BALTIMORE CITY
PUBLIC SCHOOLS

EDUCATION

CASE STUDY

Baltimore City Public School System Delivers Secure Technology to the Classroom With Absolute Secure Endpoint

School System Addresses Concerns Over Device Theft and Asset Management With Absolute

The Baltimore City Public School System (BCPSS) supports 200 schools, 8,000 teachers, and 85,000 students. The school district's mission is to provide the education students need to succeed within the 21st-century workforce. To achieve this, it is critical that students, faculty, and staff have access to the technology, tools, and resources that promote higher achievement and effective communication methods.

> We're focused on bringing technology into every classroom for every student, and we simply couldn't do that safely without Absolute.
>
> MIKE PITROFF,
> CHIEF TECHNOLOGY OFFICER,
> BALTIMORE CITY PUBLIC SCHOOL SYSTEM

THE STORY

Reducing Risk and Mitigating Device Theft

Through government funding, BCPSS implemented a 1:1 program, offering a device to every student and teacher. However, with especially high crime rates in Baltimore, the IT team had the difficult task of ensuring that all school devices—and the sensitive data they contained—were secured and accounted for.

To address this challenge, the IT team sought a solution that could reduce the risk and cost associated with laptop thefts, maintain an accurate inventory of all district-owned IT assets, and protect the data on teachers' and students' devices. In addition, the district wanted to ensure continued funding of its 1:1 program by demonstrating the return on investment for the technology initiative.

SECURITY CHALLENGES

SAFER SCHOOLS

DEVICE RECOVERY

DATA PROTECTION

THE SOLUTIONS

How They Did It

Simplifying Asset Management for Thousands of Devices

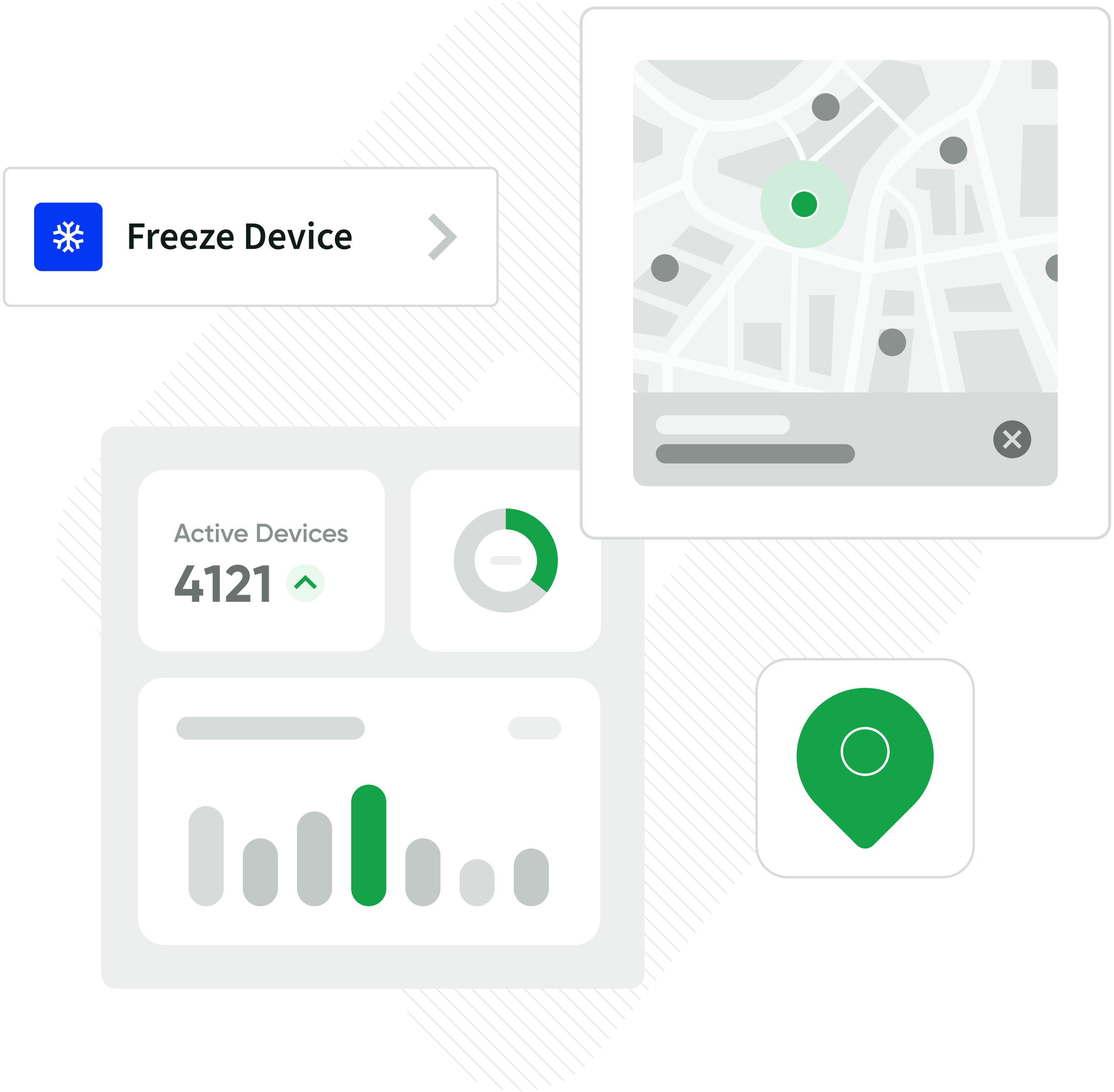
Mike Pitroff, Chief Technology Officer for BCPSS, knew that the district couldn't manage the burden of tracking and securing thousands of laptops without assistance. "Absolute Secure Endpoint gave our IT department peace of mind," explained Pitroff. "It would be impossible for us to manage thousands of laptops without a complete software solution."

Enhanced Visibility Across All Devices, No Matter Where They Are

Once activated, the Absolute Persistence® technology enabled a constant connection to all devices owned by the district. Tracking is achieved via any Internet connection, regularly collecting asset information from each device regardless of its physical location. This allows administrators to know where laptops are located, who is using them, and what's installed on them.

Keeping Devices and Data Safe

Absolute Secure Endpoint allows BCPSS to ensure devices and data are always protected. If suspicious behavior is detected and security measures are required, BCPSS' IT team can use the cloud-based console to remotely freeze the device or delete the data. In the event of a theft, the Absolute Investigations team will engage with local law enforcement to recover the device.



> Absolute Secure Endpoint is an integral part of the BCPSS Information Technology Plan, and it is installed on every single mobile device in the district.
>
> MIKE PITROFF,
> CHIEF TECHNOLOGY OFFICER,
> BALTIMORE CITY PUBLIC SCHOOL SYSTEM

THE RESULTS

Protected Devices = Safer Schools

With Absolute Secure Endpoint, the Baltimore City Public School System was able to address its security concerns and embrace technology with a sense of security. For the Baltimore City Public School System team, Absolute Secure Endpoint:

- ✓ Helps address device theft and tracking concerns
- ✓ Provides their IT team with the ability to use a cloud-based console to remotely freeze the device or delete data if suspicious activity is detected
- ✓ Gains visibility into how a device is being used, where the devices are, and what is installed on them

ABSOLUTE®

Trusted by nearly 21,000 customers, Absolute Software is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections — helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks.

Request a Demo