DOCUMENTO TÉCNICO: **SEPTIEMBRE 2020**

Conseguir más por menos

Simplificar la seguridad de los terminales a través de una plataforma en la nube

vmware® Carbon Black

Índice

Introducción. 3
VMware Carbon Black Cloud 4
Nuestro factor diferenciador: técnicas de análisis del comportamiento . . . 4
Nuestro factor diferenciador: protección superior 5
Nuestro factor diferenciador: visibilidad procesable. 6
Nuestro factor diferenciador: operaciones simplificadas 7
Servicios que se pueden prestar a través de VMware Carbon Black Cloud 8
NGAV y EDR conductual 8
Supervisión y clasificación de alertas 8
EDR empresarial 9
Auditoría y corrección 9
Conclusión 9

Introducción

Los profesionales de TI y de seguridad saben que el panorama de las amenazas es dinámico. Cada día, los atacantes se vuelven más listos e inventan nuevas técnicas para evitar que les detecten. Ahora que los ataques sin programa malicioso y en memoria constituyen el 72 por ciento de las vulneraciones[1], los antivirus tradicionales ya no bastan para proteger los sistemas. De hecho, menos de un tercio de las organizaciones creen que los antivirus tradicionales puedan detener los ataques avanzados con programas de secuestro que son tan comunes hoy en día.[2]

Para hacer frente a este mayor riesgo, muchas organizaciones han optado por añadir más productos a la pila de seguridad que ya tenían, aumentando así el coste y la complejidad de los entornos. Actualmente, el 60 por ciento de las organizaciones empresariales usan por lo menos 25 herramientas diferentes de ciberseguridad para gestionar, investigar y responder a las amenazas a la seguridad.[3] Lamentablemente, esta complejidad no guarda correlación con la eficacia por varios motivos.

1. Demasiados silos
   Contar con diversas soluciones no es suficiente si no pueden funcionar de forma conjunta. Las organizaciones trabajan con datos, sistemas y consolas que funcionan de forma aislada. En caso de tener que realizar una investigación, los profesionales tienen que trabajar con conjuntos de datos dispares de múltiples soluciones de seguridad. Esto lo convierte en una tarea complicada y dilatada que, en última instancia, no ofrece bastante información sobre el contexto en el que se ha producido el incidente.
2. Gestión complicada
   Tener diversos sistemas y productos es una carga para los profesionales de TI y de seguridad. Supone una complejidad excesiva y mucha formación. De hecho, más de la mitad de las organizaciones que tienen implementadas más de 50 soluciones de seguridad definen su coordinación de la seguridad como «muy complicada» y, a causa de esto, casi la mitad (el 49 por ciento) de las alertas legítimas no se corrigen.[4] Esto implica un riesgo considerable para la organización, ya que las personas dedican menos tiempo a lo importante.
3. Efecto sobre el rendimiento de los terminales
   La ejecución de múltiples sistemas acaba sobrecargando a los terminales. Cuantos más agentes se añaden, más lentos se vuelven. Los análisis antivirus y otros modelos de protección requieren una potencia de procesamiento excesiva y, si se produce un problema, la visibilidad limitada que proporcionan estos sistemas supone una importante pérdida de productividad, sobre todo si se tienen que volver a crear imágenes de las máquinas. Algunos usuarios desactivarán por completo la seguridad de los terminales; una situación que, en el mejor de los casos, supone un incumplimiento y, en el peor, abre las puertas a una vulneración grave.

La mayoría de los equipos de TI y de seguridad tienen dificultades para contratar suficiente personal de seguridad cualificado. El 32 por ciento de los profesionales de la ciberseguridad creen que su organización está llevando a cabo las acciones necesarias para hacer frente a los efectos que tiene la falta continuada de conocimientos en ciberseguridad.[5] Además, los profesionales que ejecutan varias soluciones aisladas sobrecargan tanto a su reducido personal que no le permiten ser efectivo. Con un mercado tan escaso, los recursos cualificados tienen que centrarse en las actividades de seguridad esenciales y no se les debe sobrecargar con la tarea de intentar descifrar la información procedente de varios sistemas dispares.

Por si fuera poco tener que abordar estos desafíos en cuanto al personal, además los equipos de TI y de seguridad tienen diferentes exigencias. Sucede con demasiada frecuencia que estos profesionales se enredan en discusiones interminables sobre las concesiones que implica añadir una nueva herramienta de seguridad. Los profesionales de TI centran sus esfuerzos en el rendimiento de las máquinas y la productividad de los usuarios finales, mientras que a los profesionales de seguridad les preocupa tener la información adecuada y el control necesario para detener los ataques y proteger los datos.

---

1. Verizon: «2019 Data Breach Investigations Report», mayo de 2019.
2. Ponemon Institute: «The 2017 State of Endpoint Security Risk», noviembre de 2017.
3. Resumen de ESG: «Security Infrastructure and Market Changes in Progress», agosto de 2020.
4. Cisco: «2018 Annual Cybersecurity Report», febrero de 2018.
5. Informe de investigación de ESG: «The Life and Times of Cybersecurity Professionals 2020», junio de 2020.

«Uno de nuestros objetivos era consolidar nuestros productos de seguridad. Lo que conseguimos con VMware Carbon Black fue combinar varios sistemas en uno solo. El factor que realmente lo diferenciaba de otras soluciones que analizamos fue su capacidad de seguir el ritmo de las nuevas amenazas».

WILLIAM BOCASH
RESPONSABLE DE TI
STONEWALL KITCHEN

Cuando el equipo de seguridad quiere añadir una nueva herramienta que requiere la implementación de un nuevo agente, a menudo el equipo de TI difiere y obliga al equipo de seguridad a sustituir a un agente ya implementado o a dedicar mucho tiempo a defender el valor que el nuevo producto aportará a la empresa. Este tipo de negociación puede convertirse en una discrepancia política entre departamentos que acaba afectando negativamente a las funciones principales de ambos.

En resumen: los profesionales de TI y de seguridad quieren hacer más tareas, pero se ven limitados por los trabajadores, los recursos y los efectos en los terminales que supondrá añadir más herramientas y agentes.

Las organizaciones necesitan una solución más sencilla y flexible. Una solución que pueda eliminar las desavenencias entre el equipo de TI y de seguridad y que les permita unir fuerzas en una empresa con una única fuente fiable. Una solución que sea fácil de usar y configurar, que ofrezca suficiente flexibilidad para admitir una amplia gama de servicios de seguridad para terminales, que incluya suficientes opciones de personalización para ajustarla a las circunstancias específicas de cada organización, y que crezca y se pueda ampliar fácilmente según las necesidades y la madurez de la seguridad. Todo ello sin tener que añadir agentes, implementaciones ni formación adicionales.

VMware Carbon Black Cloud

Simplificación de la seguridad de terminales consolidada

En VMware, somos conscientes del estado actual de la seguridad de terminales y hemos diseñado una solución que se encuentra en una posición privilegiada para satisfacer las necesidades actuales.

VMware Carbon Black Cloud™ es una plataforma de protección de terminales (EPP) nativa de nube, que combina el refuerzo inteligente de la seguridad del sistema con la prevención de comportamientos necesaria para mantener a raya las amenazas emergentes, mediante un solo agente ligero y una consola fácil de usar. En vez de tener que implementar una serie de productos, cada uno con una configuración y una política propias, esta solución ofrece varias funciones de seguridad a través de una plataforma común en la nube que comparte un sensor, una consola de nube y un conjunto de datos. A medida que cambian los requisitos, es muy fácil y sencillo añadir nuevos servicios. Así se elimina la necesidad de invertir capital de nuevo o de implementar nuevos agentes.

La plataforma está creada en un completo conjunto de datos de terminales que se puede usar y compartir entre diferentes herramientas y servicios, tanto si son de VMware como de otros proveedores. De este modo se crea una única fuente fiable y aporta contexto a la seguridad en general. Esta plataforma se construyó con el convencimiento de que la seguridad debe crecer y cambiar según el panorama de las amenazas va evolucionando.

Nuestro factor diferenciador: técnicas de análisis del comportamiento

Una cámara de videovigilancia en el terminal

En VMware, nos centramos en comprender los patrones de comportamiento de los atacantes que nos permitan detectar y detener en tiempo real ataques nunca vistos. ¿Cómo se puede evitar un ataque sin archivos sin comprender la forma en la que se ha ejecutado? ¿Cómo se puede reconocer algo nunca antes visto usando tan solo datos históricos de ataques? Para proporcionar la mejor seguridad posible, es importante comprender la forma de actuar de los atacantes. Por eso el análisis del comportamiento es la base de todo lo que hacemos.

Para hacer posible este análisis, recopilamos datos exhaustivos sobre los terminales. Una seguridad eficaz de los terminales se sustenta sobre los datos completos y la visibilidad detallada que proporcionan.

VMware Carbon Black Cloud no tiene igual. La mayoría de soluciones de seguridad de los terminales solo empiezan a registrar los datos cuando determinan que una actividad es sospechosa. Este enfoque suele pasar por alto actividades anteriores que son esenciales para diagnosticar la causa principal. Cuando surge un problema, ya sea con la seguridad de los terminales o la ciberintegridad, es difícil investigarlo rápidamente y obtener información sobre los nuevos patrones de ataque. En cambio, esta plataforma examina continuamente la actividad del terminal, tanto si parece que se desarrolle con normalidad como si no, y analiza los comportamientos. Así los profesionales de seguridad disponen del contexto y la confianza necesaria para defender los sistemas.

Se analizan 200 terabytes de datos de terminales en la nube. Es decir, multiplicamos por 13 la cantidad de iMessages procesados.

Se analizan a diario 500 000 millones de eventos de seguridad. Es decir, multiplicamos por 150 la cantidad de búsquedas de Google que se pueden realizar durante el mismo período.

VMware ha pasado casi una década entera desarrollando y puliendo la capacidad de recopilar ingentes cantidades de datos de forma fiable, analizarlos de forma rentable y almacenarlos de forma segura, y además hacerlo sin que la red se vea afectada. Al utilizar el potencial de la nube, somos capaces de analizar más de 200 terabytes de datos sobre terminales y más de 500 000 millones de eventos de seguridad a diario. Es decir, multiplicamos por 13 la cantidad de iMessages procesados y por 150 la cantidad de búsquedas de Google que se pueden realizar durante el mismo período. Estas potentes técnicas de análisis refuerzan los varios servicios de seguridad de terminales que se ofrecen en la plataforma nativa de nube.

Nuestro factor diferenciador: protección superior

Detenga más ataques, recupere el control de los terminales y no se preocupe tanto

Nuestro enfoque único proporciona una ventaja a la hora de proteger los terminales. Al analizar los patrones de comportamiento de los atacantes, VMware Carbon Black Cloud puede detener los ataques, ya sean ataques vistos con anterioridad o no. Además, ofrece visibilidad sobre cómo han ido evolucionando esos ataques. Esta visibilidad nos permite detectar nuevas formas de ataques, desarrollar las defensas de seguridad de forma constante y ofrecer a nuestros clientes un control personalizable de la situación de seguridad. De este modo, las organizaciones se pueden preparar para enfrentarse en el futuro a adversarios que cambian constantemente sus métodos.

Lo logramos aplicando aprendizaje automático y modelos de comportamiento para analizar los datos de los terminales e identificar actividades maliciosas, lo que nos permite detener todo tipo de ataques antes de que afecten a los sistemas esenciales. El análisis de transmisiones procede del procesamiento de flujos de eventos, una técnica que lleva años implementada en varios sectores, desde la detección de fraudes relacionados con tarjetas de crédito hasta la negociación de alta frecuencia. Al centrarse en el análisis continuado del comportamiento en vez de las detecciones de momentos específicos, la plataforma puede reconocer cuándo una serie de acciones que han sucedido a lo largo del tiempo son sospechosas. La plataforma detiene los ataques tanto con programa malicioso como sin él, también los ataques que sacan partido del software benigno para llevar a cabo acciones maliciosas. Por ejemplo, un ataque que utilizase un intérprete de comandos como PowerShell para buscar y cifrar todos los archivos del disco se podría ejecutar por completo de forma remota sin que ninguno de los archivos fuera detectado por cualquier tipo de prevención basada en firmas. Sin embargo, el proceso que ejecutase los comandos podría mostrar de todas formas patrones de comportamiento parecidos a un programa de secuestro. Esto se detectaría y se detendría. Las amenazas a la plataforma, los patrones de amenazas y los indicadores que puedan pasar desapercibidos a los antivirus tradicionales y de aprendizaje automático, se pueden identificar dirigiendo la atención hacia la causa principal de los ataques. A posteriori, estos conocimientos se pueden aplicar para predecir mejor los ataques futuros.

VMware Carbon Black Cloud ofrece protección inmediata (para quien quiera configurarla y olvidarse de ella) y la opción de aplicar políticas muy personalizables. Esto permite a las organizaciones abordar específicamente las deficiencias o los puntos ciegos para trastocar ataques futuros. Los profesionales de TI y de seguridad pueden crear políticas de control personalizadas para grupos de trabajo concretos de su entorno, controlar la frecuencia de las actualizaciones y definir exactamente los tipos de procesos que se permite o no se permite ejecutar, así como la forma de manejar la ejecución que no sea de confianza. Por ejemplo, a las aplicaciones desconocidas se les podría denegar cualquier tipo de operación, o se les podría permitir que se ejecutaran pero no que establecieran ninguna conexión de red ni invocaran a los intérpretes de comandos. Este nivel de control granular garantiza que los profesionales que necesitan un control específico de sus máquinas lo puedan tener, a la vez que se detienen los ataques avanzados. A la hora de proteger los terminales, es importante reconocer que existen muchas maneras de recopilar inteligencia para la detección de amenazas y de utilizar todos los recursos disponibles. Más de 75 de los proveedores líderes mundiales en respuesta a incidentes usan VMware Carbon Black para investigar vulneraciones cada día, lo que les proporciona información sobre los ataques más recientes. La unidad de análisis de amenazas dedicada de VMware Carbon Black utiliza esta información y estudia más a fondo las tendencias actuales de los ataques, para asegurarse de que nuestros análisis estén al día en todo momento y evolucionen para proteger contra ataques nuevos. Además, nuestros clientes tienen acceso a una comunidad de usuarios que cuenta con más de 30 000 expertos en seguridad, lo que permite a los miembros interactuar entre ellos y enterarse de la información y la inteligencia más actuales.

Nuestro factor diferenciador: visibilidad procesable

Refute conjeturas y elimine deficiencias de seguridad, rápidamente

VMware Carbon Black Cloud identifica las nuevas amenazas, da prioridad a los ataques más graves y ofrece visibilidad detallada de la cadena de ataques, lo que permite a los profesionales comprender, investigar y corregir los ataques rápidamente.

Las herramientas aisladas pueden dificultar que se entienda bien lo que sucede en los terminales y obligan a los profesionales a descifrar la información necesaria, que procede de varias fuentes. Sin embargo, nuestra plataforma ofrece una visión completa de lo ocurrido en el pasado y de lo que ocurre en el presente. Gracias a las posibilidades que ofrece un entorno de TI completo, los profesionales de seguridad obtienen una visibilidad detallada del estado de los terminales. Así, pueden eliminar las deficiencias y los puntos ciegos, acelerar las investigaciones y la corrección, y lograr una reducción considerable del tiempo de permanencia.

Todos los profesionales de seguridad salen beneficiados con esa visibilidad, pero en especial el personal que persigue las amenazas y el que responde a los incidentes, que necesita tener un acceso rápido y claro a los datos para investigar las amenazas, perseguirlas y corregirlas. Con nuestro enfoque, las investigaciones que suelen tardar días o semanas se pueden completar en cuestión de minutos. Las sofisticadas funciones de detección combinan inteligencia para la detección de amenazas personalizada y suministrada en la nube, listas de seguimiento automatizadas e integraciones con el resto de la pila de seguridad para adaptar de forma eficiente las labores de persecución en toda la empresa.

El rápido y ágil proceso de búsqueda y focalización de la plataforma, que incluye jerarquías y plazos, permite comprender bien cómo se ha ejecutado el ataque. Averiguar exactamente dónde ha estado un atacante y qué ha hecho, así como identificar la causa principal, son tareas fáciles que se completan en cuestión de minutos para poder eliminar rápidamente las deficiencias que hay en las defensas. Al poder investigar y corregir cualquier terminal de forma remota, los profesionales de seguridad pueden reducir la implicación de los profesionales de TI y se elimina la creación de imágenes y los tiques de soporte innecesarios.

La plataforma, para ampliar y complementar los datos de eventos del sistema operativo que recopila de forma continua, ofrece herramientas para compilar información adicional que no se recopila ni es recomendable recopilar de forma continua. Gracias a las funciones de auditoría y corrección en tiempo real, a los equipos de seguridad y de TI les resulta más rápido y sencillo evaluar el estado del sistema y cambiarlo para fortalecer su entorno contra las amenazas más relevantes. Esta posibilidad de crear consultas personalizadas ofrece visibilidad de los detalles particulares sobre el estado actual de todos los dispositivos y cargas de trabajo, tanto los que se encuentran en la red como los que no. A continuación, los profesionales pueden responder a esta información aislando los sistemas infectados para impedir el desplazamiento lateral, creando un Secure Shell remoto en cualquier terminal, recopilando y almacenando datos forenses adicionales para la investigación tras el incidente, o ejecutando scripts para la corrección completa.

Los administradores también tienen la opción de hacer consultas acotadas a grupos concretos de dispositivos o incluso a dispositivos específicos. De este modo, el usuario puede empezar con un enfoque general y después pasar a uno más granular, centrándose solo en las máquinas importantes dentro de la investigación o la auditoría en particular.

Al tener las herramientas adecuadas para recopilar rápidamente toda la información necesaria para comprender bien un ataque y tomar medidas inmediatas de forma remota, los profesionales pueden reducir el tiempo de permanencia y minimizar el riesgo en su entorno.

«[VMware Carbon Black] nos proporciona una única consola, [de modo que resulta más fácil] gestionarlo y consolidarlo todo desde un solo sitio. […] Podemos revisar el sistema de los usuarios y realizar investigaciones de forma remota. Eso en realidad nos ayuda a hacer análisis directamente en el terminal y a la vez tomar medidas inmediatas».

HAARIS FAIZAN
INGENIERO SÉNIOR DEL CENTRO DE OPERACIONES DE CIBERSEGURIDAD
ST. GOBAIN

Nuestro factor diferenciador: operaciones simplificadas

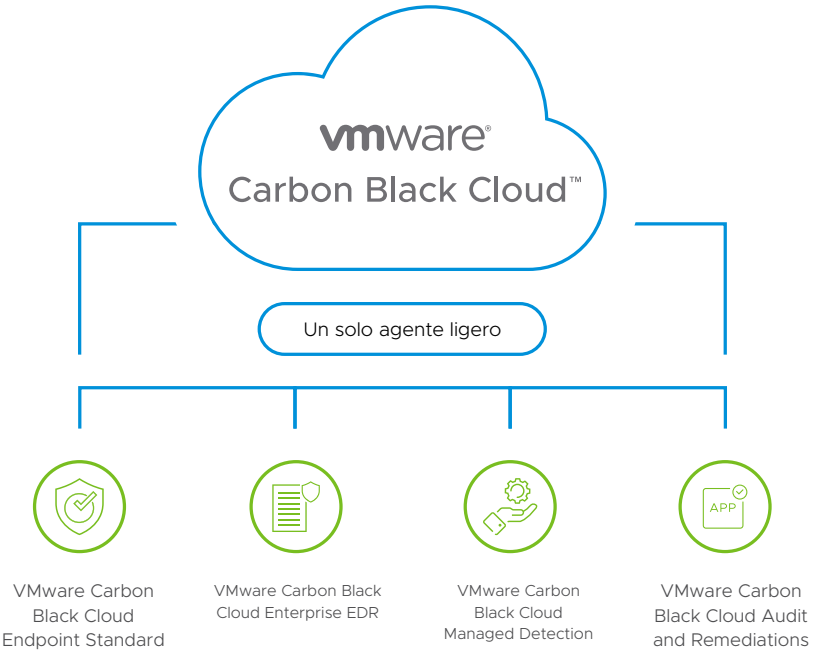

FIGURA 1: diagrama de los productos VMware Carbon Black Cloud.

Elimine la complejidad de tener distintos proveedores y la proliferación de agentes

Si bien la mayoría de programas de seguridad para terminales requieren varios sistemas aislados entre sí que son un estorbo para los usuarios finales y complican la gestión, VMware Carbon Black Cloud proporciona una única plataforma consolidada que satisface diversas necesidades de seguridad de los terminales. Aunque algunos proveedores de antivirus han empezado a usar consolas basadas en la nube, no están aprovechando todas las ventajas que ofrece la nube para las operaciones y los análisis de seguridad. Además, otros proveedores se autodenominan «plataformas» cuando en realidad operan como una suite de productos independientes. A diferencia de esas soluciones, nuestra plataforma nativa de nube ofrece varios servicios a través de un solo sensor ligero que permite a las organizaciones consolidar los productos de seguridad. Nuestra consola unificada y centralizada proporciona a los profesionales acceso a numerosas funciones y al completo conjunto de datos.

Esta plataforma facilita la implementación de varios servicios de seguridad sin poner en riesgo el rendimiento de los terminales. No es necesario comprar ni poner en marcha una infraestructura local y nuestras políticas predefinidas se personalizan rápidamente para ajustarse a cualquier entorno. Además, cuando una organización decide que ha llegado el momento de ampliar las funciones de seguridad, puede añadir nuevas características sin interrupciones, nuevos sensores ni costes de implementación.

VMware Carbon Black Cloud se adapta automáticamente a los nuevos ataques para que los terminales continúen protegidos sin necesidad de actualizaciones manuales. Atrás queda la carga de tener que distribuir grandes actualizaciones de firmas. Nuestra protección automática contra las amenazas más nuevas y avanzadas ofrece a las organizaciones acceso a las nuevas características actualizadas en cuanto están disponibles.

Mejore la situación de seguridad

Cuando las herramientas de seguridad pueden colaborar entre ellas, ofrecen mayor visibilidad, más contexto y, en última instancia, mejor protección en general. A diferencia de las soluciones tradicionales que se encuentran en silos, nuestra plataforma es extensible y se basa en API abiertas, de modo que se integra fácilmente con el resto de la pila de seguridad de las empresas. Hay muchas integraciones prediseñadas de

varios proveedores de soluciones líderes como, entre otros, IBM, Splunk, LogRhythm o ForeScout. Esta visibilidad compartida permite comprender los problemas que afectan a los equipos de seguridad y de TI para reducir la fricción y simplificar los flujos de trabajo. Al añadir contexto que otras soluciones no ofrecen, los profesionales de seguridad y de TI pueden sacar más partido a sus datos. El acceso a datos sin filtrar agiliza la investigación y el análisis y permite identificar y corregir más ataques.

Por ejemplo, la estrecha integración con IBM QRadar permite a los administradores utilizar soluciones líderes de detección y respuesta en los terminales (EDR) y de antivirus de nueva generación (NGAV). Estas soluciones les sirven para ver y detectar actividad de los terminales directamente desde la consola de QRadar, así como para tomar medidas. Cuando la situación lo requiere, los analistas de seguridad pueden hacer correcciones inmediatamente en el punto en riesgo desde la consola de QRadar, aprovechando así los flujos de trabajo y agilizando la respuesta.

Aparte de las integraciones, los datos recopilados del terminal se pueden exportar rápidamente de los flujos de datos de la plataforma para usarlos según las integraciones y los tratamientos personalizados de cada cliente. Las API abiertas permiten a las organizaciones crear paneles de gestión personalizados para la generación de informes y la gestión integradas. Y también permiten crear nuevos flujos de trabajo que respaldan y mejoran sus programas de seguridad. Cuando se unifican las operaciones de seguridad de las herramientas de seguridad, la situación general de seguridad de una organización puede mejorar drásticamente y reducir el tiempo de permanencia y el riesgo.

Servicios que se pueden prestar a través de VMware Carbon Black Cloud

NGAV y EDR conductual

La solución de NGAV y EDR conductual de VMware Carbon Black utiliza aprendizaje automático y modelos de comportamiento para analizar los datos de los terminales e identificar la actividad maliciosa que le permita detener todo tipo de ataques antes de que afecten a los sistemas esenciales.

VMware ofrece una prevención potente y flexible que puede evitar los ataques perpetrados con y sin programas maliciosos y mediante programas de secuestro. Los evita automáticamente, tanto si el terminal tiene conexión como si no, desde cualquier sitio del mundo. Asimismo, se mantiene siempre al día en el ámbito de las amenazas, siempre en constante cambio, con el fin de bloquear nuevos ataques que no se hayan visto antes y que a otras soluciones se les pueden pasar por alto. Las funciones líderes de VMware dirigidas a la detección y respuesta revelan la actividad de las amenazas en tiempo real, de modo que las organizaciones puedan responder a cualquier tipo de ataque en cuanto se identifique. La causa principal de un ataque se puede desvelar en cuestión de minutos a través de visualizaciones en las que se muestra cada fase del ataque con detalles de la cadena de ataque fáciles de seguir. VMware Carbon Black Cloud Endpoint™ Standard permite a los administradores clasificar inmediatamente las alertas aislando los terminales, creando una lista de aplicaciones no permitidas o cancelando procesos. Los profesionales pueden usar Secure Shell para acceder a cualquier terminal dentro o fuera de la red, así como para llevar a cabo investigaciones completas y recomendaciones de forma remota.

Supervisión y clasificación de alertas

El servicio de supervisión y clasificación gestionadas de alertas que ofrece VMware Carbon Black proporciona a los clientes un equipo de expertos en seguridad de VMware de primer orden que colaboran estrechamente con las organizaciones que necesitan más recursos para validar las alertas y establecer prioridades, identificar nuevas amenazas y agilizar las investigaciones.

Los expertos de VMware ubicados en Estados Unidos analizan las alertas procedentes de VMware Carbon Black Cloud, las validan y establecen prioridades. Esto ayuda a garantizar que a las empresas no les pase por alto ninguna amenaza importante. El servicio añade a las alertas un contexto adicional generado por personas, como puede ser relacionar las alertas con la misma causa principal, ayudar a optimizar las operaciones o resolver los

MÁS INFORMACIÓN

Para programar una demostración personalizada o probar un producto gratis en su organización, visite *carbonblack.com/request-a-demo.*

Para obtener más información o comprar productos VMware Carbon Black, llame al +44-118-908-2374 en EMEA o al +1-855-525-2489 en Estados Unidos, escriba un correo electrónico a *contact@carbonblack.com* o visite *carbonblack.com/products/vmware-carbon-black-cloud*.

problemas de seguridad. Los expertos en amenazas de VMware identifican de forma proactiva las amenazas mediante la supervisión de la actividad de las amenazas en millones de terminales, los consejos sobre ataques generalizados y la detección y confirmación retroactivas de nuevas amenazas basándose en técnicas de detección iterativas. En los informes mensuales se resumen los datos sin filtrar de las alertas y se convierten en recomendaciones prácticas que ayudan a los profesionales de seguridad a tener una visión más completa y a seguir mejorando la eficacia.

Enterprise EDR

VMware Carbon Black® Cloud Enterprise EDR™, nuestra solución para perseguir amenazas y responder a incidentes (IR), ofrece visibilidad continua para los centros de operaciones de máxima seguridad y profesionales de IR.

Las investigaciones que suelen tardar días o semanas se pueden completar en cuestión de minutos. Carbon Black Cloud Enterprise EDR correlaciona y visualiza amplia información sobre los eventos en terminales para ofrecer a los profesionales de TI y de seguridad más visibilidad de sus entornos. El sofisticado método de detección que incluye la solución permite usar la supervisión de indicadores de vulneraciones (IoC) con la inteligencia para la detección de amenazas de su elección, como pueden ser sus propias fuentes personalizadas. En esta solución, el reconocimiento automatizado de las tácticas, las técnicas y los procedimientos (TTP) de Carbon Black Cloud Endpoint Standard se amplía con datos y herramientas de investigación detallada que ayudan a comprender los ataques actuales y los patrones de ataque a más largo plazo. Gracias a la función para perseguir amenazas de VMware Carbon Black Cloud, los profesionales tienen la capacidad de responder y corregir en tiempo real para así detener los ataques activos y subsanar los daños rápidamente.

Auditoría y corrección

VMware Carbon Black® Cloud Audit and Remediation™, nuestra solución de evaluación y corrección en tiempo real, permite a los equipos de seguridad y de TI evaluar y cambiar el estado del sistema para reforzar el entorno a fin de hacer frente a las amenazas más relevantes. De este modo los equipos pueden analizar sin esfuerzo los dispositivos, las cargas de trabajo y los contenedores, y contraponerlos a los estándares o las normativas desde una única consola para minimizar los riesgos y simplificar los informes operativos en todo el parque informático.

Carbon Black Cloud Audit and Remediation ofrece a los administradores una visibilidad muy detallada del estado actual de todos los terminales. Automatiza los informes operativos en niveles de parches y evalúa la ciberintegridad de TI. Al combinarlo con las funciones de VMware para perseguir amenazas, Carbon Black Cloud Audit and Remediation proporciona un nivel sin precedentes de visibilidad que agiliza la investigación y la persecución de amenazas.

Conclusión

VMware Carbon Black Cloud utiliza los datos sin filtrar de todos sus productos de seguridad para proporcionar a los clientes lo siguiente:

- Protección superior mediante el uso de análisis de transmisiones y modelos predictivos para anticiparse a las amenazas más sofisticadas
- Visibilidad procesable para agilizar las investigaciones y permitir a los profesionales responder ante las amenazas con total confianza gracias a una visión completa de los eventos pasados y presentes
- Operaciones simplificadas mediante la consolidación de varias funciones en la nube usando una única consola, un solo agente y un solo conjunto de datos en los terminales
- Extensibilidad de la plataforma gracias al uso de integraciones prediseñadas y API abiertas para compartir datos en la pila de seguridad y sacar el máximo partido

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304, USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es