Lenovo ThinkShield

Why you need enhanced security against attacks on meeting room solutions.

By 2025, the number of video conferencing devices on the market will be six times as high as in 2021.[1] With this boom comes a hidden threat: increased cyberattacks at every level. As you scale up your fleet of conferencing devices, here are a few reasons security needs to be at the center of your strategy.

1 Internet of Things (IoT) attacks are becoming more common

As IoT attacks continue to rise, your conferencing devices need multiple layers of protection in place to reduce the risk of vulnerabilities — from manufacturing to ongoing monitoring and management.

112M IoT cyberattacks took place worldwide in 2022[2]

87% YOY increase in IoT malware incidents[2]

2 USB ports are a growing threat vector

As USB-borne malware among cybercriminals becomes more common, disabling USB ports is becoming a best practice for conferencing devices.

52% of malware is capable of propagating through removable media[3]

81% of USB-borne threats are capable of disrupting operational technology[3]

3X increase in USB-borne malware in the first half of 2023[4]

50% of surveyed employees will insert a flash drive they found in the parking lot into a company device[5]

3 Data breaches are costly and difficult to predict

Data breaches and their costs are on the rise, and many corporate security professionals admit they are not as prepared as they would like to be.

$4.35M the average cost of a data breach per incident, up 12.7% since 2020[6]

40% of chief security officers admit their orgs are unprepared for the rapidly changing threat landscape[7]

Enhance security at every level

Lenovo ThinkShield for ThinkSmart provides reliable conferencing solutions with security baked in to defend your business without compromising end-user productivity.

Supply chain assurance: Secures the entire device lifecycle by thoroughly vetting suppliers, components and processes. Every step is controlled, audited and tamper-proof.

Below the OS: Built-in remote management, self-healing BIOS, secure wipe and firmware security solutions defend against software/hardware attacks by ensuring firmware integrity and providing real-time alerts.

OS-to-Cloud security: By partnering with world-class software vendors like Absolute, SentinelOne, Secret Double Octopus, BufferZone, Sepio, Blancco and more, we help protect our customers' hybrid workforces.

Lenovo secure authentication: Protect each device with secure authentication backed by hardware-based Trusted Platform Module (TPM) 2.0.

USB port control: Prevent unwanted access to a device with remote blocking of USB ports and USB Boot Enable/Disable.

BIOS/SVP change management (Premium feature): Elevate security with control at the BIOS level.

Ready to learn more? Connect with our team.

[1] Video Conferencing Devices to Grow Six Times by 2025 – Frost & Sullivan.
[2] Annual number of IoT attacks global 2022 – Statista.
[3] Industrial Cybersecurity USB Threat Report 2022 – Honeywell Forge.
[4] Huge increase in USB malware in first half of 2023 – Techzine Europe.
[5] Why are USB sticks wrinkle-free? – CIO.
[6] 2022 Cost of a Data Breach Report – Security Intelligence.
[7] Cybersecurity Solutions for a Riskier World – ThoughtLab.

Smarter technology for all

Lenovo