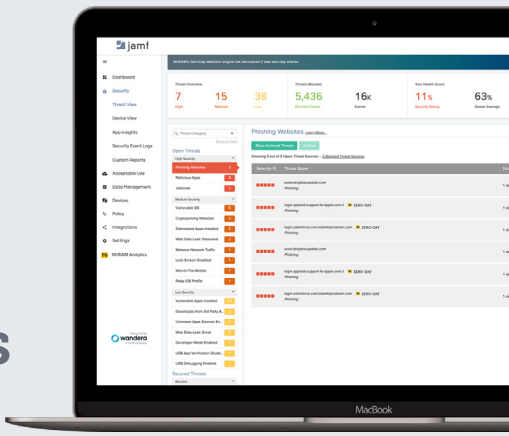
jamf

THREAT DEFENSE DE JAMF

Proteja sus dispositivos, usuarios y aplicaciones de las ciberamenazas



Threat Defense de Jamf proporciona seguridad en la nube que opera en el dispositivo y en la red

Potente seguridad de terminales

Threat Defense detecta y corrige la más amplia gama de amenazas de terminales, como vulnerabilidades de dispositivo, malware y apps de riesgo. Se llevan a cabo evaluaciones integrales de riesgos para identificar amenazas, lo que permite que las políticas de seguridad se apliquen en tiempo real.

Las defensas de la red protegen a los usuarios y los datos

Detenga los ataques antes de que lleguen a las defensas de la red interna. La protección de contenidos bloquea sitios maliciosos, como sitios de phishing de día cero nunca antes vistos, diseñados para robar credenciales corporativas. Asimismo, Threat Defense evita el comando y control y la filtración de datos al bloquear la conectividad a sitios de riesgo. Las conexiones se protegen automáticamente cuando se detecta un ataque de intermediario.

Acceso adaptado a sus aplicaciones

Maximice su posición de seguridad brindando únicamente acceso a las aplicaciones de empresa a dispositivos seguros y de confianza. Threat Defense supervisa de manera continua un amplio conjunto de datos de telemetría y contextuales que pueden servir para blindar el acceso a las aplicaciones a terminales comprometidos o que presenten un alto riesgo. La solución de acceso de red Zero Trust, así como Jamf Pro (la solución de administración de Jamf) permiten aplicar políticas de acceso adaptado de manera nativa.

jamf

Detección y prevención de amenazas integrales

Protección de la red desde el día cero

Threat Defense identifica y bloquea incluso los ataques más sofisticados de red, como los intentos de phishing de día cero, la comunicación de comando y control y el cryptojacking. El servicio funciona con cualquier tipo de app, así como en navegadores web, portales de correo electrónico, redes sociales y aplicaciones de SMS.

Evaluación de riesgos en tiempo real

Threat Defense evalúa de manera continua los riesgos de los terminales (desde sistemas operativos vulnerables hasta perfiles maliciosos), y permite a las organizaciones que identifiquen rápidamente los dispositivos que no están en cumplimiento. Así, las organizaciones pueden aplicar políticas reales de Zero Trust.

Datos detallados sobre aplicaciones

Threat Defense proporciona una inteligencia de aplicación avanzada que puede usarse en flujos de trabajo para vetar apps y en investigaciones de seguridad. Se genera una puntuación para cada aplicación, junto con un informe detallado que contiene los permisos y las URL integradas que ponen en riesgo tanto a los datos del usuario como a los de la organización.

Cifrado dinámico de datos

Threat Defense evita que una infraestructura Wi-Fi comprometida exponga datos sensibles gracias al uso de cifrado en tiempo real. Este servicio funciona en segundo plano y no requiere interacción con el usuario.

Características y capacidades de seguridad líderes

Defensa de terminales siempre activa

Threat Defense protege a los teletrabajadores y a los dispositivos móviles mediante el uso de una app de terminal para identificar software malicioso, configuraciones vulnerables y conexiones de riesgo antes de que se produzca una brecha.

Informes y control de políticas en tiempo real

El motor de políticas unificadas permite a los administradores configurar rápidamente una política de seguridad. La aplicación y cumplimiento de las políticas entran en vigor de inmediato, y permiten que estas se vayan modificando y ajustando sobre la marcha. Los informes detallados pueden consultarse en el portal de Threat Defense o bien exportarse a herramientas de terceros gracias a integraciones fáciles de usar.

Políticas de acceso condicional con Conditional Access

Prohíba el acceso a las aplicaciones de la empresa cuando el umbral de riesgo supere los valores predefinidos. Las políticas de acceso condicional de Conditional Access pueden aplicarse de manera nativa dentro de la red Threat Defense o mediante la integración con Jamf o un proveedor de identidad.

Operaciones y gestión unificados

Threat Defense se integra directamente con la infraestructura de administración y permite que el servicio se implemente rápidamente a los dispositivos gestionados. Esta integración también simplifica los procesos de control de eventos y búsqueda de amenazas de ThreatOps, ya que agrega nombres humanos legibles a los informes.

Threat Defense de Jamf combina a la perfección con sus servicios de IT y tecnologías existentes.

Las completas integraciones con Microsoft, Google, Cisco y otros proveedores aportan todavía más valor a su infraestructura tecnológica.

jamf

www.jamf.com

Para obtener más información sobre cómo Threat Defense puede proteger a usuarios, dispositivos móviles y datos corporativos, visite jamf.com.