
Protect Microsoft IoT LTSC Devices with Trellix.

Maintain Software Integrity, Uptime, and Control Across OEM Device Lifecycles.

OEM devices are built to operate reliably in the field, often in environments where unplanned downtime, software drift, or unauthorized changes can increase support costs and disrupt operations. Microsoft IoT LTSC provides a stable operating system foundation. Trellix Application and Change Control helps protect the approved software image, control what runs, and manage how changes happen over time.

Trellix Application and Change Control

OEMs define a trusted golden image, then Trellix enforces it, allowing only approved applications, blocking unauthorized executables and scripts, and governing how changes are made. Protection extends across the full stack including applications, files, registry, user accounts, and system configurations.

Golden Image Protection

Define the approved device image, including software, files, and configurations, then help keep that image intact through deployment, service, and maintenance.

Application Control

Allow only approved executables, scripts, drivers, and applications to run, helping reduce software risk without requiring constant signature updates.

Change Prevention

Block or restrict out-of-policy changes to critical files, directories, registry keys, user accounts, and configurations.

Controlled Maintenance

Enable approved updates through trusted users, signed certificates, trusted processes, directories, and maintenance windows.

Air-Gapped Support

Support connected and air-gapped environments, including remote or distributed systems where continuous cloud connectivity may not be available.

Real-time Visibility

Every change event is logged: what changed, when, and who initiated it. Data needed for root cause analysis, audit compliance, and incident response.

Customer Outcomes with Trellix Application and Change Control

Customer Challenge	Trellix Adds	Customer Outcome
Embedded devices must run reliably for years	Protection for applications, files, configurations, and the approved software image	Greater confidence across long deployment lifecycles
Unauthorized software can create security and uptime risks	Intelligent allowlisting to help ensure only approved code can run	Reduced malware risk and stronger control over device execution
Unplanned changes can lead to outages	Change prevention and file integrity monitoring	Less configuration drift and fewer unexpected disruptions
Updates still need to happen safely	Trusted update paths and controlled change processes	Easier maintenance without opening the system to unnecessary risk
Teams need to understand what changed	Real-time visibility into change events	Faster troubleshooting and stronger accountability

Complementary Trellix Technologies

Application and Change Control is the foundation. For environments that require additional layers, Arrow can help OEMs integrate complementary Trellix solutions:

- **Trellix Device Control** secures USB and removable media ports, preventing unauthorized data transfer and peripheral-based threats.
- **Trellix Endpoint Security (ENS)** adds real-time threat prevention, web control, and firewall for connected systems.

Build more secure, resilient embedded systems with Microsoft IoT LTSC and Trellix from Arrow. Contact Arrow to learn how Trellix protects IoT deployments from unauthorized code, unplanned changes, and software integrity risks.

Ideal Use Cases

Microsoft IoT LTSC and Trellix Application and Change Control are well suited for:

- Industrial automation and manufacturing systems
- Medical and healthcare equipment
- Retail and point-of-sale systems
- Transportation and logistics systems
- Safety, security, and monitoring devices
- Operational technology environments
- Remote or distributed systems with long service lives
- Legacy systems that require additional control and visibility

In Partnership with



Via Email

windowsIoT@arrow.com

Online

arrow.com/winIoT

06_23_2026