



DATA SHEET

Digital Threat Monitoring

Early threat warning for your digital footprint



HIGHLIGHTS

- Real-time monitoring of digital threats to your assets
- Early warning that your company or data are being mentioned or targeted
- Alerts when your company or data have been exposed or compromised
- Supporting intelligence context from industry leading security experts
- Reconnaissance tailored to your organization
- Customizable intelligence analyst support

Traditional cyber defenses are designed to protect the assets that exist within your network — whether at the network edge or within the server and on the endpoint.

But in today's highly connected world, you also need to protect your assets that extend beyond your perimeter—such as your organization's brand, personnel and integrated partner community. Visibility into threats against these assets can be just as important as visibility into threats aimed directly at your internal resources.

FireEye Digital Threat Monitoring™ reduces this risk by providing early visibility into the threats your exposed assets face. It delivers this service through a unique combination of advanced technology and the world's leading threat intelligence. The service enables you to proactively combat risks such as leaked credentials, public exposure, threats to assets and other potential monetary or credibility losses. You gain visibility into otherwise inaccessible facets of the web, with focused analysis from FireEye intelligence experts who can make use of the entire FireEye Threat Intelligence organization.

The Visibility and Insight You Need

Digital Threat Monitoring is powered by proprietary automated web reconnaissance technology that collects and analyzes web content, both on the open and dark web. It primarily targets sites used for communication by malicious actors. Using keyword queries specified by you (which may include brands, VIPs and partner organizations), the service conducts an analysis and generates threat alerts on potentially significant matches.

Threat alerts are accessible via the Alerts Dashboard within the FireEye Intelligence Portal. Each alert includes alert status, source and severity attributes, in addition to valuable insights to help manage your monitored assets. The Alerts Dashboard also enables you to take specific actions, such as communicating with a FireEye analyst, on individual or multiple alerts.

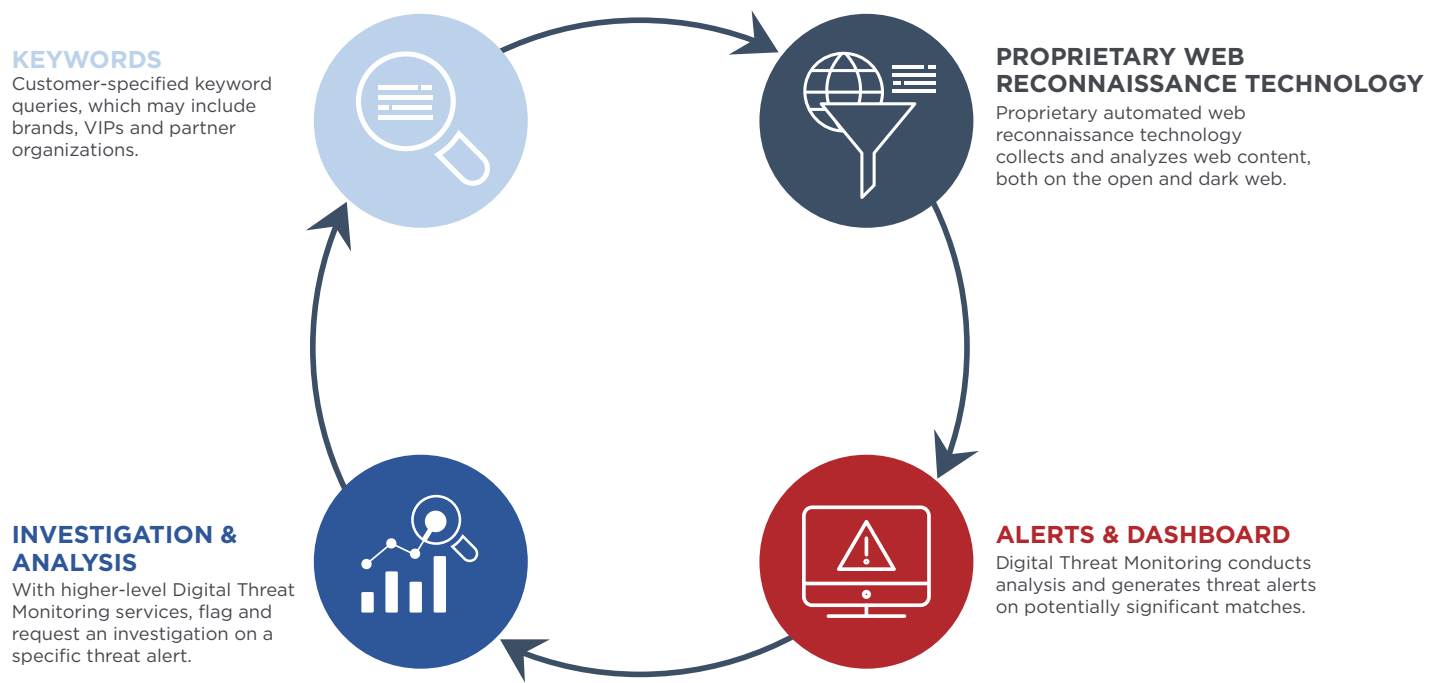


Figure 1. How FireEye Digital Threat Monitoring works.

With higher-level Digital Threat Monitoring services, you can flag and request an investigation on a specific threat alert. A FireEye intelligence analyst conducts a deep assessment and responds with additional context to help you understand the threat. Where appropriate, the analyst will provide any insight they have along with any related FireEye Threat Intelligence.

Table 1. FireEye Digital Threat Monitoring service descriptions.

The delivery option you choose for the Digital Threat Monitoring service depends on the monitoring timeframe and the level of analyst support you need.

Service	Description
Digital Threat Assessment	A one-time, point-in-time assessment performed over 30 days using customer-selected keyword queries. FireEye intelligence analysts deliver a single report that assesses identified threats and includes insights.
Digital Threat Monitoring Standard (Subscription)	Continuous monitoring of customer-selected keyword queries across the open, deep and dark web. Relevant matches generate alerts accessible within the FireEye Intelligence Portal.
Digital Threat Monitoring Advanced (Subscription)	Standard subscription plus up to 40 investigations performed by FireEye intelligence analysts.
Digital Threat Monitoring Enterprise (Subscription)	Standard subscription plus up to 80 investigations performed by FireEye intelligence analysts.

The following table highlights the key differences between the various levels of Digital Threat Monitoring offerings.

Table 2. Comparison of Digital Threat Monitoring service capabilities.

Entitlements	Digital Threat Assessment	Digital Threat Monitoring Standard	Digital Threat Monitoring Advanced	Digital Threat Monitoring Enterprise
Onboarding	Yes	Yes	Yes	Yes
Unlimited Keywords	Yes	Yes	Yes	Yes
Unlimited Users	-	Yes	Yes	Yes
Threat Alerts	-	Yes	Yes	Yes
Keyword Categories	All	All	All	All
Investigations	-	via Expertise On Demand	40 per year / 10 per quarter	80 per year / 20 per quarter
FireEye Intelligence Portal Access	-	Yes	Yes	Yes
Digital Threat Alert Summaries	-	Yes	Yes	Yes
Self-Serve Keyword Management	-	Yes	Yes	Yes

Early Warning in an Evolving Landscape

FireEye Digital Threat Monitoring provides early warning that your brand, data, and VIPs are being mentioned, targeted or exposed. This solution helps identify breaches, exposures and digital threats across the open, deep and dark web to deliver insights about your organization's exposure within the evolving threat landscape and provide the following benefits to your security program and posture:

- **Relevance:** Reconnaissance specifically tailored to your organization.
- **Visibility:** Alerts when your company or data have been exposed or compromised.
- **Preparedness:** Early warning that your company or data are being mentioned or targeted.
- **Expertise:** Intelligence context and analysis from industry leading security experts.
- **Unique Threats:** Real-time data collection and alerting that monitors the digital threat profile of your organization.

To learn more about how FireEye Digital Threat Monitoring can help reduce risk by providing early visibility into threats outside your perimeter, visit <https://www.fireeye.com/solutions/cyber-threat-intelligence/digital-threat-monitoring.html>.

FireEye, Inc.

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

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. I-EXT-DS-US-EN-000211-03

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.

