LAS FRONTERAS DE LA RED SE HAN HECHO MÓVILES

Los días en los que las fronteras de la red de una organización llegaban hasta el perímetro de sus edificios han terminado. Vivimos ya en un mundo conectado 24/7. Los empleados quieren conectarse a su trabajo de la misma forma que lo hacen en sus vidas personales: siempre que quieran y desde donde quieran.

Los empleados de hoy llevan smartphones, tablets y portátiles y pocas veces se lo piensan dos veces antes de utilizar sus dispositivos personales para el trabajo o los dispositivos corporativos para sus actividades personales. Los trabajadores con alta movilidad superarán en 2015 los 1500 millones de personas o el 37% de los trabajadores de todo el mundo, según fuentes de IDC.[1]

Los empleados se conectan a la red Wi-Fi más cercana sin preocuparse mucho sobre la seguridad de la fuente, con tal de que les conecte a Internet. Y descargan datos de la misma forma. Quieren disponer inmediatamente de la información. Desgraciadamente la gente que tiene prisa es más propensa a cometer errores.

Con este cambio, la necesidad de la seguridad móvil es más importante que nunca, especialmente cuando se estima que en 2014 unos 11,6 millones de dispositivos fueron infectados con malware.[2] Aunque esto puede representar menos del 1% de la población de dispositivos, se espera que la tasa de malware en móviles se incremente ya que estos dispositivos se están convirtiendo en la fuente más valiosa de información. Las aplicaciones móviles para la banca electrónica, el almacenamiento de tarjetas de crédito, y sí, los datos corporativos cada vez tienen más presencia en estos dispositivos, haciendo que estas plataformas sean un objetivo aún más atractivo para los hackers.

Sin siquiera saberlo uno de nuestros empleados ha podido entrar en un sitio malicioso, o descargar un virus de forma inadvertida. Solo se necesita un virus para que desde un dispositivo infectado, con técnicas sencillas de propagación, se infecte toda la red de su empresa.

El desafío es que con más tipos de dispositivos a proteger, una mayor variedad de versiones de aplicaciones software y múltiples sistemas operativos, el papel de la Tecnología de la Información (TI) se hace cada vez más complejo. Añada a esto la existencia de más empleados bien intencionados aunque frecuentemente menos cuidadosos que toman sus propias decisiones de TI acerca de cómo conectarse, qué descargar y dónde se encuentra la línea de "suficiente seguro", y la infraestructura de TI termina con un sinnúmero de vulnerabilidades potenciales.

[1] IDC Worldwide Mobile Worker population 2011-2015 Forecast (Doc #232073)
[2] Annual State of the Net Survey, Consumer Reports, 2013

Los errores ocurren. Los documentos confidenciales terminarán en las manos equivocadas. Su red está más expuesta que nunca. Los dispositivos sufrirán infecciones, se perderán, o lo que es peor serán robados. Desde la perspectiva de la tecnología de la información, ¿cómo puede asegurarse que la fuerza de trabajo móvil de largo alcance está completamente protegida?

Un enfoque completo de protección consideraría los mejores métodos de securización de los puntos de contacto potenciales que un hacker podría buscar. La implementación óptima sería un enfoque perfecto que proteja todos esos activos usando una única solución integrada.

ENFOQUES ACTUALES PARA LA SEGURIDAD MÓVIL

Hoy en día existen muchas opciones para proporcionar seguridad a los distintos elementos de la experiencia móvil. Existen productos de seguridad para dispositivos y red como Good Technology, Cisco, Zscaler, y Palo Alto Networks, que protegen parte de la experiencia móvil, así como una amplia lista de enfoques de protección de documentos ofertados por una gran variedad de proveedores de programas de cifrado. Sin embargo, todo ellos arrastran una serie de limitaciones significativas.

Para asegurar las conexiones remotas, muchas soluciones móviles consisten en una Virtual Private Network (VPN) básica que conecta con la empresa. La VPN asegura la conexión siempre que los datos que necesita se encuentren dentro de los límites de la oficina. Si sus datos los proporciona un site de tipo software as a service (SaaS), no evitará que sus empleados accedan a ellos fuera de la VPN. Tampoco protege los dispositivos de sus empleados ante la exposición a sitios peligrosos.

Para proteger los datos de la organización que residen en un dispositivo es necesario implementar lo que se conoce como un contenedor. El contenedor separa sus datos corporativos de sus datos personales. Aunque esto permite una separación de lo relativo al negocio y lo personal, no evita que el dispositivo pueda acceder a sitios peligrosos. Tampoco evita los errores humanos a la hora de enviar accidentalmente datos confidenciales al destinatario equivocado.

Para los documentos, el enfoque típico es protegerlos por contraseña usando una solución de un proveedor OEM o del mercado secundario. Una vez que un documento está bloqueado, solo puede desbloquearse introduciendo una contraseña o disponiendo del mismo software de cifrado que utilizó el remitente. Las contraseñas se pierden, se olvidan o quedan expuestas constantemente. Y una vez que alguien tiene la contraseña, ya tiene acceso al documento para siempre.

Para el dispositivo, una organización típica implementará lo que se conoce como Mobile Device Management (MDM). MDM permite que el departamento de TI de la organización tenga el control sobre el dispositivo. Si la organización cree que el dispositivo está en peligro (con independencia de si realmente lo está o no), tienen permiso para borrarlo por completo. Todos sus datos corporativos y personales se perderán. Esto puede suceder incluso si el dispositivo es BYOD y es propiedad del empleado.

Los problemas con las soluciones actuales pueden resumirse con las siguientes deficiencias:

1. **Protección de datos y documentos limitadas** — Los enfoques de protección por contraseña son del tipo configurar y olvidarse. Asumiendo que los usuarios la recuerden, cualquiera que tenga la contraseña — amigo o enemigo — tiene acceso total al mismo para siempre. Como las soluciones de contenedor protegen los documentos que se encuentran en su interior, no proporcionan protección a los documentos que abandonan el contenedor a través de email u otros medios.

2. **Protección limitada frente a las amenazas** — Las soluciones móviles pueden proteger los datos que residen en el dispositivo pero no protegen frente a usuarios que descargan contenido malicioso. Sin una protección frente a amenazas, un dispositivo todavía puede infectarse.

3. **Protección de red limitada** — La mayoría de soluciones del mercado actual dejan brechas de seguridad o protegen la red limitando significativamente la libertad de acceso del empleado.

4. **Elecciones limitadas de TI para los dispositivos en peligro** — Los empleados se ven forzados a aceptar las políticas de "borrado total" incluso en sus propios dispositivos si quieren acceder a la red de la compañía o al correo.

Si sus soluciones actuales aplican las cuatro, dos, o únicamente una de las situaciones anteriores, todavía siguen sin ser lo suficientemente buenas. Y esto es porque el verdadero objetivo es proporcionar una experiencia móvil perfecta que maximice la productividad de los empleados sin comprometer la seguridad. Hoy en día ninguna de las soluciones del mercado proporciona protección de datos, dispositivos y red en una única solución.

SEGURIDAD MÓVIL ÓPTIMA: PROTECCIÓN CONTINUA EN UNA ÚNICA SOLUCIÓN

Asumiendo una cobertura equivalente, cualquier departamento de TI le contará que prefiere gestionar una única solución integrada que varias individuales. Una solución integrada perfecta con múltiples funcionalidades de seguridad móvil es el enfoque preferido. Este tipo de acercamiento es importante, porque cuando se gestiona una red, es vital disponer de un control granular. La granularidad es la capacidad de centrarse en detalle en la gestión de dispositivos individuales o documentos, o ampliar la visión para ver toda la red.

Check Point consciente de ello, ha diseñado una completa solución de seguridad móvil llamada Check Point Capsule. Ésta habilita el acceso fácil a sus datos de la empresa sin interferir con sus datos personales o aplicaciones, amplía las políticas de seguridad interna de su compañía a los dispositivos móviles, y proporciona protección continua para sus documentos corporativos de una forma única en el mercado. Check Point Capsule ha sido diseñada teniendo en mente al usuario y al director de TI. Proporciona la simplicidad y libertad de uso que demanda el usuario, y la granularidad de gestión y seguridad que necesita el departamento de TI. Como solución integrada, Check Point Capsule no es proclive a las brechas de seguridad que normalmente se asocian con los productos individuales integrados de forma poco sólida. Está diseñada para la protección completa.

La experiencia de seguridad móvil completa es lo que verdaderamente diferencia a Check Point Capsule. Las siguientes secciones describen las posibilidades de protección que ofrece. Su facilidad de uso combinada con su protección granular potenciará la productividad de su organización.

FUNCIONALIDADES PRINCIPALES

- Control de acceso seguro para el personal de la empresa
- La información corporativa almacenada localmente se aloja en un entorno de tipo sandbox y se cifra
- Comunicación cifrada integrada para el acceso remoto
- Borrado remoto solo de los datos de la empresa
- Detección y bloqueo de dispositivos móviles rooteados o con jail-break
- Single Sign-On (SSO) para mayor facilidad de uso e incremento de la seguridad
- Soportado en dispositivos Android e iOS

SECURIZANDO DISPOSITIVOS

Muchas empresas no se preocupan en crear una capa de seguridad independiente para los dispositivos móviles de sus empleados. Confían en la seguridad predeterminada que proporciona el dispositivo móvil. Cuando implementan una capa de seguridad adicional, normalmente usan una solución Mobile Device Management (MDM).

Los móviles que se pierden o roban pueden suponer una situación de compromiso para los datos corporativos más sensibles. Solo en EE.UU. más de 4,5 millones de teléfonos móviles se perdieron o se robaron en 2013.[3] El número de teléfonos y tablets que se pierden de forma temporal es mucho más alto. Cuando el empleado es el propietario del dispositivo y se le permite el acceso a la red de la empresa según la política Bring Your Own Device (BYOD), los valiosos datos personales del empleado se mezclan con los datos empresariales en el mismo dispositivo. Cuando un dispositivo se gestiona a través de soluciones MDM, todo el dispositivo podría ser borrado si el departamento de TI sospecha que pudiera estar expuesto. Por el contrario, la mejor solución sería proteger la información empresarial sin afectar a los datos personales guardados en el teléfono en una situación en la que pudiera haber sido perdido o robado.

Check Point Capsule es una aplicación que proporciona un entorno seguro y cifrado para los datos de empresa en dispositivos móviles. Esto evita que se produzcan fugas de información entre los datos personales y los de empresa. Se accede mediante un número de identificación personal (PIN) que es independiente del PIN de bloqueo de la pantalla del móvil. Una vez introducido, el usuario tiene acceso a su correo de empresa, calendario y contactos, además de a los documentos seguros, aplicaciones basadas en Web y la intranet segura de su organización.

Check Point Capsule es fácil de instalar, se configura automáticamente y funciona en cualquier dispositivo móvil iOS o Android. En el caso de que un dispositivo se ponga en peligro o fin de contrato de un empleo, todos los datos y accesos habilitados a través de la aplicación pueden borrarse fácilmente de forma remota sin afectar a los datos personales del empleado.

Las organizaciones que implementan Check Point Capsule se benefician de un aumento en la productividad, resultado de una movilidad que no compromete la seguridad del dispositivo.

[3] Juniper Research, Diciembre de 2013

FUNCIONALIDADES PRINCIPALES

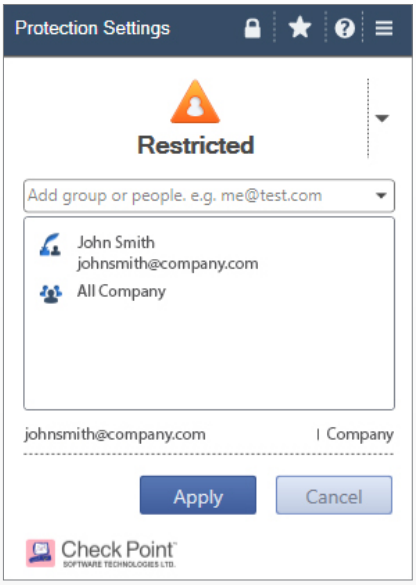
- Securizar los documentos por omisión tras su creación.
- Acceder a los documentos sin contraseñas
- Crear autorización de acceso a los documentos por grupos o de forma particular
- Ver y editar documentos en ordenadores personales, smartphones iOS y Android, y en tablets
- Los permisos pueden definirse para lectura, edición, impresión, cambio de clasificación, eliminar protección, modificación de usuarios autorizados, impresión de pantalla y copiar y pegar.
- Cifrado para proteger datos sensibles
- Monitorizar el acceso al documento y el historial de uso

SECURIZANDO DOCUMENTOS

Hoy en día la mayoría de las organizaciones optan por no proteger en absoluto los documentos, o bien hacerlo mediante el uso de una protección básica por contraseña. Además de tener que recordarlas, el aspecto negativo de las contraseñas es que una vez que alguien las consigue, tiene acceso a ese documento para siempre.

Compartir documentos con compañeros de trabajo, socios y clientes es una actividad del día a día en las empresas. De media se envía información sensible fuera de la organización cada 49 minutos.[4] Casi el 85% de las organizaciones han usado Dropbox para compartir documentos de empresa.[5] Piense en la gran cantidad de medios que existen hoy en día para compartir información y el número de brechas que dejan en la seguridad. Los documentos confidenciales se adjuntan a los correos electrónicos, se comparten en alojamientos en la nube, se transfieren vía FTP o se copian a llaves USB y se intercambian cada día en el trabajo. Una vez que un documento ha abandonado la organización, normalmente no hay información o control sobre QUIÉN accede a él, y de QUÉ OTRAS formas se está compartiendo.

Check Point Capsule proporciona una solución de seguridad de documentos completa. Los usuarios establecen la seguridad cuando crean los documentos. Pueden cifrar los documentos confidenciales, así como definir quién puede acceder a ese documento y qué puede hacer con él. Los destinatarios autorizados pueden acceder sin problemas y usar los documentos sin necesidad de recordar contraseñas. La administración on premise (en las instalaciones) permite a las organizaciones verificar y auditar quién ha compartido documentos, revisar el historial de uso y rechazar el acceso de forma remota. Check Point Capsule también proporciona un seguimiento del documento y controles a través de toda la duración o tiempo de vida del mismo. Los documentos pueden compartirse con total confianza, porque la seguridad sigue al documento a donde quiera que vaya durante su tiempo de vida.



[4] Fuente: Informe de seguridad 2014 de Check Point
[5] Fuente: Informe de seguridad 2014 de Check Point

FUNCIONALIDADES PRINCIPALES

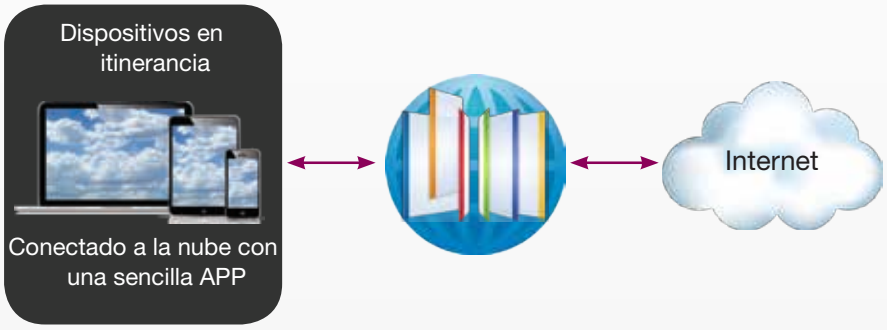
- Amplía la seguridad corporativa a dispositivos móviles en cualquier lugar usando una única política
- Incluye IPS, Control de Aplicaciones, Filtrado URL, Antivirus, Anti-Bot, y Emulación de Amenazas (Threat Emulation)
- Centros de datos por todo el globo para ofrecer el mejor nivel de latencia y rendimiento
- Soportado en plataformas iOS, Android, Windows, y MAC
- Los registros pueden extraerse y almacenarse localmente o verse online
- Integración con Active Directory para el reconocimiento de identidades

PROTEGIENDO LOS DISPOSITIVOS MÓVILES Y SU RED DE LAS AMENAZAS

Sus empleados con dispositivos móviles quieren acceder al mismo tipo de información que acceden los empleados que trabajan en los puestos de las oficinas. Al mismo tiempo, resulta crítico proporcionar a los empleados con alta movilidad el mismo nivel de seguridad que tienen los empleados en las oficinas. Hoy en día, el 93% de las organizaciones poseen dispositivos móviles que acceden a su red, y el 79% ha informado sobre incidentes de seguridad en 2014.[6]

El objetivo es extender las políticas de seguridad de su organización para proteger los dispositivos móviles donde quiera que vayan. Check Point Capsule crea una conexión segura desde su dispositivo móvil. Proporciona un acceso perfecto y direcciona todo el tráfico a través de una nube segura para conseguir una protección completa utilizando las mismas políticas que se aplican en su red corporativa. Esto evitaría que los dispositivos accedieran a archivos y páginas web peligrosas, y protegería los dispositivos del daño de bots y otras ciberamenazas. Anti-bot, Antivirus, Control de Aplicaciones, Filtrado URL, Emulación de Amenazas y el Sistema de Prevención de Intrusiones (IPS) son sistemas que protegen a los usuarios móviles de las amenazas como si se encontraran en las oficinas de la empresa.

Check Point Capsule permite a las organizaciones proporcionar seguridad a través de las operaciones del negocio, proporcionando una protección siempre activa y al día para los usuarios móviles fuera del perímetro de seguridad de su empresa. Check Point es considerada la mejor protección de seguridad de red en su clase según NSS Labs en su último análisis de 2014.[7] Las mismas políticas de seguridad corporativa que protegen su organización se aplicarán a sus dispositivos móviles con Check Point Capsule. La monitorización y gestión de la red y los dispositivos se integra y simplifica a través del sistema de gestión Check Point Security Management.



[6] Informe de estudio sobre seguridad móvil de Check Point 2013
[7] Next Generation Firewall (NGFW) Security Value MapTM (SVM), Informes de análisis comparativos, NSS Labs, 2014

GESTIONANDO LA SEGURIDAD MÓVIL

Contar con una protección móvil completa es algo que resulta cómodo, pero lo sería mucho menos si cada característica requiriera de su propio software de gestión y supervisión. Gestionar una solución móvil integral usando múltiples herramientas software sería muy complicado y costoso para una organización, y conduciría a brechas de seguridad.

Con Check Point Security Management, el departamento de TI posee una única interfaz desde la que se puede supervisar y controlar todos los aspectos de su implementación de Check Point Capsule. Las políticas de seguridad de toda la organización se gestionan desde el mismo panel de control inteligente SmartDashboard. Si la organización está utilizando gateways de seguridad Check Point en sus instalaciones, obtiene el beneficio adicional de llevar las mismas políticas de seguridad corporativa a la nube, y aplicar una única política de seguridad en toda la organización. Si solo utilizan Check Point Capsule, entonces contarán con una interfaz web de fácil uso para configurar las políticas.

Check Point Capsule ofrece una protección móvil completa en una experiencia única e integral. Con Check Point Capsule, los empleados que están fuera o de viaje tendrán las mismas protecciones que en la oficina. Los dispositivos móviles estarán protegidos. Los documentos se encontraran protegidos dentro de los dispositivos e incluso cuando abandonen sus dispositivos, sin tener que enviar o compartir contraseñas. Y lo más importante, su red corporativa permanecerá segura incluso cuando accedan a ella unos pocos, cientos o incluso miles de dispositivos móviles.

RESUMEN

La revolución de la movilidad ya está aquí. La fuerza de trabajo con alta movilidad mundial parece que se incrementará hasta los 1670 millones en 2018, lo que supondrá el 41,8% del número de trabajadores a nivel mundial según Strategy Analytics.[8] Los patrones de uso entre lo que sería una disciplina corporativa y las libertades personales se están difuminando rápidamente. Cada vez se hace más importante proteger su organización de forma proactiva asegurando la fuerza de trabajo móvil.

El Departamento de TI necesita asegurar la red móvil, protegerla de los ataques e infecciones que cada vez se hacen más relevantes en los dispositivos móviles, y proteger los documentos de su organización ahora y en el futuro.

Check Point Capsule combina todas estas capacidades de protección en una única solución integrada. Check Point Capsule crea un entorno seguro móvil que protege a los dispositivos portátiles de las amenazas en cualquier lugar y asegura los documentos de la empresa donde quiera que vayan. En resumen, una solución que ofrece una libertad móvil completa sin comprometer la seguridad.

[8] Global Mobile Workforce Forecast Update 2012-2018, Strategy Analytics, 2014

Acerca de Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd., es el mayor proveedor mundial especializado únicamente en seguridad, que proporciona soluciones líderes en la industria y protege a los clientes de ciberataques con una tasa inigualable de capturas de malware y otros tipos de amenazas. Check Point ofrece una completa arquitectura de seguridad para defender desde las redes empresariales hasta los dispositivos móviles, además de la gestión de la seguridad más intuitiva e integral. Check Point protege más de 100.000 organizaciones de todos los tamaños. En Check Point, aseguramos el futuro.

Oficinas centrales mundiales
5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100

Oficinas EE.UU.
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

Oficinas España
C/Vía de las Dos Castillas, 33 – Edificio Ática 6, Pta. 3ª, Oficina D-1
28224 - Pozuelo de Alarcón (Madrid)

www.checkpoint.com
Email: **info_iberia@checkpoint.com**