CASE STUDY

Keeping a Metropolis on Track

Everyone recognizes the "If you see something, say something" signs posted at public transportation sites around the country. And, sure, vigilant commuters will react when they see suspicious behavior or an unattended bag. But what happens when the threat is invisible?

Trustwave®

Client Spotlight

One of the country's largest regional transportation agencies, this client had to secure more than 400 different sites, both above and below ground. Its jurisdiction spans a 5,000-mile area across two states and encompasses stations and terminals with wildly fluctuating temperatures. If anything went wrong, five million-plus daily riders might be affected.

The Challenge

That was the dilemma faced by a transit network that serves more than two billion (yes, billion with a "b") riders annually. Providing network security across a densely populated urban area is incredibly difficult no matter the scope of the assignment—but this project was made even tougher by the fact that 75,000 separate devices had to be protected across hundreds of bus terminals, train stations and other transportation hubs. The stakes are higher, still, because a single breach can disrupt travel in one of the largest cities in the United States.

> *"Consider 75,000 devices, extreme station temperatures, and the 24/7, 365-days-a-year nature of transport operations—and you have an environment more challenging than most any other imaginable."*

This client's networks were similarly complicated: Imagine a mishmash of thousands of miles of new fiber optic cables running alongside lots of old copper wire, with an added heap of broadband wireless networks that provide internet access to both the system's workers and riders. Layer on less-than-ideal circumstances—stations with no air-conditioning or heat, train vibrations, electromagnetic interference, and the 24/7 nature of transit operations—and you have an extremely challenging production environment.

The Solution

Trustwave's centralized and flexible network access control (NAC) solutions allowed the agency to proactively monitor tens of thousands of devices at all times, helping ensure they met stringent security standards. When a device failed to meet those policies, it could be immediately identified and quarantined from the rest of the network until the problem was fixed. Trustwave also created ruggedized versions of its security devices that were built to withstand the dust, extreme temperatures and vibrations that are common around transit stops.

As the Internet of Things grows, overseeing the security of massive numbers of devices will become a far more common mandate. Automation and clear, centralized policy management are required to tame what would otherwise be a nightmarish and horribly expensive endeavor. With proper systems in place, transit authorities and other municipal systems can reliably protect its workers, riders, and infrastructure 365 days a year, 24 hours a day—rain or shine.

Industry Threat

According to the U.S. Department of Transportation, public transit and rail operations provide nearly 11 billion annual passenger trips. Because it's part of the country's critical infrastructure and reaches so many people, transit operations are increasingly targeted by nefarious actors. One municipal transit agency learned this firsthand, when a ransomware attack crashed its ticket payment system. Potential victims go far beyond regional transportation authorities, too: Hackers have demonstrated how easy it is to take control of cars driving along a highway.

> *"As the Internet of Things grows, overseeing the security of massive numbers of devices will become a far more common mandate."*

Trustwave®

CS-TRN-0118