Tigermeeting

The Walled Garden:

Achieving Maximum Security Through Serverless On-Premises Architecture

White Paper

Zoltan Arpadffy, CTO

Contents

Introduction

Tigermeeting is the leading on-premises solution for meeting room management, digital signage and access control — fully decentralized, serverless, and built for extreme scalability.
Designed for enterprise-grade reliability, it offers a perpetual licensing model with no hidden costs or cloud dependencies.

How could we achieve this? The answer is simple: We listen to our customers.

We own the technology. We know the industry. We are passionate about what we do. We consider customer needs. We adjust our product and service roadmap accordingly. Our consistent Blue Ocean strategy and focus on the market earned us respect from both customers and competitors.

We see that our products are able to provide great and affordable service for schools, universities, offices and organizations with simple, functional, efficient and reliable meeting room management solution - that is already highly appreciated worldwide.

Executive Summary

In the modern enterprise, "Smart Office" initiatives often introduce significant vulnerability. To gain the convenience of digital room booking and signage, organizations frequently surrender data sovereignty to cloud-based SaaS providers, creating new vectors for data exfiltration and third-party risk.
This white paper analyzes an alternative architectural paradigm: Serverless On-Premises. Specifically, we examine how Tigermeeting's distributed database technology allows organizations to deploy enterprise-grade meeting management tools that operate entirely within the Local Area Network (LAN). By eliminating both the central server "honeypot" and the dependency on external cloud processing, this architecture offers the industry's most secure profile for sensitive environments, including government, defense, finance, and R&D.

The Hidden Risks of Cloud-Based Room Management

When a meeting room panel displays "Project Aurora Strategy Session - 2:00 PM," it is broadcasting highly sensitive metadata. In a cloud-first architecture, this data travels from the corporate network to a third-party vendor's cloud, is processed, stored, and then sent back to the device.

This round-trip journey introduces three critical security flaws:

- Data Sovereignty Loss: The data resides on servers the organization does not own, often in jurisdictions subject to foreign data access laws (e.g., The CLOUD Act).
- Expanded Attack Surface: The system requires a constant, open connection through the firewall to the vendor's cloud, creating a potential bridge for attackers.
- Vendor Supply Chain Attacks: If the SaaS provider is compromised, every client connected to their cloud is potentially vulnerable.

The Tigermeeting Architecture: A "Zero-Trust" Approach

Tigermeeting rejects the premise that local utility requires global connectivity. Instead, it utilizes a High Watermark Distributed Database architecture that allows the system to function autonomously within the organization's "Walled Garden."

The Distributed Data Mesh

Unlike traditional on-premises systems that rely on a central SQL server (a single point of failure and a primary target for attackers), Tigermeeting distributes the configuration and logic across the endpoint devices (room screens) themselves.

- No Central Server: There is no dedicated Windows or Linux server to patch, secure, or monitor.
- Encrypted LAN Communication: Devices communicate exclusively with each other over the local network using encrypted protocols.
- Transient Administration: The Admin App is not a permanent service running on the network. It is a client-side tool that connects only when a configuration change is required, leaving no permanent administrative "back door" open.

Key Security Advantages

Elimination of the "Honeypot"

In network security, a central server storing all calendar data and access logs is a "honeypot"-a high-value target. If an attacker breaches a traditional server, they gain control of the entire facility's signage and schedules.
Tigermeeting decentralizes this risk. Because the "database" is fragmented and replicated across the mesh of screens:

- There is no single repository to hijack.
- Compromising one screen (physically) does not grant remote control over the rest of the ecosystem.
- Lateral movement is restricted because the devices do not have privileged access to a central core-because the core does not exist.

Total Data Sovereignty (GDPR & Compliance)

For sectors with strict compliance requirements (GDPR in Europe, FZ-152 in Russia, or defense-level protocols), the physical location of data storage is paramount.

- Internal Storage Only: With Tigermeeting, room schedules, meeting subjects, and attendee names never leave the physical premises.
- No Third-Party Storage: Tigermeeting (the vendor) has no access to your data. There is no "Tigermeeting Cloud" storing your meeting logs.
- Audit Simplicity: Proving compliance is straightforward because the data flow diagram shows no egress traffic to external processing entities.

Invisible to the Outside World

A fundamental principle of security is "stealth." A system that cannot be reached from the internet is infinitely harder to hack.

- Air-Gap Capable: Tigermeeting can run on a completely air-gapped network (physically isolated from the internet) if using internal Exchange servers.
- No Inbound Ports: The system does not require opening inbound ports on the corporate firewall.
- Port Stealth: The communication ports (UDP/TCP) used for device synchronization are only active within the specific LAN segment, making the traffic invisible to external scanners.

Secure Integration with Corporate Calendars

A common security concern is how an on-premises system connects to cloud calendars like Microsoft 365 or Google Workspace without exposing data.

Tigermeeting employs a Direct-to-Source model:

- Direct API Calls: The room screens act as individual clients. They fetch free/busy status directly from the Calendar Provider (Microsoft/Google) via secure API.
- No "Man-in-the-Middle": Crucially, this traffic does not pass through Tigermeeting servers. The vendor never sees, touches, or stores your credentials or token exchanges.
- Tokenized Authentication: Modern OAuth2 authentication is used, meaning no passwords are stored on the devices, only revocable access tokens.

Conclusion: Security by Design, Not by Policy

Policies and firewalls are necessary, but architectural security is superior. By choosing a solution that fundamentally does not require external connectivity to function, organizations remove entire categories of risk.
Tigermeeting's Serverless On-Premises model offers the rarest of combinations in the IT world: the modern functionality of a smart office with the hardened security posture of a legacy, isolated network. For the security-conscious enterprise, it is the only logical choice.

Technical Appendix: Security Specs

Encryption: High-grade encryption for all device-to-device communication.
External Dependencies: None (unless syncing with external Cloud Calendars).
Data Residence: 100% Local (RAM/Flash storage on endpoint devices).

Contact information

Email: info@tigermeeting.app

Web: https://tigermeeting.app/en/contact

Customer Support: support@tigermeeting.app

More information can be obtained under “About” menu in the Admin Application.

Social media

Follow us on social media to get event updates on product news and new releases.

LinkedIn https://www.linkedin.com/company/tigermeeting/

Facebook https://www.facebook.com/tigermeeting/

Instagram https://www.instagram.com/tigermeeting

Reddit https://www.reddit.com/u/tigermeeting/

GitHub https://www.github.com/tigermeeting

X(Twitter) https://x.com/tigermeeting

YouTube https://youtube.com/@tigermeeting

Threads https://www.threads.net/@tigermeeting

Tik Tok https://www.tiktok.com/@tigermeeting

Telegram https://t.me/tigermeeting

Pinterest https://www.pinterest.com/tigermeetingroom/

WhatsApp

https://www.whatsapp.com/channel/0029VanwIDn6LwHgKMtMF90S

Weixin / WeChat