FIREEYE™

SOLUTION BRIEF

Managed Defense for Endpoint Security

Expert-driven protection from impactful cyber attacks

HIGHLIGHTS

- **Rapid Threat Containment:** Integrated detection and response capabilities to quickly detect, investigate and contain endpoints to expedite response
- **Cutting-Edge Threat Intelligence:** Backed by advanced threat researchers leveraging cutting edge detection techniques
- **Answers, Not Alerts:** Analysts thoroughly investigate critical threats, providing detailed Investigation reports to accelerate response to effectively respond.
- **Managed Defense Consultants:** Security experts serve as your main point of contact to facilitate additional support such as analysis of malware samples, in-depth forensic analysis or on- site incident response.

Seventy-eight percent of organizations reported being affected by a successful cyber attack in 2018. While organizations need to become proactive about effective cyber defenses, most continue to remain reliant on reactive, technology based, security solutions to protect their most valuable assets.

To be better equipped against cyber attacks, you need a trusted partner to monitor your network and endpoints around the clock with a proactive, analyst-driven approach that leverages the latest threat intelligence cultivated from frontline experience.

You need FireEye Mandiant Managed Defense for Endpoint Security.

Expert-Driven Detection and Response
Managed Defense for Endpoint Security enables enterprises to increase the effectiveness of enterprise security programs with industry leading endpoint security and managed detection and response.

Managed Defense for Endpoint Security is a managed detection and response service that leverages the full power of FireEye, combining FireEye Mandiant frontline expertise, along with industry-leading threat intelligence and FireEye Endpoint Security. These capabilities augment your security team to drive detection and investigation activities that reveal even the most sophisticated attacker.

Managed Defense analysts partner with your security operations center to provide in-depth review of attacker activity along with customized response recommendations, delivering the context needed to take definitive action.

How It Works

Managed Defense for Endpoint Security uses FireEye endpoint technology to provide real-time visibility across the enterprise, including ICS and cloud infrastructure.

You are notified immediately when evidence of compromise has led to an investigation, the status of which can be tracked via a secure portal while our analysts continue to investigate the incident to completion

You also receive a detailed summary report that provides threat context along with remediation recommendations to form an effective response and help prevent attackers from completing their mission.

Selected Features

- Product detections: real-time detection engine, Exploit Guard
- Analyst-driven detections: webshells detection (identifies web-based backdoors, upload tools, and command shells on servers)
- Endpoint hunting and investigation data collection: process list from memory, registry hive list, service list, port list, scheduled tasks, event logs, Windows services, prefetch entries
- One-click containment through Managed Defense portal

Why FireEye Mandiant

FireEye Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tools, tactics and procedures.

WHY MANAGED DEFENSE

- **Experience**
  Draw on the experience of Mandiant incident response teams, who spend 200,000+ hours per year on the most impactful breaches
- **Faster Detection**
  Median time to investigate and respond with Managed Defense is 67 minutes
- **Cost effective**
  Development and maintenance of in-house capabilities can take a lot of time, money and resources
- **Intelligence**
  Access to nation-state grade intelligence collection supported by 150+ intelligence analysts
- **Powerful Defense**
  Proprietary technology stack incorporates FireEye technology and intelligence
  - 150 million FireEye product detections
  - 22 million Managed Defense alerts ingested
  - 170 thousand Analyst Investigations
  - 91% of high priority threats resolved without Rapid Response
  - 98% of Rapid Response incidents resolved without full incident response

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.