



# Zeguro and Airgap Partner to Provide Small and Medium-Sized Businesses with Comprehensive Risk Management Solutions

---

SAN FRANCISCO, CALIFORNIA, UNITED STATES, August 12, 2021 /EINPresswire.com/ -- [Zeguro](#) announced today that it will partner with [Airgap](#) Networks, an industry-first provider of agentless Ransomware Kill Switch™ solutions, to provide small and mid-sized companies with comprehensive Ransomware risk management solutions.

In an era where ransomware and malware attacks are increasing in frequency, businesses are increasingly seeking better security solutions in tandem with insurance. [Cyber insurance](#) providers have long advocated for their clients to leverage other threat mitigation tools, which reduce the risk of operational impact from cyber threats, thereby keeping business secure and decreasing premiums. This partnership between Zeguro and Airgap builds upon this symbiotic concept and enables organizations to pursue actionable risk management strategies across both paths. By utilizing Airgap Network's Ransomware Kill Switch in combination with Zeguro's threat mitigation process, organizations around the globe can better safeguard their digital assets at an affordable price.

While the digital footprint is expanding, the footprint of cybersecurity is not expanding at the same rate. Airgap Networks' CEO and Co-Founder, Ritesh Agrawal, says businesses need to review their cybersecurity budget and investment in conjunction with their digital transformation pace. Zeguro and Airgap have entered into a joint partnership promising unprecedented assurance and zero-trust damage control to minimize a potential attack surface.

With Airgap's Ransomware Kill Switch, organizations can instantly block all lateral data paths of an attack, preventing spread within an organization. This drastically limits the downtime and financial damage caused by ransomware and other malware attacks. Organizations can also utilize Airgap's Zero Trust Isolation model, which addresses common network vulnerabilities that allow ransomware and malware to propagate within a company. Organizations can put Zeguro Cyber Safety Security policies in actions per risk severity and automate the policy enforcement through the Ransomware Kill Switch to contain and stop the Ransomware spread in real-time.

Previously, access to advanced cybersecurity technologies has been a luxury often limited to large corporations. With Airgap and Zeguro, businesses of all sizes can effectively manage threats and prevent unauthorized intrusions through endpoint isolation, ransomware vulnerability scanning, cyber insurance, and more. Zeguro customers can save even more on

their cyber insurance when they become customers of Airgap Networks.

Zeguro's mission is to simplify cybersecurity and cyber insurance for small and medium-sized businesses. Airgap's customers can take advantage of its partnership with Zeguro to affordably attain coverage for loss of income from a breach, payment fraud, ransomware, regulatory fines, and more.

"Our goal is to bring together a robust ecosystem of cybersecurity partners to help our customers. As a result of our partnership with Airgap, businesses of all sizes can be better protected against ransomware attacks, while saving time and money.", said CEO and Co-Founder Sidd Gavirneni.

#### For More Information

Meet Airgap and Zeguro at HIMSS 2021 C100-81 for a Ransomware Kill Switch demo.

#### About Zeguro

Zeguro provides holistic risk management to organizations of all sizes through its integrated cybersecurity and cyber insurance solutions, including a suite of Cyber Safety tools for risk mitigation and compliance and insurance premiums tailored to the size, sector, and profile of a company. To learn more about Zeguro, please visit [zeguro.com](https://zeguro.com).

#### About Airgap

Airgap is the leading Cybersecurity solution provider of the agentless Anti-Ransomware platform. Our industry's first Ransomware Kill Switch™ is designed to stop the spread of malware in enterprise networks and locks down the most critical network assets at the first indication of compromise with zero trust control and policy enforcement over the device-to-device and device-to-application communications. For more information and support, please email [support@airgap.io](mailto:support@airgap.io)

Luis Marte

Zeguro

[Luis@zeguro.com](mailto:Luis@zeguro.com)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/548664741>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.  
© 1995-2021 IPD Group, Inc. All Right Reserved.