AIRGAP™

SOLUTION BRIEF

Real-Time Ransomware Detection & Containment

Airgap is the first line of defense against lateral propagation of ransomware attacks within OT and IT environments.

In recent years, ransomware-as-a-service attacks have increased in frequency and sophistication making it harder for incidence response teams to detect and respond to them. Attacks such as Conti and Lockbit ransomware have moved beyond traditional attack techniques to become increasingly professional and streamlined in tactics, techniques, and procedures (TTPs).

Traditionally, early detection of attacks and threat vectors has primarily been managed by anti-malware and antivirus software deployed across almost all systems from enterprise servers to employee endpoints. However, the growing number of successful ransomware attacks has proven that relying solely on existing endpoint protection tools is not sufficient to protect organizations.

AIRGAP™

Introducing Airgap Ransomware Early Detection™

What RED™ Is?

Airgap Ransomware Early Detection (or RED™) is an extension of the Airgap Networks' Zero Trust Isolation™ platform, the industry's first agentless zero-trust segmentation that stops ransomware before it can laterally propagate within the network. RED™™ delivers real-time alerts and visibility during the attack kill chain progression and in conjunction with the Airgap Ransomware Kill Switch can selectively quarantine endpoints and lock down access to mission critical applications to prevent further compromise.

How RED™ Works?

Airgap RED™ can either be deployed on a SPAN or mirror port on network switch/routers or can alternatively be deployed inline as part of the Airgap appliance, so that it can observe all network communication between endpoints and business applications.

RED™ monitors all network communications between endpoints and devices and baselines network behavior. When a potential ransomware attack such as EternalBlue, WannaCry or Conti is triggered within the network, Airgap RED™ detects presence of this attack using advanced Behavioral Detection/Machine Learning models and immediately raises a warning notification. The notification includes an anomaly score which indicates the severity of the threat detected and includes the IOC details of the attack.

Challenges

- Experts estimate a ransomware attack will occur every 11 seconds by the end 2022, costing the world's businesses and governments more than $20 billion yearly. That's nearly four times as many attacks that take place today (currently, an attack is launched every 40 seconds, according to the IBM Security Survey 2022).
- Under new law, certain businesses that are designated as "covered entities" and considered "critical infrastructure" will now be required to report cyber incidents to the U.S. Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours and disclose ransomware payments within 24 hours.
- Increasing ransomware attacks require security leaders to look beyond anti-phishing, anti-virus or endpoint solutions and response strategies to focus more on preemptive prevention and detection.

Solution

- Since most ransomware attacks start with an initial compromise or first victim using phishing or other techniques, followed by privilege escalation and lateral propagation, Airgap's early detection technology based on identifying malicious and anomalous behavioral patterns stops ransomware before they reach end users and helps prevent your data from being locked down or deleted.
- Secure your enterprise perimeter with zero-trust based Ransomware Early Detection™ and Ransomware Kill Switch™ for fast incident response and network segmentation and isolation of compromised devices in real time
- Streamline post-incident SOC/SOAR responses to quickly stop the spread of ransomware already within the network and reduce the blast radius in the event of a possible breach.

AIRGAP™

Depending upon the severity of this attack, Airgap RED™ can be configured to integrate with the Airgap Ransomware Kill Switch to quarantine endpoints, enforce stricter user credential verification (SSO/MFA) or deny access to sensitive business applications.

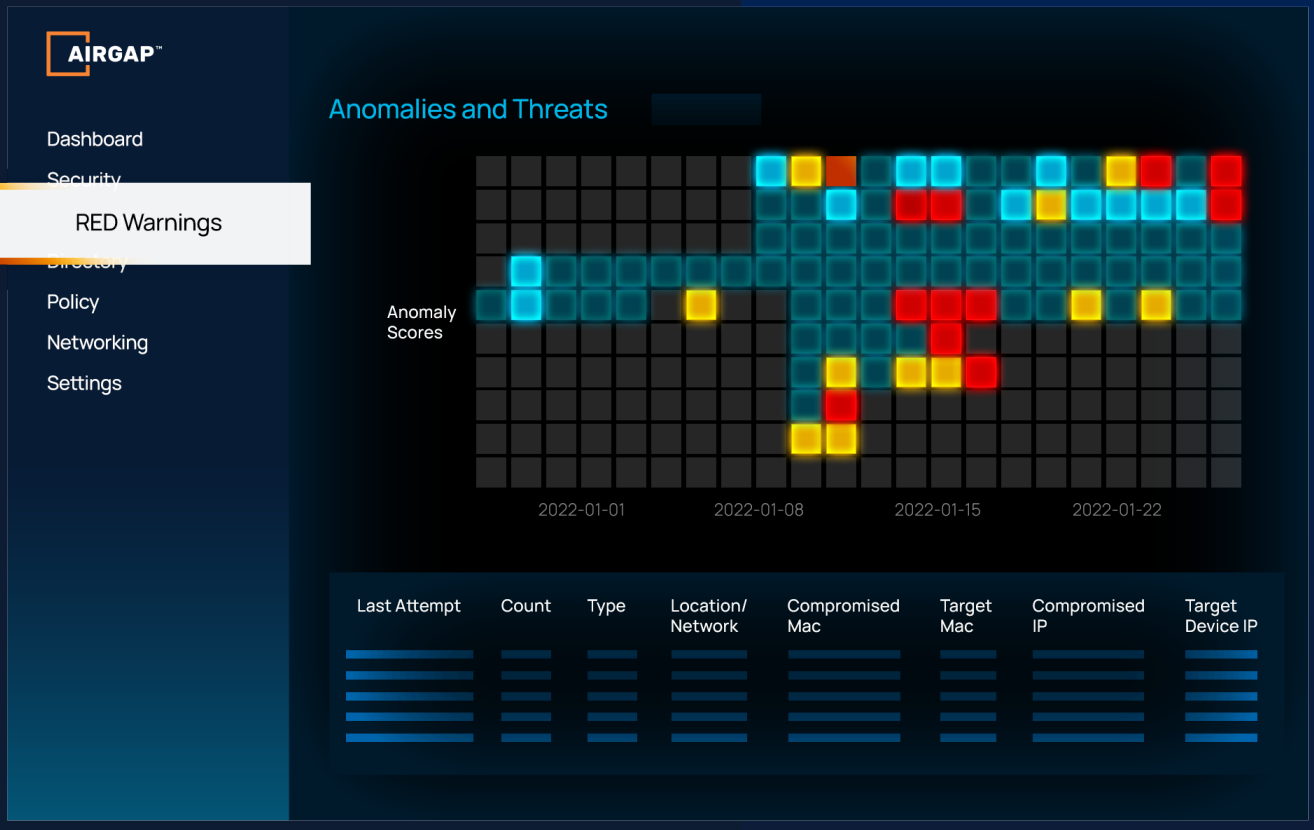
Which Threats RED™ Identifies?

Leveraging technologies such as Deep Packet Inspection, Machine Learning/AI, and Deep Learning Neural Networks, RED™ baselines network activity and compares endpoint activity, network traffic flow patterns, and other protocol actions associated with known attack patterns that have been shown to presage ransomware attacks. This "rule-less" method of identifying anomalous activities associated with ransomware attacks is very effective in detecting ransomware activities such as file encryption and lateral movement. RED™'s ML/AI architecture helps it identify new threat patterns and anomalous behavior and assist security operators in taking appropriate actions.

RED Benefits

RED™ intelligently routes traffic and identifies trusted networks to eliminate congestion, simplify monitoring, and reduce the risks associated with third-party access. Enhanced visibility, customizations, and silent deployment enables more efficient use of IT and security teams' resources while allowing holistic user activity and device posture monitoring. When potential threats are detected, Airgap RED:

- Enhanced visibility optimizes monitoring of user activity and device postures
- Customization enables granularly defined policies for individual devices
- Silent deployment makes IT and security teams more efficient



AIRGAP™

End-to-End Protection Against Ransomware Attacks

Airgap Ransomware Early Detection™ Preemptive and Proactive	**Airgap Ransomware Kill Switch™** Real Time Lateral Propagation Controls
Detect and Prevent	**Isolate and Respond**
○ Continuous threat behavior analytics and anomaly detection for early detection of ransomware. ○ Advanced Machine Learning behavioral and anomaly detection detects even low-volume targeted ransomware. ○ Rapid identification and blocking of command and control (C&C) traffic prevents ransomware from prior infections from spreading	○ Works in lockstep when suspicious IOC activities are detected to provide instantaneous enforcement with tiered DEFCON security controls over lateral (East-West) communications ○ Containment and "air-gapping" of network movement down to device-build and protocol level ○ Instant deployment of "better safe than sorry" zero trust MFA SSO when compromised ○ 24/7 autonomous sentry against entire network, inter-VLAN and intra-VLAN behaviors

Summary

Using Machine Learning and Behavioral Anomaly detection, RED™ continuously updates its predictive analytics and understanding of anomalies that can identify malicious access patterns that can happen within the network.

RED™ combines various Airgap security technologies, deep packet inspection and anomaly detection to identify and map detected threats with the MITRE ATT&CK frameworks such as:

- SMB Protocol Vulnerability Exploits
- Ransomware File Encryption
- Malicious and Anomalous access patterns
- Deviations from baseline behaviors

RED™ intelligently routes traffic and identifies trusted networks to eliminate congestion

About Airgap Networks

Based in Santa Clara, Calif., Airgap Networks develops and mobilizes zero-trust isolation platforms that deter and reduce ransomware and malware's "blast radius" by isolating platforms, databases and enterprise software within agentless ringfenced networks and multi-factor authentication-required access points. For a demo on Airgap Ransomware Early Detection, please email **red@airgap.io**

AIRGAP™

airgap.io