AIRGAP

Platform Capabilities Map

airgap.io

This document is intended to show where Airgap Networks platform capabilities map to requirements detailed in NIST 800.172. From the standard:

"800.172 is a supplement to NIST Special Publication 800-171 [SP 800-171]. It contains recommendations for enhanced security requirements to provide additional protection for Controlled Unclassified Information (CUI) in nonfederal systems and organizations when such information is associated with critical programs or high value assets. The enhanced security requirements are designed to respond to the advanced persistent threat (APT) and supplement the basic and derived security requirements in [SP 800-171]. While the security requirements in[SP 800-171] focus primarily on confidentiality protection, the enhanced security requirements in this publication address confidentiality, integrity, and availability protection. The enhanced security requirements are implemented in addition to the basic and derived requirements since those requirements are not designed to address the APT. The enhanced security requirements apply to those components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components."

Airgap Networks solution addresses the following requirements of the 800.172 document:

3.1.1e - Employ dual authorization to execute critical or sensitive system and organizational operations.

Airgap Network's application protection gateway provides a mechanism to introduce additional authentication challenges through single sign on (SSO) and multi-factor authentication (MFA). Prevent ransomware and APT from leveraging harvested credentials to spread from client networks to datacenter application enclaves. This gateway can be tied into existing authentication flows involving Oauth providers such as Okta or AzureAD.

3.1.2e - Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.

Airgap Network's zero trust isolation solution eliminates unauthorized communication between devices, as well as between devices and applications, unless permitted per policy.

3.1.3e - Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.

Airgap Networks policy-based isolation controls information flow both inter- and intra- VLAN without the need to deploy agents, employ internal firewalls, or reconfigure ACLs on routers/switches.

3.1.4e - Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations.

Airgap Network's solution enables responders to detect misconfigured or unauthorized system components. Airgap solution also allows one-click "quarantine" of misconfigured or infected endpoints to facilitate patching, reconfiguration, or other mitigation.

3.1.5e - Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.

Airgap Network's application protection gateway provides a mechanism to introduce additional authentication challenges through single sign on (SSO) and multi-factor authentication (MFA). Thus, only authorized (via policy control mechanism) and authenticated (via SSO/MFA) system can connect to organizationation systems. All unauthorized connections are rejected.

3.13.4e - Employ [Selection: (one or more): [Assignment: organization-defined physical isolationtechniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.

Airgap isolation gateway is specifically designed to logical separate (hence the name Airgap) devices/ systems from each other using a network of "1" design – that logically isolates devices/systems from each other. Airgap Networks isolation gateway is uniquely positioned to give responders granular control of network communication between systems - single device, multiple nodes, or entire portions of the network - in order to combat ransomware, APT, or advanced attackers that manage to breach perimeter defenses. This is a key and uniquely differentiating value proposition of the Airgap solution – To our knowledge, no other vendor offers a product that can logically isolate devices/systems on the network.