Education Case Study

Memphis Shelby County Schools Implements Zero Trust with iboss

See how Memphis Shelby County Schools use the iboss cloud to provide secure Internet access to their students and staff

Key Statistics

Schools:	**200+**
Students:	**106,000+**
District Ranking:	**23rd Largest District in the United States**
State:	**Tennessee's Largest School District**

About the Customer

Memphis Shelby County Schools is the largest school district in Tennessee, serving over 106,000 students across 200 schools. Memphis-Shelby County Schools (MSCS), formerly known as Memphis City Schools and Shelby County Schools, has a complex and evolving history that reflects the broader educational and social dynamics of the region. Originally operating as two separate districts—Memphis City Schools serving the urban core and Shelby County Schools covering the surrounding suburban areas—the two systems merged in 2013 following the dissolution of the Memphis City Schools charter. This unprecedented consolidation created one of the largest school districts in the United States, serving a diverse student population across urban and suburban communities. The merger aimed to streamline resources, reduce administrative overhead, and address longstanding disparities in funding and academic achievement. Memphis-Shelby County Schools (MSCS) firmly embeds student success and digital protection into its IT mission. The district's IT division serves as a customer-focused team dedicated to equipping educators and administrators with robust tools, data systems, and infrastructure that support classroom instruction, business operations, and effective student engagement. This commitment to student success drives the organization to prioritize both instruction and data protection, ensuring that young learners and educators alike benefit from a secure environment. Together, these efforts reflect MSCS's dual commitment: enabling measurable student growth through data-informed learning and proactive support, while safeguarding digital assets and personal information through modern cybersecurity policies and vigilant vendor governance.

Memphis Shelby County Schools's Challenge

Memphis-Shelby County Schools (MSCS) faced a complex and multifaceted challenge in modernizing its IT infrastructure and security posture. The project was sparked in part by expiring hardware and fragmented VPN solutions. Ultimately, this large-scale transformation required cross-departmental collaboration and a shared commitment to enhancing digital safety, security, and operational resilience district-wide. Following an initial assessment of its aging platform, the district developed a plan to replace legacy solutions and implement a Zero Trust architecture using iboss Zero Trust SASE. The goals were clear and urgent: improve content filtering, enable the detection of self-harm or harm to others, implement robust data loss prevention (DLP) capabilities, and replace aging VPN infrastructure with a more secure and scalable solution. However, midway through identifying and selecting a new product, the IT department underwent leadership turnover—twice at the Director level—posing a serious risk to continuity and momentum. Despite this disruption, the team remained focused and committed to the original vision, understanding that existing tools were outdated and increasingly costly to maintain.

The district's approach was met with additional challenges: while many third-party vendors were essential to daily operations, some refused to install security agents on their devices, creating potential gaps in visibility and control. MSCS still needed to uphold strict compliance standards and maintain centralized oversight across its environment.

Gaining buy-in early was essential; a cybersecurity-focused IT Town Hall helped align stakeholders, reinforce priorities, and secure support. The district structured the initiative into four strategic phases, starting with the identification of all digital and physical resources—such as printers, smart boards, cameras, and conference rooms—and assigning each a role within the Zero Trust model. The project, driven in part by expiring hardware and fractured VPN solutions, required broad cross-functional coordination beyond the IT department, ultimately demonstrating MSCS's commitment to long-term digital safety, compliance, and operational resilience.

Memphis Shelby County Schools's iboss Solution

To address its aging infrastructure, rising security concerns, and evolving leadership landscape, Memphis-Shelby County Schools (MSCS) committed to a phased Zero Trust security strategy using iboss Zero Trust SASE as its foundational platform. This solution aligned perfectly with the district's goals: replacing legacy VPNs, enabling advanced content filtering, detecting self-harm or harm to others, implementing data loss prevention (DLP), and ensuring scalable cloud-based security that wouldn't be hindered by physical infrastructure or personnel changes.

As the district faced resistance from some third-party vendors unwilling to install security agents on their devices, iboss browser isolation became a critical workaround. This allowed the district to maintain visibility, control, and compliance without compromising its Zero Trust standards—particularly important when external systems had to connect securely to district-managed environments. iboss's agentless architecture enabled secure access to applications while isolating potential threats from unmanaged devices.

The district also benefited from role-based access control, which supported their Phase 1 initiative to catalog and assign roles to all resources—such as printers, smart boards, cameras, and conference room systems. With iboss, MSCS was able to define and enforce least-privilege access across its entire environment, regardless of device type or location, in alignment with the core principles of Zero Trust.

Replacing their two fragmented VPN systems was another milestone. Instead of investing in new hardware, the district used iboss to establish cloud-based secure access, managed by their ISP, which greatly simplified infrastructure while increasing flexibility and scalability. This shift not only cut costs but also improved connectivity and uptime across hundreds of school sites.

In a project initially estimated by some to take up to six years, iboss's cloud-native platform allowed the district to maintain momentum through leadership turnover and accelerate implementation by breaking the project into manageable, trackable phases. The IT team also gained early buy-in through a cybersecurity-focused Town Hall, which reinforced stakeholder alignment and demonstrated how the iboss platform could evolve with district needs over time. iboss gave MSCS the tools to move from strategy to action—delivering a secure, scalable Zero Trust environment tailored to the realities of a large, dynamic public school district.

> *This was a massive project that required the help from many, not just the IT Department.*

Adam Young

Executive Director of IT Operations, Memphis Shelby County Schools

Key Results for Memphis Shelby County Schools

- Improved Security Posture: Significantly reduced attack surface by replacing legacy VPNs with secure, cloud-delivered access
- Full Visibility and Role-Based Control: Centralized visibility and granular access control across all 200+ campuses
- Agentless Protection for Third-Party Devices: Overcame securing third-party vendor access without requiring agent installation
- Advanced Content Filtering and Harm Detection: Proactive detection and response to signs of self-harm, violence, or policy violations
- Reduced Infrastructure Costs: Avoided need to replace aging VPN hardware, saving significantly on capital expenditures
- Strategic Alignment and Buy-In: Early stakeholder involvement ensured long-term commitment through leadership turnover
- Foundation for Long-Term Resilience: Established foundational Zero Trust architecture for future scalability