Kiteworks

FEATURE BRIEF

Reducing Incoming Malware Risks With Embedded Antivirus

Simple Enforcement of Zero Trust at the Content Layer

The Essential Need to Mitigate Incoming Malware Risks

Content from third parties poses a constant malware threat, whether it is uploaded via file sharing, SFTP, or forms, or sent via email, managed file transfer, and custom interfaces. Even employees pose a threat because they use untrusted personal devices on untrusted remote networks. To mitigate this risk, antivirus scanning of all incoming content is an essential component of a private content network (PCN) architecture, helping enforce zero trust at the content layer. The antivirus solutions in many cloud storage and file transfer systems, however, have limitations that create a risk of malware propagation across an enterprise, to your customers, and to external partners.

Protect Every File, No Matter How Big or How Busy

Many antivirus products have low file size limits that let larger files through unscanned, increasing your spread risk. Kiteworks' embedded WithSecure Atlant antivirus closes that gap: It scans files up to 16 terabytes, the Linux file size limit. Even under peak load, it scans 100% of incoming files, unlike cloud storage platforms that allow some unscanned files through when traffic is high.

Maximize Throughput With Distributed Scanning

For optimal performance within distributed private content networks, Kiteworks also provides the flexibility to run antivirus on every storage node within a cluster spanning multiple geographic regions. This maximizes responsiveness, especially for global teams accessing shared content.

Feature Highlights

Scan Massive 16 TB Files

Zero Trust at the Content Layer

High-performance Distributed Routing

Catch Signatures ATP Misses

Catch Malware That ATP Misses

Organizations with advanced threat prevention (ATP) technology on the perimeter might ask whether antivirus is still necessary within the private content network itself. The answer is yes: While ATP uses sandboxing and advanced analysis to detect zero-day threats, it often misses known malware caught by antivirus engines. These anti-malware layers must work together to eliminate gaps that threats can exploit.

Close the Enterprise Gaps of Endpoint Protection

Similarly, organizations that use endpoint protection might ask whether antivirus is still necessary within the private content network. Again, the answer is yes, because external content might be transferred directly to the Kiteworks file sharing repository or to legacy enterprise repositories that lack endpoint protection, and because files might exceed the size endpoint protection systems can scan.

In summary, Kiteworks enables robust, large-scale antivirus protection of incoming content. By combining essentially unlimited file size, 100% scanning, and flexible distributed deployment, Kiteworks' embedded antivirus minimizes the risk of malware for global organizations' external content communications.

Kiteworks