AIRGAP™

CASE STUDY

Networking Communications Manufacturer Adopts Zero Trust Access to Modernize Remote ITSM Workforce

Seemingly in the blink of an eye, the pandemic changed everything: how we worked and how we managed enterprise workloads. Projects that under "normal" conditions would have required years were completed in mere weeks Business models that had been dependent on 'in-person' operation successfully pivoted to digital delivery. And customers ultimately adapted and found businesses that could satisfy their demands gracefully throughout the outbreak. From the first conversation to finalizing the proof of validation, the Accton IT team rolled out Airgap Secure Asset Access™ (SAA) in just a matter of weeks.

Challenges

- Rapid adoption to sudden work-from-home orders from the Taiwanese government in response to COVID-19
- Need to limit VPN and RDP privileges into internal private applications to those whose jobs required access
- Source a cost-effective zero trust security solution for mission-critical teams located in Taiwan and China.

Solutions

- Deploy Airgap SAA Access gateway to accommodate more than 15 private apps access with Azure AD for advanced SSO MFA. During the POC phase, Airgap can provision Okta SSO MFA for validation without disrupting the user's production environment in a matter of days
- Seamlessly deliver SaaS-like secure access proxy into private applications and reduce duplicate application instances in different locations or cloud regions.
- Record and log in real-time every access session and customize security configurations based on user identity for compliance audits.

Remote IT Service Management (ITSM) became a popular ransomware target during the pandemic

One notable example is the Colonial Pipelines. They were particularly vulnerable because they ear located in highly distributed environments and necessitated the use of remote connectivity tools that are designed for easy access rather than strong security. The traditional VPN and RDP remote access approach grants excessive trust to the networks.

AIRGAP™

Ease of migration from Microsoft Hyper-V to VMware ESXi

Airgap SAA gateway supports leading virtualization hypervisors and cloud platforms so customers can deploy virtual appliances without changing any virtualization migration from Microsoft Hyper-V to VMware vCenter.

No forklift upgrade with existing IT investment preservation

The customer deployed NGFW firewalls to guard IPS/IDS North-South traffic. Airgap Zero Trust Access Gateway works in tandem with existing network security investment without forcing complex configuration changes. The easy-to-use yet powerful design constantly delights IT professionals with its scalability and simplicity.

Flexible and convenient licensing structure

Airgap works with any customer's IT organization to determine the best-licensing structure—per site or per endpoint—on an annual basis. In this case, the customer needed to accommodate mission-critical knowledge workers. Airgap provided the complete onboarding professional services and training in its inclusive package.

Airgap SAA provides VPN-less access, eliminating direct application vulnerability from outside the network. This increases productivity and reduces the potential attack surface by granting "just-in-time" time-based entry only after users pass strong SSO and MFA authentication. The solution innovatively hides legacy and vulnerable ports and protocols such as Windows RDP from adversaries.

The top use cases in this deployment include hardening access via SSH, web, and RDP legacy protocols with OpenID Connect-compatible MFA SSO challenges. SAA's role-based access control provided the critical methodology for mission-critical system administrators and IT teams with granular application roles to meet corporate compliance.

Reducing ITSM access risk with zero trust

The Taiwan-based ODM and OEM manufacturer needed secure, scalable, cost-effective zero trust access for its IT organization to improve workflow efficiency and improve its security posture. "As we considered options, we wanted to shift to a cloud-native network security platform and take a zero-trust approach," said Elvis Jan, Accton Technology's head of cybersecurity. **"Airgap gives us an easy-to-use security management for network and application isolation—by simply installing a virtual appliance without managing additional network hardware. We are connecting through our firewall, proxying our ingress traffic. This means we can connect authorized users directly to managed private applications without placing them on the network with excessive trust."**

Accton

About **Accton Technology Corporation**

Accton Technology is a Taiwanese company operating the electronics industry. It primarily engages in the development and manufacture of networking and communication solutions, as an original equipment manufacturer or original design manufacturer partner. Accton has manufacturing plants in Hsinchu, Taiwan, and Shenzhen, China, employing a workforce of more than 5,200 worldwide.