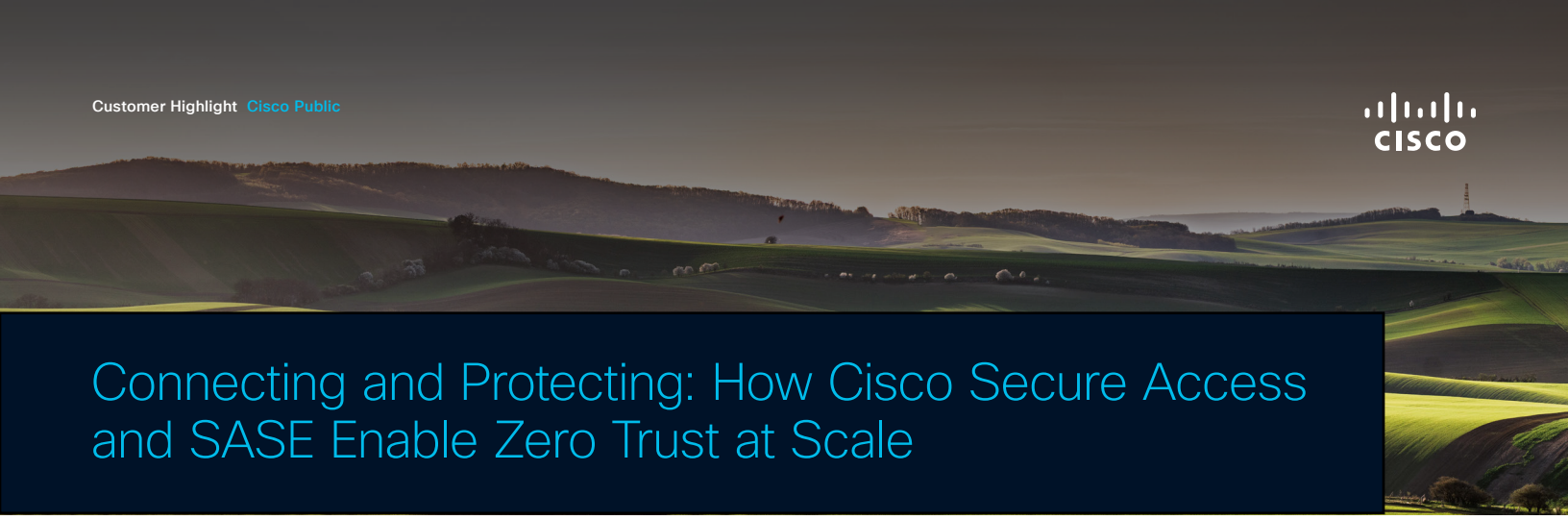

Connecting and Protecting: How Cisco Secure Access and SASE Enable Zero Trust at Scale

Industry:
Food Manufacturing

Location:
Tuscaloosa, Alabama

Organization:
Industry leader, 7,000 employees, 20 US locations, Global exports

Solution:
Cisco SASE
Cisco User Protection Suite
Cisco Breach Protection Suite

Headquartered in the U.S., Peco Foods is a fully integrated poultry processing and packaging company serving industrial, retail grocer, foodservice, and international markets. Producing over 28 million pounds of poultry each week, the company processes private-label and store-brand chicken for U.S. customers and exports items to Canada, Mexico, South America, Asia, and Eastern Europe.

High-Stakes Security Challenges for Critical Infrastructure

From hatcheries to processing facilities, Peco Foods is a U.S. leader in poultry production, producing more than 28 million pounds of ready-to-cook chicken each week for retail grocer, food service, and international markets. With operations spanning the southern U.S. from large processing facilities to rural sites in small towns, Peco's vision is to be a world-class food company.

That vision requires more than operational excellence. It demands a resilient technology and security foundation that keeps pace with growth, safeguards critical infrastructure, and supports every employee, anywhere. For Mario Manzano, Peco Foods' IT Infrastructure, Security and Collaboration Manager, these requirements quickly became high-stakes challenges.

Expansion outpaces infrastructure

As Peco expanded its footprint, each facility evolved its own mix of equipment, applications, and connectivity. Rural sites faced slow, unreliable internet, making it difficult to ensure seamless connectivity and information flow. The result was an inconsistent user experience and a patchwork of security protections.

Fragmented systems create complexity

Years of incremental technology changes left Peco with a fragmented environment of IoT devices, hardware, endpoints, servers, and traffic. While Cisco remained a trusted infrastructure provider, Peco's networking and security operated in silos, forcing Manzano's team to work across multiple platforms and vendors. Integrating solutions was challenging, adding a lot of friction and complexity, and troubleshooting often involved multiple tools and service tickets.

VPN adds complexity and leaves gaps

Peco relied on traditional VPN for remote access, an approach Manzano likened to leaving threats "at your front door" instead of at a safer distance. The VPN model also brought configuration headaches, limited visibility, and inconsistent performance for end users moving between business environments.

Modern threats outmatch legacy defenses

The turning point came in 2024, when a security incident exposed the extent of the gaps hidden within the company's traditional network design. The post-incident review revealed that cybersecurity threats were evolving faster than Peco's tools and processes.

Cisco SASE: Unified Networking and Security

To quickly close gaps, improve visibility, and accelerate detection and response Peco partnered with long-time ally Cisco to replace their fragmented, legacy infrastructure with a modern Secure Access Service Edge (SASE) framework. Four objectives guided the imperative project:

1. **Unifying networking, security and applications** into a single cloud-delivered solution.
2. **Adopting zero trust everywhere** by replacing traditional VPN with a model that puts threats at the "fence" rather than the "front door."
3. **Simplifying management** by moving to a single pane of glass environment where policies, access, and performance can all be monitored and adjusted in one place.
4. **Improving user experience** by ensuring consistent, certificate-based, location-independent access for all users. One of Manzano's key care abouts was making the experience incredibly easy for all users.

"SASE isn't just a buzzword," emphasized Manzano. "It unifies every layer of modern IT: IoT devices, endpoints, servers, DNS traffic, cloud apps, and sites spread across the map. Before this initiative, each required separate tools, configurations, and monitoring. Now, with our Cisco-powered SASE architecture, everything is visible and controllable from one unified environment."

"With our Cisco-powered SASE architecture, everything is visible and controllable from one unified environment."

– Mario Manzano,
IT Infrastructure, Security and Collaboration Manager, Peco Foods

Cisco Secure Access ZTNA foundational to SASE success

Adopting Cisco Secure Access was central to achieving Peco's SASE goals. The cloud delivered Zero Trust Network Access (ZTNA) solution removes VPN complexity, so users no longer need to pick a VPN or manually authenticate. Instead, policies apply automatically in the background, granting users secure, instant, and hassle-free access to their applications from any device, anywhere.

"Secure Access combines the flexibility we need for our use cases, business model, and technology – delivered through a single pane of glass," explained Jerold Poe, Network Projects Manager for Peco Foods. "It just works, and that's the beauty of it." By replacing Cisco Umbrella and traditional VPN with Secure Access and its identity- and device-based controls, Peco has achieved:

- **Stronger security** by reducing attack surfaces and blocking unauthorized access
- **Consistent user experience** whether in the office or remote
- **Simplified IT operations** by unifying networking and security in one platform
- **Improved compliance** through detailed visibility and policy enforcement

"We thought switching to zero trust access and making that connection in Secure Access was going to be more challenging," said Manzano. "But that wasn't the case at all. Once we began, it was completely intuitive." Peco's initial Secure Access deployment was completed in just three months, providing organization-wide secure internet access, DNS-layer security, zero trust protection for critical applications and more.

Avery Arroyo, Network Engineer at Peco Foods, agreed with Manzano: "Secure Access was very simple to deploy. We think of it as our 'eye in the sky' – a single pane of glass where we can see our environment from a top-down view." He adds that for end users, the change has been seamless. "Secure Access runs quietly in the background, letting users reach their applications without any noise, drops, or disruptions."

A Single Provider for Faster, Better, and Safer Operations

While Peco's SASE architecture is anchored by Secure Access, it's strengthened by a wide range of integrations with additional Cisco products from the Cisco User Protection Suite and Cisco Breach Protection Suite.

Cisco ThousandEyes: As an AI-powered assurance platform, Cisco ThousandEyes delivers unified, end-to-end visibility across owned and unowned networks, spanning cloud, internet, and enterprise environments. The ThousandEyes integration with Secure Access enables proactive monitoring, empowering Peco with automated, contextualized insights to rapidly pinpoint and resolve application, service, and internet performance issues, optimizing the digital experience. "The way ThousandEyes integrates with Secure Access is nothing short of genius. You have a comprehensive, quick list of telemetry that can tell you if your problem is with the endpoint, the network it sits on, the resources that device reaches out to, or something else. What used to take opening multiple tools and talking to the user is now out of the equation."

Cisco Duo: Duo integrates with Cisco Secure Access policies enabling Peco to enforce zero trust security by verifying user identities and device security posture before granting access to sensitive resources, ensuring only secure, compliant devices and verified users connect and thereby supporting continuous trust and protection of applications and data from compromised credentials and vulnerable devices. Looking forward, the company plans to deploy Cisco Identity Intelligence with Duo to gain centralized visibility, detect and respond to identity-based threats, and unify its security infrastructure.

"Every week, with every deployment, we're able to add another layer that reduces more risks. Cisco, being our one provider, is helping us get there faster, better, and with reduced risk as time goes by."

– Mario Manzano,
IT Infrastructure, Security and Collaboration Manager, Peco Foods

Cisco XDR and Cisco Secure Endpoint: By combining the power of Cisco's Extended Detection and Response (XDR) and Secure Endpoint platforms, Peco can collect and correlate telemetry from network, identity, and cloud sources, giving the security operations center a unified picture of threats.

Cisco SD-WAN: Peco is in the process of rolling out the SD-WAN cloud-managed networking solution to further improve resilience, optimize traffic flows, and make security policy enforcement consistent across all sites.

Cisco Universal Zero Trust Network Access (ZTNA): The company also plans to adopt Cisco Universal ZTNA, a scalable, identity-first approach that extends traditional ZTNA to support any application in any environment, with integrated visibility, performance, and policy control for today's complex, hybrid enterprises.

"Every week, with every deployment, we're able to add another layer that reduces more risks. We're converging everything physically and logically into one place. Cisco, being our one provider, is helping us get there faster, better, and with reduced risk as time goes by," said Manzano.

From Risk Management to Business Enabler

The shift to Cisco Secure Access and a fully integrated SASE architecture has optimized Peco's operations and transformed how quickly and effectively the company can respond to issues, protect its infrastructure, and support its users.

Efficiency gains changed the game

Prior to the rollout, field technicians often had to open multiple service tickets and jump between tools to diagnose and resolve a single problem. Now, thanks to integrations like Secure Access and ThousandEyes, they can identify root causes and resolve problems in a fraction of the time, all via a single console.

"Our field techs' minds were blown," said Manzano. "Instead of creating two or three separate service tickets, it's now one. Instead of an hour, it takes them a few minutes." Arroyo adds,

"We've seen a 60% reduction in troubleshooting time and a 7% reduction in tickets overall." From the user's perspective, the difference is even more dramatic, says Manzano. "There are no interruptions or blocks. The user experience has improved twofold, by 200%. All they need is an internet connection, and they're connected to the same resources every time."

Performance improvements go beyond raw speed. By using Secure Access to split traffic intelligently, Peco can route application flows more efficiently, improving stability even in rural locations with challenging internet connections.

Saving costs while reducing risk

Consolidating networking and security onto Cisco's integrated stack has reduced Peco's costs by:

- Eliminating overlapping licenses
- Reducing physical infrastructure requirements
- Lowering the operational burden on IT staff

From a security standpoint, Manzano's team now moves faster and more decisively. Integrated telemetry across Secure Access, Duo, ThousandEyes, XDR, and Secure Endpoint allows them to see the whole picture instantly. "We've actually removed the need to have a set of eyes on everything all the time. Automation and integration take out the guesswork," explained Manzano.

A leap in process maturity

One of the most unexpected wins was how the Cisco stack allowed Peco to skip incremental upgrades and leap directly to best-in-class solutions. This acceleration has been critical for security. In the wake of the 2024 incident, Manzano said Peco was able to close gaps much quicker than expected and they started layering on new protections nearly every week.

Future-Focused Security, Business-Focused Results

Securing operations is essential to keeping Peco running as part of the nation's critical food infrastructure. By consolidating networking and security onto Cisco's integrated SASE architecture, the company has gained the visibility, speed, and simplicity it needs to support their growth. Manzano and his team are already looking ahead. With SD-WAN deployments underway, Universal ZTNA on the roadmap, new security layers added most weeks, and Cisco's continued partnership, Peco Foods is building a security foundation that's stronger today, ready for tomorrow, and aligned with its mission to be a world-class food provider.