SOLUTION BRIEF

Ransomware Kill Switch from Airgap Networks

Securing and protecting your business with "1-click"

Ransomware leveraged by malicious actors, foreign and domestic, attacks organization networks scrambling all files. Once the network is breached and under the control of the malicious actors, the payment of ransoms for a decryption key to release is demanded. Repeated successful extortions of sizeable ransoms from organizations, across all industries, is driving the increase in ransomware attacks.

Airgap's Ransomware Kill Switch™ is built on top of our patent-pending Zero Trust Isolation platform to contain and reduce the blast radius of any malicious attacks with a "1-click" software-based switch to instantly halt ransomware propagation.

CHALLENGES	SOLUTION
Existing NGFW and EDR are unable to fully protect networks from ransomware attacks	Instantly mitigate ransomware propagation with the Ransomware Kill Switch
Take hours or days to respond to ransomware breach	Instant propagation protection confines threat
New distributed ransomware variants and Ransomware-as-a-Service (RaaS) make defending networks even more challenging	Multi-tiered network access control based on attack severity
Any ransom payments can now be illegal and will be scrutinized by the US department of treasury	Limited exposure eliminates the need for ransomware payment
Current response methods interrupt business continuity and employee productivity	Continue and maintain business operations. Limit the disruption while addressing ransomware threat.

Introducing Airgap Ransomware Kill Switch

Responding to ransomware incidence is a big challenge for average SecOps organization. Often, the SecOps teams try to isolate infected devices - only to realize that there is no easy way to identify all of the infected machines. Alternatively, the SecOps organization often resort to isolating the entire network segment or impacting business continuity. Unfortunately, there are no easy buttons when comes to ransomware incidence response - not until now.

Designed on top of Zero Trust Isolation™ Software-as-a-Service (SaaS) platform, Airgap's Ransomware Kill Switch™ mitigates the propagation of ransomware on a network. As soon as malware is detected, "1-Click" instantly stops all lateral traffic, isolating and containing any ransomware to infected devices.

Additionally, Airgap offers complete control of the Ransomware Kill Switch via APIs so that the IT organization can leverage existing tools such as SIEM, SOAR, and EDRs for rapid ransomware response.

Mitigate Attacks Instantly on Your Command

Airgap's patent pending solution is the industry's only solution that instantly locks down the entire network with a "1-click". Augmenting existing security tools, Airgap's Ransomware Kill Switch™ can be deployed on a network in minutes without any agents, forklift upgrades, or design changes.

When activated, Ransomware Kill Switch halts lateral network level communication within the protected VLANs thereby instantly stopping lateral ransomware propagation. Additionally, the Ransomware Kill Switch can instantly protect organization's crown jewels such as backup, ERP, or domain controller with a click of a button.

As soon as malware is detected, "1-Click" instantly stops all lateral traffic, isolating and containing any ransomware to infected devices.

Users may notice some side effects e.g. printing and videoconferencing will stop working temporarily. Additionally, there will be no access to backup systems, as endpoints will be not be able to communicate with storage systems such as Windows File Share (WFS). Overall the user impact is negligible, while the incident response team gets to work and investigates, secure in the knowledge that the infected device or devices are totally isolated. Once the Ransomware attack is sourced and eliminated the "1-click" can be used in reverse to instantly normalize the network.

When ransomware is discovered on the network Ransomware Kill Switch™ can be switched to varying degrees of ransomware attack severity using color coded network access and protocol control policies to stop ransomware spread at source with role-based access control (RBAC) command.

RANSOMWARE RISK LEVEL

ALL SYSTEMS ARE NORMAL

Protect the network and enforce system policies

MODERATE RISK

Protect the network and enforce Yellow policies

HIGH RISK

Protect the network and enforce Orange policies

CRITICAL RISK

Protect the network and enforce Red policies

More Information about Airgap

Airgap's Ransomware Kill Switch offers the best defense against cyber-threat propagation with a patent pending solution that can be installed in minutes without any forklift upgrades. Trusted by leading managed service providers and enterprises, Airgap addresses some of the fundamental security challenges faced by the IT organizations. To learn more or to schedule a demo, please visit us at https://airgap.io or contact us at info@airgap.io.