Zero Trust Isolation Platform

Data exfiltration, corporate extortion, and ransomware are the biggest security threats for the enterprises

The Cloud-Generation and its need to access data everywhere, on every device, creates more opportunities for attackers to compromise user-endpoints. Further, IoT deployments continue to grow and inherently vulnerable, such devices represent the largest attack surface for the distributed enterprises. Vast amount of false positive threats indicators from a wide variety of tools are overwhelming an already understaffed SecOps teams with "threat fatigue". As a result, the IT organizations are constantly challenged to keep the infrastructure compliant with regulations and industry recommended security standards while remaining agile.

Fail to Plan or Plan to Fail

It is impossible for organizations to restrict movement of bad actors over a shared LAN network that allow free flow of information without granular security controls. The attackers exploit this fundamental flaw by taking control of one of the devices to carry out mass disruption as already witnessed by widespread and ominous WannaCry and Petya Ransomware attacks. With the rise of "Work from Anywhere" culture, this problem is further amplified. The IT organization lacks visibility and control over the network that is being used to access the corporate resources. A bad actor in a public hotspot or a compromised machine at the employee's home can leverage employee's endpoint as a conduit to gain access to the business resources.

"Nearly four decades old enterprise architecture has run its course. We need a fundamental shift to make our enterprise Secure and Cloud ready" - CIO, Fortune 2000

Lateral movement is the most potent attack vector now. Somehow, the industry has forgotten to address it

To defend against relentless pursuit of the attackers, organizations typically deploy network-based malware protection solutions. However, such solutions aren't effective as employees often connect their devices to the unprotected networks outside of the organization. Alternatively, organizations may install end-point protection agents to defend against malware infection. However, such agents often ineffective, cannot be deployed on unmanaged devices. Traditional firewall policies rely on static VLAN, IP, or subnet based assignments. Once admitted to the VLAN, the endpoint is free to access corporate assets including the ability to exploit the application vulnerabilities. This often results in a compromised endpoint breaching the corporate assets. Since there isn't a credible solution available to addresses the most fundamental reasons behind majority of the cyber breaches – a shared network deployment of endpoints and lack of security controls as well as excessive access granted by traditional firewalls , it is no wonder that the cybercrime is on the rise.

Airgap's Zero Trust Isolation

The best way to defend against cyber threats

PROTECT CORPORATE DEVICES

Device to Device Isolation

Endpoint isolation is the best remedy against lateral movement of cyber threats. Leverage agentless zero trust isolation to protect corporate devices including IoTs, managed, and unmanaged endpoints.

PROTECT BUSINESS APPs & DATA

Device to App Isolation

Leverage intent-based application access to protect business Apps & Data. Allow secure access to proprietary & SaaS applications from any WiFi Network – at home, in office, or at public hotspot.

PROTECT REMOTE USERS

Remote User Isolation

Ensure your corporate devices are protected in untrusted public or home WiFi networks. Leverage Airgap's remote device isolation solution to cloak the devices and secure corporate assets.

Zero Trust Isolation Platform

Use Cases

Assured protection against Malware and Ransomware
Modern enterprises are experiencing a rapid explosion of digital footprint with managed and unmanaged devices across the board. Airgap's patent pending agentless Zero Trust Isolation solution protects both the managed endpoints including IoTs that are typically hard to secure. The Zero Trust Isolation ensures that the threat is contained within one device across the organization. Our Zero-False positive threat prevention reduces SecOps team's burden.

Secure application access
Our future most definitely involves employees shuttling back and forth between home and office. IT organizations are already finding it harder to manage multiple infrastructure stacks – remote VPN & campus Infrastructure. Airgap consolidates remote and local access with Zero Trust Secure Access for a simplified and uniform infrastructure that is delivered as a service. The intent based dynamic access controls vastly reduce the attack surface thereby preventing costly data breaches.

Remote employee security
Employees are routinely accessing business assets from home or public hotspots. These are inherently insecure networks and the employee laptops are subject to cyber threats from other devices on such networks. A bad actor in such networks can leverage employee laptop as a conduit to infect or steal corporate assets. Airgap's Zero Trust Isolation solution cloaks the corporate laptop and prevents any access from compromised devices thereby protecting corporate assets regardless of their location.

Simplified & "Ready for Business" enterprise campus
Over three decades old, the traditional enterprise blueprint is now outdated. The new world order demands cloud delivered solutions. By centralizing the campus infrastructure deployment in the Edge Cloud, Airgap offers a modern SaaS like infrastructure solution on subscription basis.

About Airgap

The world order has changed overnight. The IT organization is under more pressure and scrutiny than ever before. In addition to ensuring security, there is a strong argument in favor of modernizing enterprise infrastructure. Trusted by leading managed service providers, Airgap's patent pending enterprise grade Zero Trust Isolation platform addresses some of the fundamental security and networking challenges faced by the IT organizations. We'd love to demonstrate our solution and walk you through Airgap's core capabilities, the roadmap, and the vision. To learn more about our platform or to schedule a demo, please feel free to contact us at info@airgapnetworks.com.