AIRGAP

THE BEST DEFENSE AGAINST RANSOMWARE PROPAGATION

It is likely that you have one or more ransomware infected endpoints, unpatched application, and insecure legacy protocols operational inside the organization. Some of these systems are possibly available for rent to the highest bidder on the dark-web. If you aren't prepared for this reality, then you may be condoning imminent threat to your organization. Ransomware is the most devastating cyber threat to hit corporations in 2020. Companies' information, assets, and reputation are at risk. Airgap's Zero Trust Isolation solution provides a modern approach to quickly detect, deter, and isolate this menacing threat.

Fundamental flaws in current architecture

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

Bad actors penetrate the enterprise perimeter through many tactics and techniques including phishing, hardware exploits, removable media (USB) etc. Once inside, it is near impossible for organizations to restrict lateral movement of bad actors over a shared VLAN network architecture.

Also, the traditional firewall & VPN policies rely on static VLAN, IP, or subnet-based access controls. Therefore, once the bad actors are inside your network, they can easily exploit application vulnerabilities through the granted network access. And, organizations routinely operate legacy and insecure protocols. Bad actors leverage compromised endpoints to exploit such protocols and cripple your organization.

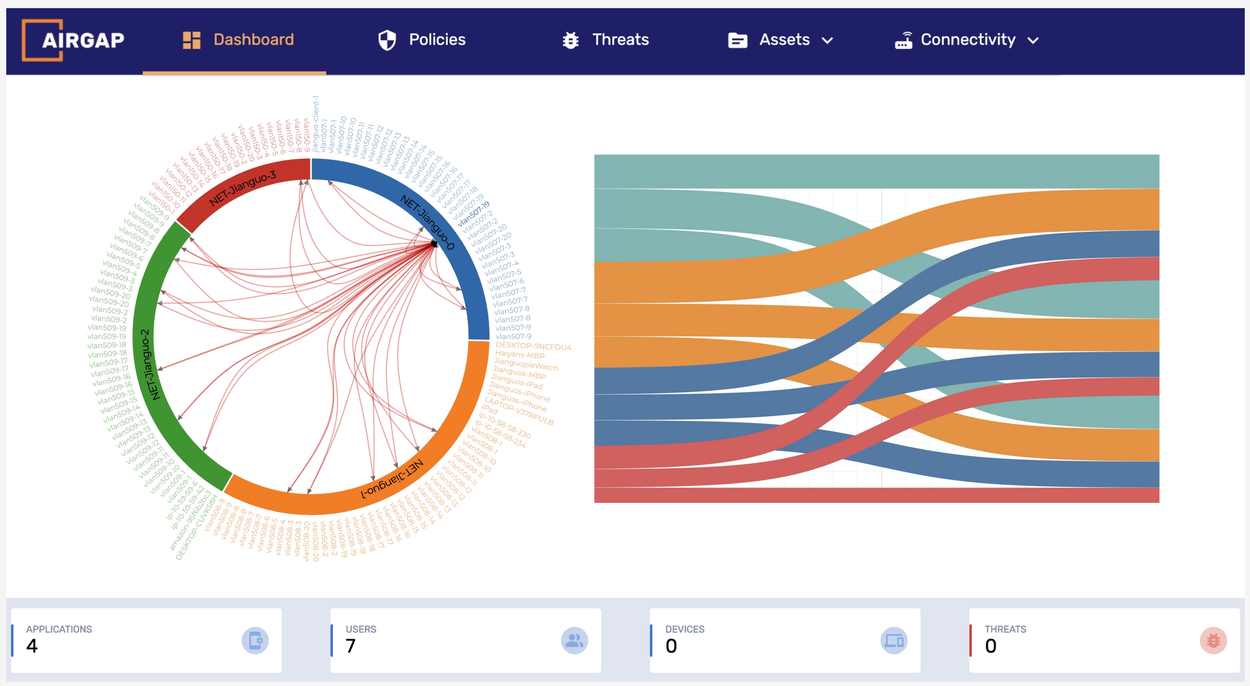
Have you thought about why your bank doesn't give you network level access to their application? Ever wondered why your IT must offer network access to all the business applications?

It shouldn't come as a surprise that 51% of the organizations were a victim of Ransomware attack in the last 12 months.

Despite spending millions on security infrastructure, enterprises expose fundamental flaws behind a majority of the cyber breaches – a shared network deployment; excessive access granted by traditional firewalls/ VPNs; and legacy protocols over unpatched systems.

AIRGAP

Therefore, we built an “Zero Trust Isolation Platform” that protects your organization even if your endpoints are breached, even if you have vulnerable and unpatched applications, and even if you are operating legacy and insecure protocols. That’s our way of assuring cyber defense for the enterprises.



THE BEST DEFENSE AGAINST RANSOMWARE PROPAGATION

Zero Trust Isolation

Don’t let one infected device bring down the enterprise

- Eliminate lateral threat propagation and defend against lateral movement of ransomware
- Continue to operate shared VLAN infrastructure without the risks

Prevent ransomware from propagating to your apps

- Eliminate network level access to business apps and prevent ransomware propagation
- For additional security, seamlessly enable MFA across the enterprise

Safeguard against legacy protocol vulnerabilities

- Auto-profile legacy protocols and permit only authorized usage
- Deploy state of the art AI/ML tools to detect and prevent known and unknown protocol exploits

UP AND RUNNING IN MINUTES, NOT MONTHS

No agents * No APIs * No design changes * No forklift upgrades * Easy Migration
Migrate one device, one network, or one application at a time

About Airgap Networks Inc.

Airgap Networks’ Agentless Zero Trust Isolation Platform offers the best defense against Ransomware propagation. The patent pending solution works for any user and any device accessing business assets from any location. Trusted by leading managed service providers & enterprises, Airgap addresses some of the fundamental security challenges faced by the IT organizations. To learn more or to schedule a demo, please feel free to visit us at https// airgap.io or contact us at info@airgap.io