

# FireEye Managed Defense

Continuous Threat Monitoring and Protection by FireEye Experts

## Highlights

- Improves threat protection and enhances the value of the FireEye Platform with 24x7 expertise from FireEye analysts
- Identifies who is attacking you, what their intention is, and how you should respond
- Assesses the risk of each attack and rapidly contains compromised devices
- Offers three service levels to align with your team's skills and risk tolerance
- Provides Global Security Operations Centers for follow-the-sun service

FireEye® Managed Defense combines 24x7 continuous monitoring with intelligence, advice, and context about today's advanced threats. Find out who is attacking you, why, and what you need to do to quickly contain the incident and pivot to incident response when necessary. Managed Defense provides three subscription levels so you can appropriately supplement your team's skills and risk tolerance.

### Continuous Monitoring

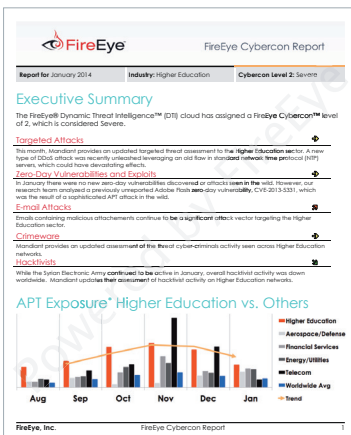
To help scale your security team, FireEye constantly monitors subscribed systems and informs you when alerts require follow up.

### Continuous Protection

Accelerate your response with expert analysts from FireEye that investigate alerts and provide detailed compromise reports for each confirmed threat.

### Continuous Vigilance

Actively pursue adversaries in your network with expert analysts that use advanced analytical techniques to find attackers hiding in remote corners of your network.



	Continuous Monitoring	Continuous Protection	Continuous Vigilance
Proactive APT and Zero-Day Alerts	•	•	•
Intelligence Reporting	•	•	•
System Health Monitoring	•	•	•
Analyst Investigation		•	•
On-Demand "Live Response"		•	•
Incident Response and Containment		•	•
Proactive Hunting for Adversaries			•
Advanced Investigative Techniques			•
Attacker Context and Risk Assessment			•

## Continuous Monitoring

**Proactive APT and Zero-Day Alerts**—when FireEye detects an APT and/or a zero-day attack, our analysts provide a proactive notification with intelligence context so you can follow up on this attack as soon as possible.

**Intelligence Reporting**—subscribers receive monthly reports and alerts about emerging industry-specific threats. The FireEye Cybercon™ report communicates the risk severity and alerts subscribers to heightened industry- or region-specific risks.

**System Health Monitoring**—for continuous assurance, customers receive proactive notifications of potential issues that could compromise detection efficacy for all subscribed systems.

## Continuous Protection

**Analyst Investigation**—the FireEye team of expert analysts evaluate detected attacks 24x7. When a potential compromise is detected, the team performs an in-depth analysis on affected systems to confirm the attack and delivers detailed reporting with actionable recommendations for threat protection.

**On-Demand “Live Response”**—FireEye analysts leverage system and network forensics on live systems to investigate, classify, and analyze the risk in real time. Information on what exactly happened and recommendations on how to contain the threat is immediately provided.

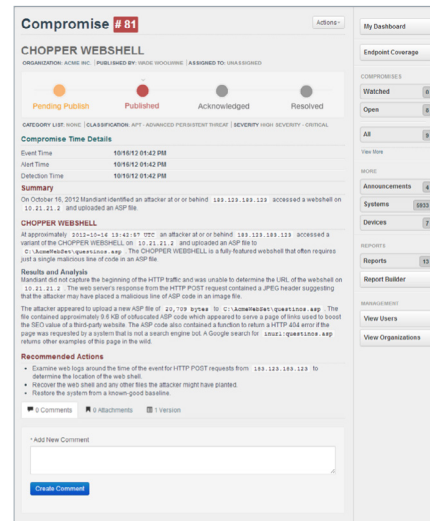
**Incident Response and Containment**—FireEye provides validated compromise reports with technical advice, contextual intelligence, and the ability to automatically contain compromised devices. In addition, the service will automatically pivot to incident response and remediation support at no additional cost for most incidents.

## Continuous Vigilance

**Proactive Hunting for Adversaries**—based on the latest intelligence about attacker tactics, techniques, and procedures (TTPs), expert analysts and forensics specialists proactively hunt for signs of compromise and investigate your systems for attackers on your network.

**Advanced Investigative Techniques**—FireEye analysts use proprietary technologies and methodologies to investigate system artifacts, perform full-packet capture, conduct netflow analysis, and reverse-engineer malware to detect indicators of compromise (IOC).

**Attacker Context and Risk Assessment**—gain deeper insights by leveraging exceptional insight into threat actor tactics, modus operandi, and geo-political context gleaned from front-line incident response work, extensive intelligence research, and 100,000+ hours of incident response activity every year.



The screenshot displays a detailed compromise report for 'CHOPPER WEBSHELL'. The report includes a status bar with 'Pending Publish', 'Published', 'Acknowledged', and 'Resolved' indicators. It provides 'Compromise Time Details' such as Event Time, Alert Time, and Detection Time. The 'Summary' section states that on October 16, 2012, Mandiant identified an attacker at IP addresses 183.133.189.123 who accessed a webshell on 10.21.21.2. The 'Results and Analysis' section describes the attacker's actions, including the upload of a new ASP file and the execution of a search engine bot. A 'Recommended Actions' section lists steps like examining logs, restoring the web shell, and restoring the system. The right sidebar shows navigation options like 'My Dashboard', 'Endpoint Coverage', and 'Reports'.