RESUMEN DE SOLUCIONES

THREATLOCKER®

ZERO TRUST ENDPOINT PROTECTION PLATFORM

How ThreatLocker®
Protects Your Business

ThreatLocker® is a Zero Trust endpoint protection platform that provides enterprise-level cybersecurity to organizations globally. Instead of relying heavily on detection methods and chasing threats, the ThreatLocker® solutions block everything that is not explicitly trusted and limit actions to only what is needed.

Zero Trust security supersedes the need for detection tools, protecting you from zero-day attacks and ransomware. The ThreatLocker® Zero Trust philosophy extends beyond Allowlisting to incorporate controlling what permitted applications can do, what storage areas can be accessed and how, and what network connections can be made. Denies and allows are recorded in real time in a Unified Audit to assist with compliance and ThreatLocker® Ops utilizes this real-time data to alert you of any blocked malicious action.

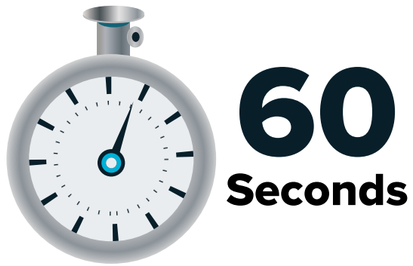
The ThreatLocker® endpoint protection platform is designed to be easy to use and integrate seamlessly into existing IT environments. Our innovative Learning Mode and rapid response time of the 24/7/365 Cyber Hero Support Team makes onboarding and implementing ThreatLocker® a streamlined process.

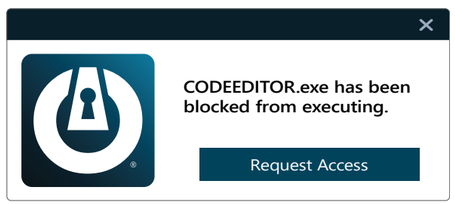
Lista Blanca (Allowlisting)

La lista de aplicaciones permitidas deniega la ejecución de todas las aplicaciones, excepto aquellas que están explícitamente permitidas. Esto significa que el software que no sea de confianza, incluyendo ransomware y cualquier otro malware, se rechazará de forma predeterminada.

Cuando el agente se instala por primera vez, opera en modo de aprendizaje. Durante este período, se catalogan todas las aplicaciones y sus dependencias que se hayan encontrado en la computadora y se crean políticas para permitirlas de forma automática. Después del período de aprendizaje, el administrador de TI puede revisar la lista de aplicaciones, eliminar las que no son necesarias y asegurar la computadora. Una vez que la computadora esté asegurada, cualquier aplicación, secuencia de comandos o biblioteca que no sea de confianza que intente ejecutarse será denegada. El usuario puede solicitar un nuevo software al administrador de TI y puede aprobarse en 60 segundos.

La lista blanca se ha considerado durante mucho tiempo el modelo de referencia para la protección de las empresas contra el malware, tanto conocido como desconocido. A diferencia de un antivirus, una lista de aplicaciones permitidas le permite controlar qué software, secuencias de comandos, ejecutables y bibliotecas pueden ejecutarse en sus terminales y servidores. Este enfoque no solo detiene el software maligno, sino que también evita que se ejecuten otras aplicaciones no permitidas. Este proceso minimiza en gran medida las amenazas cibernéticas y otras aplicaciones que no son autorizadas que se ejecutan en su red.

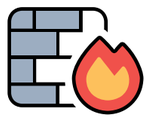




CARACTERISTÍCAS

Lista Blanca

Con la solución ThreatLocker®, Usted puede denegar la ejecución de cualquier aplicación en su dispositivo que no forme parte de la lista de aplicaciones permitidas. Esto ayuda a mitigar y evitar que se produzcan ciberataques en sus dispositivos o en toda su red.



Políticas de Aplicaciones Similares a un Firewall

Un potente motor de políticas similar a un Firewall que permite, deniega o restringe el acceso a aplicaciones a nivel granular.

Políticas Basadas en Tiempo

Permita el acceso a las aplicaciones durante un período de tiempo específico. Bloquee automáticamente la aplicación después de que la política haya expirado.

Aplicaciones Integradas

ThreatLocker® agrega automáticamente nuevos hashes cuando se lanzan actualizaciones de aplicaciones y sistemas, lo que permite que sus aplicaciones se actualicen sin interferencias y evita que se bloqueen las actualizaciones.

Ringfencing™

Ringfencing™ controla lo que las aplicaciones pueden hacer una vez que están siendo ejecutadas. Al limitar lo que puede hacer el software, ThreatLocker® puede reducir la probabilidad de que una vulnerabilidad tenga éxito o que un atacante utilice herramientas legítimas como PowerShell.

Ringfencing™ le permite controlar la forma en la que las aplicaciones pueden interactuar con otras aplicaciones. Por ejemplo, si bien Microsoft Word y PowerShell pueden estar permitidos, Ringfencing™ impedirá que Microsoft Word pueda llamar a PowerShell, lo que evitará que las vulnerabilidades, como Follina, tengan éxito.

Bajo operaciones normales, todas las aplicaciones permitidas en una máquina o servidor pueden acceder a todos los datos a los que puede acceder el usuario. Esto significa que si la aplicación se ve comprometida, el atacante puede usar la aplicación para robar o encriptar archivos. Ringfencing™ le permite quitar permisos de acceso a archivos para aplicaciones que no necesitan acceso e incluso quitar permisos de registro o de red.

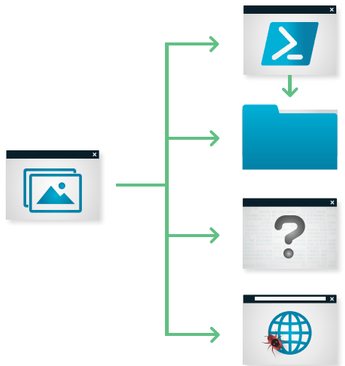


Fig. 2

Fig. 3

Figure 2: Demonstrates the Application Control Policies page, containing a list of Application policies. *Figure 3:* Demonstrates a partial policy list. The yellow fence icons appear beside Permit with Ringfence™ policies.

Cuando se implementa Ringfencing™ por primera vez, su dispositivo se alineará automáticamente con las políticas predeterminadas de ThreatLocker®. Luego, estas políticas serán automáticamente aplicadas a una lista de aplicaciones conocidas, como Microsoft Office, PowerShell o Zoom. El objetivo de las políticas predeterminadas es proporcionar un nivel básico de protección para todos los dispositivos. Cada una de estas políticas se puede manipular fácilmente para adaptarse a cualquier entorno en cualquier momento. Nuestro equipo de Cyber Heroes está siempre disponible para atender cualquier solicitud, las 24 horas del día, los 7 días de la semana, los 365 días del año.

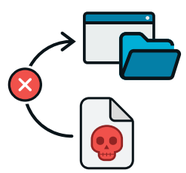
CARACTERISTÍCAS

Malware sin Archivos

Detenga el malware sin archivos limitando lo que las aplicaciones pueden hacer.

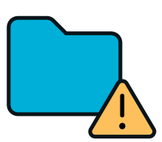
Políticas de Aplicación Granulares

Evite que las aplicaciones interactúen unas con otras, con recursos de red, claves de registro, archivos y más.



Limite Ataques a Aplicaciones

Limite los ataques a sus aplicaciones, como los saltos entre aplicaciones, controlando a qué tienen acceso a esas aplicaciones.



Limite el Acceso a sus Archivos

Una computadora promedio tiene más de 500 aplicaciones y solo algunas cuántas realmente necesitan acceder a sus archivos. Con Ringfencing™ usted decide qué aplicaciones necesitan ver qué archivos.

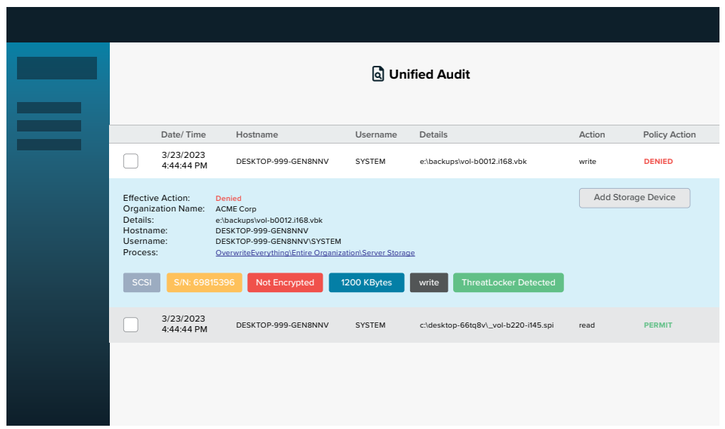
Control de Archivos

El Control de Archivos proporciona control basado en políticas sobre los dispositivos de almacenamiento, ya sea que el dispositivo de almacenamiento sea una carpeta local, un recurso compartido de red o un almacenamiento externo, como una unidad USB.

ThreatLocker® Storage Control permite establecer políticas granulares, que pueden ser tan simples como bloquear unidades USB, o tan detalladas como bloquear el acceso a sus copias de seguridad, excepto cuando su aplicación de respaldo quiere acceder a ellas.

Unified Audit proporciona un registro central de todo el acceso al almacenamiento por parte de los usuarios en la red y aquellos que trabajan de forma remota, hasta los archivos que se copiaron y el número de serie del dispositivo.

Cuando se bloquea un dispositivo de almacenamiento, al usuario se le presenta una ventana emergente donde puede solicitar acceso a dicho dispositivo. El administrador puede optar por permitir el dispositivo de almacenamiento en tan solo 60 segundos.



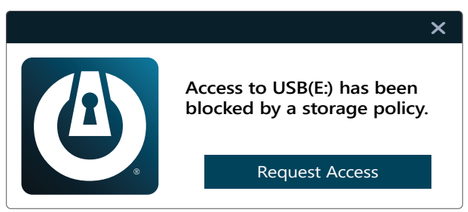


Figure 4: Demonstrates the Unified Audit page with a Storage Control Entry expanded, showing that the write access was denied.

CARACTERISTÍCAS

Auditoría de Acceso a Archivos

Se puede acceder de forma centralizada a una auditoría completa y detallada de todo el acceso a archivos en USB, red y discos duros locales a los pocos minutos de abrir un archivo.

Políticas de Almacenamiento Granulares

Estas políticas permiten o niegan el acceso al almacenamiento según el usuario, duración, aplicaciones y más.

Solicitudes de Acceso Sencillas

Al usuario se le presenta una ventana emergente con la opción de solicitar acceso al dispositivo de almacenamiento.

Bloqueo de USB Sencillo

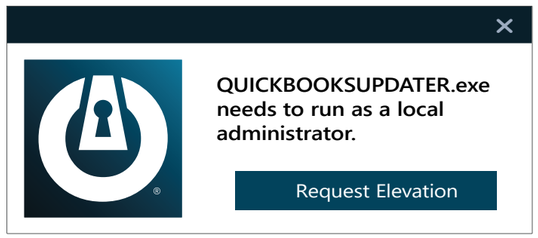
Las políticas de USB permiten el acceso según el número de serie del dispositivo, el proveedor y/o el tipo de archivo.

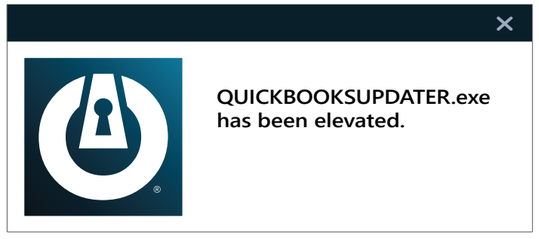
Control de Administradores

El Control de Administradores o Elevation Control, permite a los usuarios ejecutar aplicaciones específicas como administrador local, incluso cuando no tienen privilegios de administrador local.

Elevation Control pone a los administradores de TI en el asiento del conductor, lo que les permite controlar exactamente qué aplicaciones se pueden ejecutar como administrador local sin otorgar a los usuarios derechos de administrador local.

Cuando ThreatLocker® se implementa por primera vez, nuestro sistema aprende todas las aplicaciones que existen. Los administradores pueden revisar esas aplicaciones y seleccionar cuáles se pueden ejecutar como administrador local. Una vez habilitado, un usuario puede ejecutar el software como administrador local sin ingresar ninguna credencial.





CARACTERISTÍCAS

Visibilidad Total de los Derechos de Administrador

Le brinda la posibilidad de aprobar aplicaciones específicas para que se ejecuten como administrador, incluso si el usuario no es un administrador local.

Solucitudes De Permiso Centralizadas

Los usuarios pueden solicitar permisos para elevar aplicaciones y adjuntar archivos y notas para respaldar sus solicitudes.

Diferentes Niveles de Elevación

Permite establecer la duración en la cual se permite a los usuarios acceder a aplicaciones específicas mediante la concesión de acceso temporal o permanente.

Integración Segura de Aplicaciones

Ringfencing™ asegura que una vez que las aplicaciones hayan sido elevadas, los usuarios no puedan saltar para infiltrarse en las aplicaciones conectadas dentro de la red.

Control de Red

ThreatLocker® Control de Red es un firewall de terminales y servidores que le permite tener un control total sobre el tráfico de la red, lo que en última instancia lo ayuda a proteger sus dispositivos. Con políticas personalizadas, puede permitir el acceso granular en función de la dirección IP, palabras clave específicas, autenticación de agentes o ACL dinámicas.

¿POR QUÉ ES ESTO IMPORTANTE?

La red local ya no existe. Los usuarios no solo trabajan desde la oficina sino también de forma remota, lo que significa que la red que todos utilizamos se ha convertido rápidamente en Internet. Esta disolución del perímetro deja dispositivos y datos vulnerables y expuestos a amenazas cibernéticas. Es por eso que usted necesita controles de tráfico de red para proteger sus dispositivos y, por extensión, sus datos. Puede lograr esto implementando una solución de control de red (NC).

Fig. 5

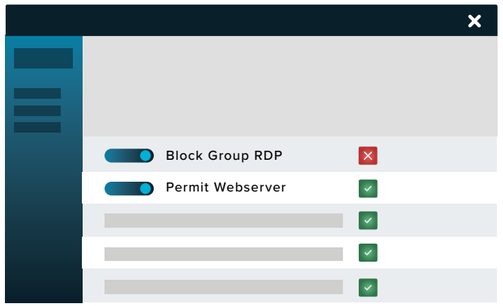
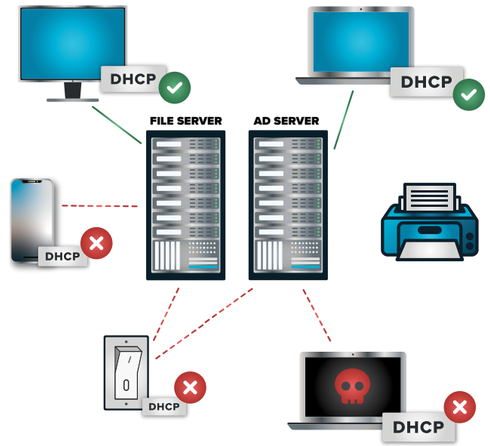


Figure 5: Depicts a partial Network Control policy list. *Figure 6:* Depicts a partial Network Control policy.

DINÁMICO ACLS

Las ACL dinámicas le permiten abrir puertos automáticamente en función de la ubicación de una computadora o grupo de computadoras en un momento determinado. Con las ACL dinámicas, la conexión entre el servidor y el cliente es directa, a diferencia de una VPN que necesita conectarse a través de un punto central.

Fig. 6



CARACTERISTÍCAS

Configurable

Control de Red brinda a los usuarios la capacidad de configurar el acceso a la red a los dispositivos mediante políticas globales y granulares.

Basada en la Nube

La solución administrada en la nube brinda a los clientes una vista centralizada de las políticas de terminales y el tráfico de red en toda su organización.

Dinámica

Control de Red permite a los usuarios denegar todo el tráfico a los servidores publicados mientras permite el acceso de una sola computadora por dirección IP o dinámicamente usando una palabra clave. Esto es genial para un usuario que viaja con frecuencia.

Seguridad de red mejorada

Asegure que los dispositivos no autorizados en su red no puedan acceder a sus servidores o terminales con ACL dinámicas.

THREATLOCKER®

ThreatLocker® improves enterprise-level server and endpoint security with zero trust controls, including Allowlisting, Ringfencing™, Elevation, Storage, Network Control, Configuration Management, and Operational Alert solutions.