Defensa contra las amenazas

para principiantes

jamf

Es un hecho: Apple ha desarrollado una de las plataformas seguras más sólidas del mercado desde que se saca el dispositivo de la caja. Sin embargo, es una plataforma objeto de cada vez más atacantes y, por ello, las organizaciones deben estar equipadas para responder y defenderse de las amenazas de hoy y del futuro.

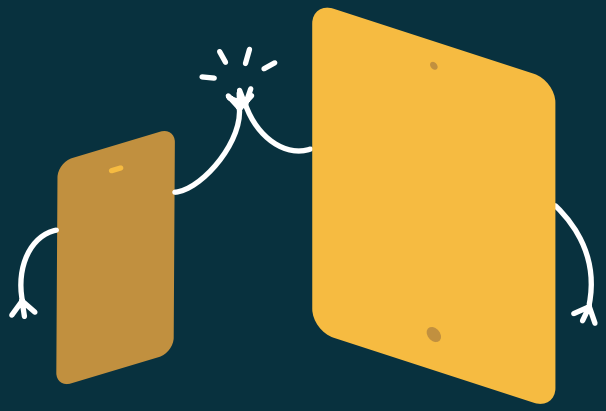
Las campañas de ataque más comunes, como el phishing, el malware y las apps vulnerables, se utilizan para vulnerar la seguridad de los dispositivos e impulsar el acceso a los recursos de la empresa y a los datos sensibles, como por ejemplo:

- Filtración al exterior de información confidencial
- Obtener acceso a los servicios de la empresa
- Recopilar datos de privacidad de los usuarios
- Interceptar las comunicaciones de la red

Jamf Threat Defense protege sus dispositivos endpoint móviles contra el peligro mediante la detección de amenazas y la prevención de ataques de phishing y malware de día cero. Esta es una de las principales preocupaciones para todas las organizaciones,

EN ESTA GUÍA, HABLAREMOS DE LO SIGUIENTE:

- Detección y prevención integral de amenazas
- Protección robusta para todos los casos de uso
- Capacidades/funciones para reportar en tiempo real
- Controles de políticas y acceso condicional
- Administración de operaciones



APPLE ES UN OBJETIVO DE PLATAFORMA CADA VEZ MAYOR PARA LOS ATACANTES DECIDIDOS Y NO DISCRIMINAN.

Las organizaciones que implementan dispositivos macOS a sus usuarios confían en Jamf Protect para proporcionar protección de los endpoints y salvaguardar su flota contra las amenazas a la seguridad, previniendo el malware y proporcionando información sobre la salud de los dispositivos. ¿Pero qué pasa con los dispositivos móviles, como los basados en iOS y iPadOS? ¿Qué tipo de seguridad para endpoints está disponible para dispositivos móviles que no sólo satisfaga sus necesidades únicas, sino que se integre con Jamf Pro para una solución de administración integral?

Entre en Jamf Threat Defense: la solución creada específicamente para proteger los dispositivos móviles Apple y a sus usuarios de las

"PROTEGE TU CUELLO"

Remontándonos a las prolíficas palabras del clan Wu-Tang, el epígrafe se refiere esencialmente a la protección de activos sensibles mediante la protección del núcleo. Para los fines de esta guía, el núcleo son los dispositivos móviles. Al fin y al cabo, son el conducto por el que los atacantes se dirigirán para acceder a los datos sensibles.

El 41% de las organizaciones experimentaron un incidente de malware en dispositivos remotos, lo que no sólo es una cantidad sorprendente, sino también un aumento considerable con respecto al año anterior, según el Informe de Seguridad en la Nube 2021.

Para los que no estén seguros de lo que hay detrás del aumento de los incidentes, la respuesta es tan simple como compleja. La erosión del perímetro de la red debido al cambio a entornos de trabajo remotos o híbridos hace que los usuarios utilicen más los dispositivos móviles para seguir siendo productivos mientras trabajan fuera de la oficina. Esa es la parte sencilla. Lo complejo es la forma en que las organizaciones transforman su infraestructura para mantener los dispositivos protegidos y los datos seguros.

Para minimizar la complejidad, el enfoque de Jamf Threat Defense se basa en la nube, mezclando potentes y avanzadas tecnologías de seguridad con una extrema flexibilidad y escalabilidad. Incluye

PROTECCIÓN DE LA RED

Entre las múltiples amenazas a la seguridad a las que se enfrentan las empresas modernas, el phishing es sólo uno de esos tipos de amenazas, pero podría decirse que sigue siendo el mayor debido a que se dirige al eslabón más débil de la cadena de seguridad: el usuario. La triste verdad es que, incluso con usuarios bien entrenados y capacitados, el margen de error sigue siendo demasiado alto, lo que significa que las tasas de éxito de los ataques son elevadas, por lo que los atacantes seguirán impulsándolos en su cadena de ataques.

Al proporcionar protección dentro de la red, Jamf Threat Defense bloquea activamente las amenazas de día cero, como los sitios web de phishing, en tiempo real. De este modo, se protegen los dispositivos de los efectos de estas campañas antes de desencadenar el ataque de explotación, impidiendo que el dispositivo acceda a estos dominios

AMPLIACIÓN DE LAS

Creada teniendo en cuenta la ampliación de funcionalidades mediante la integración con el marco API de un proveedor, Jamf Threat Defense cuenta con más asociaciones de administración de endpoints unificada (UEM) y administración de información y eventos de seguridad (SIEM) que otras soluciones de seguridad. Lo anterior significa, para los departamentos de IT y de Seguridad, que pueden maximizar la inversión existente en aparatos, apps y servicios de seguridad y administración de dispositivos para aprovechar los conocimientos sobre amenazas, los flujos de trabajo de remediación y la automatización.

Un ejemplo excelente de integración es cuando se impulsa la API de riesgos de Jamf junto con las características de Jamf Threat Defense para permitir una comunicación sin igual entre ambas soluciones de software.

ACCESO ADAPTADO

Una de las principales razones por las que las amenazas relacionadas con la accesibilidad sean tan eficaces es que si un dispositivo se ve comprometido y no hay indicadores visibles para el usuario (es decir, el dispositivo sigue funcionando con aparente normalidad), el usuario seguirá teniendo acceso a un recurso. El dispositivo procesará la solicitud y se concederá el acceso, comprometiendo también el recurso.

Jamf Threat Defense combate simultáneamente esto y eleva su postura de seguridad permitiendo sólo conexiones seguras y dispositivos de confianza para acceder a los recursos de la organización. ¿Cómo lo hace, se preguntará? Al supervisar continuamente los datos de telemetría y las entradas contextuales exclusivas de cada dispositivo para detectar anomalías. Estos, si determinan que el endpoint es de alto riesgo o está comprometido, impedirán el acceso a los recursos mediante la aplicación de políticas personalizadas.

Después de leer algo de lo que Jamf Threat Defense puede hacer para proteger su empresa y su flota de dispositivos móviles, profundizaremos un poco más en los fundamentos del software para

Jamf Threat Defense trabaja incansablemente para frustrar la innumerable lista de ataques a las amenazas a la ciberseguridad que no muestran signos de ralentización y siguen asolando el panorama de la seguridad móvil.

APRENDIZAJE AUTOMÁTICO

Permítame presentarme: MI:RIAM. No es un sustituto de Siri ni del último miembro del clan Wu-Tang, sino un motor de inteligencia avanzada que trabaja en tiempo real para identificar la más amplia gama de amenazas conocidas y de día cero. Utilizando el mayor conjunto de datos sobre amenazas, MI:RIAM recopila información de 425 millones de sensores de todo el mundo como entrada para sus algoritmos, utilizando la ciencia de datos avanzada para proporcionar una

TODOS LOS DISPOSITIVOS

¿Sólo tiene dispositivos basados en iOS y iPadOS en su flota? Está perfecto. Jamf Threat Defense tiene exactamente el tipo de protecciones de seguridad necesarias para mantener sus dispositivos Apple y su base de usuarios protegidos contra las amenazas actuales y emergentes.

¿Tiene también otros tipos de sistemas operativos en su flota de dispositivos móviles? ¡Eso también está bien! Jamf Threat Defense también es compatible con los sistemas operativos de dispositivos que no sean Apple y trabaja con la misma intensidad para mantener todos sus dispositivos móviles protegidos contra las amenazas, los datos seguros y los usuarios sin problemas de productividad. ¿Mencionamos también los múltiples modelos de propiedad, como el

"ES NUESTRO SECRETO... NUNCA ENSEÑES EL WU-TANG"

Como usuario, usted quiere saber que está protegido. Como miembro de IT, quiere saber de qué manera están protegidos sus usuarios. Pero cuando se trata de actores maliciosos, cuanto menos sepan, mejor será para mantener la postura de seguridad de su red y, en última instancia, para mantener segura la información. Y hay varios tipos de información que deseará mantener a salvo a toda costa para mantener su integridad, mantener a los equipos de IT y de seguridad alertados de los últimos datos de salud de los endpoints de la empresa y de las estrategias de

PRIVACIDAD DEL

La Información Personalmente Identificable (IPI), incluida la Información Personal de Salud (IPS), se encuentra entre los tipos de datos que los actores de las amenazas tratan de obtener. Es un efecto cíclico: cuanto más reúnan se alimenta directamente la forma en que continuarán el ataque, a la vez que les proporciona un medio para alcanzar un fin en sus propósitos criminales. Afortunadamente, Jamf Threat Defense salvaguarda la privacidad en línea mediante comunicaciones cifradas, así como la protección contra ataques de phishing. Esto se aplica no sólo a los datos personales de sus usuarios, sino también a la información sensible que puede ser necesaria para cumplir la normativa. Las características avanzadas de privacidad y los controles de políticas siguen la práctica del acceso condicional de confianza cero

DATOS EN TIEMPO REAL

Los equipos de IT y de seguridad pueden obtener informes detallados relativos a la salud de los endpoints utilizando las características de reporte por defecto que se incluyen o personalizar los detalles ajustándolos a las necesidades específicas de su organización. La adaptación de las funciones de elaboración de informes lleva a Jamf Threat Defense un paso más allá, proporcionando a los administradores datos en tiempo real dentro de la consola,
o exportándolos a un socio SIEM a través de la función de integración incorporada para visualizar los datos en paneles, o aprovechando la API para integrarse con una solución de administración unificada, como emparejarla con Jamf Pro, para transmitir datos entre los softwares, lo que permite la gestión automatizada de dispositivos y la remediación de los problemas detectados en los puntos finales.

Hay muchas cosas que puede hacer por su organización y sus usuarios, para mantener protegidos los datos, los dispositivos y las personas. Hay demasiadas cosas para poder abordarlas en este e-book. Así que este es su siguiente paso:

Solicitar una prueba

Obtenga más información con una prueba gratuita de Jamf.