Ransomware Kill Switch™ for Endpoints

SOLUTION BRIEF

The Challenge

Ransomware Disruption

Ransomware targets organizations by exploiting the implicit trust that endpoints possess within the enterprise. The ease by which ransomware can enter and spread across an enterprise is exposing how risky employee behavior can act as the weakest link within organizations. Employees clicking on suspicious phishing email or browsing questionable websites can usher ransomware into an enterprise in a matter of seconds. Once in, Ransomware can spread quickly and harshly, inflicting pain by locking up critical resources that have only one recourse – ransomware payment.

In order to properly combat these types of attacks, organizations need to build Zero Trust around each endpoint deployed in their enterprises. Zero Trust security provides the best defence against ransomware by providing a no-trust security architecture that denies ransomware an opportunity to thrive and spread throughout the enterprise. Endpoints can continue to properly access corporate resources but with an additional layer of security that isolates the risky actions of a single employee on an endpoint from endangering the entire business operations of an organization.

The Solution

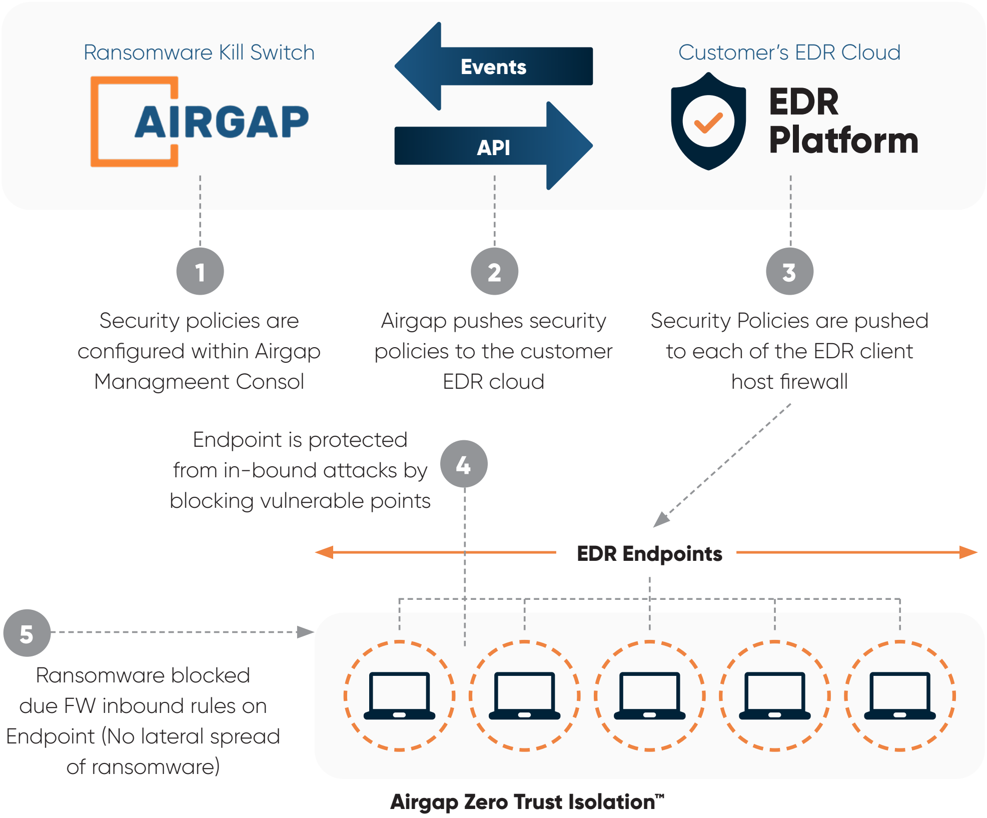
Superior Ransomware Protection

Airgap's Ransomware Kill Switch™ for Endpoints partners with the leading EDR vendors to deliver an architected and integral solution that is built around each endpoint that ensures superior security protection from ransomware. Each endpoint has an additional layer of ransomware protection that travels with the endpoint, regardless of location and employee behavior. The ease by which ransomware can enter an enterprise and laterally spread is removed, making cybercriminals work that much harder to continue to launch sophisticated campaigns that seek to infiltrate enterprises, disrupt business operations and encrypt sensitive data. Security is built around the required business operations that are performed on each endpoint, ensuring that employees can continue to work without ever noticing the enhanced level of security protection that not only protects their endpoint but the entire organization from deadly ransomware threats.

KEY HIGHLIGHTS

- **Zero-Trust Endpoints:** Zero-Trust is built around each endpoint ensuring that malicious behavior is contained at each endpoint – containing cyber-threats pain from spreading enterprise-wide.
- **Endpoint Footprint:** By utilizing existing EDR agents, footprint on each endpoint doesn't change ensuring that it doesn't impact the performance of an endpoint device.
- **Superior Anti-Ransomware protection:** Containment of ransomware and malware while allowing critical business operations to seamlessly continue from each endpoint without disruption.
- **Leading EDR Integration:** Integration with the leading EDR market technology solutions ensure that Airgap has a very flexible integration and deployment across most organizations.

Ransomware Kill Switch for Endpoints Integration


Ransomware Kill Switch
AIRGAP
Events
API
Customer's EDR Cloud
EDR Platform
1
Security policies are configured within Airgap Managmeent Consol
2
Airgap pushes security policies to the customer EDR cloud
3
Security Policies are pushed to each of the EDR client host firewall
4
Endpoint is protected from in-bound attacks by blocking vulnerable points
EDR Endpoints
5
Ransomware blocked due FW inbound rules on Endpoint (No lateral spread of ransomware)
Airgap Zero Trust Isolation™

How It Works

Airgap's Ransomware Kill Switch™ for Endpoints partners with the leading Endpoint detection and response(EDR) vendors on the market to implement the best of breed security solution that provides superior and effective security protection from ransomware.

Airgap's Ransomware Kill Switch™ for Endpoint management system integrates via API with a customer's EDR platform. Customers can then configure security policies through Airgap's SaaS management console that are then pushed as host firewall policies to each of the EDR endpoints. These configured security policies protect endpoints from in-bound network attacks such as the lateral movement of ransomware.

Airgap's management console provides detailed analytics obtained from security events generated from security policies configured on EDR's host firewall. Customers can also monitor all traffic that is passing through all endpoints that are deployed across the enterprise. Security teams can then adjust Zero Trust security policy enforcement as necessary. If a ransomware is detected on an endpoint, security teams can via Airgap's management console push a much more restricted security policy that effectively isolates the endpoint from the rest of the organization.What results is that ransomware is unable to laterally propagate to other endpoints or servers that run critical business operations. By segmenting each endpoint, without ever touching the network it ensures a seamless implementation that is invisible to end-users

Our EDR integration adds an additional layer of ransomware protection by blocking open network ports on endpoints that are used by cyber-attack campaigns to infect enterprise devices. A lack of strong inbound protection makes it much easier for ransomware to infect enterprise endpoints by exploiting open network ports such as Remote Desktop Protocol(RDP) or TeamViewer that have accounted in recent years for about 47% of ransomware infections. There is no need to install additional endpoint agents with Airgap's Agentless Zero Trust Isolation™ solution, since Airgap can utilize existing EDR agent deployments and deliver the required security policies that can immediately block endpoint ransomware infection.

Airgap's integrated security solution Ransomware Kill Switch™ for Endpoints is purposely built to block all avenues that can be exploited by ransomware campaigns to easily infect and quickly spread throughout the enterprise. By utilizing existing EDR deployments, it reduces friction while providing a forklift upgrade to an organization's ransomware defenses.

Key Features

Endpoint Protection

Endpoints are segmented with an allow-list policy that ensures that only known good behavior is allowed to occur, ensuring users can access corporate resources but with enterprise-level security.

Host-based firewall

Airgap's Ransomware Kill Switch™ for Endpoints reuses existing EDR, MDM or Window Firewall agents to enforce granular inbound access rules.

Isolation and Lateral Prevention

Isolates malicious ransomware to the originating end-point and prevents lateral spread throughout the enterprise.

Cloud Management

Management and Orchestration is done via the cloud, ensuring a seamless deployment that can take minutes to administer.

Application Learning

Airgap coalesces data communication across all endpoints to build an application dependency map that shows how normal endpoint communication should be within an organization. Airgap can build and recommend optimal stateful security policies that ensure safe interaction between endpoints and corporate resources.

Prevent Unauthorized access:

Powerful security policy built upon stateful security policies and application control access that prevents unauthorized access, ensuring that only legitimate communication is allowed.

Key Benefits

Endpoint Segmentation

Airgap provides micro-segmentation built around each end-device, allowing only required network communications and blocking all malicious activity from occurring.

Agentless

Airgap leverages existing EDR agents removing the need to install additional agents.

Location Agnostic

Regardless of location, Airgap Ransomware Kill Switch™ for Endpoints is enforced whether in the office, home or mobile hotspot.

Cloud-Based Management

Implementation and management is exclusively done in the cloud without the need for additional hardware or network configuration changes done at local enterprise level.

Conclusion

The ease by which ransomware can enter and laterally spread enterprises is forcing many organizations to rethink how they approach security that prevents catastrophic ransomware attacks and contains the spread of zero day vulnerabilities. Without effective protection, the costs to enterprises can be extremely high, disrupting business operations, incurring ransomware payments and brand damage. Airgap has rethought the approach to ransomware security and prevention by building from the ground up a security solution that is built around how ransomware is designed and operated. Airgap Ransomware Kill Switch for Endpoint solution partners up with the leading EDR providers to deliver the best-in-class security solution that can stop ransomware infection right in their tracks, allowing organizations to continue operating without any disruption to their business.

About Airgap

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication. For more information or product demo, please contact us at https://airgap.io.