visión centralizada de toda la actividad en su entorno: desde administración de políticas hasta monitorización, respuesta, cumplimiento y mucho más.

Piénselo: Contar con un único sistema de seguridad, cohesionado, en todos sus puntos de cumplimiento, reforzado con inteligencia de amenazas completa y actualizada, impulsado por una gestión unificada para toda su infraestructura de TI, incluyendo redes, entornos de nube y dispositivos móviles. Check Point Infinity ofrece todo esto, y le brinda la protección, la flexibilidad y el control que necesita para gestionar las disrupciones actuales y futuras que generan las TI, y convertirlo en un renacimiento para su negocio.

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Tel: +34 91 799 27 14
info_iberia@checkpoint.com