jamf

Seguridad 360:
Informe anual de tendencias

Introducción

El año pasado analizamos el impacto de la adopción de tecnologías remotas en la seguridad de las empresas de todo el mundo. Mientras muchas organizaciones seguían migrando a entornos de trabajo remotos e híbridos, este año la atención se centrará en la forma en que se ha adaptado el panorama de las amenazas y cómo estas tendencias representan un riesgo para la seguridad de su organización frente a las amenazas existentes, así como las de nueva creación.

Cada año, **Jamf Threat Labs**, el laboratorio de amenazas, analiza las amenazas que afectan a los dispositivos utilizados en el lugar de trabajo moderno. A medida que el personal sigue estando distribuido, nuestra perspectiva sobre el panorama moderno de las amenazas continúa evolucionando para satisfacer los constantes requisitos de cumplimiento de las normativas sobre terminales, garantizando la seguridad de los datos al mismo tiempo que se defiende la privacidad de los usuarios frente a la evolución de los riesgos.

El informe de este año explora cinco tendencias clave de seguridad que afectan a las organizaciones, con usuarios que se conectan remotamente a una multitud de aplicaciones y servicios alojados en centros de datos privados y públicos, y que dependen de diversos dispositivos móviles multiplataforma.

Dirección de tendencias 2023:

Tendencia 1 - La ingeniería social sigue a la cabeza como la principal amenaza

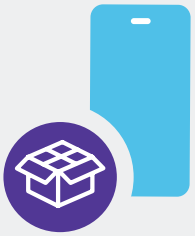
La ingeniería social, con un llamamiento específico a los ataques de phishing, encabeza la lista de amenazas importantes para la ciberseguridad. La mezcla volátil de una fuerza laboral distribuida con la relativa facilidad con la que los agentes perpetradores pueden llevar a cabo campañas de phishing conduce a obtener con éxito las credenciales de los usuarios. También conocidos como "las llaves del reino", estos tipos de ataque otorgan acceso a usuarios no autorizados a los datos almacenados localmente en el dispositivo. Lo que hace que estos ataques sean más peligrosos (o impactantes) es que a menudo permiten pivotar el acceso a otros sistemas como parte de su cadena de ataques.

La ironía de los ataques de ingeniería social es que, a pesar de habilitar sólidas configuraciones de seguridad que se adhieren a las mejores prácticas de la industria, muchas soluciones pueden hacer poco para prevenir este tipo de ataques si los usuarios son engañados para que entreguen sus credenciales a los agentes perpetradores, haciéndose pasar por alguien que no es. Lo que empeora las cosas es lo desarticulados que se han vuelto los entornos, lo que deja a muchos usuarios sin fácil acceso a los profesionales de IT y de seguridad cuando llegan correos electrónicos o mensajes SMS sospechosos que aparentemente requieren una respuesta inmediata.

Desgraciadamente, debido a la naturaleza emergente de los mensajes —escritos intencionalmente de esta forma para asustar a las víctimas y obligarlos a hacer clic en un enlace que roba sus tokens de autenticación, ejecuta código malicioso para explotar una vulnerabilidad en su dispositivo o simplemente dirige a la víctima a un sitio web falso que se hace pasar por legítimo, engañándoles para que proporcionen sus credenciales—, lo triste es que cuando el usuario decide hablar con el departamento de IT, suele ser demasiado tarde. Por ejemplo, **IBM informó** que la causa más común de una transgresión de datos no solo eran las credenciales robadas o comprometidas, sino que hasta 327 días después, también fueron las que más tardaron en identificarse.

Los ataques de phishing difieren bastante de otros tipos de ataques, ya que no se trata de agentes anónimos que mienten para obtener su nombre de usuario y contraseña. El engaño puede realizarse de diferentes maneras para obtener el mismo resultado: tomemos como ejemplo un ataque popular que se lleva a cabo en donde se encuentran puntos de acceso públicos (véase "Wi-Fi gratuito") llamado "evil twin" (gemelo malvado), por ejemplo. Un gemelo malvado se hace pasar por una red inalámbrica legítima, lo que permite a un atacante robar eficazmente cualquier dato relevante transmitido por la víctima sin su conocimiento, lo que puede evitarse si el dispositivo que accede a la red está cifrado con una **VPN o una solución de acceso a redes de confianza cero (ZTNA)**.

En 2022, el 31% de las organizaciones tuvieron al menos un usuario víctima **de un ataque de phishing.**



En 2022, se descubrió que el 16% de los usuarios exponían datos sensibles al conectarse a **puntos de acceso peligrosos.**

En conjunto, estos dos datos sugieren que:

1. Los usuarios alteran sus dispositivos mucho menos que antes, y...
2. Los agentes perpetradores están aumentando sus ataques a los dispositivos de las empresas.

Fuente: Jamf Threat Labs

Statistica calcula que actualmente **hay 432.5 millones de puntos de acceso Wi-Fi públicos disponibles en todo el mundo.** Y en 2022, se descubrió que el 16 % de los usuarios exponían datos confidenciales al conectarse a puntos de acceso de riesgo. Suponiendo que solo un usuario se conecte a cada punto de acceso de riesgo, serían 432.5 millones de usuarios transfiriendo datos a través de conexiones de red no confiables.

Las cifras no distinguen entre usuarios empresariales y personales, ni tienen en cuenta las soluciones de seguridad para terminales que pueden ayudar a frustrar los ataques de phishing, como el software de filtrado de contenidos que impide explícitamente el acceso a diversas URL y dominios maliciosos asociados a campañas de phishing.

Y lo que es más importante, según EC-Council, no tienen en cuenta **la mejor forma de proteger a su personal.** Tanto si se trata de combatir amenazas de ingeniería social como de evitar ataques de phishing desde cualquier medio de comunicación, una de las mejores medidas defensivas no es un control de seguridad, sino administrativo: **tener capacitación en ciberseguridad.** Con un programa completo de capacitación de usuarios que se integre en los procesos de incorporación, así como un seguimiento periódico con actualizaciones frecuentes sobre los ataques dirigidos a innumerables organizaciones de todo el mundo, los usuarios adquieren los conocimientos necesarios para reconocer las amenazas y evaluar los riesgos que conlleva seguir adelante con los intentos de suplantación de identidad.

Invertir en programas de capacitación para la concientización sobre seguridad para las partes interesadas de la empresa es una parte importante de la estrategia de seguridad de una empresa y no debe pasarse por alto. Esto significa impartir una formación continua y versátil a los usuarios finales que abarque una serie de buenas prácticas y los eduque sobre las amenazas más recientes que tienen más probabilidades de afectarles. Esto los capacitará para identificar los nuevos ataques y en evolución y tomar medidas proactivas para mejorar su higiene de seguridad, tanto en el trabajo como en su vida personal.

Los 10 tipos principales de ataques de phishing son:

1. **Correo electrónico:**
   Los mensajes de correo electrónico se envían a personas que simulan proceder de una fuente confiable y acreditada.

2. **Vishing:**
   Los ataques de phishing por medio de la voz cambian de medio y pasan a ser ataques orientados al teléfono (TOAD), a menudo falseando el número de la persona que llama para hacerse pasar por una fuente de confianza. Esto ocurre, por ejemplo, con las llamadas fraudulentas que dicen ser del FBI.

3. **Smishing:**
   Al igual que el Vishing, los agentes perpetradores de amenazas utilizan mensajes SMS con enlaces o archivos adjuntos en lugar de llamadas telefónicas para comprometer a los usuarios de dispositivos móviles.

4. **Redes sociales/Angler:**
   Las nuevas tecnologías dan lugar a nuevos vectores de ataque, de ahí que estos ataques se dirijan a los usuarios de las redes sociales a través de diversas plataformas. Este último, el Angler phishing, es una variación más reciente del tema de las redes sociales, en la que los atacantes se hacen pasar por personal de atención al cliente, a menudo con una cuenta de perfil falsa, para atacar a víctimas que necesitan ayuda.

5. **Spear (dirigido):**
   Es una variante del phishing por correo electrónico que utiliza un enfoque selectivo, centrándose en personas concretas dentro de una organización, como un empleado del departamento de nóminas.

6. **Whaling (caza mayor):**
   Similar al spear phishing, este ataque refina su alcance para dirigirse a ejecutivos y directores generales.

7. **HTTP/S:**
   Ataques basados en sitios web que utilizan URL que a menudo contienen errores ortográficos sutiles que pueden ser difíciles de detectar a simple vista, como "iamf.com" en lugar de jamf.com. También puede incluir dominios protegidos por SSL registrados legítimamente para eludir las funciones de comprobación de seguridad de los navegadores modernos.

8. **Falsificación de sitios web:**
   Este tipo de ataque suele acompañar a los ataques HTTP/S, emparejando un sitio web de aspecto legítimo junto a la URL maliciosa, repleto del texto, logotipos, esquemas de color y funcionalidad originales que reflejan el sitio web real, proporcionando una apariencia, aspecto y sensación de confianza.

9. **Watering Hole (abrevadero):**
   En parte spear phishing (dirigido), en parte táctico, los ataques watering hole se dirigen a grupos específicos de usuarios y a un sitio web que visitan con frecuencia. El objetivo del ataque es comprometer el sitio web infectándolo con malware para que cuando los usuarios objetivo visiten el sitio, también se infecten.

10. **Pop-up (ventanas emergentes):**
    Al igual que los anuncios emergentes de la tecnología de antaño, esta variación del phishing requiere que los agentes perpetradores infecten un sitio web con malware, luego utilicen anuncios incrustados o alertas de notificación más recientes habilitadas por los usuarios e infecten a los usuarios cuando se envía la carga útil.

Tendencia 2 – La privacidad del usuario se sienta a la mesa de la seguridad

Mientras que los fabricantes y desarrolladores, como Apple y Jamf, llevan ya algún tiempo tocando activamente el tambor de la privacidad, en general, otros proveedores de tecnología no han tenido históricamente la misma consideración por la protección de la privacidad que por otras medidas de seguridad en sus ofertas de hardware y software.

Al igual que las consecuencias de la filtración de datos personales y empresariales, el campo de batalla en torno a la protección de la privacidad de los datos de los usuarios arroja muchas víctimas en caso de transgresión. Hay que tener en cuenta que los datos personales no se recogen simplemente sin el permiso del usuario. Se están poniendo en peligro de varias maneras:

- Los Estados-nación utilizan códigos maliciosos que permiten intervenir las comunicaciones, como el micrófono de la cámara o el registro de teclas de los dispositivos de las víctimas, para espiarlas.
- Los agentes perpetradores utilizan estos datos para obtener beneficios personales o económicos, así como para ampliar las campañas de ingeniería social y chantajear a las víctimas.
- Las empresas se enriquecen vendiendo los datos recopilados sin el consentimiento del usuario a anunciantes y/o socios terceros.

En otros casos, las organizaciones que recopilan datos personales como parte de sus procedimientos operativos legítimos se encuentran en problemas debido a la insuficiencia de las protecciones establecidas para proteger los datos personales de un ataque externo, una amenaza interna o la gobernanza reglamentaria. Y en algunos casos, **las organizaciones ni siquiera son conscientes de la amenaza,** como demuestra que "el 5% de las organizaciones tendrán una aplicación potencialmente no deseada instalada dentro de su flota de dispositivos en 2022".

A primera vista, un 5% puede no parecer significativo. Pero la evaluación del riesgo va mucho más allá de las cifras. Tiene en cuenta lo siguiente:

- Identificación de activos específicos
- Cualquier vector de ataque presente
- Tipos de ataques posibles
- Probabilidad de que se produzca un ataque
- Impacto potencial si se vulnera o se pone en peligro

En esencia, la combinación de estos elementos permite a las organizaciones evaluar qué riesgo existe y cómo afectará a la continuidad de la actividad. ¿Cómo se aplica esto a los datos personales?

"El **0.4%** de los dispositivos Android tenían una app potencialmente no deseada instalada en **2022** en comparación con **0.1%** de dispositivos iOS".

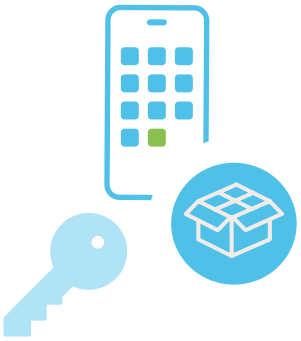
Android es un ecosistema abierto que da lugar a aplicaciones más riesgosas. Apple ha creado un ecosistema cuidado de aplicaciones y ofrece protecciones más estrictas de la privacidad de los usuarios que limitan la introducción de estas aplicaciones riesgosas.

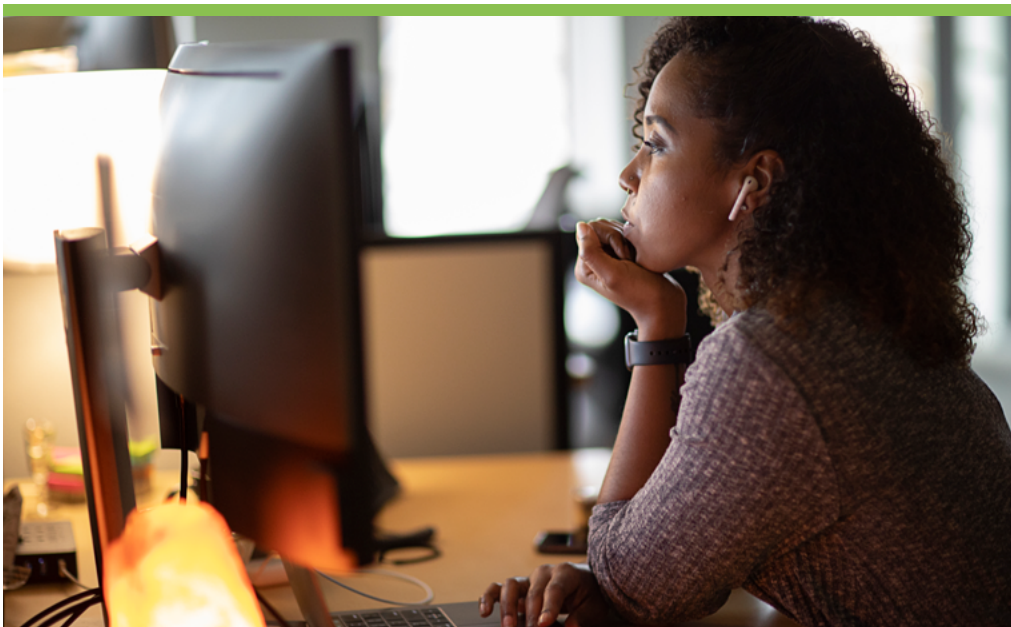
No se puede subestimar el último punto, relativo al impacto potencial si se vulnera o se pone en peligro, ya que ataca directamente al corazón de los controles reguladores y a la forma en que funcionan para mitigar los riesgos, impidiendo las filtraciones de datos que violarían las leyes reguladoras (más adelante en este informe se habla del cumplimiento).

Los controles eficaces de la privacidad siguen ganando protagonismo junto a los controles de seguridad, no solo para imponer el cumplimiento de la normativa cuando sea necesario, sino también para limitar la exposición de los datos privados de los usuarios como parte de una estrategia de seguridad más amplia. Debe extenderse a todas las soluciones, procesos, partes interesadas y flujos de trabajo dentro de una organización para construir la seguridad general de los datos junto con la creación o implementación de todos los componentes en toda la empresa, no como una idea tardía.

Las soluciones de administración ayudan a alinear las políticas organizativas con los requisitos de la normativa y reducen la carga de administración al permitir que el departamento de IT designe las aplicaciones de la empresa. Esto garantiza que todos los tipos de datos estén protegidos en toda la infraestructura, independientemente del tipo de dispositivo o ubicación.

Al aprovechar la administración de múltiples modelos de propiedad de dispositivos, las organizaciones logran un equilibrio entre la seguridad de las aplicaciones y los datos y la aplicación de configuraciones seguras a los propios dispositivos para acceder a los recursos empresariales de forma segura, al mismo tiempo que permiten a los usuarios controlar en última instancia los datos privados asociados a sus aplicaciones personales y al uso de sus dispositivos. Las empresas protegen los datos de propiedad que son tanto sensibles por naturaleza como confidenciales, al tiempo que mantienen un enfoque de "no intervención" en los datos privados de los usuarios, **permitiendo a los usuarios finales controlar el nivel de acceso** a estos datos, mejorando aún más las protecciones generales de la privacidad, sin importar si los dispositivos forman parte de un programa BYOD, de dispositivos propiedad de la empresa que forman parte de la iniciativa CYOD/COPE o de una mezcla de estos modelos.





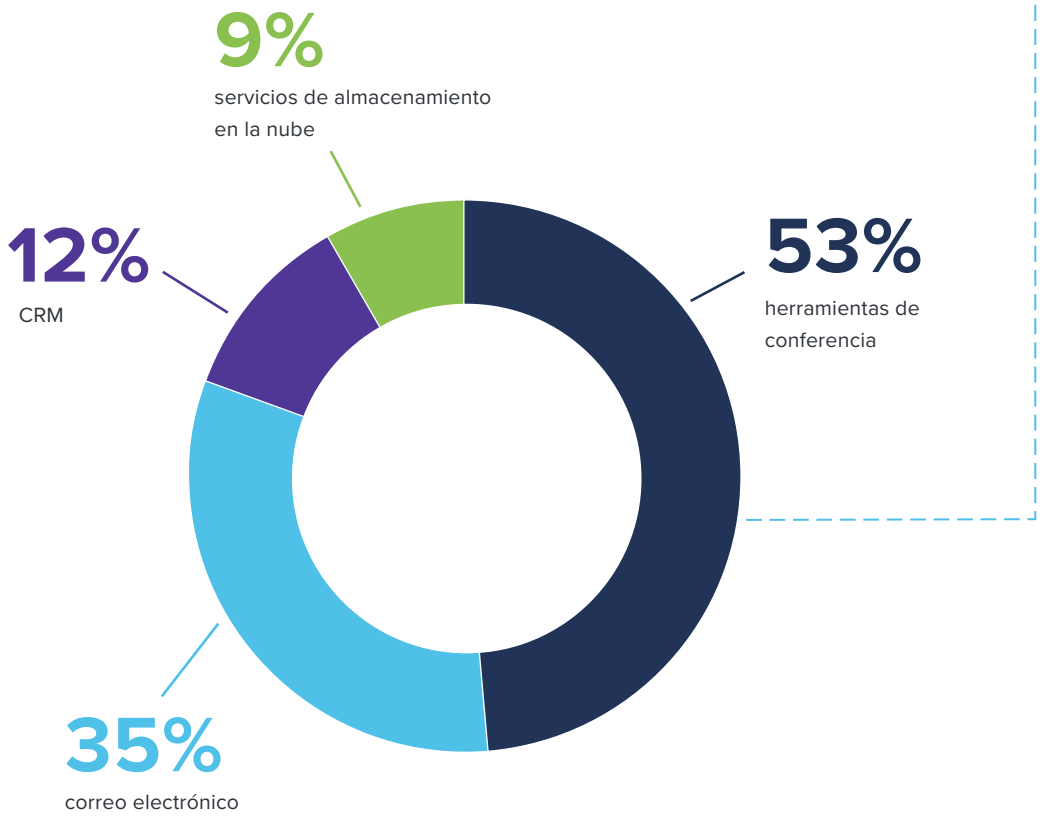
Tendencia 3 – Ataques convergentes de agentes perpetradores en nuevas amenazas

Algunas buenas noticias en el frente del malware para macOS: el total de infecciones por malware no mostró signos de crecimiento con respecto al año anterior. La mejor noticia: en 2022, **las nuevas infecciones de malware descendieron** de algo más de 150 millones a unos 100 millones de infecciones, según el registro continuo de programas maliciosos y aplicaciones potencialmente no deseadas (PUA) de AV-Atlas.

El tráfico de red malicioso, que se refiere a los Indicadores de Compromiso (IoC) basados en la red que pueden observarse en los patrones de comunicación entre el dispositivo y los servidores de Internet, sigue siendo cada vez más frecuente. Normalmente, el tráfico de red malicioso solo se observa en entornos de producción y no puede identificarse simplemente evaluando el código estático. Por eso es tan importante vigilar activamente la salud de las terminales al evaluar los factores de riesgo combinados.

No es nuevo el hecho en sí de que los agentes perpetradores vinculen varios ataques; sin embargo, el panorama moderno de las amenazas es que se está viendo cómo cada vez más de estas amenazas convergentes se utilizan activamente en forma salvaje para atacar a las fuerzas laborales distribuidas de nuevas formas, con el fin de obtener acceso no autorizado a servicios y recursos protegidos. En un solo mes de 2022, el 53% de los dispositivos comprometidos accedió a herramientas de conferencia, mientras que el 35% accedió al correo electrónico, el 12% a un CRM y el 9% a servicios de almacenamiento en la nube.

En un solo mes de 2022, el **53%** de los dispositivos comprometidos accedió a herramientas de conferencia, mientras que el **35% accedió al correo electrónico,** el **12% a un CRM** y el **9% a servicios de almacenamiento en la nube.**



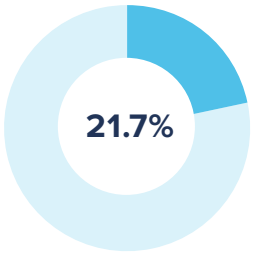
Ejemplo de ataque sofisticado

Un empleado recibe un mensaje de spear phishing que parece proceder de un colega. El mensaje incluye un enlace a un "documento de trabajo", que inyecta un código malicioso en el dispositivo de la víctima que recopila sus credenciales a la vez que entrega una carga útil de ransomware. Al mismo tiempo que pide rescate por los datos sensibles, el atacante utiliza las credenciales para obtener un mayor acceso a la infraestructura de la organización. Por último, el software malicioso realiza dos funciones más: añade la terminal como parte de una botnet utilizada para atacar a otras organizaciones mientras busca otros dispositivos que infectar, extendiendo posteriormente el proceso y haciendo crecer la botnet.

El mensaje general aquí es que los ataques pueden adoptar más de una forma y pueden producirse en cualquier periodo y, a menudo, sin ser detectados. Algunas cadenas de ataques se producen poco después del compromiso, como el ransomware, mientras que otras son más tácticas y requieren más tiempo, como la construcción de una botnet para atacar sistemas con ataques de negación de servicio distribuido (DDoS).

Esta convergencia es difícil de proteger, ya que las víctimas no suelen conocer el alcance del ataque hasta que la siguiente oleada comienza a impactarlas. Aun así, ciertas prácticas pueden mitigar algunos riesgos y limitar o aliviar en gran medida el impacto de otros. La supervisión activa de las terminales y la recopilación de datos de telemetría sobre el estado de salud de las mismas es un dato fundamental para los administradores, ya que proporciona una visibilidad profunda de los dispositivos y de su estado en relación con varios vectores, como los niveles de parches, sobre todo porque los comportamientos sospechosos que pueden indicar que un dispositivo está en peligro no son vistos ni percibidos por un usuario final.

Hablando de administración de parches, la administración del ciclo de vida de las aplicaciones es fundamental para mitigar el riesgo de vulnerabilidades del sistema y garantizar que las aplicaciones cuentan con el máximo nivel de seguridad para protegerse de las amenazas conocidas. Esto es especialmente importante si se tiene en cuenta que las tiendas de aplicaciones de terceros a menudo ofrecen versiones de aplicaciones legítimas que contienen código malicioso, infectando los dispositivos de los usuarios. Imagine las versiones gratuitas de aplicaciones de pago como cebo para atraer a las víctimas, por ejemplo.



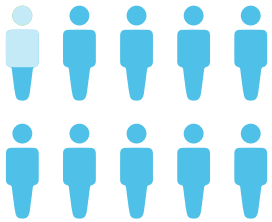
El **21.7%** de los dispositivos Android accedieron a tiendas de aplicaciones de terceros, en comparación con el **0.002%** de los **dispositivos iOS.**

Las tiendas de aplicaciones de terceros son una forma habitual de trastornar el proceso de revisión de aplicaciones que protege los dispositivos y a los usuarios.

El **0.02%** de los dispositivos Android estaban rooteados y el **0.001%** de los **dispositivos iOS tenían jailbreak** en 2022.

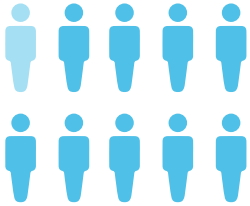
A pesar del pequeño porcentaje, es notable que el número de dispositivos Android afectados duplica al de Apple. Y si pensamos en la cantidad abstracta de dispositivos Android y Apple que hay en el mundo, no es difícil imaginar la magnitud de esta situación.

Mientras que algunos sistemas operativos (OS) permiten la carga lateral de aplicaciones, otros, como iOS, exigen que los dispositivos tengan primero un jailbreak para anular la protección que mantiene a los dispositivos basados en iOS a salvo de la ejecución de código no firmado. Bloquear los dispositivos es solo una parte de la ecuación. Es crucial identificar los dispositivos con jailbreak en tiempo real para remediar eficazmente este vector de amenaza.



0.004% de los usuarios y **0.3%** de las organizaciones tenían un dispositivo con **jailbreak** o **rooteado** en 2022.

Estadística del año pasado:

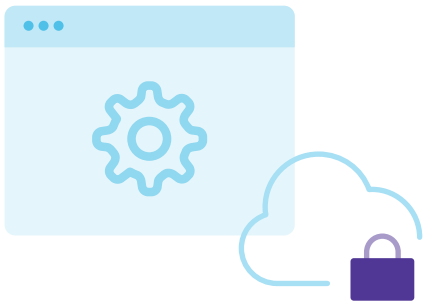


Menos del 1% de las organizaciones tenían un dispositivo con **jailbreak** o **rooteado** en 2021.

Ataques a la cadena de suministro

Los ataques contra la cadena de suministro o contra **terceros** han tenido históricamente repercusiones más amplias que se adentran en varias capas — y atraviesan las organizaciones de la cadena— antes de alcanzar **el verdadero objetivo del atacante.** Sus efectos son a menudo de gran alcance y afectan a las empresas de todo el mundo, sin importar la solidez de su dispositivo de seguridad.

Prevenir estos ataques es una propuesta delicada, principalmente porque las organizaciones carecen de autoridad para exigir a cada organización (o a sus contratistas) de la cadena de suministro que mitigue los factores de riesgo de forma significativa. Lamentablemente, lo mismo ocurre con la protección de su organización contra estas amenazas por las mismas razones. Sin embargo, como señalan la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) y el Instituto Nacional de Normas y Tecnología (NIST) en su documento técnico conjunto **Defending Against Software Supply Chain Attacks (Defensa contra los ataques a la cadena de suministro de software**), un elemento clave para "reforzar la capacidad de una organización para prevenir, mitigar y responder a tales ataques" es observar las mejores prácticas de la industria como parte de una estrategia de seguridad integral de defensa en profundidad que incluya un examen de los procesos de seguridad de los proveedores a través de auditores externos independientes para verificar que los socios de usted (y, posteriormente, los socios de los proveedores) están tomando las medidas de mitigación adecuadas antes de que se produzca un ataque.



Tendencia 4 – Cumplir la normativa forma parte de la pila de seguridad

Una tendencia creciente, junto con la seguridad de los datos de las organizaciones, es la importancia de la privacidad de los usuarios. Esto es más frecuente en materia de cumplimiento, sobre todo de la normativa estatal, federal y regional. Considere la forma en que el Reglamento General de Protección de Datos (GDPR) y la Ley de Privacidad del Consumidor de California (CCPA) realizan mayores avances en la protección de los derechos de los usuarios a la privacidad a nivel nacional y estatal, respectivamente, o cómo la tecnología financiera —entre las industrias más reguladas a nivel mundial— está sujeta a múltiples facetas de gobernanza.

He aquí algunos ejemplos de cómo múltiples leyes reguladoras funcionan por sí solas o en conjunción con otras para lograr el cumplimiento de la normativa en determinados sectores:

Ley Sarbanes-Oxley de 2002 (SOX): dicta condiciones específicas para las prácticas contables

Ley Gramm-Leach-Bliley (GLB): aborda los niveles mínimos de protección de la ciberseguridad necesarios para mantener la seguridad de la información

Autoridad Reguladora del Sector Financiero (FINRA): detalla explícitamente cómo se relacionan los procesos empresariales para garantizar la protección de los inversionistas mediante operaciones justas y honestas en el sector de los valores

A la luz de las normativas de cumplimiento que afectan a las empresas de determinados sectores y de su alcance mundial, que exigen a las organizaciones afectadas el cumplimiento de leyes que pueden estar fuera de su jurisdicción, las organizaciones se encuentran con la necesidad de ejercer un mayor control sobre los flujos de trabajo para mantener la privacidad y la administración de los tipos de datos protegidos —como la información de identificación personal (PII), la información sanitaria protegida (PHI) y la información de inteligencia empresarial (BII)— a medida que se recopila, procesa, almacena, modifica, comparte y destruye siguiendo los deseos del usuario y/o las normativas.

Cumplir la normativa puede ser una tarea difícil que requiera una seria consideración, administración y apoyo, incluso si los dispositivos y los datos son administrados por la organización. Pero, ¿qué pasa con la aplicación de la normativa a través de una fuerza de trabajo distribuida que debe ser capaz de acceder a los recursos de la organización desde cualquier lugar, en cualquier dispositivo y en cualquier momento? Las complicaciones añadidas de las fuerzas de trabajo en las instalaciones y las remotas/híbridas pueden ser un punto de dolor para las organizaciones con requisitos de cumplimiento y que navegan por el panorama moderno de las amenazas.

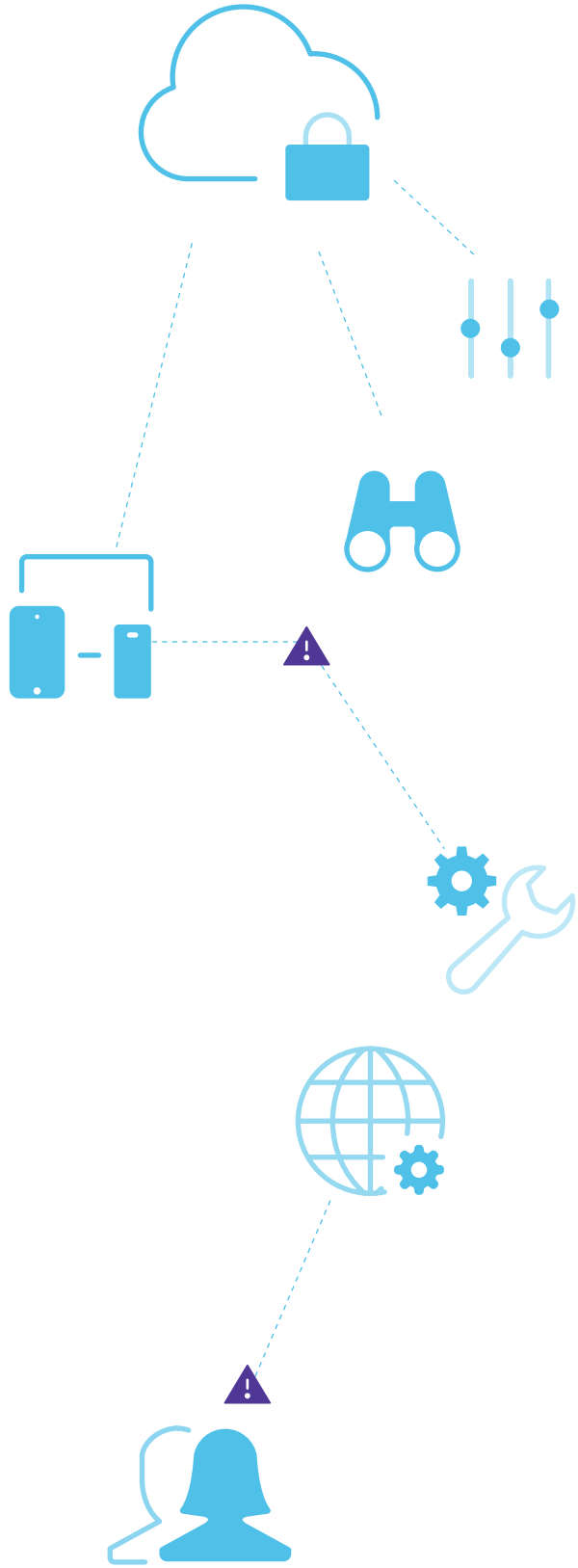
"En **2022**, el **21%** de los empleados utilizaba dispositivos mal **configurados**, lo que les exponía a **riesgos**."

Lamentablemente, las aguas del cumplimiento de la normativa se vuelven más turbias cuando se añaden a la mezcla los dispositivos de propiedad personal. En 2022, el 21% de los empleados utilizaba dispositivos mal configurados, lo que les exponía a riesgos. Más concretamente, dejar datos que podrían ser sensibles, confidenciales o de misión crítica —y potencialmente regulados— en riesgo de exposición, exponiendo a su vez a la organización (y posiblemente también al usuario) puede dar lugar a responsabilidades civiles y/o penales si se determina que se han producido transgresiones de las leyes reguladoras como resultado.

Aunque muchas organizaciones han implementado algún tipo de programa BYOD o de elección del empleado, que permite a los usuarios finales seleccionar los tipos de dispositivos y sistemas operativos con los que se sienten más productivos y cómodos, la solución para una administración eficaz del cumplimiento no puede consistir únicamente en bloquear todos los dispositivos excepto los administrados. **Vimos que el 8% de los usuarios y el 21% de las organizaciones se vieron afectados por vulnerabilidades de configuración**, lo que significa que incluso pueden verse afectados los dispositivos administrados y propiedad de la empresa. Las soluciones deben tener más en cuenta el responder a los problemas de seguridad aparte de la administración de dispositivos.

El hecho es que cualquier terminal en algún momento dado podría perderse de un parche, filtrar datos debido a una vulnerabilidad de combinación o simplemente perderse o ser robado. En cada escenario, se requeriría una acción diferente para mitigar el riesgo. Algunas situaciones podrían administrarse mediante flujos de trabajo automatizados de respuesta y remediación, pero la cuestión sigue siendo que siempre habrá un lugar también para la corrección manual.

Como ocurre con la mayoría de los debates sobre seguridad, no existen soluciones milagrosas o universales que cubran todas las necesidades para mantener la infraestructura en conformidad en todo momento. Recomendamos aplicar una estrategia de seguridad de defensa en profundidad que ofrezca múltiples soluciones convergentes para abordar sus requisitos de cumplimiento exclusivos desde muchos ángulos.



Tendencia 5 - La seguridad de los datos en entornos remotos o híbridos sigue planteando problemas

El cambio a una fuerza de trabajo remota supuso un cambio en la protección de usuarios, datos y dispositivos. Con el perímetro de la red deteriorado efectivamente, las soluciones locales fueron sustituidas por soluciones basadas en la nube para distribuir los servicios de seguridad a los usuarios que trabajan en cualquier dispositivo y desde cualquier lugar. El resultado fue una solución de seguridad para terminales que fuera más capaz y autosuficiente, con mayor capacidad de resiliencia y una sólida seguridad de aplicaciones.

Y, sin embargo, a pesar de los beneficios identificados, las organizaciones siguen experimentando retos en la seguridad de los datos a partir de los entornos de trabajo remotos e híbridos varios años después de la migración. Desgraciadamente, ningún problema claro señala al culpable. Una amalgama de problemas contribuye a una protección inadecuada de los datos. Algunos de estos problemas se deben a la falta de:

- Visibilidad en tiempo real del estado de las terminales
- Integración entre herramientas de administración y seguridad
- Procesos y flujos de trabajo automatizados
- Registro descentralizado e información sobre amenazas
- Observancia de políticas y normativas
- Programas de capacitación en seguridad para usuarios finales
- Mejores soluciones en su tipo
- Prácticas de evaluación de riesgos para identificar activos y amenazas

Por ejemplo, descubrimos que **el 64% de los dispositivos vulnerables accedía a herramientas de colaboración, mientras que el 34% accedía al correo electrónico de la empresa.** Esto indica que, aunque los indicadores de riesgo y peligro sean subjetivos y puedan variar de una empresa a otra, las tareas rutinarias como la administración de parches no se están llevando a cabo en todos los dispositivos. Esto pone en peligro los propios dispositivos y también los recursos de la organización. Incluso va más allá de las apps y las configuraciones. Jamf Threat Labs descubrió que **1 de cada 5 dispositivos ejecutaba un sistema operativo que no estaba actualizado.** Es esencial que exista seguridad en todas las capas de una estrategia de defensa en profundidad, empezando desde el nivel del sistema operativo, para proteger a los usuarios y a las organizaciones.

Esto pone aún más de manifiesto la necesidad real de visibilidad de su flota de dispositivos y de cómo interactúan con la infraestructura de su organización, especialmente si su industria está regulada. Este requisito se agrava si se tiene en cuenta que la mayoría de los organismos reguladores exigen que las organizaciones demuestren su cumplimiento mediante auditorías programadas periódicamente, realizadas por reguladores que buscan verificar que los datos protegidos y las terminales que interactúan con ellos estén asegurados de acuerdo con la gobernanza reguladora.

Pero la evaluación de los activos y las amenazas que afectan a su organización y la telemetría correspondiente para identificar las terminales afectadas es solo una parte de la solución. Se necesitan soluciones modernas para mitigar los riesgos y aplicar decisiones de acceso en tiempo real. Las tecnologías heredadas, como las VPN para proteger las conexiones remotas, no pueden competir con las nuevas tecnologías diseñadas para afrontar los retos de los lugares de trabajo distribuidos y el panorama moderno de las amenazas. ZTNA permite la conexión a aplicaciones y servicios solo después de verificar que el dispositivo y el usuario tienen permiso para acceder a los servicios solicitados y cumplen los requisitos mínimos de "salud" para hacerlo de forma segura.

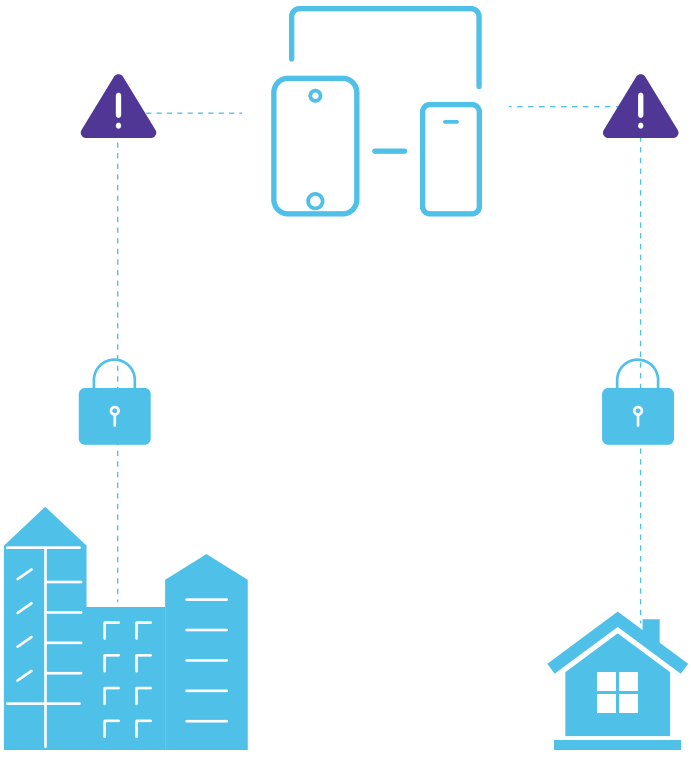
Diseñadas teniendo en cuenta las redes y los flujos de trabajo modernos, las soluciones de ZTNA mitigan los riesgos y protegen los datos, al tiempo que son lo suficientemente flexibles como para garantizar que las aplicaciones y los datos personales sigan siendo privados. Más allá de eso, los usuarios autorizados solo tienen acceso para conectarse a las apps a las que están autorizados a acceder siguiendo el principio del menor privilegio mientras se enruta el tráfico empresarial a través de microtúneles, lo que evita que los atacantes que comprometen a un solo usuario accedan a todas las aplicaciones a las que el usuario está autorizado a acceder. Gracias a la segmentación integrada de los túneles de tráfico, se impide que los atacantes realicen movimientos laterales por toda la red, lo que limita eficazmente las amenazas.

Otra pieza clave es la integración segura de las soluciones mediante el aprovechamiento de las API para compartir datos críticos de telemetría y salud de las terminales con soluciones que limiten el índice de éxito de las amenazas a los dispositivos, los usuarios y los datos confidenciales. Esto contrasta fuertemente con las soluciones adicionales o independientes, en las que las herramientas de seguridad disponibles en el mercado funcionan de forma independiente, pero carecen del componente de integración que impulsa una solución holística de defensa en profundidad.

A medida que los agentes perpetradores hacen evolucionar sus herramientas, las organizaciones deben aprovechar sus soluciones para prevenir los ataques conocidos y mitigar el riesgo de los nuevos. Con esto último en mente, la caza de amenazas sigue creciendo y prosperando en las organizaciones, ayudando a sus equipos de IT y de seguridad a identificar, mitigar y remediar amenazas desconocidas y novedosas antes de que puedan dar lugar a transgresiones de datos. Las tecnologías de Inteligencia Artificial (IA) y Aprendizaje Automático (ML) han demostrado su eficacia en varias industrias, y la ciberseguridad es una de ellas en el que las soluciones aprovechan cada vez más la mayor potencia de procesamiento y las capacidades de análisis del comportamiento para aprender, predecir eficazmente y contrarrestar a los actores de amenazas y sus ataques a velocidades con las que los administradores humanos simplemente no pueden competir.

Centre su estrategia en la administración de dispositivos móviles (MDM) para proteger tanto los dispositivos personales como los que sean de propiedad de la empresa y mantener los parches actualizados. Implemente seguridad en las terminales para evitar el malware mientras recopila datos de telemetría enriquecidos mediante la supervisión activa de las terminales. Una API es una forma excelente de compartir de forma segura datos de inteligencia sobre amenazas entre estas dos soluciones y permite a las organizaciones mantener los requisitos de cumplimiento mediante la aplicación basada en políticas. La incorporación de soluciones de administración de identidades y accesos centraliza la administración de credenciales y la concesión de permisos a recursos organizativos aprobados, al tiempo que añade la autenticación multifactor (MFA) para proteger el acceso.

Esto se integra con soluciones de seguridad modernas, como ZTNA, para proteger las conexiones a través de cualquier red, incorporar ML para cazar nuevas amenazas, detener los ataques antes de que puedan comenzar y sustituir las VPN heredadas por soluciones modernas que segmenten las solicitudes de acceso para mitigar las amenazas basadas en la red. Y, por último, recopilar todas las amenazas relevantes y el estado de salud del dispositivo en tiempo real para automatizar de forma integral la gestión del ciclo de vida del dispositivo.



Recomendaciones

A medida que nos acercamos a la marca de los tres años desde que la pandemia mundial provocó un cambio drástico en los entornos de trabajo globales, el enfoque para muchos ha pasado de **"¿cómo continuamos las operaciones comerciales?"** a **"¿cómo mantenemos a los usuarios remotos y los recursos de la organización continuamente protegidos?"**

Una de las razones clave del cambio de mentalidad es que, a pesar de ser remotos desde hace varios años, los equipos de IT y Seguridad están dando soporte a más del doble de usuarios remotos en la actualidad (46%) que en antes de la pandemia (21%), según el **informe The State of Security 2022** de Splunk. La investigación global de Splunk descubrió que "no solo seguimos viendo más ataques, sino también más transgresiones reales".

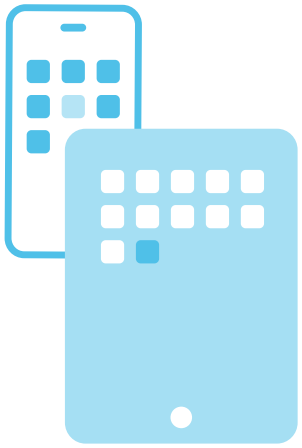
Esta combinación del aumento de las cifras de ataques, la evolución del panorama de amenazas y la creciente necesidad de proteger los recursos a los que acceden los usuarios remotos subraya la afirmación realizada en el informe Security 360 del año pasado:

> Las soluciones de acceso remoto seguro deben ser lo bastante flexibles y ágiles para permitir (y no bloquear ni estorbar) la productividad.

Este año completamos esta afirmación añadiendo:

> La seguridad de las terminales debe proporcionar una convergencia de soluciones de seguridad, aprovechando una base sólida y una visibilidad detallada con tecnologías avanzadas, como ML, para desarrollar flujos de trabajo seguros automatizados que sirvan para alinearse con las políticas organizativas y las normativas de la industria.

En última instancia, las organizaciones deben desarrollar una estrategia de seguridad de defensa en profundidad, moderna y en la nube, que responda a sus necesidades actuales y, al mismo tiempo, proporcione la escalabilidad necesaria para satisfacer las necesidades del futuro.



Acerca de esta investigación

Nuestro objetivo es identificar las principales tendencias de seguridad que surgen en el nuevo mundo del trabajo híbrido. La información y las estadísticas que se encuentran en este documento son el resultado de nuestro análisis de tendencias de seguridad dentro de una muestra de 500,000 dispositivos protegidos por Jamf, que abarcan iOS, macOS, iPadOS, Android y Windows, a través de 90 países, durante un período de 12 meses. Este análisis se realizó en el cuatro trimestre de 2022. Los metadatos analizados en esta investigación proceden de registros agregados que no contienen información personal ni de identificación de la organización. Nuestra intención con este análisis no es invocar el miedo, sino educarle a usted y a sus usuarios sobre las opciones disponibles y sobre la mejor manera de mantener seguros todos los aspectos de los datos del dispositivo, del usuario y de la organización.