Case Study

Secure Self-Service Kiosks Powered by Synaccess Switched PDUs

Synaccess

Overview

A leading **kiosk manufacturer** was contracted by a **major U.S. Telecom Giant** to design and deploy secure, self-service kiosks for retail locations nationwide. These kiosks were designed not only to **dispense SIM cards** but also to allow customers to **pay bills, process transactions, and print receipts**. To ensure maximum reliability, robust network security, and streamlined remote management, Synaccess Switched Power Distribution Units (PDUs) were integrated into each kiosk.

The Challenge

The telecom provider required highly secure kiosks equipped with reliable hardware and stringent security standards. Maintaining uptime and minimizing technician visits were critical project objectives. Key challenges included:

Ensuring Uptime

Kiosks needed reliable remote troubleshooting and power cycling capabilities to prevent downtime.

Robust Network Security

Minimizing exposure of kiosk infrastructure to cybersecurity threats was essential for compliance and operational security.

Remote Diagnostics & Troubleshooting

Technicians required visibility into power metrics for real-time diagnostics and support.

Peripheral Device Reliability

Kiosk controllers and receipt printers—critical for payment confirmation—were known to frequently lock up, requiring physical resets.

The Solution: Synaccess Secure & Intelligent PDUs

To address critical reliability and security needs, Synaccess PDUs were integrated into the kiosk solution, providing:

🔹 Remote Power Cycling & Troubleshooting

Device watchdogs and automated alerts enabled instant secure remote reboot capabilities, allowing technicians to reset kiosk hardware (computers, sensors, payment systems, printers) quickly without physical site visits, significantly reducing downtime.

🔹 Real-Time Current Monitoring

Built-in current measurement provided remote, real-time visibility into kiosk power usage. This allowed technicians to monitor equipment health, proactively identify potential issues, and remotely diagnose hardware problems, streamlining support and maintenance.

🔹 Advanced Network Security

- **IP Whitelisting:** Only authorized IP addresses could interact with the PDUs.
- **Protocol Minimization:** Disabled unnecessary services to reduce cyber-attack surfaces.
- **Network Isolation:** Installed using an isolated internal network interface separate from external-facing networks.

🔹 Peripheral Device Recovery

Receipt printers—often prone to freezing—were placed on PDU-controlled outlets. This allowed automatic or remote power cycling to quickly restore service and ensure uninterrupted payment and receipt functionality.

🔹 Data Security Compliance

Detailed documentation streamlined the provider's security compliance process.

Results

By utilizing Synaccess PDUs, the kiosk provider successfully deployed highly secure, reliable, and remotely manageable kiosks, achieving:

Reduced Downtime

Remote power cycling and real-time monitoring enabled swift troubleshooting, minimizing service interruptions.

Enhanced Security Posture

The secure, isolated network environment, combined with IP-based access control, minimized cybersecurity risks.

Streamlined Maintenance

Remote diagnostics and automatic printer resets reduced service calls and improved operational efficiency.

Simplified Security Compliance

Clear documentation expedited approval and audits.

Conclusion

By integrating Synaccess Switched PDUs into secure self-service kiosks, the telecom provider achieved superior operational reliability, robust security, and streamlined remote maintenance. Synaccess's combination of intelligent power control, secure network design, and comprehensive monitoring enabled a successful, large-scale rollout that ensured continuous SIM dispensing, payment processing, and receipt printing—all aligned with stringent security and performance standards.