DATA SHEET

Threat Intelligence Subscriptions

Inform your business and not just your appliance

HIGHLIGHTS

- Provides comprehensive actionable threat intelligence on a wide range of subjects
- Visibility beyond the typical attack lifecycle, adding context and priority to global threats
- Improves asset protection and better informs business risk decisions
- Aligns security programs and resources against your most likely threats and actors
- Addresses tactical, operational and strategic use cases
- Improves prioritization and remediation of security alerts and the patching of security vulnerabilities

Cyber attackers are often better trained, better funded and better staffed than many security organizations. Cyber attacks are increasingly more complex and the resulting damage more severe. Finding and retaining a qualified security professional is tough enough, but finding the numbers needed to fully meet these challenges would be cost prohibitive.

Security organizations are looking for ways to increase their own security expertise and effectiveness. They need to improve their response capabilities and ensure their defenses are aligned against the most likely threats. All without breaking the bank.

FireEye Threat Intelligence Subscriptions meets these challenges – cost effectively — with a wide range of actionable, effective security insights at the strategic, operational and tactical levels.

Table 1. Benefits of FireEye Threat Intelligence.

Intelligence Identifies...	Benefit
Which threats and actors you face because of your business, industry or region	Enables you to invest in and deploy the proper security measures to address them
Which alerts need to be investigated first with associated contextual insight	Reduces time to detection and alert fatigue, and increases staff knowledge
Which vulnerabilities to patch first based on those being exploited against similar organizations	Prioritizes patching efforts and reduces the likelihood of successful attacks

FireEye Threat Intelligence Subscriptions are tailored to the needs of your organization. Subscriptions types include:

- **Strategic:** Provides threat assessments scoped to particular industry sectors and regions; delivers analyses of how geopolitics, regulations and changes in technology shape cyber threats; and forecasts how significant cyber threat issues will evolve in the short and long term. This helps security leadership understand and manage the business and technical risks around major business decisions and security resource planning.
- **Operational:** Provides technical analysis of malware and identifies the tactics, techniques and procedures (TTPs) of known malicious actors. It also includes machine-readable indicators of compromise (IOCs) with contextual information. This helps security analysts prioritize important security alerts, hunt threats and tactically respond to identified incidents.
- **Vulnerability:** Provides intelligence assessments on identified vulnerabilities in many technologies, coupled with our proprietary assessments on the likelihood of exploitation, as well as how a particular vulnerability can be patched or mitigated. This enables the patch management team to understand what types of vulnerabilities pose the most significant threats to the organization and prioritize patching.
- **Cyber Crime:** Provides in-depth assessments and tracking of threat actors who focus on financial crime—who they target, how they carry out operations and what their intentions are. This enables security teams to understand the characteristics of threats impacting them, implement controls and hunting techniques to address those threats and to track actors of interest.
- **Cyber Espionage:** Provides intelligence on named advanced persistent threat (APT) groups associated with specific nation-states. With access to analyses on who they target and the TTPs they use, security teams are able to understand the characteristics of threats impacting them, implement controls and hunting techniques to address those threats and to track actors of interest to them.

Intelligence is generally presented in the form of reports. Machine-readable intelligence and IOCs are available, where applicable, to integrate with your existing security products such as SIEMs and vulnerability managers. FireEye Threat Intelligence Subscriptions also include several resources:

- **FireEye Intelligence Portal:** Online access to your intelligence reports and the complete historical library of FireEye Threat Intelligence related to your specific subscription. IOCs associated with specific types of intelligence can be downloaded and you can perform searches to find intelligence on actors, malware, industries, and other topic areas.
- **Analyst Access:** Access to FireEye Threat and Technical Intelligence analysts for a clearer and deeper understanding of actors, attacks, and risks. You'll gain a better understanding of how certain intelligence or events relate directly to your interests.
- **Delivery Options:** Determine how you want your intelligence delivered and how often, including email alerts and digests.
- **Daily News Analysis:** A daily email that tracks current security stories being covered by the media to give you a detailed understanding of the security landscape. It includes the media coverage of the story, FireEye's judgement on the accuracy of the story, and related FireEye intelligence to increase your understanding and response capabilities.
- **Intelligence API:** This machine-to-machine integration point enables you to use FireEye intelligence and our high efficacy IOCs within your security and network operations, vulnerability management and incident response systems.
- **Browser Plugin:** This plugin expands the technical integration of FireEye Threat Intelligence to any web page you access. It automatically scans the web page for technical indicators (such as IP addresses, domains, hashes), queries the Intelligence API for any relevant FireEye intelligence and then creates a hyperlink to that intelligence.
- **Analysis Tools:** Customers use these online, intelligence-linked utilities to inquire about specific domain names, IP addresses and threats, and upload suspect files for analysis.

Even the best security personnel can't know everything about every topic area (including actors, threats, vulnerabilities, effective remediation, threat hunting). With FireEye Threat Intelligence Subscriptions, you now have the knowledge, experience, visibility and analytical capability of FireEye, the world's leading threat intelligence organization. And now everyone in your organization will have access to the kind of information that the best security practitioners spend years learning.

The FireEye Advantage

FireEye knows more about cyber threats and the people responsible for them than anyone else. The reason for this is our unparalleled access to cyber activity and our extensive threat intelligence operations. FireEye combines adversary, victim, and campaign information with product telemetry data to produce actionable threat intelligence that no competitor can match. Our intelligence is built on:

- Field researchers in 22 countries around the world speaking over 30 languages who mine the deep and dark web to provide information on adversarial methods, motivations and infrastructure
- 15,000 network sensors in two-way mode at customer locations that provide data on what threats are hitting our customers around the world
- Four active Security Operations Centers (SOCs) (associated with FireEye's managed detection and response business) around the world that provide insights into adversary campaigns they see happening real-time
- FireEye Mandiant, the world's leading incident response organization, provides information from breach investigations on the TTPs used by advanced actors for successful attacks
- The industry's largest historical database of threat-related activity, created from data gathered across the events and incidents covered by all our experts and technology
- FireEye was named as only leader in The Forrester New Wave™: External Threat Intelligence Services, Q3 2018

DEDICATED CLIENT SUPPORT

Three levels of Intelligence Enablement and Support to choose from:

LEVEL 1

Baseline: Basic materials and processes required to use the FireEye Intelligence Portal and configure the Intelligence API into your organization.

LEVEL 2

Intelligence Coordination: Baseline + a designated Intelligence Enablement Manager, inquiry access to FireEye Intelligence Analysts, quarterly threat briefs and semi-annual formal reviews.

LEVEL 3

Intelligence Optimization: Intelligence Coordination + a designated Intelligence Optimization Analyst, additional analyst inquiries, custom threat reports, and strategic workshops and threat briefings.

To learn more, visit: **https://www.fireeye.com/solutions/cyber-threat-intelligence-subscriptions.html** and read the **Forrester report**.

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™