lookwise®
DEVICE MANAGER

Lookwise Device Manager (LDM) è una piattaforma di OT Cybersecurity che ti consente di gestire la sicurezza dei dispositivi critici della tua organizzazione proteggendo, monitorando e controllando i tuoi asset a livello centrale.

Le minacce informatiche attualmente sono una delle maggiori preoccupazioni per qualsiasi organizzazione, in quanto i criminali informatici dimostrano di essere estremamente svelti e innovativi nella creazione di nuovi tipi di attacchi logici basati su malware. I sistemi aziendali critici sono obiettivi molto interessanti per i criminali e la proliferazione di attacchi mirati rende necessaria la creazione di misure di sicurezza severe.

PROTEGGERE I DISPOSITIVI CRITICI PER IL BUSINESS

Lookwise Device Manager è una soluzione perfetta per assicurare gli alti standard di sicurezza per i dispositivi fix-purpose che sono critici per l'azienda, come ATM, terminali POS, sistemi di controllo di infrastrutture critiche, ecc.

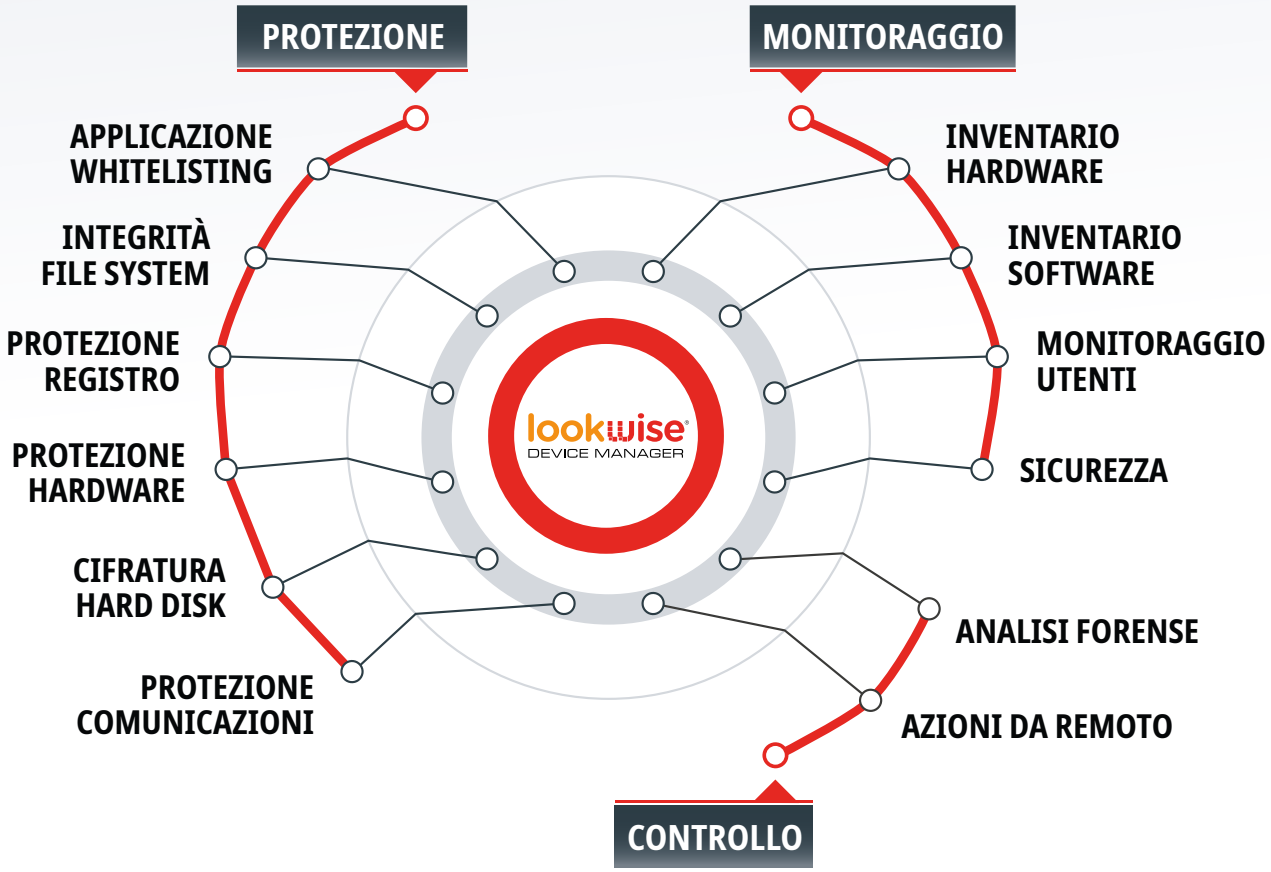
- Tecnologia premiata, agnostica e specifica per i dispositivi critici.
- Blocca, rileva e risolve qualsiasi incidente di sicurezza sui tuoi dispositivi.
- Protegge i sistemi critici dalle azioni fraudolente tramite un modello di protezione a più livelli.
- Mostra tutti gli hardware, software e utenti collegati ai tuoi dispositivi in tempo reale, rimanendo aggiornati su ogni eventuale cambiamento.
- Esegue azioni personalizzate da remoto sui tuoi dispositivi in un ambiente sicuro e controllato.
- Personalizza gli accessi e i permessi in base alle specifiche necessità dei diversi team operativi.
- Facilmente implementabile, conforme alle policy di sicurezza, con impatto minimo sulla performance dei dispositivi.
- Tempi e investimenti ottimizzati grazie ad una singola dashboard dalla quale effettuare operazioni di sicurezza remote e centralizzate.

ANALIZZA IL TUO SCENARIO

I dispositivi critici forniscono servizi essenziali che devono essere disponibili 24 ore su 24, 365 giorni l'anno. Salvaguardare la sicurezza dei dispositivi critici è essenziale: costituiscono infatti il target principale degli attacchi informatici, che mirano ad individuare ogni eventuale vulnerabilità contenuta nel software. La mancanza di un'adeguata manutenzione della tecnologia può portare a conseguenze come la frode finanziaria, l'interruzione della continuità operativa ed il sabotaggio. Dotarsi di una efficace strategia di OT Cybersecurity, basata sul giusto set di tecnologie di protezione, permette di proteggere i dispositivi critici senza interferire con l'operatività o rischiare la non conformità alle norme settoriali. Lookwise Device Manager è una soluzione di OT Cybersecurity integrata che fornisce il più evoluto set di contromisure di protezione, per reagire efficacemente ai cyberattacchi di nuova generazione basati sul malware. LDM permette di centralizzare la definizione di policy e operazioni, proteggendo migliaia di dispositivi critici senza però intaccare la continuità operativa e favorendo la conformità alle norme relative alla cybersecurity o alle policy corporative (PCI-DSS, NERC...).

MODELLO DI PROTEZIONE OLISTICO

Lookwise Device Manager è una piattaforma modulare che offre funzionalità di protezione e monitoraggio per garantire una appropriata sicurezza dei dispositivi critici. Attraverso l'attivazione di un ulteriore livello funzionale, permette di avviare azioni di controllo da remoto e personalizzate e investigare su potenziali attacchi o reagire in maniera immediata a seguito di incidenti di sicurezza.



PROTEZIONE

Protegge la tua apparecchiatura da attacchi illeciti bloccando l'accesso a risorse non autorizzate, sulla base di white list.

APPLICAZIONE WHITELISTING

Previene l'esecuzione di malware o software non autorizzati, definendo una whitelist di processi che possono essere eseguiti, controllando i parametri a livello di riga di comando per processi sensibili (interpreti o strumenti di sistema) e limitando l'accesso alle librerie critiche.
Riduce la superficie attaccabile al minimo set di processi necessari a garantire la corretta operatività del dispositivo.

PROTEZIONE DELL'INTEGRITÀ DEI FILE DI SISTEMA

Impedisce la manipolazione non controllata dei file critici o cartelle nel file di sistema e blocca l'accesso a file non validi, mediante controllo dell'hash e attraverso regole di protezione di file, estensioni globali o directory. Salvaguarda l'integrità dell'immagine del software certificato, permettendo solo ai processi autorizzati di modificare le cartelle o i file protetti e controllandone l'integrità in relazione ad un database centrale di funzioni di hash valide.

PROTEZIONE HARDWARE

Previene la connessione di hardware fraudolenti e non autorizzati, ovvero al di fuori della whitelist dei device legittimi. Inoltre, limita il livello d'accesso (lettura-scrittura) per i dispositivi di archiviazione (USB, CD-ROM, floppy disk, MTP). Semplifica la configurazione utilizzando whitelist dei dispositivi locali insieme a regole generali di permesso/divieto. È possibile inoltre visualizzare le connessioni/disconnessioni dei dispositivi autorizzati.

CIFRATURA COMPLETA DEL DISCO

Previene l'accesso all'hard disk al di fuori del sistema operativo utilizzando una cifratura a livello di settore e codici univoci gestiti in sicurezza, permettendo l'avvio da remoto e la decifratura offline. Salvaguarda la privacy dei dati in memoria con impatto minimo sulla performance e senza interferire con l'operatività del dispositivo.

MONITORAGGIO

Consente di ottenere informazioni in real time su hardware, software e utenti censiti e operanti oltre a monitorare eventi di modifica degli stessi che possono essere indicativi di azioni fraudolente.

INVENTARIO HARDWARE

Consente di ottenere a livello centrale l'inventario hardware dell'apparecchiatura, con l'opzione di inviare alert se al dispositivo vengono connessi o disconnessi degli hardware.

INVENTARIO SOFTWARE

Consente agli utenti di ottenere un inventario software e patch del sistema installati sull'apparecchiatura, con la possibilità di allertare la presenza di software non autorizzati o l'assenza di patch di sistema critici.

MONITORAGGIO UTENTE

Consente di monitorare a livello centrale modifiche relative agli utenti locali, inviando alert se vengono modificati, creati o eliminati account di utenti.

MONITORAGGIO FILE E DIRECTORY

Monitora e invia alert quando i file o le directory considerate critiche subiscono delle modifiche.

CONTROLLO

Consente di eseguire azioni sulla tua apparecchiatura da remoto, facilitando, in questa maniera, attività operative e di manutenzione.

Riavvio e modifica della password da remoto

Riavvia il dispositivo o effettua il cambio password degli utenti da remoto attraverso la console centrale.

Recupero delle informazioni

Recupera file o directory dalle apparecchiature monitorate da remoto.

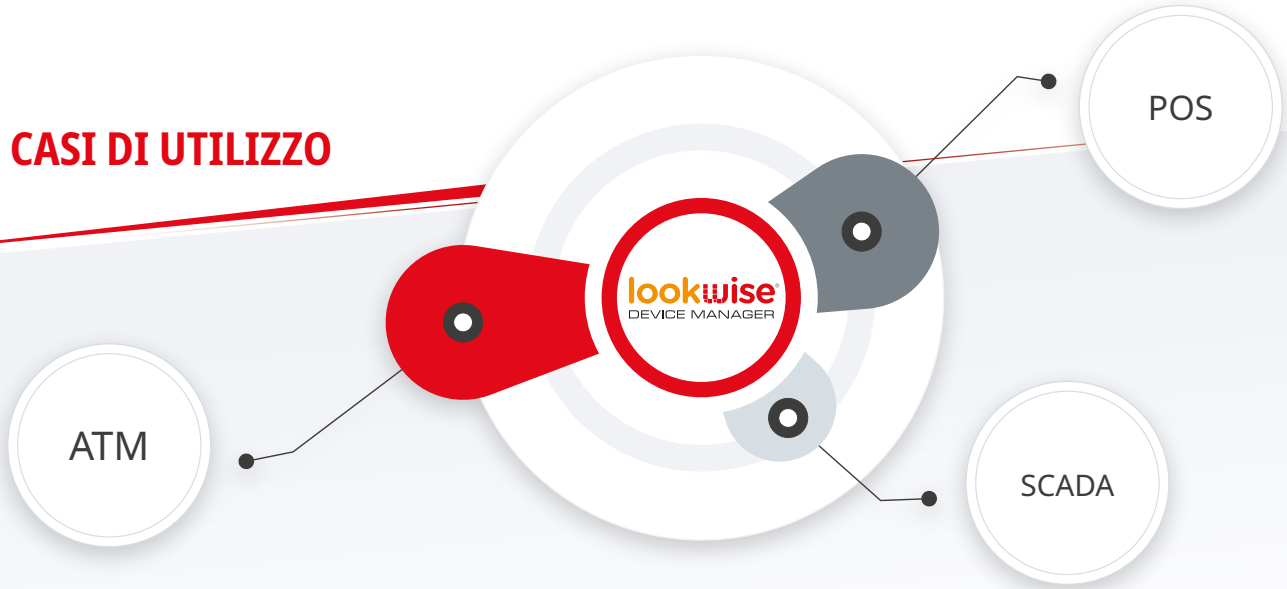
Esecuzione di azioni remote personalizzate

Crea azioni personalizzate per diverse funzioni, come l'analisi forense, la configurazione delle modifiche, implementazione delle patch, la disinfezione dal malware.

Esegue azioni personalizzate sui dispositivi, caricando o eseguendo i file binari locali o gli script, e centralizza i risultati ottenuti.

Le azioni remote sono pre-integrate nell'applicazione del Whitelisting e possono essere eseguite unicamente dalla console LDM e di Integrità del File System, non localmente sul dispositivo.

CASI DI UTILIZZO



ATM

Gli ATM per loro natura sono obiettivi molto interessanti per gli attacchi esterni, perché contengono contanti e gestiscono informazioni sensibili sulle carte di credito e codici di accesso ai conti bancari, oltre ad essere localizzati in ambienti non presidiati o non sufficientemente sorvegliati. L'utilizzo di hardware e software eterogenei a cui si aggiunge la mancanza di politiche di aggiornamento proattivo causata da impedimenti tecnici o mancanza di risorse, rende i dispositivi nella rete ATM, altamente vulnerabili.

In questo scenario, i criminali informatici sono estremamente svelti e innovativi nella creazione di nuovi tipi di attacchi locali mirati, molto più economicamente vantaggiosi degli attacchi fisici tradizionali.

POS

La natura stessa dei terminali POS, i quali gestiscono dati sensibili come numeri di carte di credito e PIN, rende questi ultimi altamente vulnerabili ad attacchi mirati o azioni fraudolente mirate.

Un sistema di whitelisting basato sul controllo delle applicazioni e dei dispositivi hardware autorizzati, consente di aumentare il livello di sicurezza nell'uso di questo strumento.

SISTEMI DI CONTROLLO NELLE INFRASTRUTTURE CRITICHE

L'automazione e i sistemi di controllo nelle infrastrutture critiche dipendono sempre più dalle comunicazioni remote e dall'interconnessione con le infrastrutture IT, ereditando così alcune delle loro intrinseche vulnerabilità e rischi.

Un cyberattacco sui sistemi di controllo può causare ingenti danni, dal blocco massivo del servizio ad un potenziale pericolo, sia per le infrastrutture che per le persone. Questi sistemi sensibili devono essere perciò protetti secondo i più elevati standard di sicurezza.

CARATTERISTICHE

Lookwise Device Manager è progettato sulla base della tecnologia Lookwise TECH di proprietà di Auriga. Questa tecnologia, specificatamente progettata per ambienti distribuiti e per sistemi operativi Windows XP/7/10, fornisce al prodotto modularità, scalabilità e flessibilità.

GESTIONE CENTRALIZZATA

- Amministrazione centralizzata e operazioni user oriented
- Creazione e distribuzione di policy da remoto
- Integrazione di alert e report sui risultati
- Dashboard unica
- Visibilità sulla base di ruoli e permessi
- Integrazione SIEM

COMUNICAZIONI

- Autenticate e crittografate
- Continue
- Compresse
- Compatibili con reti e link instabili

ARCHITETTURA

- Distribuita
- Modulare
- Flessibile e scalabile
- Dotata di bilanciamento del carico
- Aggiornamenti di nuove funzionalità da remoto
- Consumo di risorse limitato