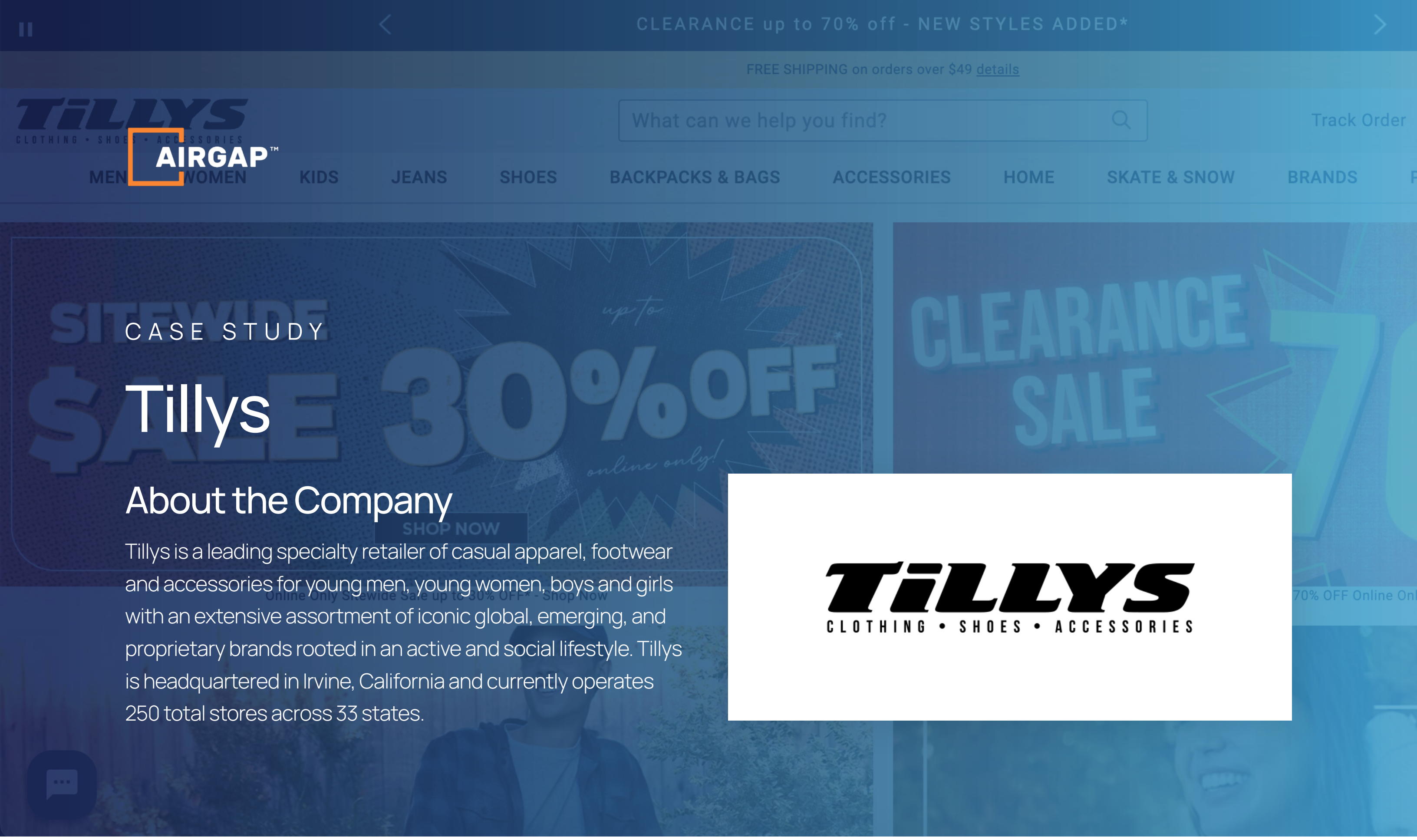


CASE STUDY

Tillys

About the Company

Tillys is a leading specialty retailer of casual apparel, footwear and accessories for young men, young women, boys and girls with an extensive assortment of iconic global, emerging, and proprietary brands rooted in an active and social lifestyle. Tillys is headquartered in Irvine, California and currently operates 250 total stores across 33 states.

Problem Statement

- Increase visibility and control of the internal traffic between user workstations, distribution centers, production servers, and IT systems
- Reduce enterprise risk and attack surface – one infected endpoint could compromise the entire network infrastructure.
- Add autonomous re-authentication MFA-based access to mission-critical assets
- Need for an agentless microsegmentation solution that covers 100% of enterprise endpoints, including security cameras, legacy systems, and headless endpoints
- Need for a rapid ransomware incident response solution
- Limited resources for design, installation, and ongoing policy maintenance

Why Tillys Selected Airgap

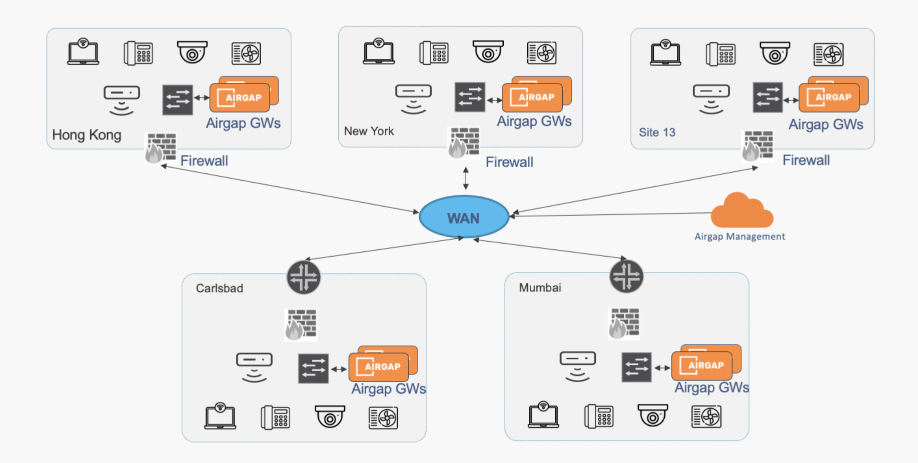
- Visibility and control for the lateral traffic across 100% of its constantly changing endpoint footprint
- Granular segmentation for IT compliance
- Single Sign On (SSO) and Multi-Factor Authentication (MFA) for mission-critical assets across the hybrid workforce and external partner/contractors
- Ease of deployment and policy management through autonomous groups, tag-based policies, and technology integrations (SIEM, EDR, Active Directory, Identity Providers)
- Rapid Ransomware response with granular, policy-driven "Ransomware Kill Switch."

Airgap Onboarding Experience

Full installation, training, and time to value in 4 days. Exceeded customers' expectations.

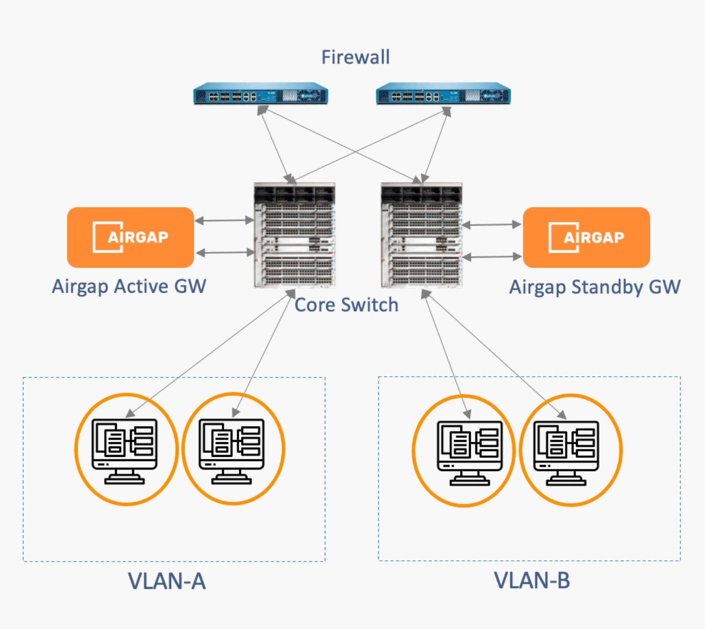
Day 1

- Technical deep dive and deployment design review with Tillys security and network architects



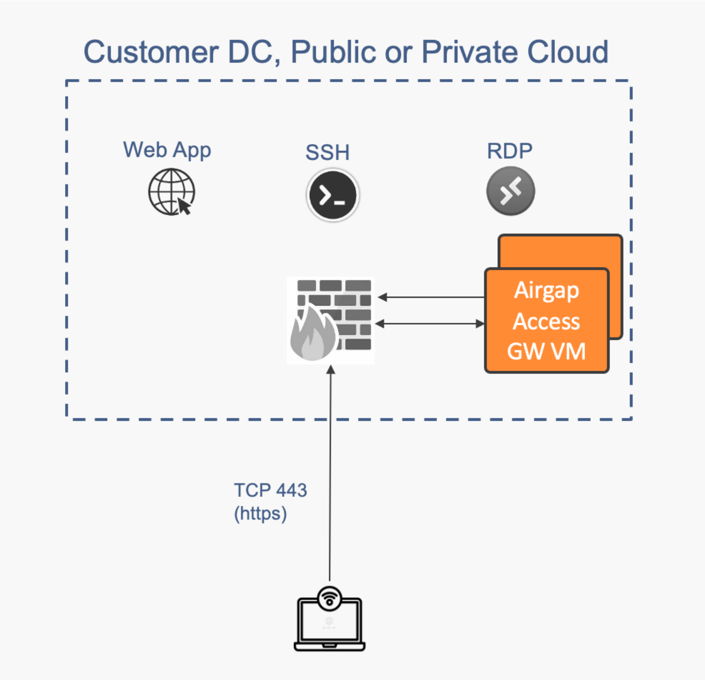
Day 2

- Airgap Gateway Appliance deployment and first VLAN (IT Workstation) onboarded



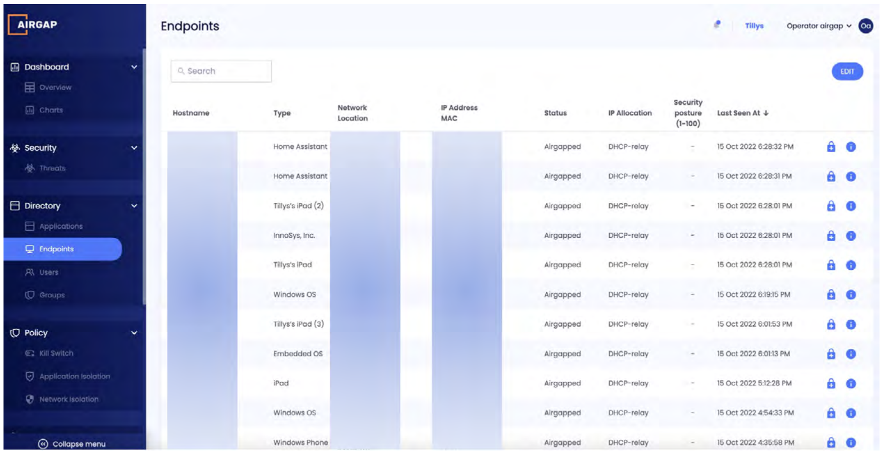
Day 2

- Deployed Airgap Secure Access (ZTNA) for the mission-critical applications



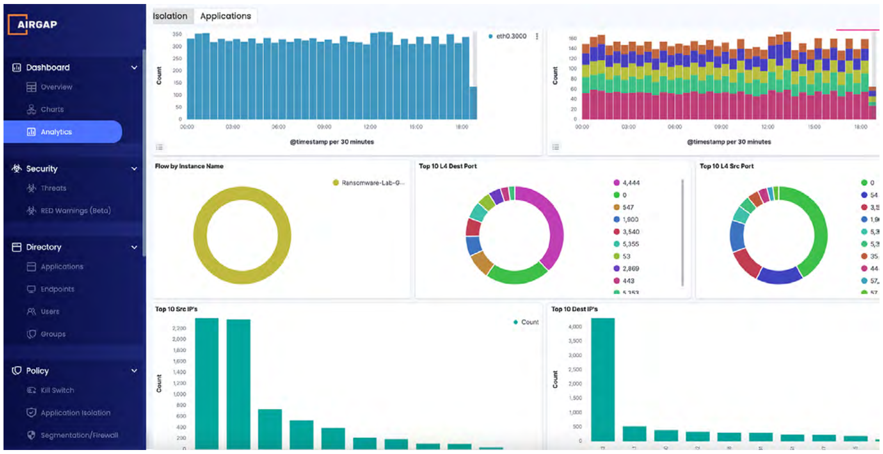
Day 3

- Review visibility and policy controls, onboard entire HQ VLANs (all users in Tillys HQ across multiple buildings)



Endpoints

Hostname	Type	Network Location	IP Address MAC	Status	IP Allocation	Security posture (1-100)	Last Seen At ↓
[redacted]	Home Assistant	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:28:32 PM
[redacted]	Home Assistant	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:28:31 PM
[redacted]	Tillys's iPad (2)	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:28:01 PM
[redacted]	InnoSys, Inc.	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:28:01 PM
[redacted]	Tillys's iPad	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:28:01 PM
[redacted]	Windows OS	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:19:15 PM
[redacted]	Tillys's iPad (3)	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:01:53 PM
[redacted]	Embedded OS	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 6:01:13 PM
[redacted]	iPad	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 5:12:28 PM
[redacted]	Windows OS	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 4:54:33 PM
[redacted]	Windows Phone	[redacted]	[redacted]	Airgapped	DHCP-relay	-	15 Oct 2022 4:35:58 PM



Day 4

- Deployed Airgap Zero Trust Segmentation for the Server VLAN (100+ engineering, test, and production servers)
- Implemented microsegmentation policies with autonomous grouping
- Configured Ransomware Kill-Switch to lock down suspect traffic gracefully to or from any endpoint
- Identified vulnerable flows and quarantined misbehaving endpoints

Conclusion

- Achieved IT compliance and reduced the attack surface in record time
- 100% of corporate endpoints across data centers, Corporate HQs, and retail stores microsegmented and protected from lateral threats
- Implemented ZTNA for hybrid workforce and external partner/contractors
- Configured Ransomware Kill Switch for a rapid incident response without business productivity loss

> “We went from the first meeting, to becoming a customer, to microsegmenting our entire footprint in just under a week. That is unheard of.”
>
> **Guido Solares,**
> **Director, Information Security and Compliance,**
> **Tillys**

About Airgap

The Airgap Unified Zero Trust platform delivers agentless segmentation, ZTNA, and automated incident response for IT, OT, and IoT environments. With Airgap, you can quickly isolate every endpoint, authenticate every transaction, and stop ransomware propagation by locking down traffic to and from suspect endpoints.

Airgap is the industry’s fastest path to true Zero Trust. With Airgap, customers can go from a patchwork of vulnerable legacy devices and applications to a fully segmented Zero Trust network in only a few hours.

Uniquely in the market, the Airgap solution requires no agents, no APIs, and no significant changes to the hardware. We can perfectly isolate what others can’t – like headless OT machines, IoT devices, and legacy applications. And secure remote worker access to campus machines with SSO/MFA.

To learn more about how Airgap can help you quickly extend Zero Trust to any environment, please visit www.airgap.io

AIRGAP™