

Sponsored by Tempered

# SMART BUILDINGS 2.0



## Airwall The next-gen air gap

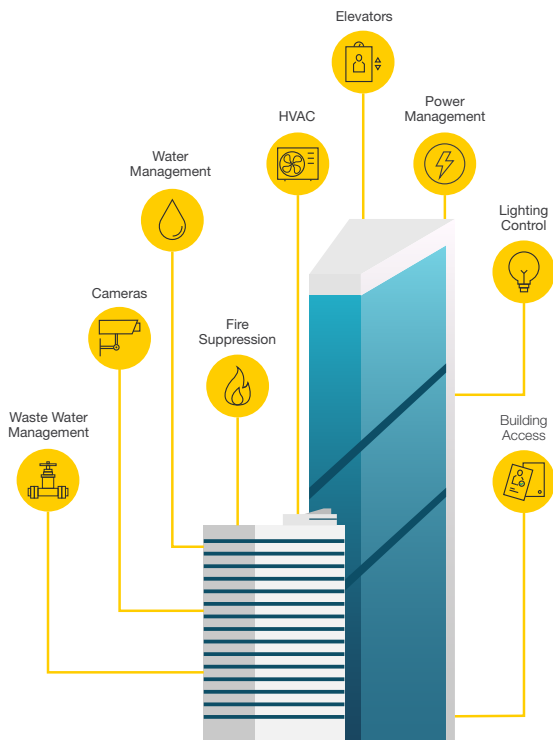
---

Find out how a top 100 U.S. University  
securely connected and isolated  
their building controls across  
**640 buildings** in record time



# A SMALL TEAM PRODUCED BIG RESULTS

The facilities automation services (FAS) group sleeps soundly knowing their smart building systems are isolated from the shared network, cloaked from unauthorized devices, and always on—with no more 2 A.M. calls.



## CHALLENGES AT A GLANCE

- ❑ Shared network with no isolation/segmentation
- ❑ Exposure to thousands of attack vectors
- ❑ Broadcast storms impacting availability
- ❑ Chaos caused by ongoing alarms and downtime: 100k alarms/week
- ❑ Unrestricted access to the network by vendors
- ❑ Dependency on IT for change/support issues

**T**he University's system design specialist leads the FAS group which is responsible for maintaining the high availability, integrity, and confidentiality of building systems supporting nearly 150,000 students and University employees.

With over 640 buildings statewide to manage, the FAS group needed to centralize and isolate plant services across the University's shared infrastructure. The HVAC systems, lighting, building access controls, and other building specific-systems were on the same flat network as their HR and finance servers (for example).

"I took over this infrastructure when it was a flat, Layer 2 network across the main campus about four years ago," he said. A lack of adequate segmentation exposed the entire network to lateral attacks by bad actors.

## Get the Full Version!

Download the full customer story and learn more about their deployment

→ [discover.tempered.io/case-studies/penn-state-university](https://discover.tempered.io/case-studies/penn-state-university)

# 50 BUILDINGS CONNECTED IN 5 DAYS




Eliminating network complexity and cost with a micro-segmentation solution

**F**inding a solution that met their requirements was not easy. Their network had grown organically over the years, and at this point was a complex mix of a flat shared Layer 2 network augmented with a new routed layer 3 network. Increasing their challenges, the building automation systems (BAS) network was a complex web of managed and unmanaged Ethernet, Wi-Fi, and cellular networks controlled by other departments.

“We looked at creating separate VLANs or [private VLANs] within the buildings, doing MAC filtering, doing access control lists, or doing building-level firewalls,” he stated. “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 and coordinate the combination of tools.

A proof-of-concept sealed the deal and

## BENEFITS AT A GLANCE

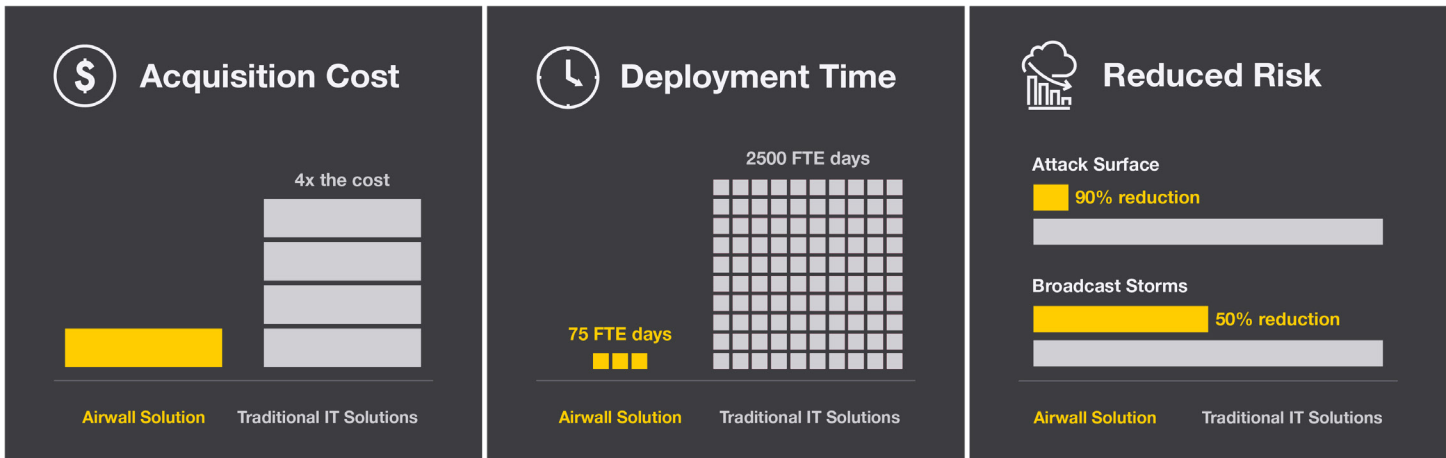
- 
**Increased Connectivity & Availability**  
 Eliminated broadcast storms, reduced alarms by 50%, and easily connected new and remote buildings
- 
**Stronger Security**  
 Reduced attack surface by 90% by segmenting and isolating their modern and legacy BAS across shared infrastructure
- 
**Reduced Costs**  
 Achieved significant cost-savings for hardware and accelerated deployment by 10x without needing additional headcount

shaped their deployment. “In less than 20 minutes, we were able to install our first cloaked overlay network without having to modify systems or involve external departments,” he said. To the FAS group,

an important aspect of the Tempered Airwall™ was the ease of management and non-disruptive deployment, which meant they could manage the network re-architecture on their own.

## A more secure network at a fraction of the cost of alternative solutions

Tom and his team connected and segmented 50 buildings in 5 days, and completed all 640 buildings in 75 days



# CONNECT, COLLECT, ANALYZE, & CONTROL

Improving availability, operational efficiency, and predictive maintenance—while minimizing overall network attack surface and mitigating risk

The main driver for the FAS group's decision to upgrade their smart building infrastructure was the need to secure and isolate communications across the University's shared infrastructure and in the field. "I wanted something that we could easily deploy and rapidly secure the infrastructure," he noted. "Now we have a private and isolated network for all our legacy and new BACnet systems. It's now simple and fast to connect and segment any building controls, over any network."

The individual building systems are locked down based on functionality, not by port. "If one of those controllers gets compromised, they only have access back to the data center, to one server. Before, if somebody compromised a building, they could get access to the data center and all the exposed applications," he explained. "Now we're able to say: 'the lighting controller can only talk to the lighting server. The elevator controller can only talk to the elevator server'."

## Improving data collection

By converging networks for multiple controls systems across 640 buildings, the FAS group is saving money through improved building efficiency and

predictive maintenance. "We're taking on more controls within the building – everything that keeps the building running. We're bringing data back through our network infrastructure and into the data center, and then either jumping it to the cloud or passing it over to other analytic systems to analyze the data," he stated.

“We're able to deploy in places that we weren't able to get to before,”

As an example, the FAS group started tracking elevator use. "We found one elevator that did 1,900 trips in one day. It was insight we never had before, and it explains why that elevator is constantly breaking down," he said. "With data analysis, we can anticipate heavy usage on student move-in days, and use predictive maintenance to prevent the occurrence of failures."

## Eliminating broadcast storms

By isolating and segmenting their BAS, the FAS group eliminated broadcast storms and increased network performance. "In case of BACnet broadcast storms it's easy to shut down traffic from a single building," he elaborated. "Before, because it was a big, flat Layer 2 daisy-chained all the way out, I'd have to shut off multiple ports. Or, if I shut off one port, it might shut off half a dozen buildings. Now I can individually control traffic from each of my buildings."

## Bringing new and remote buildings online with cellular

As the FAS group continues to expand campus properties, Tempered Networks' broad connectivity options enables them to connect the most remote sites across separate networks. Recently, the FAS group connected a building in the middle of a cornfield using cellular, where it would have cost over \$100,000 to establish a fiber connection. "We're able to deploy in places that we weren't able to get to before," he said.

Ultimately this means the FAS group can retro-fit older buildings and bring new buildings online without having to involve external department or wait for the local ISP to activate the primary wired connection.

## Easily segmenting network access

The FAS group now easily manages their large vendor ecosystem, instead of dealing with the complexity of ACLs, VLANs, VPN tunnels, and insecure port forwards. They provide simple and segmented remote network access for employees, contractors and vendors, as an alternative to traditional VPN-based access, without leaving open pinholes in their firewalls. The result? They no longer worry about rogue access points and can give and revoke network access instantly.

Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500

