Airgap Networks

Defending Data, Devices, and Applications

Introduction

Today's mobile workforce, SaaS applications, and increased remote working, exacerbated by the covid-19 pandemic (many workers needed to leverage their unprotected home systems), are among the many drivers in the decentralization of the Enterprise network. Users, data, devices and applications are moving beyond the security of the traditional enterprise network controls. This is driving the need for organizations to upgrade the previously inflexible inside-versus-outside corpo-rate resources access approach. It is imperative that the security implementation must be far more dynamic and user centric.

IT team's goals also include meeting user expectations of an 'in-the-office-like' quality of experience (QoE) from anywhere, any device and at any time. Taking advantage of this increased and changing threat landscape, malicious actors, including Nation-State hackers, are attacking with sophisticated, targeted, widespread and often undetected malware.

In this paper Airgap Networks outlines strategies to complement and harden existing enterprise security postures including Zero Trust Isolation, Policy simplification, the industry's first Ransomware Kill Switch, and implementation of secure access controls for protecting business assets.

Airgap Solutions

Zero Trust Isolation
Ring-fence every device, including IoTs on the network

Ransomware Kill Switch
Instant protection against ransomware propagation

Secure Application Access
Access control and management from any device or location

Policy Simplification
Identity and service aware implementation

Zero Trust Isolation

Airgap's Zero Trust Isolation™ Software-as-a-Service (SaaS) platform can be implemented within minutes without the need for forklift upgrades, agents, or APIs. Airgap complements existing infrastructure and ensure enterprise assets are protected against wide range of cyber threats including ransomware propagation.

> "...zero trust can **reduce the 'blast radius'** of a ransomware attack, yet many organizations continue to keep deferring implementation"[1]
>
> **Gregory Touhill**
>
> *Former Federal Chief Information Security Officer of the United States*

Airgap Zero Agentless Trust Isolation™ platform ring-fences every endpoint (workstations, IoTs, BYODs, TVs, HVAC, bulbs, thermostats etc.,) using network controls. The SaaS-based policy manager provides full visibility and control for every network attached device.

Ransomware Kill Switch

Emergency Stop all lateral traffic movement

Despite a methodical approach and millions invested in security solutions, every security organization must be prepared for an imminent ransomware attack. Under the circumstances, most organizations consider shutting down the entire network in order to stop further ransomware propagation causing business and productivity disruptions. This approach can specially be disruptive for many industries such as healthcare, manufacturing, critical infrastructure etc.

Worry no more...

Airgap's Ransomware Kill Switch™ instantly stops all unauthorized communication inside the enterprise ensuring that there is no more ransomware propagation. The incident response team can now source and mitigate the ransomware, secure in the knowledge that the ransomware will not propagate across the network. This surgical approach ensures that the enterprise business and productivity doesn't come to a scrunching halt. Once the ransomware threat has been thwarted, resuming normal operation is as easy as flicking the switch.

Designed on top of Airgap's Zero Trust Isolation™ platform, the Ransomware Kill Switch is the best defense when under ransomware attack.

[1] *Zero trust: A solution to many cybersecurity problems*

Access Control

Given the increasingly distributed nature of the organizational assets – users, devices, applications, and data – organizations must ensure strict access control tied to centralized user and identity frameworks. That is why Airgap's Zero Trust Isolation™ platform implements a multi-protocol proxy that protects business assets from untrusted access.

Airgap employs modern identity aware Single Sign-On (SSO) and Multi-Factor Authentication (MFA) access control techniques versus the VLAN, zone, and subnet based access controls granted by traditional firewalls. This ensures that only authorized users and devices are granted access to the business assets. More importantly, Airgap's solution is agnostic to underlying ports or protocols used for accessing business assets and ensure protection for all protocols including legacy and vulnerable protocols such as SMB, RDP, etc.

Conclusion

Airgap's Zero Trust Isolation™ Software-as-a-Service platform offers the best defense against cyber-threat propagation. Airgap's patent pending solutions work for any user, any device from any location. Airgap solutions can be installed rapidly without the need for forklift upgrades, agents, or APIs.

To learn more or to schedule a demonstration, **please visit us at https://airgap.io or contact us at info@airgap.io**