



Why Your IT Team is Terrified of Your Conference Room: A Guide to Zero Trust AV



If you walk into your main conference room right now, what do you see? You probably see a sleek 85-inch display, a neat little touch panel on the table, a soundbar tucked under the screen, and maybe a couple of sleek microphones hanging from the ceiling. To you, it looks like a place where collaboration happens.

To your IT Director, it looks like a flashing neon sign that says "ENTER HERE" to every hacker within a thousand-mile radius.

I'm Eric C. Berg, and at **Simply Innovative Unified Communications**, we've seen the evolution of the boardroom firsthand. There was a time when AV (Audio-Visual) was the domain of the "facilities guy." You plugged in a VGA cable, a projector hummed to life, and that was it. But those days are long gone.

In 2026, your conference room is no longer an island. It is a dense cluster of networked IT endpoints. And if your IT team seems a little stressed when you ask to add a new "smart" camera to the network, they aren't being difficult: they're being realistic. We've officially moved out of the "plug-and-play" era and straight into what I call the "plug-and-prey" era.



The Identity Crisis: When a Microphone is a Computer

The fundamental shift that has happened over the last few years is that AV devices have become specialized computers. Your camera has an OS. Your speakers have IP addresses. Your unified communication systems are deeply integrated into your corporate network.

Because these devices are on the network, they are subject to the same threats as a laptop or a server. However, they are often managed with about 10% of the security oversight. This is why "Zero Trust AV" isn't just a buzzword; it's a survival strategy.



1. Legacy Hardware 'Ghosts'

One of the biggest reasons IT teams lose sleep is what we call "Legacy Ghosts." Most companies refresh their laptops every three years. But that expensive codec or high-end display in the executive boardroom? That might stay there for seven, eight, or even ten years.

These legacy devices often run on ancient, unpatched versions of Linux or proprietary firmware that hasn't seen a security update since the era of Tiger King. These are the perfect entry points for "lateral movement." A hacker doesn't need to crack your firewall if they can exploit a vulnerability in a 2018-era room controller. Once they are "in" the controller, they can pivot to the rest of your network.

At Simply Innovative, we look at what we do as more than just mounting screens; we are lifecycle managers. If a piece of gear can't receive security patches, it's not an asset: it's a liability.

2. Data Harvesting via the "Helper" Tech

Think about your room scheduler: that little tablet outside the door that shows if the room is busy. It needs to talk to your Microsoft 365 or Google Workspace environment to work. If that device is unencrypted or running on a generic "guest" network with weak credentials, it can be scraped.



It's not just about knowing who is meeting and when. These IoT sensors and schedulers can be used to harvest internal credentials. In a world where data is the new oil, your conference room is a potential oil spill waiting to happen. If your integrator didn't set up these devices with dedicated service accounts and limited permissions, you're essentially leaving a key to your digital front door under the welcome mat.



3. AVoIP Vulnerabilities: The High-Bandwidth Backdoor

AV over IP (AVoIP) is the gold standard for modern offices. It allows us to send 4K video and high-fidelity audio over standard network switches. It's flexible, scalable, and powerful. But it's also a massive amount of data.

A single misconfigured switch can lead to two major problems:

1. **Network Paralysis:** If AV traffic isn't properly managed via IGMP snooping and dedicated VLANs, a high-bandwidth video stream can flood your network, causing your VOIP phones to drop and your internet to crawl.
2. **The Backdoor:** Because AVoIP requires high-level access to network ports, a poorly secured AV switch can become a backdoor. If a bad actor gains access to the AV network, and that network isn't properly segmented from your sensitive financial or customer data, the game is over.

The Philosophy of Zero Trust AV

So, how do we fix this? We stop treating AV like furniture and start treating it like infrastructure. This is the core of the **Zero Trust AV** philosophy.

In a Zero Trust model, we assume the network is already compromised. Therefore, no device: whether it's a \$20,000 LED wall or a \$200 document camera: is trusted by default. Every device must be verified, validated, and limited in its scope of communication.



The Simply Innovative "Secure Room" Checklist:

- **VLAN Segmentation:** Your AV gear should live in its own "walled garden." It should be able to talk to what it needs to, and absolutely nothing else. Your microphones have no business "talking" to your accounting server.
- **AES-256 Encryption:** Whether it's the video signal traveling across the hall or the control signals moving from the tablet to the display, everything must be encrypted.
- **802.1X Authentication:** This ensures that only authorized devices can get a network connection. If someone walks into your room and plugs their laptop into a stray network jack meant for a camera, the network should shut that port down instantly.
- **Firmware Governance:** We don't just install and walk away. We provide a roadmap for keeping hardware updated.



Is Your AV a Bridge or a Breach?

I often tell my clients that a poorly designed AV system is just a very expensive security hole. You want your technology to be a bridge: something that connects your team, fosters collaboration, and helps you grow. You don't want it to be the breach that ends up on the front page of the news.

If your current integrator hasn't mentioned "network security," "VLANs," or "encryption" during your design phase, you aren't getting a modern UC solution. You're getting a headache.

At **Simply Innovative Unified Communications**, we pride ourselves on being the bridge between the AV world and the IT department. We speak both languages fluently. We understand that "cool" doesn't matter if it isn't "secure."

If you're worried about what's lurking in your conference room, let's take a look. You can check out our [about page](#) to see how we approach these challenges, or browse our [MFG list](#) to see the secure vendors we trust.



Resource: The Zero Trust AV Framework

This section is designed to be saved or printed as a quick-reference guide for your internal IT and facilities teams.

Problem

Traditional AV installations focus on "uptime" and "ease of use," often at the total expense of network security. This creates "Shadow IT" where unmanaged, unpatched, and unencrypted devices reside on the corporate backbone, providing an easy entry point for lateral movement and data exfiltration.

Technical Insight

Modern AV devices are essentially IoT endpoints. Many utilize standard network protocols (SIP, H.323, SRTP) but lack the endpoint detection and response (EDR) tools found on standard workstations. AVoIP (Audio-Visual over IP) creates massive multicast traffic that can destabilize a network if not managed via Layer 3 segmentation and proper IGMP configuration.

The Simply Innovative Solution

We implement a **Zero Trust AV Architecture** that includes:

- **Micro-segmentation:** Isolating AV traffic into dedicated, firewalled VLANs.
- **Identity Management:** Utilizing 802.1X or MAC-based filtering to prevent unauthorized hardware "spoofing."
- **End-to-End Encryption:** Mandating AES-256 for all signal distribution.
- **Lifecycle Hardening:** Regular firmware audits and the removal of legacy hardware that no longer meets modern security standards.

Call to Action

Don't wait for a vulnerability scan to tell you your boardroom is a risk. Contact Simply Innovative Unified Communications today for a **Secure Design Review**. We will audit your current signal flow, network topology, and hardware age to ensure your collaboration tools are an asset, not a target.

[Get Started with a Design Review](#) | [Visit Our Purchasing Portal](#)