FLASHPOINT

Subscription Bundles for U.S. Public Sector Customers

OVERVIEW

Flashpoint has made available bundles of its unique, proprietary software offering, together with key support services, at discounted pricing. A summary of key products and solutions offered by Flashpoint is set out in the section titled "Products and Services" below.

Flashpoint is the globally trusted market leader in intelligence for missions that demand agile, comprehensive coverage of threat actors, threat actor activity, and global issues. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the public sectors to augment their efforts to rapidly identify and mitigate threats.

Flashpoint's presence within illicit online communities since 2010 has afforded a differentiated and nuanced understanding of operating in an environment where threat actors seek anonymity to carry out illegal and malicious activities. We have developed a process to maintain unique insights into this activity, including network threats, fraud, and physical threats via a proprietary tooling and operational posture:

- Seasoned, credible, and authoritative personas who maintain passive and persistent *access to closed communities*
- *Native linguists* culturally adept to produce all-source analysis
- Integration of Flashpoint data and collections into the Flashpoint Intelligence Platform to provide *unique perspective and analysis to specific missions*
- *Internally developed tools and infrastructure* to enable full oversight of intelligence operations, enabling deeper access to closed communities

Our multilingual intelligence analysts, with years of experience navigating illicit online communities, assess whether the risk poses a threat to the customer, help maintain a high signal-to-noise ratio, and provides additional context to foreign language content.

All of Flashpoint's activities are aligned with U.S. laws and are compliant with U.S. DOJ Data Collection guidelines from illicit sources. Flashpoint is also GDPR, CCPA, and EU Privacy Shield compliant.

SUPPORTED MISSIONS & USE CASES

Flashpoint is focused on supporting the following mission spaces:

- **Cyber Threat Intelligence (CTI):** Address state and non-state actors engaged in malicious and/or illicit cyber activities.
- **Counterterrorism (CT):** Designed to prevent or thwart terrorism by state and non-state actors.
- **Global Issues:** Address new, timely and emerging trends, changing conditions, and underappreciated developments.
- **Law Enforcement:** Support law enforcement investigative efforts into criminal activity.
- **Counternarcotic**: Support counternarcotic activities. Promotion and sale of opioids, pharmaceuticals, and narcotics are seen on Illicit forums and marketplaces.

Examples of Flashpoint use cases that demonstrate our capabilities across multiple mission spaces include:

- Identified vulnerabilities and corresponding exploits in near real-time.
- Identified key individuals involved in terrorist activity, as well as new tactics, techniques, and procedures (TTPs) of terrorist organizations and individuals, specific to communication, collaboration, and dissemination of propaganda.
- Established new selectors and means of communication used by terrorists within closed communities.
- Identified a leak within an organization who was selling NPI and/or classified information.
- Developed an understanding of foreign investments in other countries.
- Identified hard-target intelligence organizations targeting U.S.-based pharmaceutical companies working on COVID-19 research and vaccines.
- Identified and supported the mitigation of threats from actors participating in fraud related to COVID-19 financial support initiatives, including Paycheck Protection Program (PPP) and the CARES Act.
- Provided raw Intelligence on the sale and distribution of narcotics, opioids, and pharmaceuticals
- Attributed cyber-attacks of different entities to specific threat actors.

PRODUCTS AND SOLUTIONS

Flashpoint has made available bundles of its proprietary, commercial-off-the-shelf software offering, together with key support services, at discounted pricing.

A summary of the various products and solutions offered by Flashpoint are below.

Flashpoint Intelligence Platform: Grants customers access to our archive of finished intelligence reports, data from illicit forums, chat services, marketplaces, and risk intelligence observables in a single finished-intelligence experience.

Key features include a universal search for all Flashpoint illicit community data, intuitive pivoting from reports into a sanitized copy of threat-actor conversations, and translated conversations, enabling native language content from illicit communities in English within the platform. Flashpoint's datasets include:

- **Finished Intelligence:** Access to analytical reports produced by our intelligence analysts that cover a wide spectrum of illicit underground activity, including crimeware, fraud, emerging malware, violent extremism, and physical threats. Finished intelligence reports include reference to the actor profiles and primary source data across illicit online communities used by Flashpoint experts to create those reports.
- **Forums:** Access to signal-rich discussions from illicit threat-actor communities supplements and complements internal data with targeted data from highly curated sources.
- **Chat Services and Message Boards:** Access to around-the-clock conversations within threat-actor channels to monitor and gain insights across threat-actor communities. Collections include Telegram, Discord, 4chan and 8chan.
- **Risk Intelligence Observables (RIOs):** A high-fidelity feed of cyber observables. RIOs integrate with security operations to enrich user data with additional context.
- **Technical Indicators:** Access to indicators of compromise (IOCs) and technical data across Flashpoint datasets.
- **Paste Sites:** Enables access to openly shared research, data leaks, and other plain text files frequently used by anonymous sources and threat actors to share malicious activity, providing a broader view into open web data.
- **Card Shops:** Users are provided credit card data including BIN numbers, country location, and expiration dates within these collections of stolen payment card data found in illicit high-end credit card shops.
- **CVEs:** Access to the latest CVEs within Flashpoint collection, including access to MITRE and NVD data, as well as CVEs discussed by threat actors as observed by Flashpoint intelligence

analysts and embedded technologies.

- **Blogs:** A view into online sources of news and information related to threat actors and collectives, allowing users to monitor activity in malicious communities comprehensively, as well as risks impacting the organization or brand.
- **Account Shops:** Identify an organization's compromised accounts found for sale in illicit account shops, further stifling the risk of employee or customer login details being used in credential stuffing attacks.
- **Marketplaces:** Access to top-tier marketplaces, where threat actors buy and sell items such as stolen credentials and personally identifiable information (PII).

API: Grants access to our intelligence reports, technical data, and uniquely sourced conversations from illicit threat actor communities, enabling users to enrich and enhance internal data with our targeted data acquired from highly curated sources.

Integrations: Our partners work with us to provide unmatched visibility into threats, empowering users with the context they need to make better decisions about cyber threats, fraud, and physical and insider threats. Integration options include Splunk, IBM QRadar, Anomali, Creative Radicals, Palo Alto Cortex XSOAR, and others.

Alerting: Receive relevant information as identified in threat actor discussions and compromised data is detected.

Request for Information (RFI): Supplements the Flashpoint subscription to Flashpoint products with the ability to ask Flashpoint intelligence analysts specific questions and receive answers to help your team fill intelligence gaps.

Sustained Support: Provides a proactive approach to teams by producing in-depth intelligence assessments to rapidly identify threats and mitigate your most critical security risks. Flashpoint can act as an extension of your team by utilizing our back-end operations tools and capabilities including a scalable non-attribution system, as well as an integrated tool to manage sources, personas, and digital footprints

Staff Augmentation: Provides a virtual full-time dedicated Flashpoint intelligence analyst who will serve as an extension of your team.

Impact Based: Enhanced Monitoring: Provides analyst in the loop pre-and post-event monitoring of keywords in Flashpoint holdings, based on intelligence requirements. Flashpoint is positioned to aid in investigative efforts, response, and recovery.

Program Maturity: Insider Threat Program (ITP): Augments existing resources and expertise to enhance or assess your need for an in-house insider threat function. The program is supported by Flashpoint's seasoned insider threat experts, who have unparalleled experience building insider threat programs from the ground up for a variety of teams ranging from Fortune 50 companies to federal government agencies.

Training Services: These courses assist with navigating cyber fraud, insider threat, and business due diligence, through open source and illicit community datasets. The training provides users hands-on engagement with extensive datasets, including how to navigate threats.

FREQUENTLY ASKED QUESTIONS

What are we offering?

Flashpoint has consolidated some of its key proprietary software offerings, together with key support services, into a single, integrated bundle at discounted prices. This document contains a summary of the Flashpoint offerings.

What problems does the Flashpoint platform solve?

Problem – How to filter out the noise from the threat landscape and how to do "more with less?"

Both the 5-user small team package and the more robust 15-user bundle will provide customers unparalleled insight into unique data sets, historic trends, as well as tradecraft sourced indicators of compromise (IOCs) and upcoming campaigns. Along with raw data, Flashpoint provides finished reporting compiled by our multilingual intelligence analysts, with years of experience navigating illicit communities online. Flashpoint analysts, data, and reporting helps the customer assess threats for potential risks, maintain a high signal-to-noise ratio, and provide additional context to foreign language content.

Problem – How to integrate threat data with current tools and methodologies?

Our API and integrations allow customers to ingest data in a way that meshes seamlessly into existing workflows. Examples of this include integration into existing threat intelligence platforms and leveraging existing team specific tools and dashboards.
Problem – How can a customer get the most out of its limited budget and how can a buyer justify Flashpoint fees to leadership?

As former analysts and operators, our customer success team understands the unique challenges faced by U.S. public sector intelligence teams. They are positioned to help the customer best utilize and maintain their "requests for intelligence" (RFI) hours throughout the life of the contract. Flashpoint is

your intelligence partner, not your intelligence vendor. We can pivot to your unique support requirements and supplement your team as mission tempo dictates.

Why is the Flashpoint platform and data more important than ever right now?

With threats ranging from COVID-19-related fraud, misinformation and disinformation campaigns, and traditional malicious cyber actors rapidly changing their methodologies, Flashpoint is an invaluable part of any agency's response plan. As agencies are tasked to "do more with less" Flashpoint can help fill the gap with near real time vulnerability and exploit identification.

Is Flashpoint the only supplier that can provide this offering?

Flashpoint's presence in, and data collection from, closed and illicit online communities since early 2010 make the platform unique from any other provider. Specifically, Flashpoint brings its customers a differentiated and nuanced understanding of operating in an environment where threat actors seek anonymity to carry out illegal and malicious activities. We have developed a process to maintain unique insights into this activity, including network threats, fraud, and physical threats via a proprietary tooling and operational posture.

A replication of Flashpoint's data, personas, and platform would not be possible in a reasonable period of time by any other vendor or through the creation of internal capabilities. Specifically, we are the only supplier that can provide the following attributes in a single offering:

- Seasoned, credible and authoritative personas who maintain passive and persistent access to closed communities.
- Native linguists culturally adept to produce all-source analysis.
- Integration of data and collections into an intelligence platform to provide unique perspective and analysis to specific missions.
- Internally developed tools and infrastructure to enable full oversight of intelligence operations, enabling deeper access to closed communities.

Who can I contact for more information?

Kyle Bentley
Sr. Account Manager
2411 Dulles Corner Park, Suite 800
Herndon, VA 20171
Main: 703-773-9227
Toll-Free: 800-262-4DLT (4358)
Email: kyle.bentle@dlt.com

PRICING AND BUNDLE

FLASHPOINT SUBSCRIPTION (OPTION 1):

- Flashpoint Intelligence Platform
- Access to All Flashpoint Datasets (Excludes Compromised Credentials Monitoring)
- Flashpoint Intelligence Platform
- 5 User Licenses
- Analysis Views and Personalized Dashboards
- Knowledge Base
- Automated Alerting
- Onboarding and Initial Training
- Customer Support
- Level 1 RFI Package (Includes 24 RFI hours annually and 1 Concurrent RFI)
- Enrichment API (Includes 250,000 search results per day)
- 1 Integration
- Customer Success Rep

Discounted Price (One Year): $99,500

FLASHPOINT SUBSCRIPTION (OPTION 2):

- Flashpoint Intelligence Platform
- Access to All Flashpoint Datasets (Excludes Compromised Credentials Monitoring)
- Flashpoint Intelligence Platform
- 5 User Licenses
- Analysis Views and Personalized Dashboards
- Knowledge Base
- Automated Alerting
- Onboarding and Initial Training
- Customer Support
- 10 Additional Licenses
- Curated Alerts - Initial package - (5 Curated Keyword Patterns)
- 25 Additional Curated Alerts
- Level 3 RFI Package (Includes 72 RFI hours annually and 1 Concurrent RFI)
- Enrichment API (Includes 250,000 search results per day)
- 3 Integration
- Customer Success Rep
- CASO Analyst Training (2 Day)

Discounted Price (One Year): $240,000

All pricing expires on 9/30/2020

ADDITIONAL OPTIONS AND DESCRIPTIONS:

PRODUCT NAME	PART #	DESCRIPTION
Customer Success	CUSTOMERSUCCESS-REP-3	Dedicated, proactive support for the license term. The Flashpoint Customer Success team is comprised of former analysts who have spent their careers serving various public and private organizations. The Customer Success team brings industry-related experience, supporting operations in cybersecurity, law enforcement, fraud, cybercrime, and counterterrorism.
Curated Alerting	CURATED-ALERTS-1	Flashpoint Curated Alerting provides relevant tactical analysis and risk assessments from illicit online communities, based on continual monitoring of intelligence requirements (IRs). Flashpoint works to create optimal queries, capturing prioritized keywords and identifiers.
API	API-ENRICHMENT-2	Flashpoint API provides near real-time access to our intelligence reports, technical data, and uniquely sourced conversations from illicit threat actor communities.
Integrations	INTEGRATIONS-OOTB-4	Enables a pre-built integration with a member of the Flashpoint integration partner network, including SIEM, TIPs, SOAR, Analytical Tools, etc.
RFI	RFI-LEVEL-1 OTHER OPTIONS AVAILABLE	The Flashpoint RFI service supplements a subscription to Flashpoint products with the ability to ask our intelligence analysts specific questions and receive answers to help fill intelligence gaps. Flashpoint RFIs are based on an hourly model.
CASO Analyst Training	CASO-AT-HALFDAY-FPS OTHER OPTIONS AVAILABLE	CASO™ is a suite of holistic training solutions focused on delivering commercial best practices to understand and exploit the publicly available information (PAI) domain with advanced and safe research techniques.
Compromised Credentials Monitoring (CCM)	CCM-ENTERPRISE-X (TBD)	Compromised Credentials Monitoring (CCM) allows users to monitor exposure of compromised credentials for their enterprise domains and email addresses.
Data Exposure Alerting	DATA-EXPOSURE-ALERTING	Identifies customer and company data, source code, or vulnerable systems within open source datasets and public facing infrastructure in order to prevent actors from leveraging exposed data for illicit activity.
Special Project	FP-SP-FPS	Special Project in accordance with Statement of Work (SOW). Engagement-based Professional Services

Threat Response and Readiness (TR2)	FP-TRR-FPS	Flashpoint Threat Readiness & Response Subscription provides organizations with a decision advantage over threats and adversaries. Our data collections, threat actor research, and threat actor engagement are uniquely provided by robust technology, unmatched multilingual intelligence analyst expertise, and a highly experienced Professional Services team. Flashpoint provides research to organizations impacted by attacks, as well as directly engages with threat actors; part of this engagement may also include providing access to cryptocurrency. As part of the Service, Flashpoint will conduct a Ransomware Workshop and Tabletop Exercise on-site at the Client's office at a date and time mutually agreeable to the parties. The service includes providing Client with the ability to deliver cryptocurrency to Threat Actors in the case of a ransomware or extortion event.
Enhanced Monitoring	FP-DDWM30-FPS2 FP-DDWM60-FPS2 FP-DDWM90-FPS2	Enhanced Monitoring provides pre- and post-event monitoring of keywords, based on customer requirements, which is critical for continuous assessment of reputation and legal obligations beyond the conclusion of an investigation or incident response. In the case of a breach, stolen data could end up on DDW markets months or years after the initial compromise has occurred. Flashpoint Professional Services (FPS) is positioned to aid in investigative efforts, response, and recovery.
Insider Threat Program - Assessment	FP-ITP-A-FPS	The FPS Insider Threat Program augments customers' existing resources and expertise to help them build or enhance an in-house insider threat function designed to detect, deter, and respond to insider threat events. This service has four primary components which include Assessment, Roadmap, ITP Program Maturity Management, and Training and Response.