DATA SHEET

FireEye

FireEye Managed Defense

Reveal covert threats and accelerate response using frontline intelligence and expertise

HIGHLIGHTS

- **Enhance Existing Investments:** Managed detection and response capabilities that can be integrated with any security operation center (SOC).
- **Full Team of Experts:** Thousands of threat analysts, malware experts, incident responders, intelligence curators and forensic experts.
- **Systematic Hunting:** Analysts proactively deploy proprietary threat hunting techniques using FireEye products and expertise.
- **Real-time Visibility:** Customizable portal serves as a conduit for communication, reporting and collaboration, as well as provides insights into ongoing assessments and response to emerging threats via our community protection dashboards.
- **Market-Leading Threat Intelligence:** Security analysts apply the latest machine, victim and adversary intelligence to locate and detail threats in your environment faster.
- **Threat Assessment Managers:** Security experts to 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.
- **24x7 Coverage:** SOCs in the United States (Virginia and California), Ireland, Germany, Singapore, Sydney and Japan provide 24x7 coverage.

Security threats continue to evolve, yet most organizations remain reliant on reactive, technology based, security solutions to protect their most valuable assets. Technology alone does not fully protect against a determined attacker. And it's difficult and costly to find, hire, train and retain security experts, especially those who specialize in finding covert threats.

You need a trusted partner to monitor your network around the clock with a pro-active, analyst-driven approach leveraging the latest threat intelligence cultivated from experience. You need FireEye Managed Defense.

Intelligence-Led Detection and Response

FireEye Managed Defense is a managed detection and response (MDR) service that combines industry-recognized cyber security expertise, FireEye technology and unparalleled knowledge of attackers to help minimize the impact of a breach.

Managed Defense is continuously fueled by the industry's largest global cyber threat intelligence capability that harnesses machine, campaign, adversary and victim intelligence gained on the front lines of the world's most consequential cyber attacks. This frontline intelligence and expertise drives detection and guides our analysts' hunting and investigation activities to reveal even the most sophisticated attacker. Our battle-savvy security analysts provide a comprehensive assessment of attacker activity along with customized response recommendations, delivering the context needed to understand threats, assess risk and take definitive action.

How It Works

FireEye Managed Defense uses our proprietary technology stack to provide real-time visibility across the enterprise, including ICS and cloud infrastructure.

FireEye's expert threat analysts leverage adversary, victim and machine-based threat intelligence to detect, investigate and proactively hunt for known and previously undetected threats.

When signs of compromise are confirmed, you are notified immediately and can review the latest findings via a secure portal while our analysts continue to investigate the incident.

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.

Understanding The Attacker

To anticipate and respond to today's increasingly sophisticated and targeted cyber attacks, you need to understand attacker motivations, intentions, characteristics and methods. This understanding comes from the knowledge gained through frontline experience.

Managed Defense analysts use proprietary investigative techniques to discover signs of intrusion, learn how attackers are operating and assess the depth of their capabilities.

Experienced analysts also use market-leading threat insights on nearly 16,000 threat actors, including more than 30 nation-state sponsored groups, ranging from China-based advanced persistent threats to Russia-based attackers.

This behavioral insight into how attackers operate enables our analysts to quickly assess a situation, scope the extent of the attacker's operational capabilities, anticipate their next move and deliver an effective plan for response.

Figure 1. Intelligence-led Detection

Proactive Hunting | **Campaign Response** | **Identify and Validate Priority Alerts**

Proactive Hunting

FireEye Managed Defense takes a proactive, analyst-driven approach to hunting, where experienced analysts apply combined knowledge and understanding of attackers and their tactics, techniques and procedures (TTPs) when searching for signs of malicious activity. Managed Defense analysts systematically hunt for evidence of new TTPs from threat actors that continuously evolve and change their methods to try to establish a foothold in target environments while attempting to evade detection.

The proprietary hunting techniques created and used by our analysts are continuously updated and adapted based upon intelligence gained through other Managed Defense customers, consulting engagements with Mandiant, a FireEye company, and FireEye iSIGHT Intelligence capabilities.

Campaign Response

As a Managed Defense customer, you'll benefit from the knowledge and experience FireEye gains by protecting over 6300 customers at the frontlines of cyber attacks.

As we observe attempted attacks on organizations similar to yours based on industry, region or technology profile or if we notice any changes in attacker techniques, we immediately start scanning for evidence of these attacks in your network. If you are not compromised, but we have evidence that you may be targeted, we will provide you with recommended steps to immunize you from the expected attack.

Identify and Validate Priority Alerts

FireEye Managed Defense analysts focus on the most impactful threats, cutting through the noise of many and often irrelevant alerts from other products to save your team time and effort by focusing on the alerts that matter. You'll benefit from the collective knowledge of our analysts and incident responders to identify threats that have the greatest potential impact, including those that may have evaded traditional security controls.

Why Managed Defense

Experience
Leverage 100,000+ hours of IR experience per year from the most impactful breaches

Intelligence
Access to nation-state grade intelligence collection supported by 150+ intelligence analysts

In-region Expertise
Seven global SOCs with in-region technical engagement managers available 24x7

Adaptive Detection
In-depth understanding of adversary TTPs to focus on detecting attacker methods and behaviors

Powerful Defense
Proprietary technology stack of FireEye technologies and intelligence

- 50 billion+ virtual machine analyses daily
- 400,000 unique malware samples processed daily
- 16 million intelligence-gathering sensors worldwide
- Rich contextual intelligence to support sensor data
- FireEye ecosystem updated every 60 minutes

Figure 2. Experience-Driven Response.

Incident Scoping

During an investigation, Managed Defense analysts will review all of the alert artifacts using all FireEye intelligence, inspect network traffic or endpoints to determine the extent of the compromise and identify the timeline across the kill chain by pulling together all applicable events. Analysts scope out the incident using proprietary techniques and intelligence gleaned from more than 100,000 hours of incident response services.

Rapid Response

For more severe attacks, Managed Defense analysts may potentially bring in additional expert resources from our malware, intelligence and incident response teams to deliver an in-depth analysis of triaged events and search across your ecosystem to determine the full extent of compromise.

Remediation Recommendations

Once we've investigated and provided an assessment, Managed Defense analysts provide remediation recommendations to expedite your response.

In the highly unlikely event that large-scale incident response is necessary, FireEye incident responders with forensic expertise can be engaged to help resolve the incident quickly and assess impact for prompt, accurate disclosure.

Guidance and Insight

As a Managed Defense customer, you'll receive access to a secure portal, which provides a conduit for customer communication, collaboration and access to reporting and intelligence. You'll also be assigned a threat assessment manager (TAM) to serve as your day-to-day contact. TAMs are experienced professionals with expertise in incident response and forensics, and provide strategic recommendations to help you improve your security posture.

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. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®