DATA SHEET

FireEye Detection On Demand

Scan content for threats at any point in your workflow

HIGHLIGHTS

- Detect and prevent known and unknown malware anywhere
- Deploy FireEye-supported plug-ins for browsers and cloud storage
- Get contextual analysis of detected malware in JSON format

Introduction

Threats can and do come from everywhere, and every company approaches security differently based on their needs, industry, and environment. But the one thing companies all have in common is a need for intelligence-backed, validated threat detection capability with enough contextual analysis to act on.

Now, with FireEye Detection On Demand, that capability is available through an API from the AWS Marketplace.

Premium threat detection in any security architecture

FireEye Detection On Demand is a cloud-native threat detection service that rapidly scans submitted content to identify resident malware. Unlike file security solutions based on file integrity algorithms, insider threat policy controls or static check mechanisms, your submissions are processed using the same technologies that power many well-established FireEye offerings.

Access to FireEye Detection On Demand is delivered through an API available from the AWS Marketplace. It can be integrated into your security operations center (SOC) workflow, SIEM analytics, data repositories, customer web applications and so on. It delivers flexible file and content analysis capabilities to identify malicious behavior wherever the enterprise needs it.

In addition to receiving a verdict on each file and piece of content submitted through Detection On Demand, you receive supporting contextual detail, such as file, registry, process and network changes, as well as relevant findings from continually updated FireEye Dynamic Threat Intelligence.

How Detection On Demand works

FireEye Detection On Demand compares your submission to the latest known tactics and signatures of threat actors using static analysis, artificial intelligence and machine learning. FireEye also determines the possibility of secondary or combinatory effects across multiple phases of the attack lifecycle to discover never-before-seen exploits and malware.

Figure 1. How Detection On Demand works.

FireEye Developer Hub

You can visit the FireEye Developer Hub at https://fireeye.dev to explore plugins and sample code and collaborate with the FireEye development community on Detection on Demand.

How to buy

Detection on Demand is available through the AWS marketplace.

When you purchase the service, you specify your need based on the number of files you expect to scan each month. Monthly file and hash submission quotas do not roll over to the next month. File submission rate will be limited to 100/minute. Hash submission rate will be limited to 200/minute.

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.