lookwise®
DEVICE MANAGER

Lookwise Device Manager ist eine zentralisierte und modulare betriebstechnische („Operational Technology-“, OT-) Cybersicherheitsplattform, die umfassende Funktionen zum Schutz, zur Überwachung und zur Steuerung Ihrer kritischen Geräte bietet.

Cyberbedrohungen zählen zu den größten Gefahren für jede Organisation. Cyberkriminelle erweisen sich bei der Entwicklung neuer Arten von Malware als äußerst flexibel und innovativ.
Geschäftskritische Systeme sind sehr attraktive Ziele für Angreifer. Starke Sicherheitsmaßnahmen sind daher von größter Bedeutung.

KRITISCHE GERÄTE SCHÜTZEN

Lookwise Device Manager ist die perfekte Lösung um hohe Sicherheitsstandards für zweckbestimmte, geschäftskritische Geräte wie Geldautomaten, Kassenterminals und Kontrollsysteme für kritische Infrastrukturen zu gewährleisten.

- Profitieren Sie von preisgekrönter, herstellerunabhängiger Technologie, die speziell für kritische Geräte entwickelt wurde.
- Schützen Sie mit dem umfassendsten mehrstufigen Schutzmodell Ihre kritischen Systeme vor böswilligen und betrügerischen Aktivitäten.
- Einfache Implementierung sorgt für die rasche Einhaltung Ihrer Sicherheitsrichtlinien mit minimalen Auswirkungen auf die Leistung Ihrer Geräte.
- Sparen Sie Zeit und Geld dank zentralisierter Sicherheitsmaßnahmen per Fernzugriff über eine einzige Benutzeroberfläche.
- Blockieren, erkennen und lösen Sie Sicherheitsvorfälle, die von Ihren Anlagen ausgehen können.
- Verschaffen Sie sich einen Echtzeitüberblick über die auf Ihren Geräten installierte Hardware und Software sowie über ihre Benutzer und lassen Sie sich über Änderungen informieren.
- Führen Sie auf Ihren Geräten individualisierte Remote-Aktionen in einer sicheren und kontrollierten Umgebung aus.
- Passen Sie Sichtbarkeit und Berechtigungen an die spezifischen Bedürfnisse der verschiedenen Betriebsteams an.

DIE UMGEBUNG VERSTEHEN

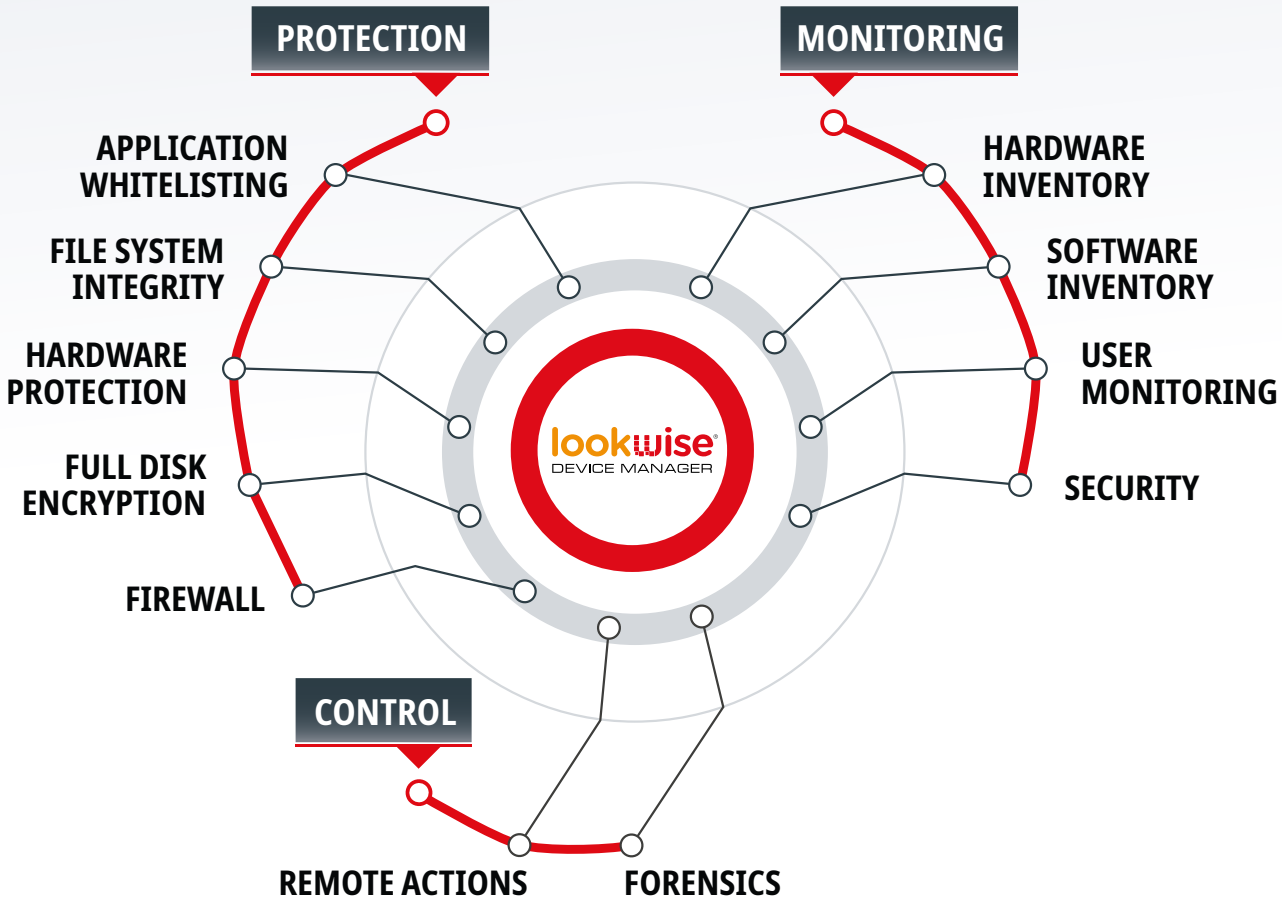
Kritische Geräte stellen wesentliche Dienste bereit, die an 365 Tagen im Jahr rund um die Uhr verfügbar sein müssen. Ihre Sicherheit hat höchste Priorität für den Geschäftserfolg: Cyberangriffe auf kritische Geräte sind sehr zielgerichtet und auf das Erkennen von in der Software enthaltenen Schwachstellen ausgelegt. Die Folgen einer nicht ordnungsgemäßen Wartung derartiger Technologie reichen von finanziellem Betrug bis zur Betriebsunterbrechung oder sogar Sabotage.

Durch die Einführung einer wirksamen betriebstechnischen OT-Cybersicherheitsstrategie, basierend auf geeigneten Schutztechnologien, ist es möglich, kritische Geräte zu sichern, ohne den Betrieb zu unterbrechen oder die Nichteinhaltung sektoraler Vorschriften zu riskieren.

Die integrierte OT-Cybersicherheitslösung Lookwise Device Manager bietet modernste Gegenmaßnahmen, die vor der neuen Generation von auf Malware basierenden Cyberangriffen schützt und darauf reagiert. Sie zentralisiert Richtliniendefinition und Betrieb an einer Stelle. So schützen Sie Tausende von kritischen Geräten ohne Beeinträchtigung der Geschäftskontinuität, was die Einhaltung von Cybersicherheitsvorschriften oder Unternehmensrichtlinien begünstigt (PCI-DSS, NERC...).

GANZHEITLICHES SICHERHEITSMODELL

Die modulare Plattform Lookwise Device Manager bietet umfassende Funktionen zum Schutz und zur Überwachung Ihrer kritischen Geräte. Eine zusätzliche Steuerungsebene ermöglicht den Benutzern, mögliche Vorfälle im Wege benutzerdefinierter Remote-Aktionen zu untersuchen oder darauf zu reagieren.



SCHUTZ

Schützen Sie Ihre Geräte anhand von Whitelists vor böswilligen Angriffen oder unkontrollierten Änderungen mit dem umfassendsten mehrstufigen Sicherheitskonzept zur Blockierung des Zugriffs auf unerlaubte Software- und Hardwareressourcen.

ANWENDUNG WHITELISTING

Verhindert die Ausführung von Malware oder unerlaubter Software mittels Erstellung einer Whitelist ausführbarer Prozesse – durch die Kontrolle von Befehlszeilenparametern für sensible Prozesse (Interpreter oder Systemtools) sowie durch die Beschränkung des Zugriffs auf kritische Bibliotheken. Reduziert die Angriffsfläche auf höchstens jene Prozesse, die für die Gewährleistung des korrekten Betriebs eines Geräts erforderlich sind.

SCHUTZ DER DATEISYSTEMINTEGRITÄT

Verhindert den Verbindungsaufbau mit betrügerischer oder nicht autorisierter Hardwaregeräte, die nicht in einer Whitelist von legitimen Hardware-Kennungen enthalten sind. Weitere Einschränkung der Zugriffsebene (Lesen/Schreiben) für autorisierte Speichergeräte (USB, CDROM, Diskette, MTP). Vereinfachte Konfiguration durch lokale Geräte-Whitelists ergänzt mit globalen Zulassen/Ablehnen-Regeln. Verbindungen/Trennungen von autorisierten Geräten können ebenfalls gemeldet werden.

HARDWARESCHUTZ

Verhindert den Anschluss von betrügerischer Hardware: Hardware-Geräte, die nicht in einer Whitelist von Hardwarekennungen enthalten sind, werden blockiert; die Zugriffsebene (Lesen-Schreiben) für Speichergeräte (USB, CD-ROM, Diskette, MTP) wird eingeschränkt.
Vereinfacht die Konfiguration mithilfe lokaler Geräte-Whitelists, ergänzt durch globale Regeln für Zulassen/Verweigern.
Das Anschließen/Trennen erlaubter Geräte kann ebenfalls gemeldet werden.

VOLLSTÄNDIGE FESTPLATTENVERSCHLÜSSELUNG

Verhindert den Festplattenzugriff von außerhalb des Betriebssystems durch Verschlüsselung auf Sektorebene und sicher verwaltete eindeutige Schlüssel. Das ermöglicht unbeaufsichtigtes Booten und Offline-Entschlüsseln.
Wahrt die Vertraulichkeit gespeicherter Daten bei minimaler Beeinträchtigung der Leistung, ohne den Gerätebetrieb zu stören.

ÜBERWACHUNG

Verschaffen Sie sich einen Echtzeitüberblick über die auf Ihren Geräten installierte Software und Hardware sowie über Ihre Benutzer und überwachen Sie Änderungen, die auf betrügerische Aktivitäten hinweisen könnten.

HARDWAREBESTAND

Gestattet dem Benutzer die Erfassung des Hardwarebestands eines Geräts mit der Option, Warnmeldungen für den Fall zu generieren, dass Hardware angeschlossen oder getrennt wird.

SOFTWAREBESTAND

Ermöglicht Benutzern, eine Bestandsaufnahme der auf dem Gerät installierten Software- und Betriebssystem-Patches zu erhalten, mit der Möglichkeit, bei Vorhandensein nicht autorisierter Software oder des Fehlens kritischer Betriebssystem-Patches, Warnungen zu erhalten.

BENUTZERÜBERWACHUNG

Gestattet dem Benutzer die Erfassung des Bestands der lokalen Benutzer des Betriebssystems und warnt ihn, wenn Benutzerkonten erstellt, geändert oder gelöscht werden.

DATEI- UND VERZEICHNISMONITOR

Überwacht als kritisch eingestufte Dateien oder Verzeichnisse und warnt den Benutzer bei Änderungen.

KONTROLLE

Führen Sie Aktionen auf Ihren Geräten per Fernzugriff aus und ermöglichen Sie dadurch den Betrieb und die Wartungsaktivitäten.

Neustart und Kennwortänderung per Fernzugriff

Führen Sie benutzerdefinierte Remote-Aktionen auf den überwachten Geräten durch und zentralisieren Sie die dadurch gewonnenen Ergebnisse.

Informationsbeschaffung

Rufen Sie Dateien oder Verzeichnisse per Fernzugriff von den überwachten Geräten ab.

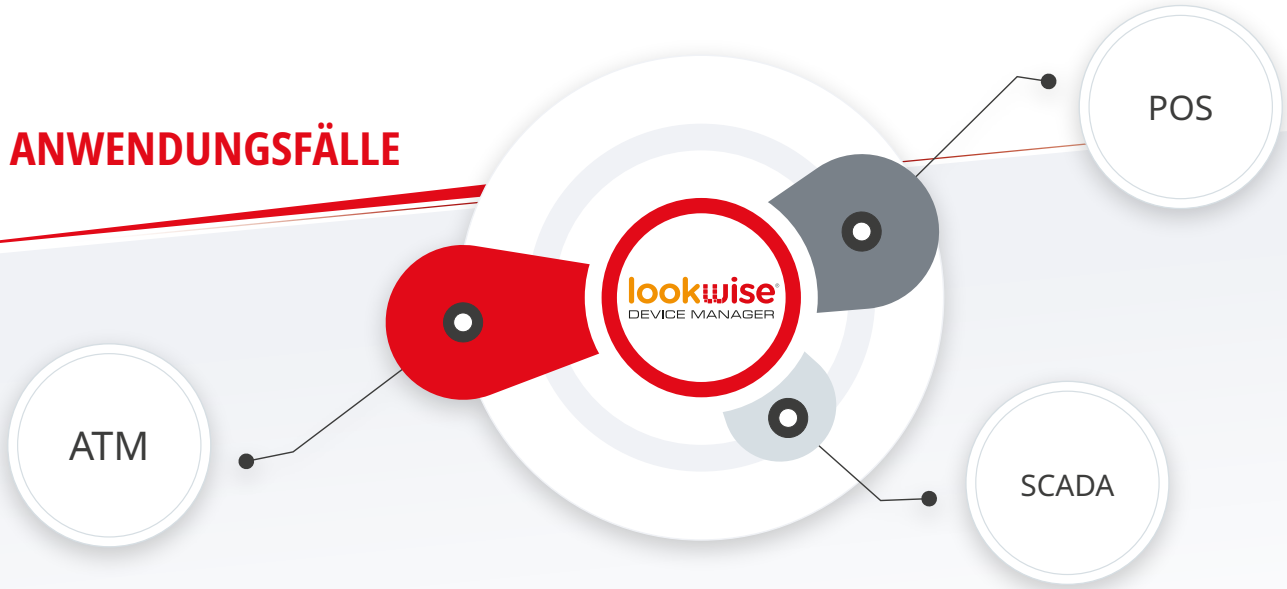
Benutzerdefinierte Durchführung von Remote-Aktionen

Erstellen Sie eigene benutzerdefinierte Remote-Aktionen für verschiedene Zwecke wie forensische Analyse, Konfigurationsänderungen, Patch-Bereitstellung und Malware-Desinfektion.

Führen Sie benutzerdefinierte Remote-Aktionen auf den Geräten aus; Laden Sie lokale Binärdateien oder Skripte hoch bzw. führen Sie sie aus und zentralisieren Sie die dadurch gewonnenen Ergebnisse.

Remote-Aktionen sind bereits in der Anwendung Whitelisting integriert und können nur über die LDM-Konsole (nicht lokal auf dem Gerät) ausgeführt werden.

ANWENDUNGSFÄLLE



GELDAUTOMATEN

Geldautomaten sind sehr attraktive Ziele für Angreifer, da sie Bargeld enthalten und der Verwaltung sensibler Daten wie Kreditkartennummern und PINs dienen. Außerdem sind sie unbeaufsichtigt oder nur unzureichend überwacht. Geldautomatennetze weisen eine Vielzahl veralteter Hard- und Software auf. Hinzu kommt das Fehlen proaktiver Upgrade-Richtlinien aufgrund technischer und wirtschaftlicher Zwänge. Das macht diese Netze von Natur aus anfällig.

Vor diesem Hintergrund sind Cyberkriminelle äußerst flexibel und innovativ, wenn es darum geht, neue Arten von gezielten logischen Angriffen zu entwickeln. Die sind wesentlich kostengünstiger als herkömmliche physische Angriffe.

KASSENTERMINALS

Kassenterminals dienen der Verwaltung sensibler Daten wie Kartennummern und PINs. Das macht sie sehr anfällig für gezielte Angriffe oder betrügerische Handlungen.

Die Kontrolle der erlaubten Anwendungen oder Hardwaregeräte anhand einer Whitelist ermöglicht den Benutzern, das Vertrauen in die Sicherheit dieser Geräte zu stärken.

KONTROLLSYSTEME IN KRITISCHEN INFRASTRUKTUREN

Automatisierungs- und Kontrollsysteme in kritischen Infrastrukturen sind mehr und mehr auf Fernkommunikation und die Verbindung mit IT-Infrastruktur angewiesen, womit sie teilweise deren Risiken und Schwachstellen ausgesetzt sind.

Ein Cyberangriff auf Kontrollsysteme kann enormen Schaden anrichten – von einem massiven Ausfall grundlegender Dienste bis hin zur potentiellen Gefährdung von Infrastruktur und Menschen. Daher sollten für diese sensiblen Systeme die höchsten Sicherheitsstandards gelten.

MERKMALE

Der Lookwise Device Manager baut auf der proprietären Auriga-Technologie Lookwise TECH auf. Dieser speziell für verteilte Umgebungen und das Betriebssystem Windows XP/7/10 entwickelten Technologie verdankt das Produkt seine Modularität, Skalierbarkeit und Flexibilität.

VERWALTUNG

- Zentralisierte Benutzeroberfläche für Verwaltung und Betrieb
- Erstellung und Verteilung von Richtlinien per Fernzugriff
- Integration von Warnungen und Meldung von Ergebnissen
- Sicherheitsdashboard
- Sichtbarkeit basierend auf Rollen und Berechtigungen
- SIEM Integration

KOMMUNIKATION

- Authentifiziert und verschlüsselt
- Kontinuierlich
- Komprimiert
- Entwickelt, um instabile Netzwerke mit niedriger Bandbreite zu unterstützen

ARCHITEKTUR

- Verteilt
- Modular
- Flexibel und skalierbar
- Lastausgleich
- Bereitstellung von Funktionen und Updates per Fernzugriff
- Sehr begrenzter Ressourcenverbrauch