SOLUTION BRIEF

Forcepoint + Kiteworks

One Joint Solution to Comprehensively Reduce Content-based Risk

A Kiteworks-enabled Private Content Network (PCN) and Forcepoint's Zero Trust Content Disarm and Reconstruction (CDR) form the first integrated solution that brings zero trust to the content layer. This delivers the highest level of protection from sensitive information leaking into malicious hands, and from threats within the content such as malware sneaking into an organization's perimeter.

One integrated solution. World-leading technology. Designed specifically for high-threat, high-consequence environments.

The Mass Proliferation of Content, and the Fragmentation of Content Communications Systems, Have Created a New Risk Gap Organizations Must Address

We've all heard the saying, "content is king," but in cybersecurity, bad or corrupt content can be an evil king if not prioritized as a potential threat. Content has two primary vulnerabilities:

- **Vulnerability #1**—The sensitive nature of the information in the content. Not all content is for public consumption; much of it is regulated, controlled, classified, and restricted. Content of this nature, if exposed to bad actors, creates significant cyber and financial risk for the organization that is sending, receiving, or storing it.
- **Vulnerability #2**—Untrusted external parties and the malicious malware they may inject within the content itself. When the content is detonated, this malware can enter the devices, networks, and systems where sensitive data is stored, damaging the target organization by subjecting their data to ransom, corruption, and destruction, or even public exposure, causing a cascade of damage to customers, regulatory actions, lawsuits, and loss of reputation.

Both content-delivered vulnerabilities independently pose significant risk, and when combined, threaten catastrophic harm to the enterprise that doesn't protect itself from them.

Applying Zero-trust Principles to the Content Layer Ensures the Highest Degree of Risk Mitigation

Fortunately, Kiteworks and Forcepoint have partnered to create a single, integrated solution that addresses this risk gap: a Kiteworks-enabled Private Content Network (PCN) delivering Content-defined Zero Trust, integrated with Forcepoint's Zero Trust CDR. This solution effectively brings complete zero trust to the content layer. Here's how it reduces risk:

- **All Entities Are Untrusted by Default, Including the Content Itself**—In zero trust, entities are not just users; content is, as well. And content can carry threats, both known and unknown. With Forcepoint Zero Trust CDR, the "trust no one" philosophy extends to "trust no content," ensuring all unstructured data (aka content) is assumed malicious. It works by extracting the valid business information from inbound files, verifying the extracted information against correct structures for the file type, and then building new, fully functional files to carry only the safe information to its destination in near real-time.

- **Least Privilege *Content* Access**—Access control is not just about access to applications. For true risk reduction, this principle needs to be carried through the application to the content assets: what content has what risk level, based on its sensitivity, combined with who is sending, receiving, viewing, altering, or saving, from where, and to where. The Kiteworks PCN ensures that least privilege is granted to each individual content class and context.

- **Comprehensive Always-on Monitoring**—You can't monitor what you can't, or don't, control and see. With a Kiteworks-enabled PCN, all the channels for communication are consolidated into one system, so controls are unified and audit logs are centralized, bringing you the monitoring that is required by zero-trust principles. Further, with Forcepoint's Zero Trust CDR, by leaving only safe content, you are ensured to monitor what's "under the hood" of every asset, delivering that extra always-on layer of protection from what might be hiding within.

Secure and Compliant Content Flows Bring Peace of Mind to Information Communications

To enable Zero Trust CDR, a solution architecture must provide two types of secure, compliant data flows. First, untrusted content files need to be delivered to the CDR server, and second, the resulting sanitized content needs to be delivered to its intended destination. Kiteworks seamlessly folds these steps into its content communications flows.

- **Untrusted Content Delivery Through Zero Trust CDR**—As the conduit for external content communications, the Kiteworks platform quarantines incoming, untrusted content files to prevent their use in the organization. It immediately sends them to the CDR for processing.

- **Sanitized Content Delivery to Its Destinations**—When near real-time CDR processing completes, Kiteworks replaces the quarantined content file with the sanitized version, thus enabling users to safely download it, save it to other repositories, or send it via email, or automation to transfer it via SFTP, managed file transfer (MFT), and other methods. Of course, Kiteworks can save the quarantined original version for further analysis.

Today's risk challenge isn't simply one of device, application, and network protection and controls—it's one of data itself. It's about how to protect your organization from compliance and financial risk due to vulnerabilities of the content it possesses. Fortunately, Kiteworks and Forcepoint recognize this risk, and are providing their customers this industry-first integrated solution that puts zero trust where it's needed most: at the content layer.

Learn more about zero trust solutions at the content layer: click kiteworks.com/contact-us/.

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.

Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

www.kiteworks.com

January 2023