BlackBerry | Cybersecurity

Evite las amenazas desde el punto final a la red

con CylancePROTECT y CylanceGATEWAY

DOCUMENTO TÉCNICO

Muchas organizaciones corren peligro de cometer el costoso error de añadir otra capa de defensa a su pila de seguridad. De hecho, añadir más capas de seguridad para abordar nuevas amenazas se ha vuelto tan común que puede parecer la única opción razonable. Con frecuencia, las organizaciones no descubrirán el problema que implica este modo de pensar hasta que sus sistemas deban lidiar con el peso aplastante de mantener un enfoque de defensa exhaustivo. Como la conocida gota que colmó el vaso, cada capa de seguridad nueva requiere de más recursos, conocimientos adicionales e implica costos extra. Esto crea un círculo vicioso del que las organizaciones no pueden salir y en el que no pueden ganar, ya que el mejor resultado requiere comprar nuevas defensas perpetuamente y, el peor, una filtración de datos.

Las organizaciones no deben intentar ganar una carrera armamentista contra los atacantes profesionales a tiempo completo. No deben intentar adaptar una serie de distintas herramientas de seguridad más antiguas a los desafíos creados por la computación móvil, los trabajadores remotos y las políticas de "use su propio dispositivo" (BYOD). De hecho, las organizaciones fuera de la industria de la seguridad cibernética deben dedicar el menor tiempo y la menor cantidad de recursos posible a combatir a los atacantes. Y para esto es precisamente que se diseñaron CylanceGATEWAY™ y CylancePROTECT®. BlackBerry utiliza inteligencia artificial (IA) y acceso a la red de confianza cero (ZTNA) para proteger continuamente a las organizaciones sin interrumpir sus operaciones comerciales.

Cuando el trabajo remoto pasó a ser un factor en las filtraciones de datos, los costos promedio totales del ataque aumentaron USD 1,07 millones, lo que se traduce en un incremento del 27,5 %.

Las organizaciones con un 50 % o más de empleados trabajando de forma remota se demoraron 58 días más en identificar y contener una filtración, lo que representa un incremento del 22 %.

Los desafíos de hoy en día requieren de soluciones modernas

La fuerza laboral actual ha experimentado varios cambios transformadores en los últimos años. Durante la pandemia de 2019, millones de empleados pasaron de la oficina al trabajo en casa. Esta migración impulsó la adopción masiva de servicios y tecnología remotos y móviles, desdibujando la línea entre la tecnología de uso personal y profesional. Varias organizaciones no estaban equipadas para adaptarse de manera segura a semejante volumen de trabajadores remotos, y es posible que al día de hoy sigan teniendo dificultades con eso. Sin embargo, la fuerza laboral remota parece haber llegado para quedarse, según una encuesta de Gartner[1] a distintos CFO; y de ser así, las empresas deben prepararse.

> *"Según el estudio, el 74 % de los CFO planea pasar a algunos de sus empleados al trabajo remoto de manera permanente".*

Muchos de estos empleados utilizarán dispositivos personales y redes que sus empleadores no pueden monitorear o controlar debidamente. Esto puede aumentar de manera significativa los riesgos y costos de una filtración de seguridad. De acuerdo con una encuesta de IBM[2]:

- Cuando el trabajo remoto pasó a ser un factor en las filtraciones de datos, los costos promedio totales del ataque aumentaron USD 1,07 millones, lo que se traduce en un incremento del 27,5 %.
- Las organizaciones con un 50 % o más de empleados trabajando de forma remota se demoraron 58 días más en identificar y contener una filtración, lo que representa un incremento del 22 %.

La cantidad y variedad de puntos finales conectados con la empresa han aumentado de la mano de la fuerza laboral remota. La cantidad de datos de propiedad exclusiva que recorre las redes y se desplaza a la nube crece exponencialmente. Esta expansión de tecnología conectada y distribución de datos fuera del firewall de la empresa acrecienta la superficie de ataque y crea brechas en la arquitectura de seguridad. Los servicios basados en la nube pueden permitir que operaciones empresariales clave se adapten al trabajo desde casa, lo que

las expone a nuevos peligros. Sin embargo, proteger cualquier dispositivo, en cualquier lugar, resulta posible si se piensa en los problemas de seguridad en relación con la confianza.

El colapso del antivirus tradicional

Piense en el enfoque tradicional del castillo y el foso de la ciberseguridad, en el que las defensas se centran en el perímetro de la red. La organización es el castillo, el firewall es el foso y la conexión exterior a Internet es el puente levadizo. Según este modelo, era posible enfocarse de manera segura en fortificar el firewall y analizar todo lo que cruzara el puente levadizo desde más allá. Sin embargo, una vez que se otorgaba acceso a la organización, se daba por sentada su confiabilidad durante toda la interacción.

Esto es similar al modelo de confianza utilizado por las herramientas antivirus (AV) basadas en firmas para identificar archivos peligrosos. Los proveedores de AV seleccionan bibliotecas de hashes (firmas) de archivos peligrosos conocidos. Si un nuevo archivo no coincide con una amenaza conocida, se supone que es seguro. Algunos proveedores emplean un enfoque similar respecto de los sitios web, otorgando o denegando permanentemente el acceso a los empleados basándose en una lista de sitios asociados con actividad maliciosa. Sin embargo, muchas amenazas no son reconocidas hasta que comienzan a hacerse de víctimas. Esto significa que las estrategias que confían en proteger a las organizaciones de amenazas conocidas suelen dejarlas indefensas frente a amenazas desconocidas y de día cero.

Los profesionales de seguridad son testigos de las desventajas de las estrategias de confianza de un solo paso a medida que más empleados trabajan desde ubicaciones remotas con dispositivos de doble uso. Piense en cómo la fuerza laboral cambiante complica algo tan común como confiar en las cuentas de usuarios conocidas:

- Los adversarios utilizan ataques de phishing e ingeniería social para robar credenciales de usuarios y obtener acceso no autorizado a recursos de la red. Cada nuevo dispositivo que almacena credenciales y cada red adicional que las transporta incrementa la superficie de ataque de una organización.
- Las redes hogareñas pueden dar servicio a una serie de puntos finales, incluso a dispositivos de la Internet de las cosas (IoT). Cada punto final conectado necesita estar protegido o excluido en cuanto a su acceso a la organización. La protección de puntos finales sólida de cada dispositivo con acceso a recursos de trabajo es absolutamente esencial para mantener la seguridad. En el pasado, las organizaciones han sufrido ataques de hacking desde dispositivos tan inocuos como el termómetro de un acuario conectado a Internet[4].
- Los usuarios de puntos de acceso de Wi-Fi públicos se exponen a distintos tipos de ataques de intermediarios, incluso cuando el tráfico está cifrado con Seguridad de la capa de transporte (TLS).
- Para realizar su trabajo de manera eficiente, los socios, contratistas y empleados remotos posiblemente necesiten utilizar redes fuera del perímetro de seguridad de la organización. Esto significa que las credenciales y los datos de la organización suelen recorrer redes no administradas y desconocidas.
- Concentrar el tráfico a través del firewall, las aplicaciones de la red a la nube y los servicios de SaaS de una organización, como requieren algunas VPN, es costoso y puede causar cuellos de botella en términos del rendimiento. El problema es especialmente grave para los dispositivos móviles de pocos recursos. En otras palabras, aplicar seguridad de forma retroactiva para abordar el tema de la fuerza laboral móvil requiere de un alto costo y un gran esfuerzo.

> *"Las credenciales comprometidas fueron el vector de ataque más común en 2021, lo que se traduce en un 20 % de todas las filtraciones[3]".*

> *"Los profesionales de seguridad y TI sénior, hasta un 80 % de ellos según algunas estimaciones[5], creen que sus organizaciones continúan vulnerables a los ataques cibernéticos a pesar de las inversiones realizadas para abordar los desafíos del trabajo desde casa".*

La clave para proteger a la fuerza laboral moderna reside en lograr dos objetivos de seguridad: proteger los puntos finales y las redes. Si cualquiera de estas tareas está incompleta, la organización corre peligro.

Proteja la red con confianza cero

Proteger la red con un marco de confianza cero es el primer paso en la creación de una postura de seguridad sólida. Un marco de confianza cero considera a cada usuario, dispositivo, aplicación y participante interno o externo como potencialmente peligrosos hasta que se pruebe lo contrario. Difiere de la autenticación de un solo paso tradicional y de la autenticación (MFA) ya que la confianza se evalúa durante el transcurso de la interacción. Las soluciones de acceso a la red de confianza cero (ZTNA) aplican este principio a la empresa y a todas las entidades con las que esta interactúa. Esto resuelve el problema de intentar establecer la seguridad mediante la verificación, autenticación y protección de una infinidad de dispositivos individualmente. Proteger a cada dispositivo sigue siendo importante, pero esa función la realiza una plataforma de protección de puntos finales (EPP). El enfoque de ZTNA se centra en abordar los riesgos de seguridad de la red asociados con la comunicación entre usuarios, dispositivos y aplicaciones.

Con el ZTNA, se requiere que todos los actores de la red establezcan y mantengan interacciones de confianza a cambio de acceso a recursos internos. Estas interacciones se monitorean continuamente y los cambios en la confianza pueden generar cambios correspondientes en los niveles de acceso u otras acciones de respuesta. Las soluciones de ZTNA combinan un gateway web seguro y un agente de seguridad de acceso a la nube (CASB) para brindar a los usuarios una solución sólida de seguridad como servicio de redes. Los usuarios obtienen acceso a un perímetro de red extendido que los protege a ellos y a sus empleados de los ataques cibernéticos.

Los gateways web seguros utilizan filtrado de URL y otros mecanismos para bloquear el tráfico a destinos de Internet, software o datos en los que no se confía. Al restringir el acceso, evitan la comunicación con entidades que pueden dañar los puntos finales y la infraestructura de TI de una organización.

Los CASB funcionan como intermediarios para los dispositivos y otros puntos finales que acceden a servicios en la nube y aplicaciones de SaaS. Evalúan todo el tráfico entre los puntos finales y las aplicaciones de SaaS, lo que permite a las organizaciones establecer y aplicar políticas de control de acceso y protección de datos.

Un marco de ZTNA puede combinar un gateway web seguro con un CASB y, luego, utilizar IA para validar continuamente la confianza para cada punto final. Es una herramienta poderosa para administrar y mantener la seguridad de la red en el lugar de trabajo y más allá.

Protección de los usuarios fuera de la oficina

La fuerza laboral moderna llegó para quedarse. Habitualmente, los empleados trabajan desde casa, viajan a reuniones o revisan su correo electrónico de forma remota después de horas. Las organizaciones necesitan una solución que aplique políticas de control de acceso centradas en los usuarios. La seguridad eficaz debe proteger a cada dispositivo utilizado por cada empleado mientras estén conectados a redes del trabajo, hogareñas o públicas.

Compatibilidad con aplicaciones en el mercado

Las organizaciones dedican dinero, tiempo y esfuerzos considerables a elegir, desplegar y mantener las aplicaciones que los empleados usan para trabajar. Esto hace que sea importante que las soluciones de seguridad de ZTNA se adapten a las aplicaciones que los empleados ya utilizan. De lo contrario, el costo total de propiedad de una solución de ZTNA aumenta tremendamente debido a que se deben volver a configurar o a desplegar las aplicaciones existentes. Muchas soluciones de seguridad alternativas son muy complejas de implementar. Otras solo pueden enrutar el tráfico desde una cantidad pequeña de aplicaciones. Al solo abordar algunos aspectos del problema más grande, ofrecen menor protección y pueden, al fin de cuentas, tener un costo de despliegue y administración mayor.

Preservación de la batería y el ancho de banda

Los usuarios móviles necesitan maximizar la vida de la batería de sus dispositivos mientras realizan tareas del trabajo. Una solución de ZTNA ofrece una huella ligera que requiere de pocos recursos. Para maximizar la conectividad y el ancho de banda, una solución debe enviar el tráfico a una aplicación de SaaS u otro sitio web sin sobrecargar los recursos de la red o ralentizar las conexiones de redes.

Protección de la privacidad

Las organizaciones quieren proteger sus datos privados, incluso de quienes confían para protegerlos. Para mantener la integridad de los datos, las empresas necesitan de una solución que detecte de manera confiable las amenazas en el tráfico de TLS sin descifrarlo ni comprometer la privacidad.

Control de acceso a aplicaciones

Es importante asegurarse de que solo los usuarios de confianza tengan acceso a aplicaciones de SaaS empresariales. Al mismo tiempo, debe seguir siendo fácil conectarse a servicios sin necesidad de que los usuarios se autentiquen varias veces. El control de acceso a aplicaciones (y la segmentación de la red) ayuda a evitar el movimiento lateral dentro de una red. La segmentación puede ocultar aplicaciones y direcciones IP para evitar que se descubran, reduciendo la superficie de ataque. Esto ofrece una capa de protección adicional que no está disponible cuando se utiliza una VPN, que brinda acceso a la red. Un usuario de VPN potencialmente obtiene acceso a cada recurso de la red. El ZTNA limita los permisos a aplicaciones y direcciones IP en particular mediante la segmentación.

CylanceGATEWAY, ZTNA impulsado por IA

CylanceGATEWAY brinda ZTNA impulsado por IA para proteger aplicaciones privadas alojadas en las instalaciones o en la nube. La solución nativa en la nube ofrece acceso solo saliente y escalable a cualquier aplicación, ocultando activos críticos de usuarios no autorizados y minimizando la superficie de ataque. Facilita la configuración y administración de políticas dinámicas y conscientes del contexto, a la vez que permite controles de acceso granulares. Además, CylanceGATEWAY se integra o coexiste de manera fluida con otras soluciones de ciberseguridad, como CylancePROTECT, para una protección de la red a los puntos finales completa.

¿Cómo funciona CylanceGATEWAY?

CylanceGATEWAY actúa como un gateway web seguro y un CASB en línea para proteger puntos finales, datos y la red más amplia. Protege dispositivos y puntos finales mediante el bloqueo del acceso a destinos en Internet con contenido inaceptable o malicioso. Se pueden restringir los sitios web que no cumplen con la política de uso aceptable de una organización incluso cuando los usuarios no están conectados directamente a la red empresarial.

CylanceGATEWAY protege los datos mediante el uso de políticas de control de acceso a la red continuas. Sus capacidades de IA brindan monitoreo de la confianza continuo para proteger a los usuarios, las redes, las aplicaciones de SaaS y otros recursos basados en la nube. Si una entidad actúa de una manera no confiable, se pueden invocar pasos de corrección automatizados y preconfigurados para proteger los recursos empresariales.

Los administradores controlan CylanceGATEWAY a través de la consola de administración basada en la nube compartida por muchos productos de seguridad de puntos finales de Cylance®. Aprovechan la IA de Cylance® para determinar si las conexiones del usuario son seguras. Los administradores también pueden establecer manualmente políticas de control de acceso a la red con un marco de ACL expresivo y bloquear a usuarios para evitar que se conecten a sitios no deseados, si así lo prefieren. Las políticas y reglas de acceso pueden definirse a nivel de la organización, el grupo y el usuario.

Las aplicaciones instaladas en un dispositivo iOS®, Android™, Windows® 10 o macOS® se comunican con CylanceGATEWAY, el cual reside en la infraestructura de BlackBerry®. Cuando las aplicaciones intentan realizar una conexión, CylanceGATEWAY utiliza políticas automatizadas y gestionadas por el administrador para bloquear la conexión, o bien, enrutarla a su destino. Proteger conexiones de puntos finales a través de CylanceGATEWAY es una manera eficaz de proteger dispositivos personales que se conectan a recursos laborales. Si bien una organización no puede controlar completamente los dispositivos propios (BYOD) y la tecnología del trabajo desde casa, CylanceGATEWAY ayuda a garantizar que esos dispositivos no se conecten con entidades peligrosas.

Bloqueo de conexiones maliciosas e inseguras

CylanceGATEWAY bloquea las conexiones de dispositivos a destinos de Internet no deseados. Por ejemplo, si un usuario hace clic en un enlace de correo electrónico malicioso, CylanceGATEWAY puede bloquear la conexión a ese destino. El motor de riesgo de IA en la nube de BlackBerry utiliza la reputación de IP y otros métodos para actualizar continuamente una lista de destinos de Internet inseguros. Esto alivia a los administradores de la carga de tener que mantener manualmente listas de destinos de Internet bloqueados.

Si una organización quiere impedir que los usuarios visiten sitios específicos, puede crear políticas de control de acceso para restringir destinos adicionales. Esto permite a los administradores evitar que todos los usuarios, usuarios específicos o grupos de usuarios accedan a sitios prohibidos, incluso si iniciaron sesión en una red externa.

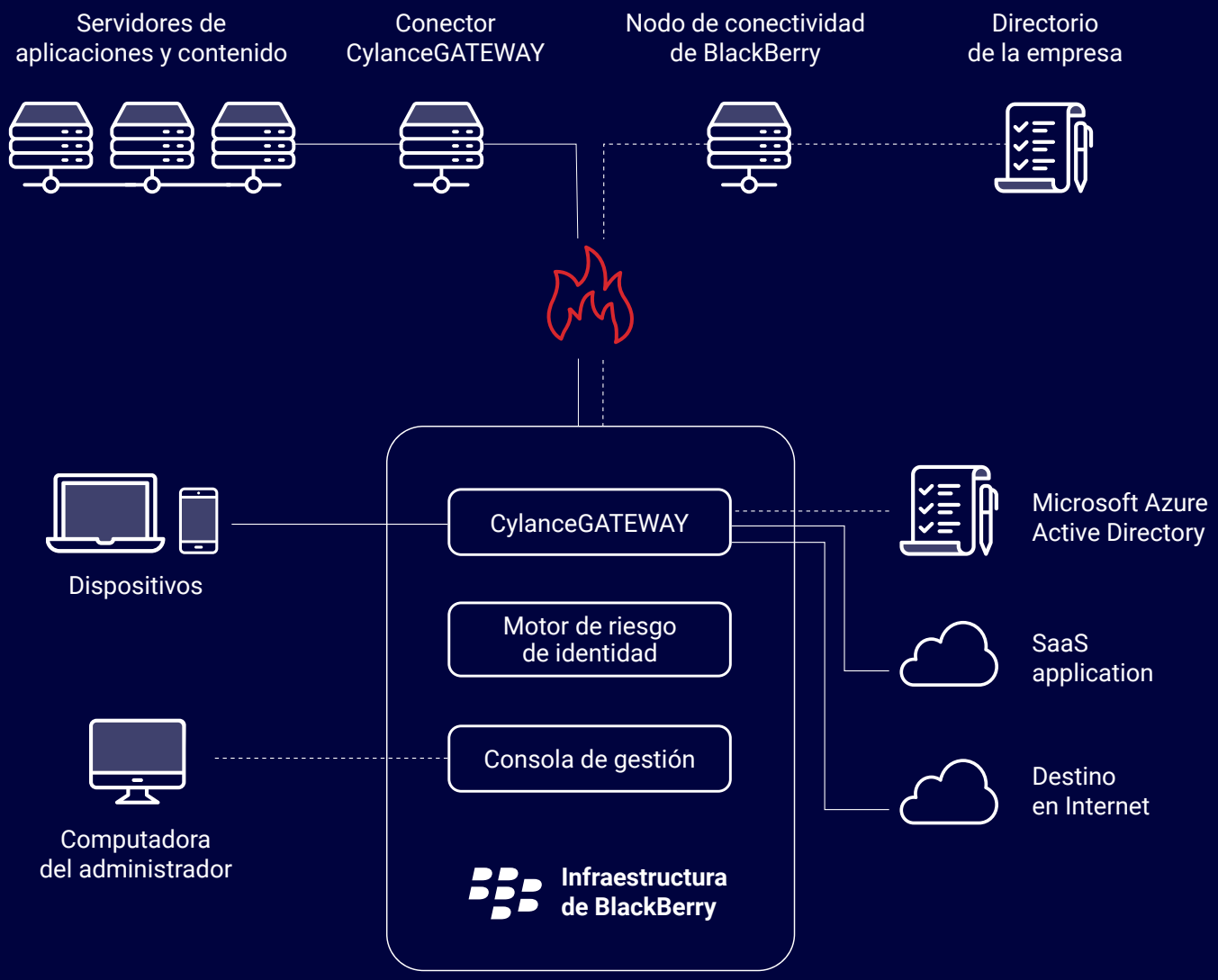
Protección de las conexiones a servicios de SaaS

CylanceGATEWAY protege el acceso a las aplicaciones en la nube de una organización mediante el análisis de la confianza de cada conexión solicitada (según el modelo de confianza cero o Zero Trust) en tiempo real. Por ejemplo, si un usuario móvil abre una aplicación de calendario de Office 365® para ver su cronograma, la aplicación de CylanceGATEWAY establecerá un túnel seguro a la infraestructura de BlackBerry. Si la IA de CylanceGATEWAY no detectó comportamiento anómalo reciente, permitirá que se realice la conexión.

CylanceGATEWAY también admite asignación de IP de origen al reenviar conexiones a servicios en la nube. Por ejemplo, CylanceGATEWAY proporciona direcciones IP de origen seguras y dedicadas para aplicaciones de SaaS que restringen el acceso por dirección IP. Simplemente se denegará el acceso a los dispositivos que intenten conectarse desde direcciones no especificadas.

Protección de conexiones a una red privada

CylanceGATEWAY puede brindar control de acceso a una red privada cuando se instala el conector de CylanceGATEWAY opcional detrás de un firewall o de redes privadas en la nube. Esto establece un túnel seguro entre la infraestructura de BlackBerry y la red privada conectada. El conector de CylanceGATEWAY permite a los usuarios comunicarse rápidamente con servidores de aplicaciones y contenido detrás de un firewall que utiliza CylanceGATEWAY en lugar de una VPN tradicional.



CylanceGATEWAY también brinda servicios de redes de túnel completo o dividido. Esta función brinda versatilidad a las organizaciones respecto del manejo de una combinación de comunicaciones empresariales y personales. El modo de túnel completo ofrece máxima protección al resguardar todas las comunicaciones entre el usuario y la red. La opción de túnel dividido permite a los administradores designar recursos específicos para una comunicación segura, a la vez que deja el resto del tráfico abierto, como las aplicaciones de uso personal.

CylanceGATEWAY admite el registro de privacidad de usuarios para dispositivos personales y VPN por aplicación, brindando así una gama de opciones de despliegue a la vez que permite que solo los usuarios autenticados de dispositivos saludables accedan a los recursos de la empresa.

Detección de amenazas a la red

CylanceGATEWAY ofrece detección de amenazas a la red de tres maneras distintas:

- Reputación del destino: Evita que los usuarios accedan a enlaces maliciosos.
- Reglas de IDS/IPS: Detecta y frustra ataques potenciales en las áreas de movimiento lateral, exfiltración de datos y comando y control.
- Anomalías conductuales (mediante IA/AA): Alerta a los administradores cuando se observan actividades inusuales.

Proteja los puntos finales con CylancePROTECT

Proteger los puntos finales es el segundo paso en la creación de una postura de seguridad sólida capaz de brindar protección contra las amenazas modernas. Las herramientas AV tradicionales que confían en coincidencia de firmas y técnicas de heurística no pueden proteger a los puntos finales de las amenazas modernas. CylancePROTECT utiliza la tecnología de IA de Cylance de séptima generación para detectar y prevenir la ejecución de malware en sistemas Microsoft® Windows®, macOS® y Linux®. Además, protege a los puntos finales con scripts avanzados y control de aplicaciones, protección de vulnerabilidades de memoria y funciones de control de dispositivos.

Mediante el despliegue de agentes de seguridad de IA directamente en los puntos finales, la protección está todo el tiempo asegurada sin tener que confiar en búsquedas en la nube o en la conexión a la red. CylancePROTECT puede detectar y prevenir más del 99 % del malware antes de que se ejecute, incluso los ataques de día cero, independientemente de la conectividad de los puntos finales. La IA de Cylance les brinda a los puntos finales una ventaja predictiva por sobre las amenazas, lo que significa que sus capacidades actuales son eficaces contra el malware que todavía no existe. En las pruebas, versiones más antiguas y sin alterar de CylancePROTECT seguían siendo eficaces en la prevención de amenazas que no aparecieron sino más de dos años después.

CylancePROTECT® Mobile es una solución de detección de amenazas móviles (MTD) que brinda a los usuarios de iOS y Android protección contra amenazas impulsada por IA avanzada a nivel de los dispositivos y las aplicaciones. Ambos productos ayudan a garantizar que el acceso a los recursos de la red solo sea posible desde puntos finales que no se han visto comprometidos. Proteger puntos finales con IA predictiva y la red con confianza cero crea un sistema de defensa sólido contra una multitud de ataques cibernéticos.

Cómo CylanceGATEWAY y CylancePROTECT utilizan IA para proteger dispositivos

CylanceGATEWAY reside en la ruta de acceso a datos de la red, utiliza la IA de Cylance para modelar los niveles de confianza de un usuario basándose en distintos factores y ajusta los niveles de acceso de forma acorde. También suma indicadores de amenazas a lo largo del entorno para descubrir amenazas potenciales y aplicar la corrección adecuada en tiempo real.

Factores conductuales

Los factores conductuales comparan las acciones actuales de un usuario con su actividad normal y la de sus colegas. Por ejemplo, ¿el usuario se conectó anteriormente a esta red? ¿Es un horario o día de la semana normal en que el usuario debe estar trabajando? ¿Es este comportamiento congruente con sus acciones pasadas y las de otros empleados?

Identificación de anomalías

La IA de Cylance detecta anomalías en los patrones de datos, comportamiento y otras fuentes. Dado que CylanceGATEWAY está en la ruta de acceso a datos, examina los patrones de uso que pueden indicar una posible amenaza. Tiene en cuenta parámetros múltiples y los enmarca de manera inteligente según el contexto. Empleando distintas técnicas,

CylanceGATEWAY puede identificar intrusos, empleados maliciosos y bots, y detenerlos antes de que causen daños. Esta capacidad integra la red empresarial con el marco de seguridad con prioridad en la prevención más amplio, posible gracias al ZTNA y la IA avanzada.

Puntuaciones de riesgo

CylanceGATEWAY calcula continuamente las puntuaciones de riesgo de los usuarios basándose en varios factores. Permite que los usuarios seguros se conecten a destinos de Internet y se autentiquen con recursos en la nube usando los controles de acceso normales de la organización. Si un cambio aumenta la puntuación de riesgo, CylanceGATEWAY reevalúa los niveles de confianza y actúa de acuerdo con las políticas establecidas. Por ejemplo, CylanceGATEWAY puede notificar a los administradores de actividad anómala, limitar o denegar acceso a recursos o solicitar pasos de autenticación adicionales.

Proteja a su organización con CylancePROTECT y CylanceGATEWAY

CylanceGATEWAY protege las redes a ambos lados del firewall empresarial. Bloquea a los intrusos y los empleados maliciosos e impide que accedan a datos de la organización. Además, detiene a los bots y otras formas de malware que infectaron a un punto final para evitar que alcancen servidores de comando y control. CylancePROTECT evita que esos dispositivos se infecten con malware de día cero, amenazas sin archivos y scripts maliciosos. Juntos, ofrecen visibilidad y seguridad con prioridad en la prevención a todos los puntos finales y las conexiones a los recursos de la red y la nube para brindar prevención contra amenazas cibernéticas de primer nivel.

Para obtener más información sobre cómo defender su organización desde los puntos finales a la red, visite blackberry.com/defend-your-network.

[1]La encuesta de Gartner a los CFO revela que un 74 % planea pasar a algunos de sus empleados al trabajo remoto de maneara permanente

[2]IBM Security 2021 Cost of a Data Breach Report (Informe de Seguridad de IBM sobre el costo de una filtración de datos del 2021)

[3]IBM Security 2021 Cost of a Data Breach Report (Informe de Seguridad de IBM sobre el costo de una filtración de datos del 2021)

[4]Hackean a un casino a través del termómetro de un acuario

[5]Cybersecurity at a Crossroads: The Insight 2021 Report (La ciberseguridad en una encrucijada: el informe de Insight 2021)

BlackBerry. Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) brinda servicios y software de seguridad inteligente a empresas y gobiernos por todo el mundo. La compañía protege a más de 500 millones de puntos finales, lo que incluye a más de 215 millones de vehículos. Con sede en Waterloo, Ontario, la compañía emplea IA y aprendizaje automático para brindar soluciones innovadoras en las áreas de la seguridad cibernética, soluciones de seguridad y privacidad de datos, y es líder en los campos de gestión de seguridad, gestión de puntos finales, cifrado y sistemas incorporados. La visión de BlackBerry es clara: garantizar un futuro conectado en el que pueda confiar.

BlackBerry. Seguridad inteligente. En todas partes.

Para obtener más información, visite BlackBerry.com y siga @BlackBerry.

BB23 | 220718