Kiteworks

PRODUCT BRIEF

Kiteworks Hardened Virtual Appliance Provides Multiple Security Layers to Dramatically Reduce Vulnerability Exploit and Impact Severity

The industry's most hardened private content communications appliance brings peace of mind to customers, reducing CVSS severity in vulnerabilities such as Log4Shell from a 10 to a 4.

Kiteworks builds security into the Private Content Network from the ground up, enveloping all its components in a hardened virtual appliance that reduces the Common Vulnerability Scoring System (CVSS) exploitability and impact metrics for any vulnerability it may contain. As a result, vulnerabilities that have high or even critical severity scores within other applications present a much lower risk for Kiteworks customers. This means better protection for private customer content and a stronger security posture in the face of advanced persistent threats.

Significantly Reduced Security Risk From Exploitability

The Kiteworks hardened virtual appliance is architected to reduce the number of potential vulnerabilities in its libraries and increase the attack complexity required to exploit them.

- **Embedded Network Firewall and WAF.** The hardened virtual appliance opens only necessary ports in its embedded network firewall and further protects content behind internal tiers of services with least-privilege access controls. It continuously monitors for—and dynamically blocks—malicious connections via its embedded IPS and malicious web requests via its embedded WAF.
- **Zero-trust Least Privilege Access.** Administrators have just a few privileged user accounts, each with narrowly defined permissions and no access to the OS. In order to get OS access for diagnosis and repair, a certified, authenticated Kiteworks support engineer obtains temporary, fully logged access via a two-step security protocol that requires explicit customer and Kiteworks approval.
- **Minimizes the Attack Surface.** Kiteworks adds only absolutely required libraries and drivers on top of a bare Linux operating system (OS) and disables unneeded functions and services.

Significantly Reduced Security Risk From Impact

The Private Content Network also invokes internal layers of protection to reduce the impact on confidentiality, integrity, and availability:

- **AI-based Anomaly Detection.** Embedded AI detects anomalous data transfers to quickly alert security personnel of a potential exfiltration.
- **Advanced Intrusion Detection and Alerts.** Kiteworks monitors the behavior of all executables, file systems, and web traffic. It enforces strict policies, sending alerts and shutting down unexpected activity before a cyberattacker can damage or exfiltrate sensitive content.

- **Zero-day Threat Blocking.** Kiteworks cuts off an exploit's direct access to content, metadata, networks, and other resources by running third-party libraries inside a sandbox on an OS level (vs. directly on the OS).

The Result? Crippling Exploits Are a Minor Remediation vs. a Major Concern

When Log4Shell was announced, enterprises around the world scrambled to alert their customers and execute emergency updates to hundreds or thousands of applications. The Log4Shell vulnerability (CVE-2021-44228) impacts an open-source logging framework called Log4j that is found in millions of applications. Its CVSS score is a 10—the highest possible severity. However, when Log4j is evaluated through the lens of the Kiteworks Private Content Network, its CVSS score is at the very most a 4. This is because Log4j's vulnerable APIs are disabled by Kiteworks, and the vulnerable third-party library is highly monitored while running inside a sandbox.

Another recent example includes Kiteworks' ongoing white box exercises where a security researcher, sanctioned and trained by Kiteworks, attempted to build and exploit a four-vulnerability chain—one of the most challenging to architect and most impactful when executed. This type of vulnerability would normally tally the most critical CVSS score of 10, requiring immediate remediation. However, Kiteworks' layers of defenses reduced the actual exploitability and impact to a non-critical score affecting only a small subset of deployments.