Ransomware Kill Switch

SOLUTION BRIEF

Introduction: A Ransomware Epidemic

The state of ransomware has reached epidemic proportions. Repeated successful extortions of sizable ransoms from organizations across all industries is driving a continued increase in attacks. Over half of global organizations are under attack, with average ransom demands in the hundreds of thousands of dollars. And many government agencies are now introducing legislation demanding further details including making such ransom payments illegal.

Once the perimeter is breached, the ransomware often propagates rapidly causing a greater deal of cyber damage to the organization. Delayed response to ransomware incidents often increases total business impacts in terms of dollars and reputation. Therefore, once impacted, the best defense by the IT organization is to shorten incident response time.

Ransomware attacks corporate networks and scrambles (encrypts) files throughout the organization. Additionally, the targeted attacks also steal corporate sensitive information such as employee or customer PII etc. Subsequently, a ransom demand is issued against the release of the decryption key or deletion of the stolen data. Often, the impacted organizations are left with no choice but to meet the ransom demands.

Due to the complexity of firewall configurations, NAC segmentation, or group policies, Security operations (SecOps) teams are strained to prepare for--and respond to--these attacks. They often cannot determine the actual exposure, especially as the attacks are often still spreading while they respond. The organization is often left with no choice but to isolate entire network segments, further impacting business continuity.

To make matters worse, the variety of threats is also increasing, with new distributed variants that even include "Ransomware as a Service." Unfortunately, there are no easy buttons when it comes to ransomware incident response--until now.

About the Ransomware Kill Switch

In response to the ransomware epidemic and other insufficiencies in network security, Airgap has developed patent-pending technologies to address the ransomware epidemic.

One of these is a unique Zero Trust Isolation™ solution for both endpoints and entire networks. With the industry's only agentless zero trust solution, Airgap protects both managed and unmanaged devices from malware attacks.

CHALLENGE

Over half of global organizations are attacked by ransomware, with average ransoms in the hundreds of thousands of dollars. Existing firewall and Endpoint Detection and Response (EDR) systems cannot protect networks from these attacks. Responses can take hours or days to mitigate and neutralize attacks. And routine introduction of new zero day ransomware variants make this even more challenging.

SOLUTION

Businesses can set defense readiness conditions based on attack severity, and instantly mitigate ransomware propagation with the Ransomware Kill Switch. Airgap's agentless solution protects all business assets such as managed and unmanaged devices as well as business applications and data. Infection exposure is tightly limited, often to a single endpoint, thus avoiding the ransomware payments or becoming the headline or getting tangled into the compliance web.

KEY BENEFITS

- Only solution to instantly stop ransomware in its tracks
- Defense readiness levels ensure the right response to attacks
- The "blast radius" of attacks is tightly limited
- Agentless solution is deployed in minutes
- Both managed and unmanaged devices are protected
- Corporate applications and other "crown jewels" are protected
- The need for payments (which are often illegal) is eliminated

Building upon Zero Trust Isolation, Airgap then developed the Ransomware Kill Switch™ to contain and mitigate lateral ransomware movement. Augmenting existing security tools, these agentless solutions can be deployed in minutes without any forklift updates or design changes.

The Ransomware Kill Switch blocks all unnecessary network communications to or from any endpoint. This dramatically reduces the threat risk in all networks, from home or remote workspaces to corporate campuses.

The Ransomware Kill Switch is the only solution that instantly blocks lateral data paths through the network with a single click, called the "1-click."

Instant Mitigation with a Secure Response

Ransomware Kill Switch sharply reduces the "blast radius" of any attack, usually to a single endpoint. When activated, the Ransomware Kill Switch surgically halts network level communication between workstations and applications.

While the incident response team gets to work and investigates, user impact is negligible. Secure in the knowledge that any infected devices are totally isolated, the response team can methodically and calmly assess and repair any damage.

Protecting Corporate "Crown Jewels"

Additionally, the Ransomware Kill Switch instantly protects an organization's "crown jewels" such as backup, ERP, or domain controllers. The immediate action is to immediately disconnect and/or isolate systems when an infection is discovered.

Following this, vetted or critical systems can incrementally be brought back online. For instance, printing and videoconferencing support can be quickly restarted, followed by backup and storage systems. Finally, once the attack is fully eliminated, the "1-click" can be used in reverse to instantly normalize the network.

Planning and Pre-incident Preparation

A key part of shortening incident response comes with proper planning. Security teams can preset the Ransomware Kill Switch according to risk levels that are appropriate to their organization. Using network access and protocol control policies, the Ransomware Kill Switch™ can be set to varying degrees (defense readiness alerts) of ransomware attack severity to stop ransomware spread at the source.

Automation and Integration

Airgap offers complete control of the Ransomware Kill Switch via APIs. Using these programmable interfaces, IT organizations can automatically enable existing security orchestration tools such as Security Information and Event Management (SIEM), Security Orchestration and Response (SOAR), or EDR/XDR solutions to bolster ransomware responses at remote endpoints.

Conclusion

Ransomware threats are growing rapidly. Airgap's Ransomware Kill Switch offers the industry's most potent ransomware defense solution against cyber-threat propagation.

While there are many security companies trying to prevent ransomware from entering networks, Airgap's Zero Trust Isolation protects your organization even if your perimeter is breached or if you have unpatched vulnerable servers inside your data center. Airgap's Ransomware Kill Switch is built upon this zero-trust paradigm. Additionally, the patent-pending solution can be installed in minutes without any forklift upgrades.

About Airgap

Airgap addresses the most fundamental security challenges faced by IT organizations. It's Zero Trust Isolation solutions are trusted by leading managed service providers and enterprises. Based out of Silicon Valley, California, the venture backed company is founded by highly experienced cybersecurity experts.

To learn more or to schedule a demo, please visit us at https://airgap.io or contact us at info@airgap.io.