

A woman with long dark hair, wearing a light-colored trench coat, is looking down at a smartphone in her hands. She is standing on a city street at night, with blurred lights from cars and buildings in the background. A shopping bag is hanging from her arm.

Cisco Access Manager for Secure Retail Operations

80%

Of retailers experienced cyberattacks in the past year.

59%

Of retail organizations are adopting network monitoring technologies at higher rates than other industries.

80%

Of all shopping still happens in store.

Key Benefits

1. Protect revenue-critical store operations.

Control network access to POS and payment systems, order and inventory platforms, customer data, loss-prevention tools, and building systems based on user and device context.

2. Apply consistent policy across your retail network.

Extend identity-based access across supported Meraki stores, branches, and distribution sites while reducing location-by-location VLAN and ACL changes.

3. Keep associate access aligned.

Use Microsoft Entra ID context to apply the right network access as seasonal associates join, change roles or locations, and leave.

4. Reduce risk from connected store devices.

Apply appropriate access to shared handhelds, scanners, kiosks, cameras, sensors, facilities systems, and other IoT.

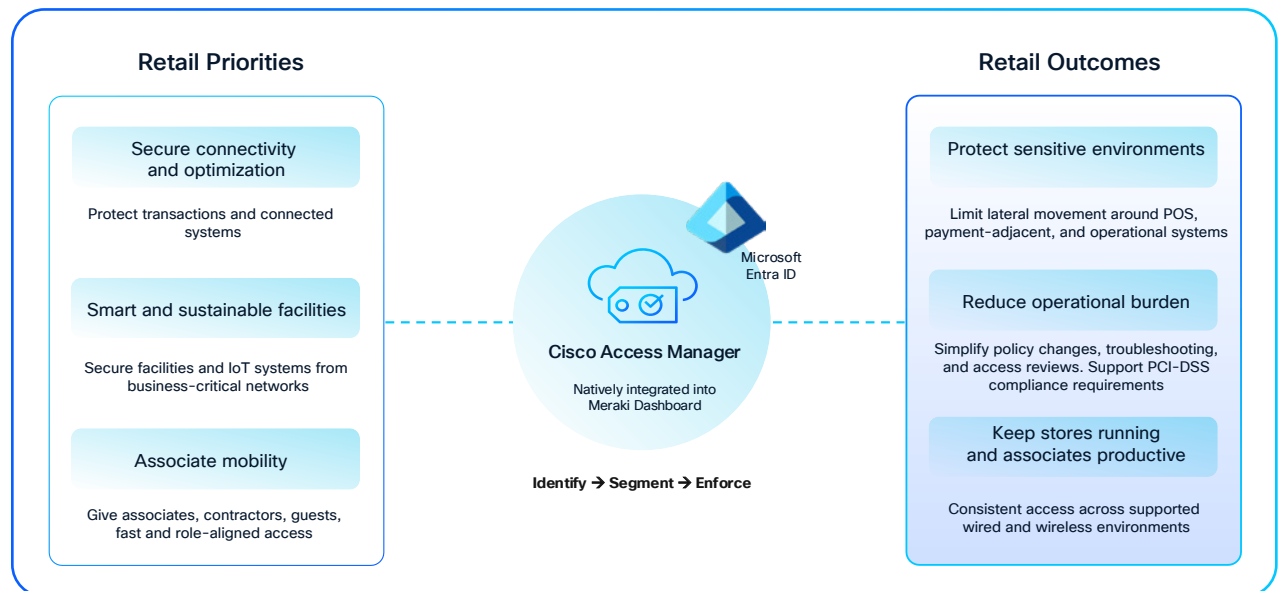
5. Reduce NAC complexity and overhead.

Deliver identity-based access as SaaS in the Meraki Dashboard without separate NAC appliances, external RADIUS servers, or dedicated policy infrastructure.

Protect every store without slowing operations

Retail transactions, fulfillment, associate tasks, and connected experiences depend on systems remaining available and secure. Seasonal hiring, contractor access, staff movement, and growing numbers of POS, cameras, scanners, kiosks, facilities systems, and IoT make access harder to manage. Location-specific rules can drift, creating inconsistent policy and broader-than-intended access to sensitive systems.

Cisco Access Manager makes identity native to supported Meraki wired and wireless networks. Delivered as SaaS in the Meraki Dashboard and powered by Cisco Identity Services Engine, it uses identity, role, device, and network context, including Microsoft Entra ID roles and groups, to determine what each connection can reach. Retail teams can apply consistent policy across locations, reduce lateral movement, support PCI DSS access controls, and keep access aligned as users and devices change.



Make identity part of every connection

Cisco Access Manager helps you:

- Translate associate roles into access. Use Microsoft Entra ID roles and groups as associates join, change roles or locations, and leave.
- Support diverse retail devices. Authenticate corporate, shared, and operational devices with EAP-TLS, EAP-TTLS, identity PSK, and MAC Authentication Bypass.
- Segment by purpose and risk. Use VLANs, group policies, and Security Group Tags where supported to limit reach to sensitive systems.
- Scale consistent policy. Reduce store-by-store VLAN and ACL administration.
- Gain unified visibility. See who and what connects from the Meraki Dashboard.

Unlike traditional appliance-based NAC deployments, Access Manager is delivered through the Meraki Dashboard and uses supported Meraki infrastructure. This reduces the need for separate NAC appliances and external RADIUS infrastructure, helping lean education IT teams deploy and scale access policy with less operational complexity.

Strengthen access across your retail network

See how Cisco Access Manager can protect store operations and customer experiences with consistent identity-based access across supported Meraki networks. Explore the product, request a demo, or start a trial at <https://www.cisco.com/site/us/en/products/security/access-manager/index.html>.

