lookwise®
DEVICE MANAGER

Lookwise Device Manager (LDM) es una plataforma de ciberseguridad OT centralizada y modular que ofrece un conjunto completo de funcionalidades para proteger, monitorizar y controlar sus dispositivos críticos.

Las amenazas cibernéticas son uno de los mayores problemas de cualquier organización, ya que los ciberdelincuentes son muy ágiles e innovadores a la hora de producir nuevos tipos de ataques lógicos basados en malware. Los sistemas críticos de las empresas son objetivos muy atractivos para los atacantes, por lo que es fundamental establecer medidas de seguridad estrictas.

PROTECCIÓN DE DISPOSITIVOS CRÍTICOS

Lookwise Device Manager es una solución perfecta para garantizar un alto nivel de seguridad en los dispositivos de propósito específico que son críticos para el negocio, como los cajeros automáticos, los terminales de punto de venta o los sistemas de control de infraestructuras críticas.

- Benefíciese de una tecnología galardonada e independiente del fabricante, diseñada específicamente para dispositivos críticos.
- Proteja sus sistemas críticos contra actividades maliciosas y fraudulentas con el modelo de protección por capas más completo del mercado.
- Despliegue de forma fácil y rápida para cumplir con sus políticas de seguridad, con un impacto mínimo en el rendimiento de sus dispositivos.
- Ahorre tiempo y dinero gracias a la operación de seguridad remota y centralizada desde una única GUI.
- Bloquee, detecte y resuelva los incidentes de seguridad que puedan surgir de sus activos.
- Visualice en tiempo real el hardware, el software y los usuarios instalados en sus dispositivos, y manténgase al tanto de cualquier cambio.
- Ejecute acciones remotas personalizadas en sus dispositivos en un entorno seguro y controlado.
- Ajuste la visibilidad y los permisos a las necesidades específicas de los diferentes equipos de operaciones.

ENTIENDA SU ENTORNO

Los dispositivos críticos proporcionan servicios esenciales que deben estar disponibles las 24 horas del día, los 365 días del año.
Mantenerlos seguros es primordial para tener éxito, ya que los ataques cibernéticos a los dispositivos críticos son muy selectivos y están diseñados para detectar cualquier vulnerabilidad de las aplicaciones instaladas.
Si no se mantiene adecuadamente esa tecnología, las consecuencias van desde el fraude financiero hasta la interrupción de la continuidad del negocio o incluso el sabotaje.
Al poner en marcha una estrategia eficaz de ciberseguridad OT, basada en una serie de tecnologías de protección adecuadas, se pueden proteger los dispositivos críticos sin interrumpir las operaciones ni arriesgarse a incumplir la normativa del sector. Lookwise Device Manager es una solución integral de ciberseguridad OT que ofrece el conjunto de medidas más avanzadas para proteger y responder a la nueva generación de ciberataques basados en malware.
Centraliza la definición de políticas y operaciones en un solo lugar, lo que permite proteger miles de dispositivos críticos sin afectar a la continuidad del negocio y faciltando el cumplimiento de las las políticas corporativas o de las normativas en materia de ciberseguridad. (PCI-DSS, NERC...).

MODELO INTEGRAL DE SEGURIDAD

Lookwise Device Manager es una plataforma modular que ofrece un conjunto completo de características para proteger y monitorizar sus dispositivos críticos, y añade una capa de control adicional que permite a los usuarios ejecutar acciones remotas personalizadas para investigar o reaccionar ante posibles incidentes.

PROTECCIÓN

Proteja sus dispositivos contra ataques maliciosos o cambios no controlados gracias a un sistema exhaustivo de seguridad por capas y basado en listas blancas que bloquea el acceso no autorizado a recursos de software y hardware.

LISTA BLANCA DE APLICACIONES

Evita la ejecución de programas informáticos malignos o no autorizados al definir una lista blanca de procesos que pueden ejecutarse, controlar los parámetros de la línea de comandos para los procesos vulnerables (intérpretes o herramientas del sistema) y restringir el acceso a las librerías críticas.
Reduce la superficie de ataque al conjunto mínimo de procesos necesarios para garantizar el correcto funcionamiento del dispositivo.

PROTECCIÓN DE LA INTEGRIDAD EN EL SISTEMA DA ARCHIVOS

Evita la manipulación no autorizada de archivos o carpetas críticas en el sistema de archivos bloqueando el acceso a ficheros con hashes SHA-256 inválidos, en base a reglas globales de extensiones, directorios o rutas de los archivos.
Conserva la integridad de la imagen del software certificado, lo que permite que solo los procesos de confianza modifiquen los archivos o carpetas protegidos y controla su integridad frente a una base de datos centralizada de hashes SHA-256 válidos.

PROTECCIÓN DE HARDWARE

Evita la conexión de dispositivos de hardware fraudulentos o no autorizados que no estén incluidos en una lista blanca de sistemas legítimos. Limita aún más el nivel de acceso (lectura-escritura) para los dispositivos de almacenamiento autorizados (USB, CDROM, disquete, MTP). Simplifica la configuración utilizando listas blancas locales complementadas con reglas generales allow/deny (permitir/denegar). También se puede reportar la conexión/desconexión de dispositivos autorizados.

CIFRADO DE DISCO COMPLETO

Evita que se acceda al disco duro desde fuera del sistema operativo utilizando un sistema de cifrado por sectores y claves únicas gestionadas de forma segura, lo que permite iniciar el sistema sin supervisión y llevar a cabo el descifrado fuera de línea.
Mantiene la confidencialidad de los datos almacenados con un impacto mínimo en el rendimiento, sin interferir en las operaciones del dispositivo.

MONITORIZACIÓN

Vea en tiempo real el software, el hardware y los usuarios instalados en sus dispositivos y supervise los cambios que puedan ser indicio de actividades fraudulentas.

INVENTARIO DE HARDWARE

Permite a los usuarios obtener un inventario del hardware del dispositivo, con la opción de generar alertas en caso de conexiones o desconexiones del hardware.

INVENTARIO DE LAS APLICACIONES

Permite a los usuarios obtener un inventario de los parches de software y de sistema operativo instalados en el dispositivo, y les permite alertar en caso de presencia de software no autorizado o de ausencia de parches críticos.

MONITORIZACIÓN DE USUARIOS

Permite obtener un inventario de los usuarios locales del sistema operativo, y recibir una alerta en caso de creación, modification o eliminación de cuentas de usuario.

MONITORIZACIÓN DE ARCHIVOS Y DIRECTORIOS

Monitoriza y alerta a los usuarios cuando se modifican archivos o directorios que se consideran críticos.

CONTROL

Ejecute acciones remotas en sus dispositivos, facilitando así las operaciones y actividades de mantenimiento.

Reinicio remoto y cambio de contraseña

Reinicie el dispositivo o cambie la contraseña de los usuarios del dispositivo de forma remota desde la consola central LDM.

Recuperación de información

Recupere de forma remota archivos o directorios de los dispositivos monitorizados.

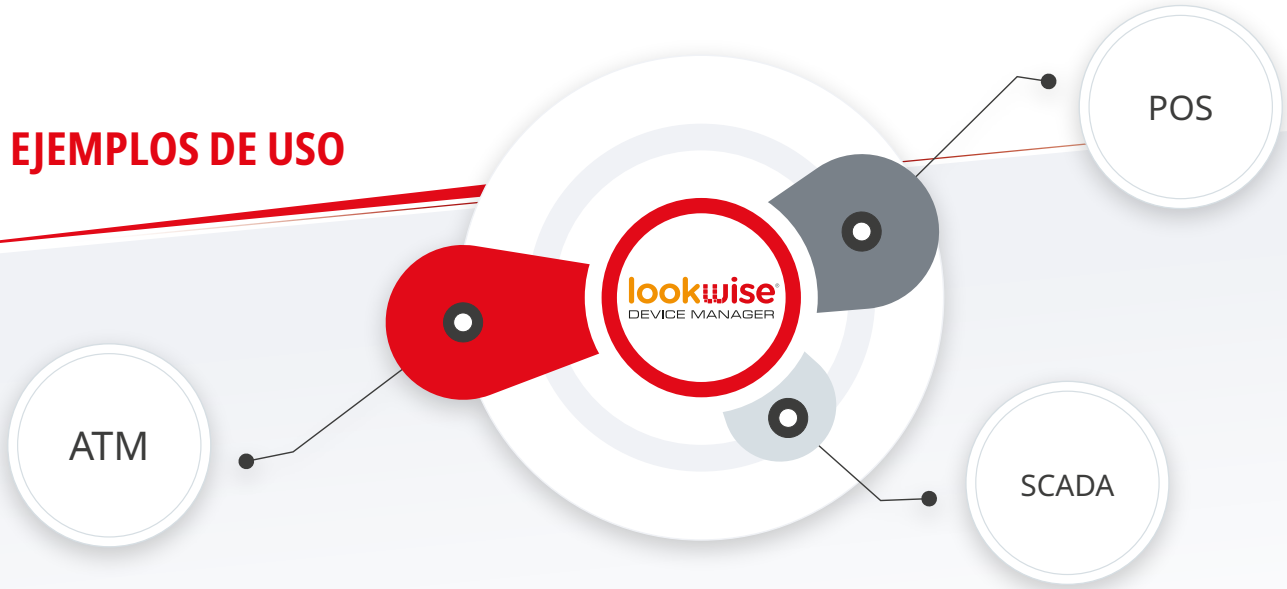
Ejecución remota de acciones personalizadas

Cree sus propias acciones remotas personalizadas para diversos propósitos como análisis forense, cambios en configuración, instalación de parches o desinfección de malware.

Ejecute acciones remotas personalizadas en los dispositivos, cargando o ejecutando binarios o scripts locales, obteniendo y centralizando los resultados.

Las acciones remotas están preintegradas con los controles de lista blanca de aplicaciones e integridad del sistema de archivos y solo pueden ejecutarse desde la consola LDM (no localmente en el dispositivo).

EJEMPLOS DE USO



CAJEROS AUTOMÁTICOS

Los cajeros automáticos son objetivos muy atractivos para los atacantes porque contienen dinero en efectivo y gestionan información sensible, como números de tarjetas de crédito/débito y PIN, y se encuentran en entornos desatendidos o no suficientemente vigilados. La gran variedad de equipos y aplicaciones heredados en las redes de cajeros automáticos, junto con la falta de políticas activas de actualización debido a las limitaciones técnicas y económicas, hacen que estas redes sean entornos intrínsecamente vulnerables.

En este escenario, los ciberdelincuentes son muy ágiles e innovadores a la hora de producir nuevos tipos de ataques lógicos dirigidos, que son mucho más rentables que los ataques físicos tradicionales.

TERMINALES DE PUNTO DE VENTA

La naturaleza de los terminales de punto de venta, que tratan datos sensibles como números de tarjeta y PIN, los hace muy vulnerables a los ataques dirigidos o a las acciones fraudulentas.

Gracias a un control basado en listas blancas de las aplicaciones o dispositivos de hardware autorizados, los usuarios pueden tener mayor confianza en la seguridad de estos equipos.

SISTEMAS DE CONTROL EN INFRAESTRUCTURAS CRÍTICAS

Los sistemas de automatización y control de las infraestructuras críticas dependen cada vez más de las comunicaciones remotas y de la interconexión con la infraestructura informática, heredando algunos de sus riesgos y vulnerabilidades.

Un ciberataque a los sistemas de control puede causar un daño importante, desde la denegación masiva de los servicios básicos hasta poner en peligro tanto la infraestructura como a las personas. Por lo tanto, deben aplicarse las medidas de seguridad más estrictas a estos sistemas tan sensibles.

CARACTERÍSTICAS

Lookwise Device Manager se basa en la tecnología propietaria de Auriga Lookwise TECH. Esta tecnología, diseñada específicamente para entornos distribuidos y para sistemas operativos Windows XP/7/10, aporta al producto su modularidad, escalabilidad y flexibilidad.

GESTIÓN

- Administración centralizada y GUI de operaciones
- Creación y distribución remota de políticas
- Integración de alertas e informes de resultados
- Panel de control de seguridad
- Visibilidad basada en roles y permisos
- Integración SIEM

COMUNICACIONES

- Autenticadas y cifradas
- Ininterrumpidas
- Comprimidas
- Compatible con redes inestables y con ancho de banda limitado

ARQUITECTURA

- Distribuida
- Modular
- Flexible y escalable
- Balanceo de carga
- Despliegue remoto de funcionalidades y actualizaciones
- Consumo de recursos muy reducido