Providing Robust Security for Mac-Lab™/ CardioLab™ AltiX AI.i Systems on Windows 10 IoT Enterprise LTSC 2021

By Avinash Kumar

Introduction

The Mac-Lab | CardioLab | ComboLab AltiX AI.i systems rely on a secure and stable operating system to safeguard sensitive patient data, and aimed at providing uninterrupted medical procedures. While Windows® 11 introduces new security features, the Mac-Lab | CardioLab | ComboLab AltiX AI.i systems on Windows 10 IoT Enterprise Long-Term Servicing Channel (LTSC) already incorporate these enhanced security measures. This whitepaper explains how the security features of Windows 10 IoT Enterprise LTSC 2021 match those of Windows 11, emphasizing the strategic choice of Windows 10 IoT Enterprise LTSC 2021 for its stability and long-term support.

Windows 10 IoT Enterprise LTSC 2021: End of Support Date

Windows 10 IoT Enterprise long-term servicing channel (LTSC) provides 10 years of security servicing to a static Windows 10 feature. For more details regarding LTSC refer Supporting References from Microsoft.

Operating System	End of Support Date
Windows 10 IoT Enterprise LTSC 2021	Jan 13, 2032

Enhanced Security Features on Windows 10 IoT Enterprise LTSC 2021

Windows 10 IoT Enterprise LTSC 2021 is equipped with advanced security features that align with the enhancements found in Windows 11. These include:

Virus and Threat protection: Windows Defender

Windows Defender® is now called Microsoft® Defender Antivirus and shares detection status between Microsoft 365 services and interoperates with Microsoft Defender for Endpoint. Microsoft Defender Antivirus Windows Defender includes powerful analytics, security stack integration, and centralized management for better detection, prevention, investigation, response, and management of virus and system threats.

- **Advanced Machine Learning:** Improved with Advanced Machine Learning and AI models that enable it to protect against Apex attackers using innovative vulnerability exploit techniques, tools and malware.
- **Emergency Outbreak Protection:** Provides Emergency Outbreak Protection that will automatically update devices with new intelligence when a new outbreak has been detected.
- **Certified ISO 27001 Compliance:** The cloud service analyzes for threats, vulnerabilities and impacts, and confirms that risk management and security controls are in place.
- **Next Generation Protection:** Controls have been extended to protection from ransomware, credential misuse, and attacks that are transmitted through removable storage.
- **Integrity Enforcement Capabilities:** Enables remote runtime attestation of Windows 10 platform.
- **Tamper-proofing Capabilities:** Uses Virtualization-based security (VBS) to isolate critical Microsoft Defender for Endpoint security capabilities away from the OS and attackers.
- **Improved Support:** Improved Support for non-ASCII file paths for Microsoft Defender Advanced Threat Protection (ATP) Auto Incident Response (IR).

- **Windows 11:** Comes with an updated version of Windows Defender.
- **Windows 10 IoT Enterprise LTSC 2021:** Also features Windows Defender that can be updated to the latest version. Mac-Lab/CardioLab systems fully support and are validated with Windows Defender which is enabled by default in our Acquisition and Review Workstations. The most common third-party advanced endpoint security products provided by McAfee®, Symantec® and Trend Micro™ are supported. Additionally, next generation AV products such as CrowdStrike™ and Carbon Black™are also supported.

Threat protection: Windows Defender Firewall

Windows Defender Firewall now offers the following benefits:

- **Reduced risk:** Windows Defender Firewall reduces the attack surface of a device with rules to restrict or allow traffic by many properties, such as IP addresses, ports, or program paths. Reducing the attack surface of a device, increases manageability and decreases the likelihood of a successful attack.*
- **Safeguard data:** With integrated Internet Protocol Security (IPsec), Windows Defender Firewall provides a simple way to enforce authenticated, end-to-end network communications. It provides scalable, tiered access to trusted network resources, helping to enforce integrity of the data, and optionally helping to protect the confidentiality of the data.
- **Extend value:** Windows Defender Firewall is a host-based firewall that is included with the operating system, so there's no other hardware or software required. Windows Defender Firewall is also designed to complement existing non-Microsoft network security solutions through a documented application programming interface (API).
- **Easier to analyze and debug:** The Windows Defender Firewall is also now easier to analyze and debug. IPsec behavior has been integrated with Packet Monitor (pktmon), an in-box cross-component network diagnostic tool for Windows.
- **Enhanced Event Logs:** Windows Defender Firewall event logs have been enhanced to ensure an audit can identify the specific filter that was responsible for any given event. This enhancement enables analysis of firewall behavior and rich packet capture without relying on other tools.
- **Windows 11:** Includes Windows Defender Firewall by default.
- **Windows 10 IoT Enterprise LTSC 2021:** Mac-Lab/CardioLab Acquisition and Review Workstations ship with the Windows Defender Firewall enabled and pre-configured to allow the Mac-Lab/CardioLab required network traffic while blocking other network traffic.

Information protection: BitLocker

BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices.

- **Windows 11:** Supports BitLocker.
- **Windows 10 IoT Enterprise LTSC 2021:** All Mac-Lab/CardioLab systems shipped have BitLocker enabled by default. In addition to this drive level encryption, application-level encryption is applied to patient data files using uniquely created certificate keys managed by the Microsoft Windows certificate store and implementing AES256 file level encryption on all data at rest.

Trusted Platform Module (TPM)

A TPM (Trusted Platform Module) is used to improve the security of your PC. It is used by services like BitLocker drive encryption to securely create and store cryptographic keys, and to confirm that the operating system and firmware on your device are what they are supposed to be and have not been tampered with.

- **Windows 11:** Requires TPM 2.0 for all systems.
- **Windows 10 IoT Enterprise LTSC 2021:** Mac-Lab/Cardio Lab systems ship with TPM 2.0, which supports hardware-based security.

Secure Boot

Secure Boot is an important security feature designed to prevent malicious software from loading when your PC starts up (boots).

- **Windows 11:** Requires Secure Boot for all systems.
- **Windows 10 IoT Enterprise LTSC 2021:** Mac-Lab/Cardio Lab systems ship with Secure Boot enabled, providing a secure boot process and hardware-based security. Additionally, the systems support and encourage site specific bios level password security and control.

Transparent Data Encryption (TDE)

Transparent data encryption (TDE) encrypts SQL Server Database. This encryption is known as encrypting data at rest.

- **Windows 11:** Supports Transparent Data Encryption (TDE) for encrypting SQL Server Database.
- **Windows 10 IoT Enterprise LTSC 2021:** The Mac-Lab/CardioLab AltiX AI.i system enables Transparent Data Encryption (TDE) for encrypting Microsoft SQL Server 2022 Database by default.

Virtualization-Based Security (VBS)

Virtualization-Based Security (VBS) uses Windows Hypervisor to virtually isolate a segment of main memory from the rest of the operating system. Windows uses this isolated, secure region of memory to store important security solutions like log-in credentials and code responsible for Windows security, among other things.

- **Windows 11:** Supports Virtualization-Based Security (VBS).
- **Windows 10 IoT Enterprise LTSC 2021:** Virtualization-Based Security (VBS) is already implemented and enabled, leveraging hardware virtualization to create and isolate a secure memory region, protecting critical security information.

Identity protection: Credential Guard

Credential Guard is a security service in Windows 10 built to protect Active Directory (AD) domain credentials so that they cannot be stolen or misused by malware on a user's machine. It is designed to protect against well-known threats such as Pass-the-Hash and credential harvesting.

- **Windows 11:** Supports Credential Guard.
- **Windows 10 IoT Enterprise LTSC 2021:** Credential Guard is supported and configured to protect Active Directory (AD) domain credentials.

Information protection: Windows information protection

Windows Information Protection is now designed to work with Microsoft Office and Azure™ Information Protection. You can also now collect your audit event logs by using the Reporting configuration service provider (CSP) or the Windows Event Forwarding (for Windows desktop domain-joined devices).

- **Windows 11:** Available in Windows 11.
- **Windows 10 IoT Enterprise LTSC 2021:** Also available in Windows 10.

Other security improvements: Windows security baselines

Microsoft has released new Windows security baselines for Windows Server and Windows 10. A security baseline is a group of Microsoft-recommended configuration settings with an explanation of their security effect.

- **Windows 11:** Supports Windows security baselines.
- **Windows 10 IoT Enterprise LTSC 2021:** Mac-Lab/CardioLab Acquisition and Review Workstations ship with the Microsoft secure baseline policy applied. The Microsoft Security Baseline provides enhanced security on top of the base Windows 10 installation.

Other security improvements: Windows Security App

Windows Security App improvements now include Protection history, including detailed and easier to understand information about threats and available actions, Controlled Folder Access blocks are now in the Protection history, Windows Defender Offline Scanning tool actions, and any pending recommendations.

- **Windows 11:** Improvement available in Windows 11.
- **Windows 10 IoT Enterprise LTSC 2021:** Improvement also available in Windows 10 LTSC.

Other security improvements: WPA3 H2E standards

WPA3 H2E standards are supported for enhanced Wi-Fi security.

- **Windows 11:** Supports WPA3 H2E
- **Windows 10 IoT Enterprise LTSC 2021:** WPA3 H2E is also supported in Windows 10 LTSC. The Acquisition system and GE HealthCare Review Workstation do not use wireless. The customer may optionally use wireless (Wi-Fi) on the Software-Only Review Workstation.

Long-Term Servicing Channel (LTSC): stability and predictability

Windows 10 LTSC is explicitly designed for environments that require a stable and predictable platform, such as medical devices. Microsoft's commitment to LTSC ensures that:

- **Security updates:** Regular security updates are provided without introducing new features that could affect system stability. This approach maintains the integrity and functionality of medical devices.
- **Stability:** The LTSC branch minimizes the risk of unexpected changes that can come with feature updates, keeping the system stable and reliable for long-term use.
- **Compliance:** Adhering to regulatory requirements is easier with LTSC, as it provides a consistent and controlled environment, essential for medical devices that need to maintain strict compliance standards.

Supporting References from Microsoft

Microsoft emphasizes the role of LTSC in maintaining secure and stable platforms for critical applications. According to Microsoft:

Long-Term Servicing Channel: "The LTSC is designed for devices and use cases where features and functionality will not change. It provides 10 years of security servicing to a static Windows 10 feature set."

Reference: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/ltsc-what-is-it-and-when-should-it-be-used/ba-p/293181

Security and stability: “Specialized systems—such as devices that control medical equipment, point-of-sale systems, and ATMs—often require a longer servicing option because of their purpose. These devices typically perform a single important task and do not need feature updates as frequently as other devices in the organization. It is more important that these devices be kept as stable and secure as possible than up to date with user interface changes. The LTSC servicing model prevents Enterprise LTSC devices from receiving the usual feature updates and provides only quality updates to ensure that device security stays up to date.“

Reference: https://techcommunity.microsoft.com/t5/internet-of-things-blog/windows-for-iot-long-term-servicing-channel-explained/ba-p/2836254

Conclusion

The Mac-Lab |CardioLab | ComboLab AltiX Ai.i systems on Windows 10 IoT Enterprise LTSC 2021 are designed to leverage robust security features akin to those of Windows 11. By implementing Windows Defender, Windows Defender Firewall, BitLocker, Trusted Platform Module, Secure Boot, Transparent Data Encryption, Virtualization-based security, and Credential Guard, our systems achieve the highest levels of protection.

Additionally, the choice of Windows 10 IoT Enterprise LTSC 2021 provides a stable, predictable, and compliant platform, essential for maintaining the integrity and functionality of critical medical devices. With ongoing security updates and a focus on long-term support, Windows 10 IoT Enterprise LTSC 2021 remains a reliable choice for safeguarding patient data and enabling uninterrupted medical services.

*For detailed and substantiated information regarding Microsoft-related claims and statements, please visit the official Microsoft website.

JB32953XX

GE HealthCare