Kiteworks

SOLUTION BRIEF

Accelerate Threat Detection and Response

Embedded Managed Detection and Response

MDR Speeds Threat Response Without Burdening Staff

Organizations are finding it harder and harder to respond to the increasing rate of sophisticated cyberattacks, both because of flat budgets and a tight cybersecurity talent market. They frequently fill the gap by engaging a turnkey MDR service that remotely delivers the entire cycle from threat detection to response.

At Kiteworks, we operate a dedicated subset of MDR focused exclusively on Kiteworks Enterprise product deployments and include it in your subscription. It harmonizes with your IT security stack, processes, and enterprise MDR vendors.

Turnkey Detection, Telemetry, and Response

Your system is automatically onboarded into the Kiteworks Embedded MDR service during initial deployment when you enable the virtual appliance connection to the cloud-based MDR/update server.

We've built extensive threat detection inside the hardened virtual appliance, and telemetry automatically alerts the Kiteworks security operations center (SOC) with the indicators of compromise (IOCs) and essential context.

- Detects activity anomalies vs. baselines
- Monitors files, ports, services, processes, web interfaces, users, etc.
- Anonymizes compliance-sensitive information
- Some local automatic remediation, such as blocking an IP address

Continuous Monitoring and Threat Intelligence

The highly trained and experienced Kiteworks SOC team continuously monitors telemetry from all Kiteworks systems worldwide, all day, every day. They have thorough knowledge of the product's internals and detection methods, and can quickly detect and analyze individual threats, trends, and coordinated attacks.

Solution Highlights

Built-in Detection and Telemetry

24/7 SOC and Security Engineering

Focused Threat Intelligence

Remote Auto-patching

Tight Coupling of Product Development With the SOC Speeds Responses

The Kiteworks security development engineers work closely with the SOC engineers to investigate any perceived threat or vulnerability. They assess the severity and exposure, and monitor other feeds to identify additional threats and vulnerabilities:

- External threat intelligence feeds
- Black box and white box bounty hunter vulnerability submissions
- Third-party penetration test findings
- Vulnerability scans

Automatically Delivers Responses to All Kiteworks Systems Worldwide

A hallmark of enterprise MDR is the ability to remotely orchestrate a response to an individual attack. Kiteworks Embedded MDR also orchestrates a response remotely, but since all the hardened virtual appliances are identical, it can operate across the entire product installed base rather than just one customer at a time. The Kiteworks engineers analyze threat intelligence from across the product installed base and other feeds, identify threats, develop remediations, and then remotely apply them to all connected customer systems. Kiteworks employs a variety of remediation methods:

- **Embedded WAF rule updates** – identifies and blocks new web and REST API threats
- **Code patches** – remediates vulnerabilities in the operating system, open source, and Kiteworks-written code*
- **Admin console alerts** – informs your administrators to take specific mitigation actions

Note that updates of WAF rules and code take effect immediately and automatically without the need for your staff's involvement.

The Kiteworks product also enforces frequent updates of your organization's contact information to help ensure our SOC team can communicate directly with your administrative team in the event of a critical threat.

Kiteworks Embedded MDR Reduces Cyber Risk

Kiteworks' turnkey, Embedded MDR utilizes built-in software for detection, telemetry, and system updates—combined with the services of highly trained and experienced SOC and security development engineers—to accelerate the timeline from detection to response. This reduces the risk of cyber threats compromising sensitive information and damaging your organization's business and reputation, while making life easier for your overburdened IT security staff.

*Remote code patching is planned for late 2024. All plans are subject to change without notice.