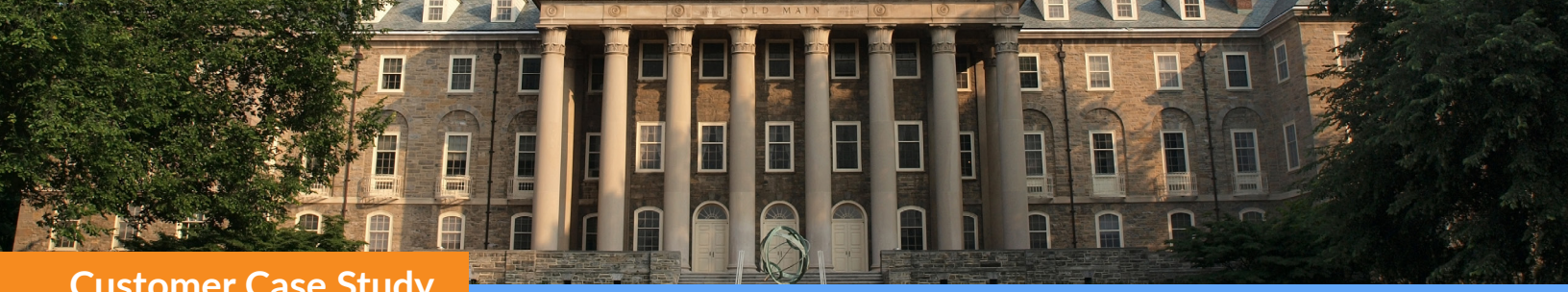


Customer Case Study

Penn State's Secure Network Transformation

Their journey to connect and micro-segment Building Automation Systems amid chaos.

Customer Requirements

- BACnet traffic segmentation from shared infrastructure across 640+ buildings.
- Centralized control of hundreds of BACnet systems, spanning multiple state-wide campuses
- Maintain legacy network while building out new infrastructure
- Enhance security posture

Solution

- Micro-segmentation isolates and cloaks BACnet traffic – removing it from the 'attack surface'
- Easy adds, moves and changes for secure contractor access to specific devices on the network via centralized orchestration
- Simple, centralized provisioning manageable by non-technical staff

Benefits

- Achieved project goals, on time, at a quarter of the cost of traditional networking and security solutions
- Workforce savings – Simplicity of IDN setup and provisioning made it possible to accomplish with existing staff
- Dramatic performance improvements due to reclaimed network bandwidth by eliminating broadcast storms

Listed among the top 100 universities in the world and cited as one of the "Top 50 Best Universities" in America, Penn State University is a well-rounded and highly competitive institution. When it came time to upgrade their aging infrastructure across their expansive campus, the stakes were high, resources tight, and "game time wouldn't wait."

The university was under the gun to reduce risk and increase efficiency by isolating and centralizing its BACnet (Building Automation and Control network) system. BACnet streamlines access to facility automation applications such as heating, ventilating, and air-conditioning (HVAC), lighting control, access control, and fire detection systems.

With Penn State's commitment to excellence and optimization of its campus facilities for students and staff, ongoing major construction projects run concurrently, which means hundreds of contractors, technicians, and vendors require network access.

Over 640 buildings are spread across dozens of state-wide campuses. Their network attack surface was significant with many rogue access switches and wireless access points. With BACnet communications openly traversing Penn State's flat network, orders were to get the BACnet traffic segmented. According to Tom Walker, systems design specialist and project lead at Penn State, "Everyone who has deployed BACnet has experienced its disruptive broadcast storms that impacts performance and can create outages in other parts of the network."

The IT team's plate was overflowing, so the Plant Services staff was on their own for this huge undertaking. Time was ticking with a looming deadline to complete the project before the university's students arrived at the end of summer. Using outside contractors to help re-engineer the network was out of the question due to cost. To make things thornier, the communication infrastructure upon which BACnet rode was a spider web of direct, wireless and cellular network connections.

A Swift and Smooth Deployment at a Fraction of the Cost

The university chose a micro-segmentation solution from Tempered Networks to isolate and cloak its BACnet traffic. Tempered Networks' IDN solution enabled the facilities staff to rapidly segment their BACnet deployment with simple 'point-and-click' centralized management across the entire campus deployment.

TEMPERED NETWORKS

Now, Tempered Networks' solution creates secure, private overlay networks on top of the physical network, where only explicitly trusted systems or endpoints are allowed onto the overlay. Tempered Networks' HIPswitches work in conjunction with the Conductor, Tempered Networks' centralized orchestration engine that creates, manages and monitors device configurations and security policies.

Fronting each BACnet router with a HIPswitch ensured that the BACnet traffic was properly segmented – significantly reducing security risk. And, the simplicity of bringing building automation systems online via the Conductor's intuitive UI meant the facilities staff could manage the network re-architecture on their own. No disruption to the underlying network and no IT support needed.

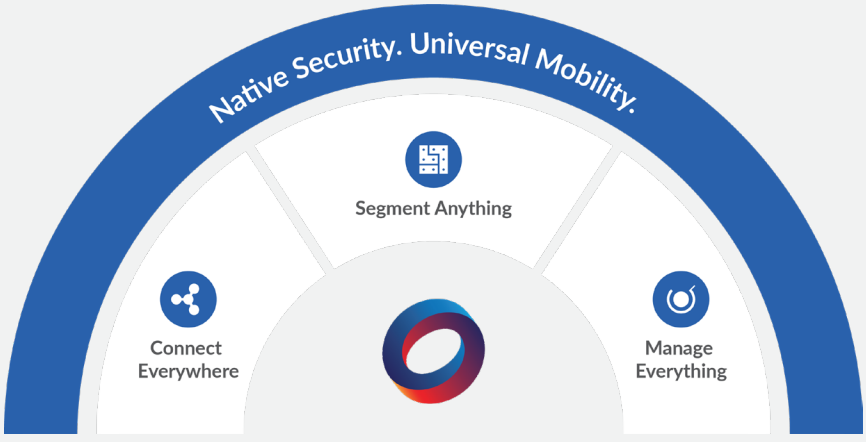
In addition, using proper micro-segmentation the Plant Facilities team has overcome the issue of broadcast storms by effectively isolating and restricting noisy BACnet traffic to encrypted network segments.

The small Plant Facilities crew comprised of two Network Admins, two System Admins, along with four Technical Services installers were able to complete the project on time and under budget. The cost of Tempered Networks was a quarter of what the team had anticipated, as compared to traditional network security techniques. "We looked at creating separate VLANs or (private VLANS) within the buildings, doing MAC filtering, doing access control lists, or doing building-level firewalls," Walker says. "But when we started looking at scalability, it gets crazy. For some of those options, I'd have to hire at least two more people just to manage the toolsets."

Connectivity Without Constraints

Today, the Facilities team can quickly cloak, connect, and micro-segment any device or system (including legacy) with point-and-click simplicity. It's non-disruptive and fast to implement because it requires few if any changes to existing network infrastructure. PSU's successful journey to connect and protect their expansive building automation systems encompassed:

- Centralizing and securing plant services across the LAN and WAN
- Supporting aging legacy systems and vulnerable endpoints
- Maintaining the old network while building out new infrastructure
- Securely extending connectivity to any location – even to the middle of a cornfield!



Experience the same simplicity, security, and cost-savings that our customers achieved.

To learn more or schedule a no obligation demo, email info@temperednetworks.com or visit www.temperednetworks.com

