Ransomware Kill Switch for the Manufacturing Industry

SOLUTION BRIEF

Introduction

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.

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. Corporations are often left with no choice but to isolate entire network segments, further impacting business continuity.

Airgap provides an Anti-Ransomware Technology™ that stops the spread of ransomware in your environment. This agentless solution provides zero-trust isolation and identity-based segmentation. It can be implemented with no change to your existing network design or topology, creating microsegmentation for any devices protected by Airgap.

The technology supports the industry's first Ransomware Kill Switch™, providing an automated solution to lock down your most critical network assets at the first indication of an attack.

Securing the Manufacturing Industry

To remain competitive and gain operational advantages, today's modern manufacturers depend more heavily than ever before on automation, connectivity, and digital communications. The transformation to Industry 4.0 forces companies to combine next-generation technologies like IoT devices and Artificial Intelligence with existing/legacy OT solutions. This paradigm creates an environment that is difficult to protect and becomes a prime target for cyber threats like ransomware.

The creation of today's industrial control networks are a result of years or decades of devices and deployments. Cyber security was not a focus for most of these systems and is often overlooked or lacking completely.

CHALLENGE

Ransomware and data extortion attacks are the fastest growing threats that organizations face today. Over half of global organizations are attacked, with average ransoms tripling in the last year to just under $500,000 in this multibillion-dollar underground business.

Once you are compromised, existing firewall and Endpoint Detection and Response (EDR) systems cannot protect your network from the spread of ransomware. It can take days or weeks to mitigate and recover from attacks.

SOLUTION

Businesses can set defense readiness policies based on attack severity, and instantly stop ransomware propagation with the Ransomware Kill Switch. Airgap's Anti-Ransomware Technology is agentless and protects both managed and unmanaged devices.

Infection exposure is tightly limited—often to a single endpoint—and the need for ransomware payments is eliminated.

KEY BENEFITS

- Agentless solution is deployed in minutes
- 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
- 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

As cyber threats and ransomware are increasing at an epidemic rate, the manufacturing sector is faced with many challenges protecting their IoT industrial networks. The most common issues are:

Visibility: Industrial network device inventory is in constant flux. Manufacturers cannot secure communications between devices if all the devices are not identified and are constantly changing.

Control: Given this complicated and ever-changing environment, controlling which devices can and should communicate makes enforcing even basic security practices a monumental task.

Productivity versus Security: As IT and OT teams are forced to work together to implement, upgrade and secure these new industrial networks, balancing the need for security without impacting production is a difficult balance.

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 modern security needs.

One of these is a unique Anti-Ransomware Technology that provides zero-trust isolation for individual endpoints or entire networks. With the industry's only agentless zero trust solution, Airgap protects both managed and unmanaged devices from malware attacks.

Building upon this platform, Airgap developed the Ransomware Kill Switch for an instant response to ransomware attacks. Ransomware Kill Switch contains and mitigates lateral ransomware movement. Augmenting existing security tools, these agentless solutions can be deployed in minutes without any forklift upgrades 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. Infected devices are ring-fenced so that threats cannot be propagated beyond isolated devices.

The Ransomware Kill Switch allows customers to customize security policy for lateral communication as well as private and SaaS applications. Policies can be set for several categories. In the example shown, the categories are Yellow for lateral threat propagation, Orange for protecting crown jewels such as backup systems, and Red for protecting key applications (Figure 1).

Figure 1: The Ransomware Kill Switch

The Ransomware Kill Switch instantly stops ransomware propagation without disrupting business functions.

The Ransomware Kill Switch sharply reduces the "blast radius" of any attack, usually to a single endpoint. When activated, the Ransomware Kill Switch halts lateral network level communication within protected VLANs.

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.

Visibility and Control

What you can't see, you can't protect. Most IT organizations are blind to lateral traffic since it is not feasible to capture traffic from all access switches. Airgap's unique solution provides complete visibility into all transactions in and out of every protected endpoint, allowing for real-time business/security policy creation and enforcement.

Thus, in addition to providing the necessary security, Airgap helps IT organizations meet compliance requirements across many industries. This is all achieved without making any change to the existing infrastructure, networks, or IP addresses.

Protecting Corporate "Crown Jewels"

When protecting an organization's "crown jewels" such as backup, ERP, or domain controllers, the immediate action is to immediately quarantine 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.

Automation and Integration

A flexible and open solution, Ransomware Kill Switch integrates easily with existing security systems. 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.

Conclusion

While there are many security companies trying to prevent ransomware from entering networks, only Airgap's Anti-Ransomware Technology 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 offers the industry's most potent ransomware defense solution against cyber-threat propagation with a patent-pending solution that can be installed in minutes without any forklift upgrades.

About Airgap

Airgap addresses the most fundamental security challenges faced by IT organizations. Our Anti-Ransomware Technology—including the industry's only Ransomware Kill Switch—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.