lookwise®
DEVICE MANAGER

Lookwise Device Manager (LDM) is a centralised and modular OT cybersecurity platform that offers a comprehensive set of functionalities to protect, monitor and control your critical devices.

Cyber threats are one of the biggest concerns for any organisation, with cyber criminals proving to be extremely agile and innovative in producing new types of logical attacks based on malware. Business critical systems are very attractive targets for attackers, making it critical to set strict security measures.

PROTECTING CRITICAL DEVICES

Lookwise Device Manager is a perfect-fit solution to ensure high security standards in fix-purpose devices that are critical to the business, such as ATMs, point of sale terminals or critical infrastructure control systems.

- Benefit from award-winning, vendor-agnostic technology specifically designed for critical devices.
- Protect your critical systems from malicious and fraudulent activities, with the most comprehensive layered protection model.
- Easily implementable to quickly comply with your security policies, with minimal performance impact on your devices.
- Save time and money thanks to remote and centralised security operations from a single GUI.
- Block, detect and solve security incidents that may arise from your assets.
- Get real-time visibility into the hardware, software and users installed on your devices, and stay in loop with any changes.
- Execute customised remote actions on your devices in a secure and controlled environment.
- Adapt visibility and permissions to the specific needs of the different operations teams.

UNDERSTAND YOUR ENVIRONMENT

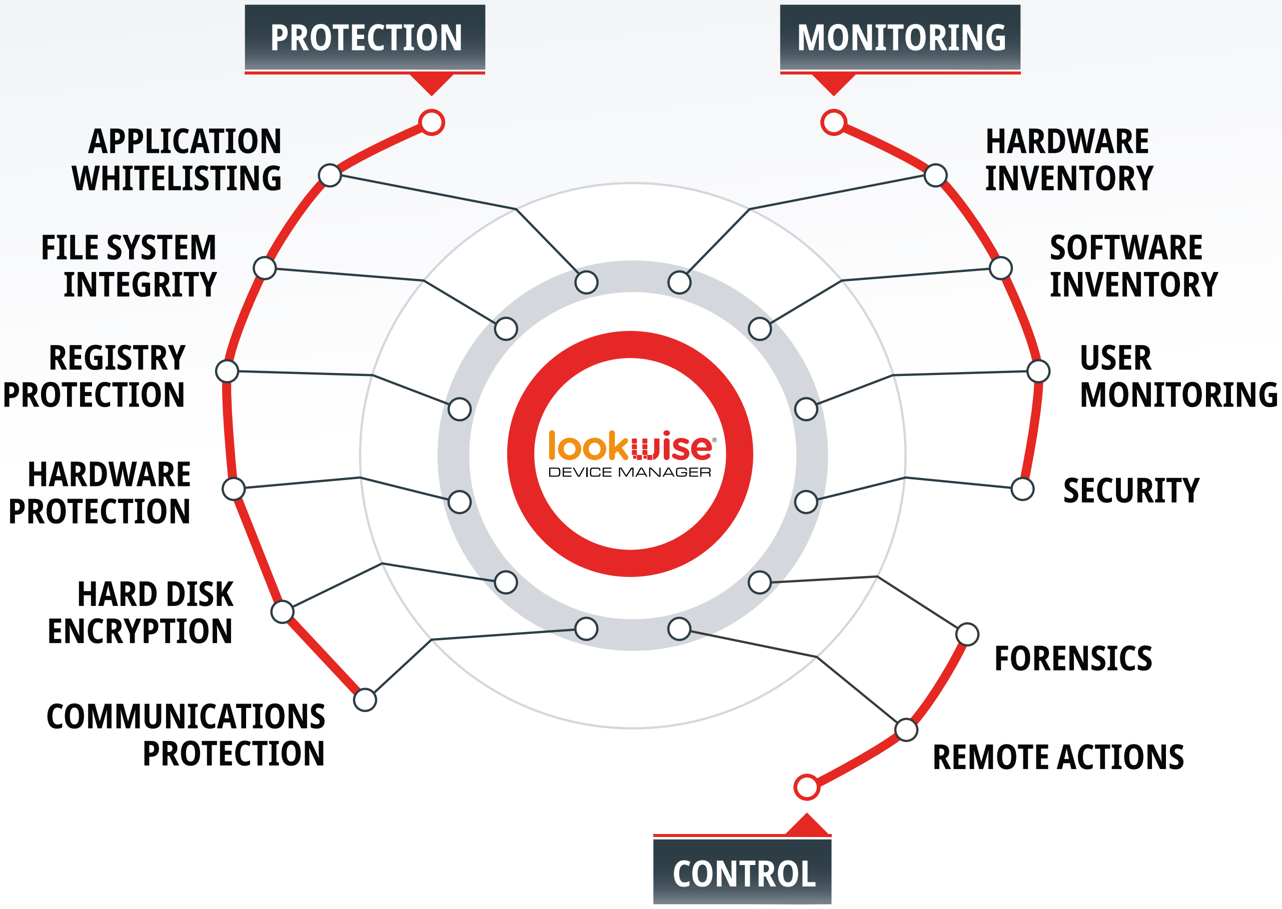
Critical devices provide essential services that need to be available 24/7, 365 days a year. Keeping them secure is paramount to success, as cyber-attacks on critical devices are highly targeted and designed to spot any embedded software vulnerabilities. The consequences of not maintaining such technology properly ranges from financial fraud to business continuity interruption or even sabotage.

By putting an effective OT cybersecurity strategy in place, based on the right set of protection technologies, it is possible to secure critical devices without disrupting operations or risking non-compliance with sectorial regulations.

Lookwise Device Manager is an integrated OT cybersecurity solution that provides the most advanced set of countermeasures to protect and respond to the new generation of cyber-attacks based on malware. It centralises policy definition and operations at a single point allowing you to protect thousands of critical devices without affecting business continuity and favoring compliance with cybersecurity regulations or corporate policies. (PCI-DSS, NERC...).

HOLISTIC SECURITY MODEL

Lookwise Device Manager is a modular platform that offers a comprehensive set of features to protect and monitor your critical devices, adding an extra control layer that allows users to run custom remote actions to investigate or react to potential incidents.



PROTECTION

Protect your devices against malicious attacks or uncontrolled changes, with the most comprehensive layered security approach to block access to unauthorised software and hardware resources, based on whitelists.

APPLICATION WHITELISTING

Prevents execution of malware or unauthorised software by defining a whitelist of processes that can be executed, controlling command-line parameters for sensitive processes (interpreters or system tools) and restricting access to critical libraries.
Reduces the attack surface to the minimum set of processes that are needed to guarantee the correct operation of the device.

FILE SYSTEM INTEGRITY PROTECTION

Prevents uncontrolled manipulation of critical files or folders in the file system while blocking access to files with invalid SHA-256 hashes, based on global extension, directory or file protection rules.
Preserves the integrity of the certified software image, allowing only trusted processes to modify protected files or folders and controlling its integrity against a central database of valid SHA-256 hashes.

HARDWARE PROTECTION

Prevents connection of fraudulent or unauthorized hardware devices not included in a whitelist of legitimate hardware identifiers. It further limits the access level (read-write) for authorized storage devices (USB, CDROM, floppy disk, MTP). Simplifies the configuration using local device white lists complemented with global allow/deny rules. Connections/disconnections of authorized devices can also be reported.

FULL DISK ENCRYPTION

Prevents hard disk access from outside the operating system using sector-level encryption and securely managed unique keys, allowing for unattended booting and off-line decryption.
Preserves storage data confidentiality with minimal performance impact not interfering with the device operations.

MONITORING

Obtain real-time visibility on the software, hardware and users installed on your devices and monitor changes that might be indicative of fraudulent activities.

HARDWARE INVENTORY

Allows users to obtain a hardware inventory of the device, with the option to generate alerts in case of hardware connections or disconnections.

SOFTWARE INVENTORY

Allows users to obtain an inventory of the software and operating system patches installed in the device, with the ability to alert in case of presence of unauthorized software or absence of critical operating system patches.

USER MONITOR

Allows users to obtain an inventory of the local operating system users, alerting them in case of creation, modification or deletion of user accounts.

FILE AND DIRECTORY MONITOR

Monitors and alerts users when files or directories deemed critical are modified.

CONTROL

Remotely execute actions on your devices, thus facilitating operations and maintenance activities.

Remote reboot and password change

Reboot the device or change the password of the device users remotely from the central LDM console.

Information retrieval

Remotely retrieve files or directories from the monitored devices.

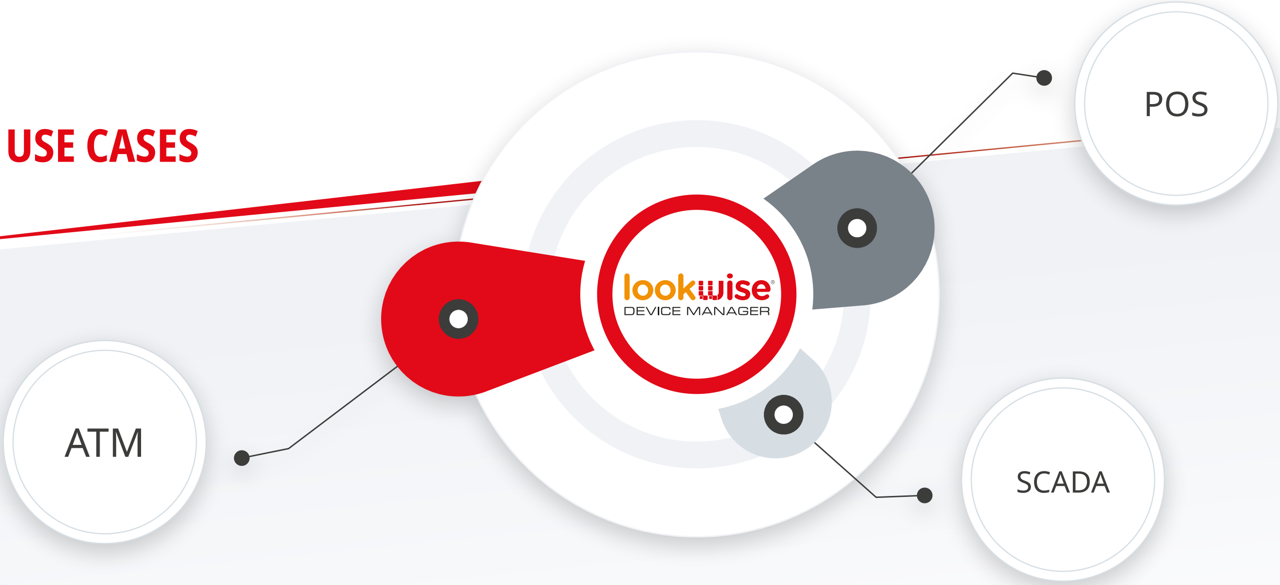
Custom Remote Action Execution

Create your own customised remote actions for multiple purposes like forensic analysis, configuration changes, patch deployment, malware disinfection.

Run custom remote actions on the devices, uploading or executing local binaries or scripts, obtaining and centralising the results.

Remote actions are pre-integrated with Application Whitelisting and File System Integrity, and can only be executed from the LDM console (not locally on the device).

USE CASES



ATM MACHINES

ATMs are very attractive targets for attackers because they contain cash and manage sensitive information like credit / debit card and PIN numbers, while being in unattended or insufficiently surveilled environments. The wide variety of legacy hardware and software in ATM networks, coupled with a lack of proactive upgrade policies derived from technical and economical constraints make these networks inherently vulnerable environments.

In this scenario, cyber-criminals are extremely agile and innovative in producing new types of targeted logical attacks, which are much more cost effective than traditional physical attacks.

POINT OF SALES TERMINALS

The nature of Point of Sale terminals, that handle sensitive data like card numbers and PINs, makes them very vulnerable to targeted attacks or fraudulent actions.

A whitelisting-based control of the authorised applications or hardware devices, allows users to raise the level of confidence in the security of this equipment.

CONTROL SYSTEMS IN CRITICAL INFRASTRUCTURES

Automation and control systems in critical infrastructures are more and more dependent on remote communications and interconnection with IT infrastructure, inheriting some of its risks and vulnerabilities.

A cyber-attack on control systems can cause tremendous damage, from massive denial of basic services to putting both infrastructure and people in potential danger. Therefore the highest security standards should be applied to these sensitive systems.

lookwise®
DEVICE MANAGER

CHARACTERISTICS

Lookwise Device Manager is built on the basis of Auriga's proprietary technology Lookwise TECH. This technology, specifically designed for distributed environments and for Windows XP/7/10 OS, provides the product with its modularity, scalability and flexibility.

MANAGEMENT

- Centralised administration and operations GUI
- Remote policy creation and distribution
- Integration of alerts and reporting on results
- Security dashboard
- Visibility based on roles and permissions
- SIEM integration

COMMUNICATIONS

- Authenticated and encrypted
- Continuous
- Compressed
- Designed to support unstable and low bandwidth networks

ARCHITECTURE

- Distributed
- Modular
- Flexible and scalable
- Load balancing
- Remote deployment of functionalities and updates
- Very limited resource consumption

AURIGA
the banking e-volution

Headquarters:
Bari (Italy)

Offices:
Auriga International

www.aurigaspa.com