BlackBerry | Cybersecurity

CylancePROTECT

Seguridad de puntos finales preparada para el futuro

FICHA TÉCNICA

Los ataques de ransomware han escalado un 62 % año tras año, con el consecuente impacto en empresas de todos los tamaños[1]. La complejidad de estos ataques también se ha profundizado. Los ataques adversariales de IA aprovechan las limitaciones de las soluciones de seguridad actuales. Las herramientas antivirus tradicionales requieren firmas y técnicas de heurística; sin embargo, esto presupone que ya se conocen todos los tipos de ataques posibles. Pero, en los tiempos que corren, el malware muta a diario, o incluso a cada hora, lo que hace que las herramientas basadas en firmas resulten obsoletas. Esto crea la necesidad de contar con un enfoque basado en la prevención más sólido respecto de la seguridad de los puntos finales. Se han desarrollado nuevas soluciones para puntos finales de última generación, pero estas soluciones confían en conexiones en la nube y son vulnerables a ataques complejos que pueden infectar los sistemas.

BlackBerry ha redefinido qué puede y debe brindar a las organizaciones una solución de protección de puntos finales al utilizar un modelo automatizado enfocado en la prevención. Este enfoque, encabezado por la solución CylancePROTECT® y con el soporte de un modelo de IA probado y maduro, ofrece 100 % de protección según lo informado por SE Labs[2]. CylancePROTECT evita las fugas deteniendo el ransomware, el phishing y las amenazas de día cero al mismo tiempo que brinda protección contra ataques basados en scripts, sin archivos, de memoria y mediante dispositivos externos. CylancePROTECT hace todo esto, con o sin conexión, en puntos finales en los que se ejecuta Windows®, MacOS®, Linux®, Android™ o iOS®, facilitando la protección total en toda la organización.

Capacidades

Análisis del sistema programados y a pedido

- La flexibilidad se une al cumplimiento, la calidad y los procesos de clientes que requieren análisis de seguridad integrales del sistema en momentos específicos.

Control de scripts

- Mejore la protección Macro 4 mediante la identificación de scripts maliciosos en documentos Excel y determine las medidas apropiadas a seguir.
- Detenga y evite que se ejecuten scripts no autorizados
- Benefíciese de las capacidades de “listas blancas” y listas seguras granulares
- Admita MacOS, Microsoft® y Linux
- Prevenga la ejecución de comandos PowerShell de una única línea

Protección de memoria

- Identifique y detenga en forma proactiva el uso malicioso de la memoria
- Prevenga los ataques de solo memoria como el escalamiento de privilegios
- Benefíciese de realizar exclusiones granulares y mejorar los informes y la resolución de problemas

CylancePROTECT PARA DISPOSITIVOS DE ESCRITORIO

El modelo de algoritmo que utiliza CylancePROTECT significa que no hay firmas, ejecución de parches, análisis del sistema o puntos finales lentos debido a que la solución de seguridad se ejecuta en ellos. Los clientes que han hecho el cambio de productos antivirus tradicionales reactivos basados en firmas han visto un ROI de hasta el 99 %, una reducción de la cantidad de imágenes de máquinas del 97 %, un desempeño de hardware y batería prolongado, y una reducción del 90 % en las horas de personal que se requieren para administrar la solución[3].

La arquitectura de CylancePROTECT consiste en un único agente ligero que se administra a través de la consola en la nube basada en software como un servicio (SaaS) de BlackBerry. La consola en la nube se integra fácilmente con herramientas de seguridad y sistemas de administración de software existentes. Existen opciones de administración híbrida y en las instalaciones disponibles para entornos desconectados (air-gapped). El agente de puntos finales detectará y prevendrá el malware en el host, independientemente de si hay una conexión a la nube y sin la necesidad de actualizaciones continuas. CylancePROTECT es capaz de detectar malware y colocarlo en cuarentena ya sea en redes abiertas, aisladas o virtuales. El enfoque basado en el aprendizaje automático de BlackBerry detiene la ejecución de código dañino sin importar si se tiene conocimiento previo o si se emplea una técnica de ofuscación desconocida. Ningún otro producto antimalware se compara con la precisión, facilidad de administración y eficiencia de CylancePROTECT.

La arquitectura de CylancePROTECT consiste en un único agente ligero que se administra a través de la consola en la nube basada en software como un servicio (SaaS) de BlackBerry.

Capacidades

Control de aplicaciones

- Bloquee dispositivos con funciones fijas
- Visualice el inventario de aplicaciones total, ya sea en toda la organización, o en un punto final específico
- Evite binarios dañinos o la modificación de un binario
- Bloquee sistemas específicos y restrinja cualquier cambio

Aplicación de políticas de uso de dispositivos

- Controle el uso de dispositivos de almacenamiento masivo USB
- Prevenga el robo de datos a través de medios extraíbles

Controles de acceso basado en los roles (RBAC)

- Minimice el riesgo con administración de roles más granular con RBAC personalizado
- Mejore las restricciones de acceso a la red basado en los roles de los usuarios individuales
- Limite los derechos de acceso de los empleados a solo la información que necesitan para realizar su trabajo
- Benefíciese de que los usuarios existentes no se vean impactados

Protección de Android mejorada

- Análisis de malware de Android™ e informe de amenazas por SMS
- Atestación de Samsung Knox®

Integración con Intune

- Identifique los riesgos o vulnerabilidades y saque provecho de Intune para remediar según la condición de riesgo del dispositivo.

CARACTERÍSTICAS DE CylancePROTECT

Evita que se ejecuten cargas útiles de día cero a través de un modelo resiliente basado en IA.

Aplicación de políticas de uso de dispositivos

Controla qué dispositivos se pueden utilizar en el entorno y elimina los dispositivos externos como posibles vectores de ataques.

Prevención de malware impulsada por IA

Utiliza IA probada en el campo para analizar toda aplicación que intente ejecutarse en un punto final antes de que logre hacerlo.

Identifica en forma proactiva el uso malicioso de la memoria (ataques sin archivos) con respuestas de prevención automatizada inmediatas.

Gestión de scripts

Mantiene control total de cuándo y dónde se ejecutan los scripts en el entorno.

Control de aplicaciones para dispositivos con funciones fijas

Garantiza que los dispositivos con funciones fijas se mantengan en perfecto estado en forma continua y elimina la desviación que ocurre cuando hay dispositivos no administrados.

Capacidades

Tienda de aplicaciones de UEM para Android y escaneo de malware de APK

- Examina todas las aplicaciones de la tienda de aplicaciones de UEM de BlackBerry®, lo que incluye las aplicaciones personalizadas y de clientes, y las protege contra malware.

Detección de phishing y URL maliciosas

- Utiliza la IA para detectar automáticamente y detener URL maliciosas, lo que incluye a aquellas con elementos de suplantación de identidad (phishing) incorporados.

Creación segura de aplicaciones

- Permite a socios y compañías desarrollar aplicaciones seguras y personalizadas para dispositivos accesibles para la empresa.

Verificación de integridad de aplicaciones de IOS® para aplicaciones de BlackBerry Dynamics SDK

- Garantiza la integridad de las aplicaciones desarrolladas en la plataforma BlackBerry® Dynamics™ SDK.
- Permite que se carguen en los dispositivos únicamente aplicaciones seguras e impide que se manipulen aplicaciones de BlackBerry.

CylancePROTECT PARA DISPOSITIVOS MÓVILES

Ahora, más que nunca, las organizaciones están utilizando dispositivos móviles para competir en un mercado ágil y en evolución, y para mantener a sus empleados conectados. Por primera vez, más de la mitad de todos los dispositivos conectados a Internet son móviles[4]. Al mismo tiempo, los ataques de suplantación de identidad (phishing) a través de dispositivos móviles son más predominantes que nunca antes, con un incremento de incidentes del 300 % en América del Norte solo en el último año[5]. Mientras que, históricamente, el enfoque de las soluciones de seguridad empresariales se mantuvo en los dispositivos de escritorio, cada vez más empresas descubren la amenaza creciente de los ataques de phishing de malware que apuntan a dispositivos móviles, en especial dentro de aplicaciones.

El daño causado por estos ataques puede ser significativo, teniendo en cuenta los índices cada vez mayores y sin precedentes de filtración de información de identificación personal (PII) y otros datos críticos.

Esto lleva a que cada vez más organizaciones adopten una inspección profunda de paquetes (DPI) y otras capacidades para protegerse contra ataques maliciosos.

No resulta sorprendente, por lo tanto, que el mercado de defensa ante amenazas móviles (MTD) muestre un crecimiento tan marcado. La MTD ofrece una capa adicional de seguridad al prevenir, detectar, remediar y mejorar la higiene de seguridad general para los distintos niveles de la flota móvil y las aplicaciones de una organización.

La solución de MTD de Blackberry, CylancePROTECT® Mobile, incrementa la seguridad de referencia que brinda la UEM de BlackBerry al abordar las amenazas maliciosas avanzadas en los dispositivos móviles. CylancePROTECT Mobile monitorea los ataques a nivel del dispositivo y las aplicaciones y va más allá de la seguridad que brindan los contenedores de aplicaciones básicos.

- A nivel del dispositivo, CylancePROTECT Mobile identifica las vulnerabilidades de seguridad y las posibles actividades maliciosas al monitorear las actualizaciones del sistema operativo, los parámetros del sistema, las configuraciones de los dispositivos y las bibliotecas del sistema.
- A nivel de las aplicaciones, CylancePROTECT Mobile utiliza sandboxing de aplicaciones y análisis de código, así como pruebas de seguridad de aplicaciones, para identificar malware y grayware.

Además, CylancePROTECT Mobile identifca todo malware que pueda ingresar a través de aplicaciones de carga lateral, malware único basado en firmas o simulaciones, añadiendo así una capa de seguridad adicional a la plataforma BlackBerry Dynamics SDK. Esto permite a socios y compañías desarrollar aplicaciones seguras y personalizadas que pueden cargarse en dispositivos accesibles para la empresa.

CASOS COMUNES DE USO DE CylancePROTECT

CylancePROTECT brinda una prevención de amenazas de espectro completo que detiene las filtraciones de puntos finales al resolver los siguientes casos de uso:

- identificar y bloquear archivos ejecutables maliciosos sin la necesidad de realizar actualizaciones constantes o de una conexión a la nube;
- identificar las vulnerabilidades de seguridad y las posibles actividades maliciosas al monitorear las actualizaciones del sistema operativo, los parámetros del sistema, las configuraciones de los dispositivos y las bibliotecas del sistema;
- controlar dónde, cómo y quién puede ejecutar scripts;
- administrar el uso de dispositivos USB e impedir que se utilicen dispositivos no autorizados;
- detener ataques de malware sin archivos;
- bloquear dispositivos con funciones fijas como quioscos, terminales de POS, etc.;
- prevenir los ataques de día cero y el ransomware;
- detener los ataques y las vulnerabilidades basadas en la memoria;
- utilizar sandboxing de aplicaciones y análisis de código, así como pruebas de seguridad de aplicaciones, para identificar malware y grayware;
- identificar todo malware que pueda ingresar a través de aplicaciones de carga lateral, malware único basado en firmas o simulaciones;
- proteger los puntos finales ya sea que los usuarios estén o no conectados.

CONOZCA MÁS

CylancePROTECT es apenas una de nuestra amplia gama de soluciones de seguridad de primera línea que ofrece BlackBerry. Obtenga más información sobre nuestra selección completa de paquetes de seguridad que le brindan a su organización seguridad inteligente, en todas partes.

[1] https://www.cisa.gov/uscert/sites/default/files/publications/AA21-243A-Ransomware_Awareness_for_Holidays_and_Weekends.pdf

[2] https://www.blackberry.com/us/en/products/cylance-endpoint-security/se-labs-breach-response-report

[3] https://www.blackberry.com/us/en/success-stories/2019-forrester-tei-report

[4] https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

[5] https://www.blackberry.com/us/en/forms/enterprise/report-bb-2022-threat-report-aem

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.

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

BB23 | 2200825