VMWARE WORKSPACE ONE TRUST NETWORK

Seguridad para el espacio de trabajo digital en evolución

PRESENTACIÓN GENERAL

VMware Workspace ONE™ Trust Network™ les ofrece a las organizaciones un enfoque moderno e integral de la seguridad empresarial para sus empleados, aplicaciones, terminales y redes. Workspace ONE Trust Network aumenta las capacidades de seguridad inherente de la plataforma inteligente de Workspace ONE mediante una red enriquecida de soluciones de socios integradas que ofrece monitoreo continuo del riesgo y rápida respuesta de mitigación en el espacio de trabajo digital, ya que cuenta con capacidades para proteger, detectar y remediar amenazas modernas.

VENTAJAS CLAVE

Workspace ONE Trust Network simplifica la seguridad y la administración con un marco de confianza y verificación. Con Workspace ONE Trust Network, las organizaciones de TI pueden lograr lo siguiente:

- Eliminar silos de solución de seguridad con un marco basado en la acción que proporciona una vista integral y reduce la complejidad del espacio de trabajo digital
- Combinar de manera exclusiva acceso, administración y seguridad de aplicaciones y dispositivos con información y automatización para reducir los riesgos en toda una red de computación de usuario final
- Aprovechar una red de socios abierta y confiable y seguir usando inversiones existentes, lo que ayuda a reducir los costos

Seguridad: el obstáculo más grande en su estrategia de espacio de trabajo digital moderno

Un espacio de trabajo digital puede quintuplicar[1] la productividad de los empleados, ya que les ofrece un acceso simple y seguro a las aplicaciones y los datos desde el dispositivo que prefieran. A medida que las organizaciones siguen avanzando hacia la transformación digital, la red de espacio de trabajo digital que abarca empleados, aplicaciones, terminales y redes sigue creciendo y evoluciona más allá del perímetro tradicional, con tendencias comunes tales como la adopción de dispositivos propios del usuario final (Bring Your Own Device, BYOD) y la proliferación de TI. Y a medida que el perímetro tradicional se desvanece, comienzan a aparecer ciberamenazas avanzadas, como los ataques de día cero, ataques de tipo "man in the middle" (MITM), suplantación de identidad, bots y ransomware.

La seguridad es la prioridad principal de inversión en movilidad y espacio de trabajo digital[2]. Sin embargo, las herramientas de seguridad existentes solo le ofrecen a TI una visibilidad limitada, ya que se concentran únicamente en silos de seguridad que proporcionan funcionalidad heredada. Como resultado, se logra una estrategia de parches que impacta sobre las organizaciones con altos costos, debido a su complejidad y a que se requieren tareas manuales para proteger un espacio de trabajo digital. Por lo tanto, la seguridad se ha convertido en el obstáculo más grande para la estrategia del espacio de trabajo digital moderno.

Seguridad predictiva e integral en la organización sin perímetros

Se debe cumplir un nuevo conjunto de requisitos para satisfacer las necesidades de seguridad sin comprometer la experiencia de usuario:

1. Para obtener una vista integral, las organizaciones deben usar un marco que establezca confianza entre los componentes que brindan seguridad en su red.
2. Y, para reducir los riesgos de manera constante, las organizaciones deben ser capaces de tener en cuenta la información de su entorno a fin de tomar decisiones predictivas y automatizadas respecto a la seguridad de su espacio de trabajo digital.

Workspace ONE Trust Network les ofrece a las organizaciones un enfoque moderno e integral de la seguridad empresarial para sus empleados, aplicaciones, terminales y redes. Workspace ONE Trust Network ofrece un conjunto de capacidades para prevenir, detectar y remediar las amenazas modernas en el espacio de trabajo digital en evolución, con base en un marco de confianza y verificación. Cuando se establece la confianza en el espacio de trabajo digital, el resultado es un sistema interconectado de menor privilegio que fortalece los empleados haciendo que la seguridad los siga. Para administrar los riesgos relacionados con las ciberamenazas modernas, Workspace ONE Trust Network combina información de la plataforma inteligente de Workspace ONE con soluciones de seguridad de socios de confianza para ofrecer seguridad automatizada y predictiva en el espacio de trabajo digital.

1 Fuente: https://www.vmware.com/radius/impact-digital-workforce/

2 Encuesta para compradores de tecnología móvil de CCS Insights, diciembre de 2017

Proteger, detectar y remediar

La pregunta no es si una organización deberá enfrentar un ciberataque: la pregunta es cuándo. Con este panorama en mente, los equipos de seguridad y operaciones de TI pueden administrar los riesgos de ciberseguridad mediante la simplificación del mapeo de funciones de seguridad. Por ejemplo, se usa un marco como NIST Cybersecurity Framework para obtener competencias proporcionadas por Workspace ONE Trust Network:

- Las competencias de seguridad comienzan por la protección de un espacio de trabajo digital, lo cual incluye evitar malware que use aprendizaje de máquinas, evitar la filtración de datos de aplicaciones basadas en la nube empresarial y proteger las redes de microsegmentación de las amenazas persistentes avanzadas (advanced persistent threats, APT).
- El uso de monitoreo continuo y adaptativo les permite a los equipos de seguridad y operaciones de TI detectar amenazas en aplicaciones y terminales de escritorio y móviles cuando dichas amenazas ingresan al espacio de trabajo digital.
- Una vez que se ha detectado la amenaza, Workspace ONE Trust Network puede automatizar la corrección; de esta manera, se aprovecha un potente motor de decisiones. Cuando la detección de un ataque se basa en anomalías del comportamiento, se puede iniciar una política automatizada para bloquear el acceso a los datos corporativos.

Unificación de la administración y la seguridad de dispositivos, aplicaciones y accesos con técnicas de análisis

Workspace ONE Trust Network combina las capacidades de seguridad inherentes de la plataforma inteligente de Workspace ONE, que incluyen administración y seguridad de aplicaciones, dispositivos y accesos con técnicas de análisis, para conectar de manera exclusiva silos de administración creados por las soluciones de seguridad. El servicio de Workspace ONE Intelligence service impulsa técnicas de análisis en la plataforma de Workspace ONE y proporciona recomendaciones, correlación y agregación de datos de espacio de trabajo para ofrecer información integrada y automatización. Mediante la integración de las capacidades de Workspace ONE Trust Network con el servicio de Intelligence, las organizaciones pueden ofrecer monitoreo continuo de riesgos de seguridad y respuestas rápidas de mitigación en el mundo sin perímetros de la actualidad.

Un motor de decisiones ayuda a correlacionar información, como dispositivos corporativos fuera de la red con comportamiento del usuario, para detectar amenazas y automatizar la corrección mediante políticas de acceso. La información integrada de datos de amenazas y el estado detallado de cumplimiento del dispositivo ofrecen una forma sencilla de identificar y reducir problemas de seguridad en tiempo real y, de esta manera, mejorar la higiene de seguridad del espacio de trabajo digital. Con el motor de decisiones, TI puede generar normas para automatizar y optimizar tareas comunes, como corregir terminales de Windows 10 vulnerables con un parque fundamental y configurar controles de acceso condicionales para aplicaciones y servicios a nivel individual o grupal.

Aprovechamiento de la red enriquecida de soluciones de socios de confianza

Para lograr una seguridad integral en todo el espacio de trabajo digital, se debe establecer confianza entre los componentes que brindan seguridad alespacio de trabajo digital, que está en evolución y crecimiento. Workspace ONE Trust Network aprovecha las interfaces de programación de aplicaciones (Application Programming Interface, API) integradas en la plataforma de Workspace ONE para proporcionar un marco de confianza. Estas API permiten que Workspace ONE se comunique con una red enriquecida de soluciones de seguridad y, en última instancia, le ofrecen a los administradores la vista integral que desean para simplificar la seguridad y la administración. Mediante la conexión de silos de soluciones de seguridad, los clientes pueden aprovechar las inversiones existentes para mejorar de manera exponencial el monitoreo constante y el análisis de riesgos para obtener tiempos de respuesta más rápidos. Como resultado, se obtiene una estrategia de seguridad predictiva basada en tendencias y patrones que se puede escalar con implementación.

MÁS INFORMACIÓN

Si desea obtener más información sobre Workspace ONE Trust Network, visite: https://www.vmware.com/latam/products/workspace-one/security.html

Pruebe un Hands-on-Lab gratis: https://www.vmware.com/go/workspace-hol

PARA OBTENER MÁS INFORMACIÓN O PARA ADQUIRIR PRODUCTOS DE VMWARE,

LLAME AL
877-4 -VMWARE (fuera de Norteamérica, llame al +1-650 -427-5000),

VISITE
http://www.vmware.com/latam/products o haga una búsqueda en línea para encontrar un revendedor autorizado.

Funciones clave

Las organizaciones pueden aprovechar estas capacidades de seguridad fundamentales que ofrece Workspace ONE Trust Network para impedir, detectar y remediar el panorama de ciberamenazas en evolución.

COMPETENCIA	DESCRIPCIÓN
Una plataforma básica de espacio de trabajo digital que conecta soluciones de seguridad	Simplifique la seguridad y la administración con un marco de confianza en el que se aprovechan las API para establecer una comunicación entre una red de seguridad abierta y Workspace ONE.
Administración de accesos que simplifica el negocio	Ofrezca a TI las herramientas necesarias para suministrar aprovisionamiento de aplicaciones, un catálogo de autoservicio, autenticación de factores múltiples e inicio de sesión único (Single Sign-on, SSO) para todas las aplicaciones.
Optimización de la experiencia de usuario y la seguridad con políticas contextuales	Controle la autenticación mediante políticas de acceso condicional basadas en el estado de cumplimiento del dispositivo, la solidez de la autenticación del usuario, la privacidad de datos, la ubicación del usuario y más.
Políticas de prevención de pérdida de datos (DLP) para evitar la filtración de datos	Introduzca políticas de cifrado de datos en el nivel del dispositivo, cifrado de datos y seguridad de hardware. Configure políticas, incluidas cifrado de datos en el nivel del dispositivo, emparejamiento de dispositivos, seguridad de WiFi y cumplimiento de TLS. Monitoree en busca de amenazas de malware, aplicaciones maliciosas, ataques en la memoria o dispositivos con jailbreak y corrija automáticamente con un bloqueo remoto, borrado del contenido del dispositivo, bloqueo de acceso o controles personalizables de cuarentena de dispositivo.
Seguridad de aplicaciones sin sacrificar la experiencia de usuario	Utilice los controles de seguridad que se incluyen en las aplicaciones seguras de productividad de VMware: VMware Boxer™, Browser™ y Content Locker™. Detecte amenazas y automatice el proceso de corrección para demás aplicaciones y servicios de computación en nube.
Cifrado de datos estáticos y en tránsito	Autentique y cifre el tráfico desde las aplicaciones en los dispositivos hacia el centro de datos con VMware Tunnel. Proteja los datos estáticos y en tránsito de las aplicaciones mediante el cifrado AES de 256 bits.
La microsegmentación automatiza la seguridad en las redes	Minimice la superficie de ataque en el centro de datos mediante las capacidades de microsegmentación de VMware NSX®, lo que permite automatizar la seguridad en la red.
La información integrada y la automatización impulsan la seguridad predictiva	Identifique y reduzca problemas de seguridad en tiempo real con información integrada de datos de amenazas y el estado detallado de cumplimiento del dispositivo suministrado por Workspace ONE Intelligence.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com/latam

N.º de elemento: 130019wf-vmw-fy19q1 euc launch-trust network-ds-a4-106 3/18