Tempered

Simple & Secure PCI DSS Compliance

Gain control over PCI audit scope while dramatically improving security posture

Decrease IT CapEX and OpEx costs by **25%**

Reduce PCI compliance time by up to **30%**

Reduce attack surface by **90%**

The challenges of PCI DSS compliance

Adhering to Payment Card Industry Data Security Standard (PCI DSS) requirements is a necessary part of doing business today. Any organization that stores, processes, or transmits cardholder data (CHD) and/or sensitive authentication data (SAD) must establish, maintain, and demonstrate compliance. Organizations are struggling to achieve PCI compliance across distributed CHD systems and hybrid environments. The increased sophistication of attacks that bypass traditional defenses has accelerated breaches. Organizations now spend more time focusing on security than ever before.

Even if an organization is deemed PCI compliant, its network and assets are not necessarily protected against cyberattacks. This risk is evident by the number of well-known organizations that were deemed PCI compliant and yet breached. Oftentimes corporate networks are flat, with security that stops at the edge and not at the individual host or service. Connections are secure until they get to the edge of the network, then a patchwork of VLANs, Access Control Lists, routing rules, firewall policies, and other technologies are used.

These IT barriers reduce the agility of your overall business and result in an inflexible, complex network architecture that does not provide secure connectivity or scale for all your resources. These technologies are also prone to human error, which creates costly overhead and diminishes your organization's security posture. Better security is still needed to prevent intrusion into your network and the theft of credit card information.

PCI DSS requirements (v.3.x)

Requirement 1 Install and maintain a firewall configuration to protect CHD	**Requirement 2** Do not use vendor-supplied defaults for system passwords and other security parameters	**Requirement 3** Protect stored CHD	**Requirement 4** Encrypt transmission of CHD
Requirement 5 Use and regularly update anti-virus software	**Requirement 6** Develop and maintain secure systems and applications	**Requirement 7** Restrict access to CHD by business need-to-know	**Requirement 8** Assign a unique ID to each person with computer access
Requirement 9 Restrict physical access to CHD	**Requirement 10** Track and monitor all access to network resources & CHD	**Requirement 11** Regularly test security systems and processes	**Requirement 12** Maintain a policy that addresses information security

Secure & segmented PCI DSS compliance with Airwall

Airwall is Tempered's Zero-Trust Software-Defined Perimeter that unifies networking and security. It is purpose-built to overcome the challenges caused by today's complex and inherently vulnerable networks. Airwall overlays your existing infrastructure and delivers secure and segmented connectivity for any device, across any environment, anywhere in the world. Organizations can connect, encrypt, and segment any host or service across physical, virtual, and cloud environments, with little modification to underlying switching and routing infrastructure.

Airwall easily removes systems and devices that do not belong 'in scope,' to achieve secure and segmented connectivity. Segmentation can be enforced at the device level between all sensitive PCI systems, assets, and hybrid cloud and datacenter environments.

Airwall also provides true peer-to-peer secure networking for any device and supports the key requirements and controls of PCI DSS. This secure networking is all done with a simple, sustainable, and operationally efficient enterprise architecture. Airwall ensures better control of the audit scope for PCI systems and assets by enforcing a software-defined perimeter, and clearly defines how credit card data moves on the network.

How Airwall helps organizations stay PCI compliant

Airwall helps organizations become PCI compliant faster than ever before. Protecting and connecting PCI systems and assets with non-traversal micro-segmentation becomes simple, verifiable, and nearly hack-proof. With micro-segmentation, organizations are able to reduce the attack surface, the impact of system vulnerabilities, and unauthorized access. The result is simple and secure connectivity, which adheres to PCI DSS compliance requirements across any network environment. Airwall achieves a level of security and connectivity that isn't practical or feasible with other tools.

Here's how Airwall helps organizations follow-through on PCI DSS requirements:

	PCI DSS Requirement (v.3.x)	What Airwall Does
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Provide simultaneous network transport and security that, by default, provides the highest security standards. Initial management passwords are forced changed at initial login. No management password available or configurable for CLI.
4	Encrypt transmission of CHD	Encrypt CHD in motion using military strength AES 256 across open and public networks. While local syslog / reporting data is not encrypted, TLS can be used for external syslog in transit.
5	Use and regularly update anti-virus software	Hardened physical Airwall Gateways have operating systems that are not accessible. Furthermore, a PCI device cloaked and encrypted by Airwall can be placed in its own "quarantine network" with the aid of third-party zero-day antivirus services.
6	Develop and maintain secure systems and applications	Software undergoes strict security testing for possible vulnerabilities before every code release.

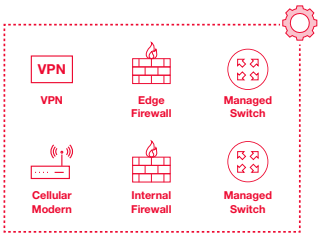
	PCI DSS Requirement (v.3.x)	What Airwall Does
7	Restrict access to CHD by business need-to-know	Restrict access to CHD by providing identity-based access on a need-to-know basis, where access is logged and can be regularly audited.
9	Restrict physical access to CHD	Provide additional login requirements for remote user access.
10	Track and monitor all access to network resources & CHD	Can be involved by logging Airwall activity and securely offering encrypted log files to a log depository.
11	Regularly test security systems and processes	Vulnerability tests are completed for each software release.
12	Maintain a policy that addresses information security	Can be involved with company security policies that address information security.

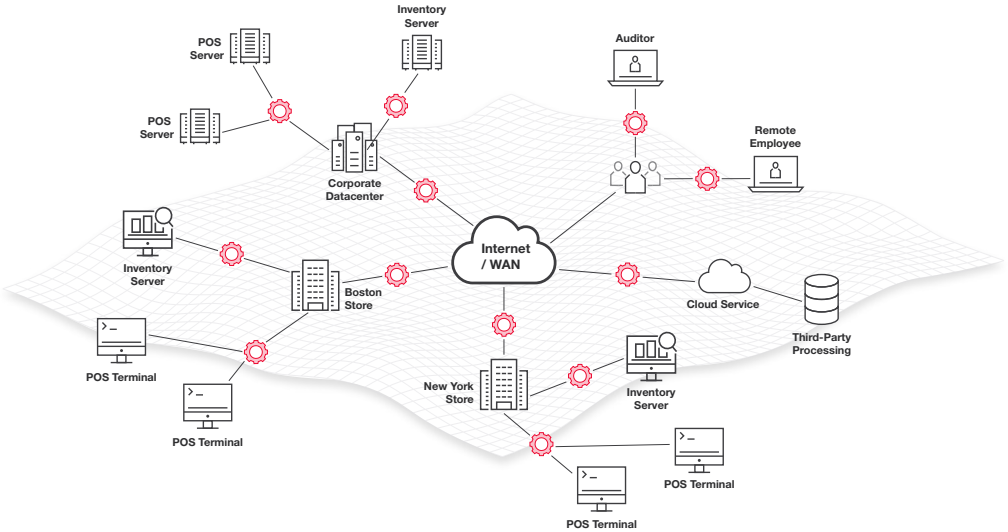
Before Airwall

Creating and maintaining PCI DSS compliant environment is complex and expensive:

- Managing a complex patchwork of VPNs, VLANs, ACLs, and other technologies
- Edge-to-edge encryption and a lack of segmentation, increasing security vulnerabilities
- PCI audit scope often includes non-related resources due to lack of segmentation, further increasing the complexity and cost of PCI compliance

Existing Network





After Airwall

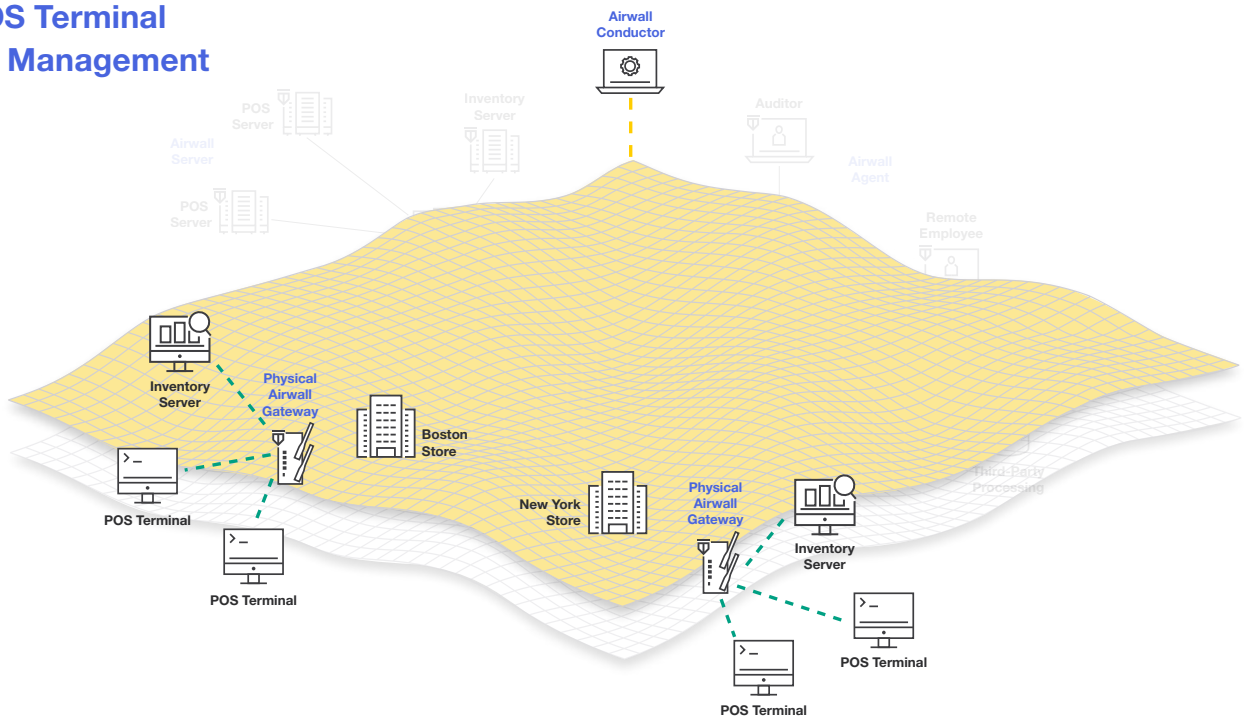
With a single solution, secure connectivity for PCI systems and assets is now fast and simple:

- Peer-to-peer encryption and device-level micro-segmentation significantly improves security
- PCI audit scope now only includes related PCI systems and assets, with simple reporting that makes PCI compliance fast and cost-effective
- No need to implement a separate PCI network apart from existing business network, saving significant capital spend and operational costs
- Simplify implementation of controls through a common intuitive management interface, drastically reducing errors
- Easy to securely add new applications and services, while remaining in compliance
- Auditing of all users and systems is straightforward and easy to achieve on a continuous basis

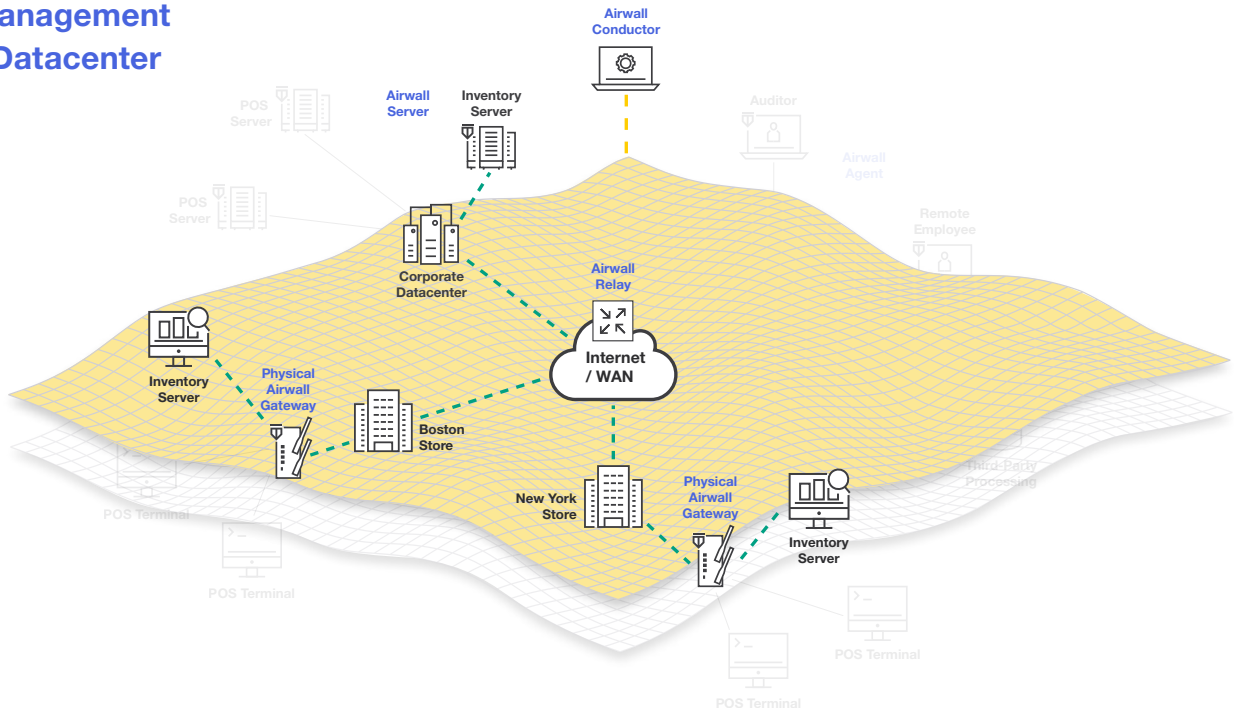
PCI-compliant network use-cases

Create secure, compliant CHD networks across the most demanding network infrastructures. Here are a handful of sample use cases:

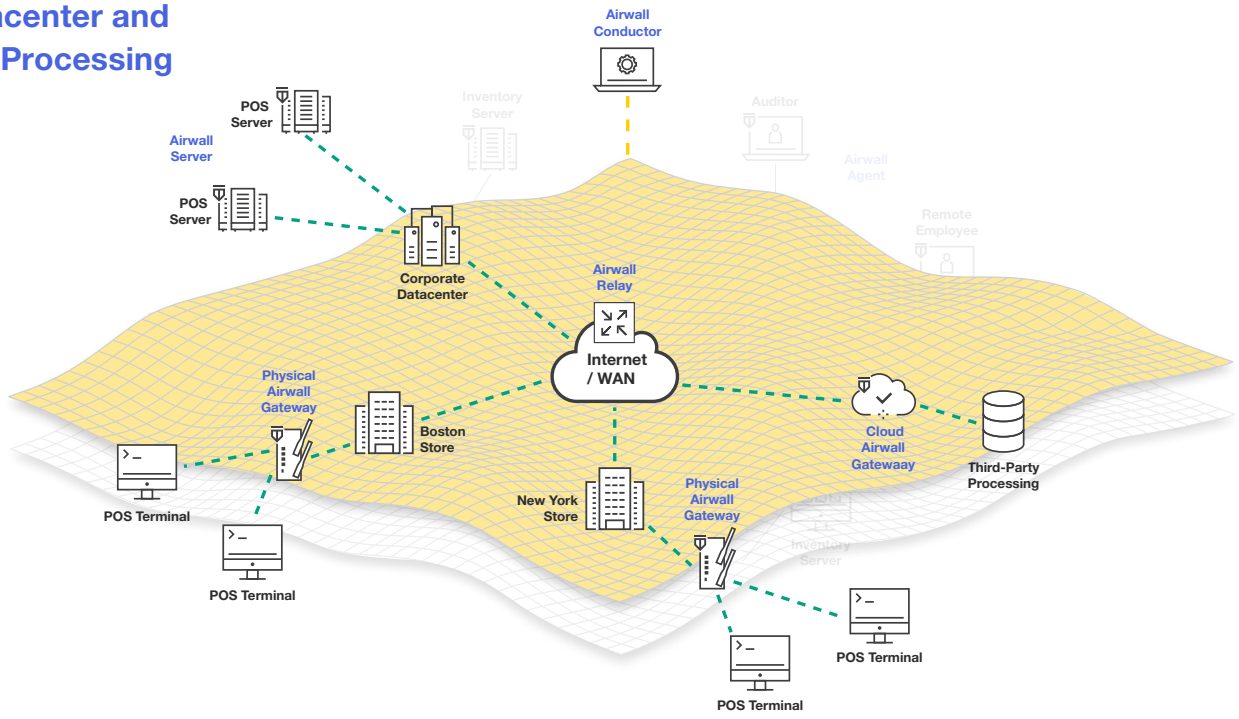
In-Store POS Terminal & Inventory Management



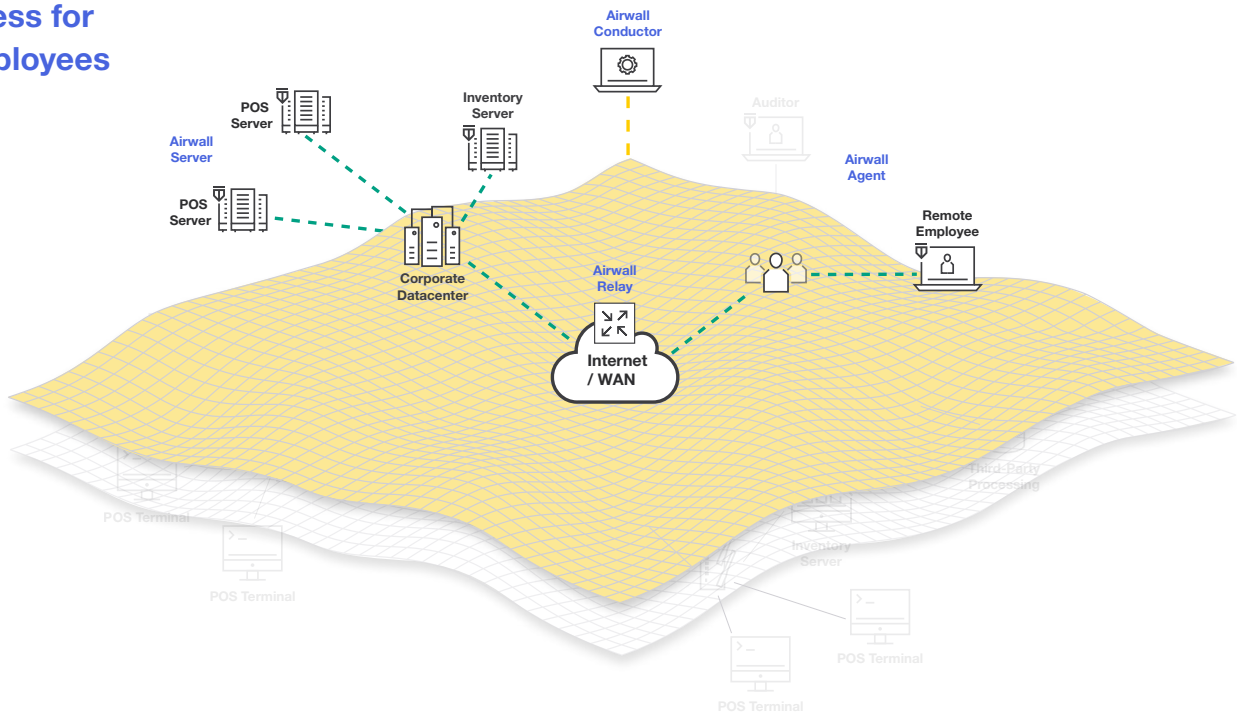
Inventory Management In-Store to Datacenter



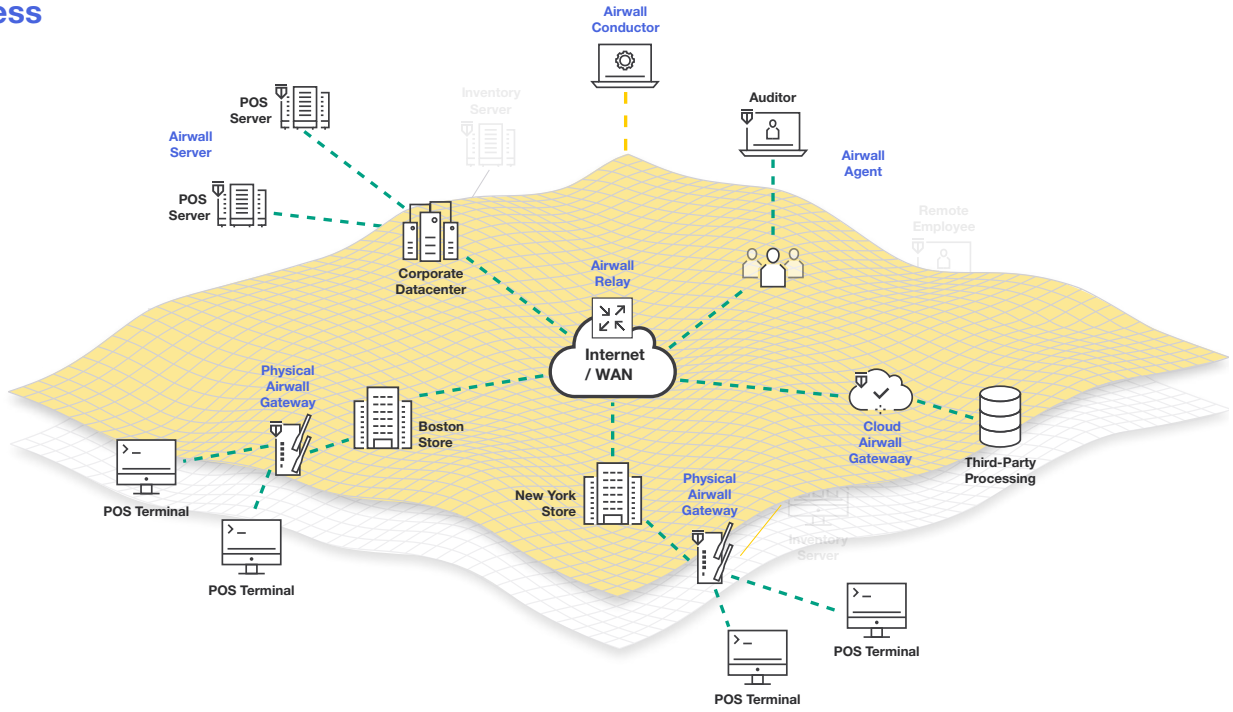
POS to Datacenter and Third-Party Processing



Secure Access for Remote Employees

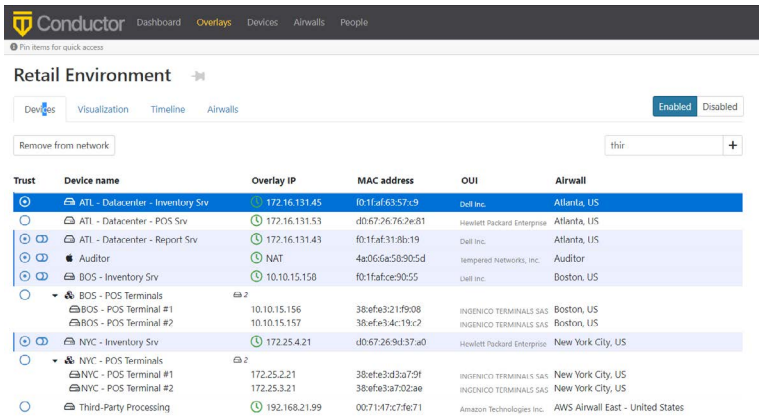


Secure Access for Auditors

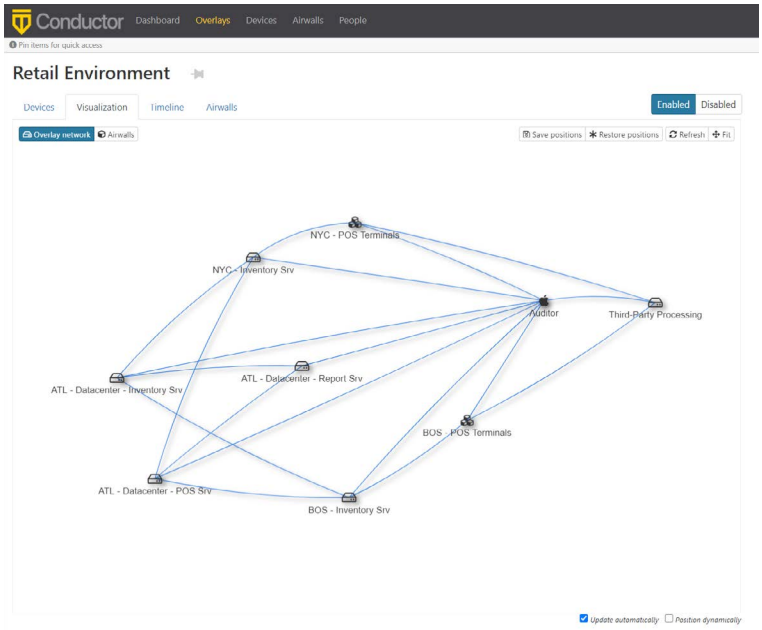


Simple management reduces complexity & time-to-deploy

The pitfalls of improper or complex network segmentation include disruption to your operations or increased exposure to data theft. Airwall solves this by providing an intuitive, policy-based orchestration engine that is point-and-click simple and micro-segments to the device and application level. You can now reduce deployment times by up to 97% and securely provision new resources in minutes, instead of days or weeks.



Point-and-click simple policy configuration makes it incredibly easy to securely configure your network



Airwall's powerful Visual Trust Map allows you to see specific trust relationships

A better way forward

Tempered's Airwall is based on the principle that it should be easy to protect, connect, and manage devices on your network. Airwall ensures PCI DSS compliance with a platform that easily creates and maintains intuitive hyper-secure networks across complex infrastructures. The result is Zero-Trust Network Access (ZTNA) across the enterprise that is impervious to lateral movement.

Enable PCI DSS compliance for your organization.

Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500