FLASHPOINT

Flashpoint for the Public Sector: Proven, Trusted Threat Intelligence

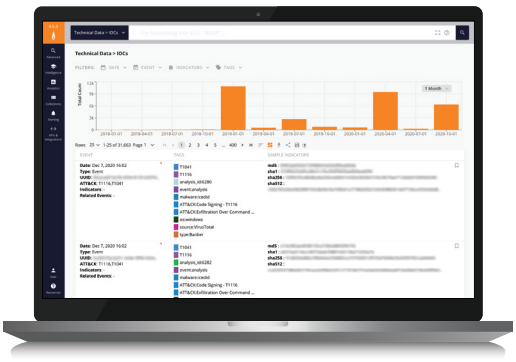
Flashpoint is the leader in delivering proven, trusted threat intelligence to public sector agencies. Federal, state and local government agencies rely on Flashpoint's combination of best-in-class cloud-based software and services to give them the edge they need against threats, bad actors, criminals and nation states.

The scale of today's harmful activities—fraud, theft, ransomware or cyber extortion, money laundering, hacking, trafficking, exploitation and more—can overwhelm internal public sector teams and sideline agencies in their missions. Flashpoint provides quick, safe access to relevant data and threat intelligence that is openly sourced, actively monitored and vetted by human analysts. With it, agency teams have immediate access to the insider knowledge, insights, visibility and context they need to safely and decisively take action.

Flashpoint is more than just cyber intelligence openly sourced from online communities, services and sites. Expert human tradecraft is applied in proprietary ways to acquire, normalize, collate and contextualize threat information. Flashpoint focuses on where the threat actors communicate, collaborate and congregate and then delivers a unique combination of innovative technology paired with cyber, human and signals intelligence to expose it. This combination is backed by analysts steeped in regional culture, understanding of the relevant threats and language.

Flashpoint Solution Benefits for the Public Sector

- Safe access to large, curated collections of publicly available information
- Cloud-based environment that is portable, scalable and extensible
- Intelligence that is vetted, proven, trusted and evidentiary
- Real-time and historical context available on-demand
- Innovative solution ensures fast starts, quick turns backed by proven tradecraft and processes



The vetted intelligence is hosted on the secure Flashpoint Intelligence Platform. The Platform is a cloud-based solution with powerful search, analysis and collaboration features that enable users to quickly find and work on what matters most. The Platform also contains an evergreen knowledge base of intelligence, malicious actor profiles and tutorials, custom alerting features, and daily news briefs with analytical commentary.

The solution allows agency teams to quickly and effectively identify and analyze the chatter around a threat by exposing the online conversations driving the actual threat indicator.

The result is streamlined access to vetted and timely intelligence stores, served up in an easy-to-use web-based portal that can be safely accessed on any device. If more processing support is needed, Flashpoint provides Finished Intelligence and offers a Request for Information (RFI) service to address any intelligence gaps. If public sector agencies prefer to use their internal tools for analysis, the Flashpoint API delivers near-real-time access to the intelligence on the platform.

Flashpoint Products

- FLASHPOINT INTELLIGENCE PLATFORM
- FLASHPOINT API
- COMPROMISED CREDENTIALS MONITORING
- PAYMENT AND CREDIT CARD FRAUD MITIGATION
- BRAND EXPOSURE PROTECTION

Flashpoint Services

- EXTORTION MONITORING SERVICE
- CURATED ALERTING
- THREAT RESPONSE & READINESS
- REQUEST FOR INFORMATION (RFI)
- TAILORED REPORTING SERVICE (TRS)
- PROGRAM AND CAPABILITY MATURATION
- TRAINING SERVICES
- DIRECTED ACTOR ENGAGEMENTS

Flashpoint was named a "Strong Performer" in the 2021 Forrester Wave™ for External Threat Intelligence Services (ETIS)

For more information download the full Forrester Total Economic Impact™ of Flashpoint report

Trustworthy, timely threat intelligence is risky and difficult to obtain

Openly sourced cyber intelligence is the single most effective tool an organization has in its fight against bad actors and the risk of malicious activity. As the amount of data generated by an increasingly interconnected world continues to evolve and explode, cyber-sourced intelligence workflows increase in value. And in their risk and difficulty to navigate.

Online communities and marketplaces on surface, deep and dark web properties continue to explode with users and information. And this has presented a boon for cyber-sourced threat intelligence workflows. Unlike traditional data mining, which seeks to establish and maintain defined data sources, cyber-sourced intelligence workflows work best in a sea of all possible and reachable open resources. However, access to this growing trove of information often requires specific tools, levels of identity and anonymity, or earning the trust of an illicit community. Sometimes, it requires all three. It can take months to establish a pattern of engagement that bad actors will trust. Traditional public sector agencies don't have the training, workforce, or technology to develop and continuously maintain trusted connections to illicit communities on the chance they will need them someday. And, the practice of developing and maintaining these connections presents an enormous risk to agency personnel and their systems.

Additionally, the quantity of data to be collected, interrogated and managed is enormous. It's also unstructured and massively disorganized. A poster's personal, organizational, and network information must be considered for analysis, verification and extraction. Technology like advanced computing systems, existing OSINT tools, natural language processing, along with artificial intelligence and machine learning algorithms can help. But these tools and technologies come at a steep cost, big learning curves and often require dedicated in-house expert teams to use them effectively.

Finally, trustworthiness and reliability are critical for the effective use of openly sourced intelligence. Even if it has been collected and through machine analytics, data by itself is not useful or credible. And, bad actors know they are being watched and are deploying misinformation campaigns as chaff. Analysis and vetting by knowledgeable experts are necessary to establish context, value and credibility—particularly in the global economy. This can present challenges when there are cultural and language components to the information being analyzed.

Flashpoint Sources

Flashpoint actively tracks and collects thousands of illicit online communities and discussions, providing users the ability to safely access and search across datasets including:

- ✓ Forums
- ✓ Chat Services
- ✓ Paste Sites
- ✓ Blogs
- ✓ 4chan & 8chan
- ✓ Social News Aggregation & Discussion Sites
- ✓ Technical Indicators
- ✓ Account and Card Shops
- ✓ Marketplaces

Flashpoint democratizes access to expertly processed intelligence

With capabilities developed initially as a counter-terrorism response to the 9/11 attacks, Flashpoint has spent two decades creating and honing best-in-class technologies, tools and capabilities to combat bad actors. The Flashpoint solution was built by a team of experts with tradecraft skills honed during years of operating in the most austere online environments, training in elite government and corporate environments, and building and leading intelligence programs across all sectors. The result is an easy-to-use solution that helps public sector agencies of all sizes dramatically improve their intelligence capabilities.

Unified Technology + Tradecraft

For threat intelligence to be timely, relevant and useful, it must be produced through a combination of technological innovation and extensive tradecraft. Flashpoint has integrated both into a scalable proprietary solution that effectively accumulates, analyzes, and distributes openly source threat intelligence. The intelligence is then delivered in a clean private cloud-based portal environment with robust search capabilities.

Flashpoint's foundation is a revolutionary platform that connects to millions of online sources such as communities, forums, marketplaces, chat services, paste sites, blogs, technical data, CVEs and more. Flashpoint concentrates the collection on where the threat actors are communicating and congregating. The intake also includes posts on boards like 4chan and 8chan and social news sites like Reddit, Gab and others.

These sources are open in nature, but often require prolonged engagement to understand the intent and gain trust—months or years of consistent, reliable engagement. Additionally, some sources have language, contextual and culture barriers that function as filtering agents. Through trained and experienced human resources, Flashpoint continuously develops, evaluates and nurtures these connections to create a reliable stream of verified intelligence that will yield highly actionable or extremely informative information. Each source is vetted and recorded so that its intelligence can be traced back to specific dates and instances, supporting evidentiary needs.

New sources can be spun up quickly. When Parler shut down in 2021, the Flashpoint team shifted to MeWe collections in under 72 hours, providing a nearly seamless transition for those interested in that stream.

Flashpoint makes it safe to roam in illicit worlds

Currently, Flashpoint exposes unique sources representing a diverse mix of languages, illicit activities and discussions supporting a wide range of activities. These include (but are not limited to): asymmetric operations and criminal activities (credit card fraud, account takeover activities, money laundering, hacking and exploitation tools, doxxing operations and tradecraft, insider threat solicitations and offerings, crypto-currency discussions and more) and threats to third parties.

Flashpoint continuously pulls data from those sources into a non-malicious, private network. It is then analyzed and indexed by skilled intelligence practitioners. Once the data has been processed, it is exposed to Flashpoint users through the easy-to-use Flashpoint Intelligence Platform. There, with just a simple web browser on any internet-enabled device, users can easily search, acquire, comment on and share the intelligence with other Flashpoint users in their account.

Because the data is exposed through the Flashpoint Intelligence Platform, Flashpoint delivers the unique ability for public sector agencies to have a direct line of sight into the collected intelligence—without the risk. Agency teams can 'live in it'— safely observe, review and analyze these discussions and engagements—from the safety of the Flashpoint platform.

Flashpoint supercharges existing intelligence capabilities

For many public sector agencies, current threat intelligence capabilities are often constrained by three key factors: workforce, expertise and time. Flashpoint delivers on all three fronts without forcing agencies to overhaul their workflows or ramp up on a host of new tooling.

Flashpoint strategically complements the activities and feeds of government solutions that are not as responsive to ever-changing threats by continuously delivering up-to-the-minute, high-value intelligence. Because Flashpoint sources are targeted to illicit communities that have been nurtured over time, and the resulting intelligence has already been collected, indexed, analyzed and verified by Flashpoint experts, users can be assured that they are handling actual, vetted intelligence products. They can spend more time in the intelligence, not getting the intelligence. The time savings for agency teams are substantial, with hours and days of collection and analysis being saved.

The delivery can be in whatever way works best for an agency's existing intelligence workflows. Vetted and curated intelligence along with Risk Intelligent Observables (RIOs) and Common Vulnerabilities and Exposures (CVEs) can be pulled through the Flashpoint API and into agency-specific applications for further processing and analysis. Or, agency users can log onto the Flashpoint Intelligence Platform using any web browser on any device and engage with the intelligence directly.

If the agency user chooses to log on directly to the platform, the intuitive and easy-to-use interface makes it easy to find, comment and share the intelligence they need.

Acting as a force multiplier, the Flashpoint solutions become an additional source of highly valued intelligence that agency teams can easily use to accelerate investigations and actions. Public sector agencies can use Flashpoint solutions and teams to instantly improve their threat posture in response to national security, economic and law enforcement challenges. And, if needed, public sector agencies can reach back into Flashpoint experts for additional details, analysis, or new sources.

Flashpoint platform and features overview

Flashpoint's philosophy of developing products and services is characterized by collection, collation and synthesis. With this approach, Flashpoint centers development on making information and massive amounts of data available safely and securely, directly and via API, and maintaining historical repositories of information that can be sourced over time by teams.

The core of the Flashpoint solutions is the Flashpoint Intelligence Platform, a massively scalable software-as-a-service (SaaS) cloud platform that delivers the following features and capabilities:

- **Optical-Character Recognition (OCR)** capabilities identify text, logos, and objects from multimedia within Flashpoint collections
- **Custom dashboards, visualizations and analytics** help teams quickly find what matters
- **FP Collab** enables trusted colleagues to share and discuss intelligence to facilitate more effective decisions around risk
- **Knowledge Base** helps teams stay up-to-date with rapidly updated topic pages on threat actors and tactics, current events, malware families and country studies
- **Daily Intelligence Standups** help users prepare for the day with an overview of notable news stories with Flashpoint commentary
- **Actor profiles** deliver a comprehensive snapshot of an actor's tactics, techniques and procedures (TTPs)

- **Automatic Translations of our datasets across 25+ languages,** providing a wider range of search results from foreign language sources within Flashpoint collections.
- **Finished intelligence** reports and briefs enable the reader to see the whole picture, with in-depth tactical and strategic finishes to guide decision-making
- **Threat actor discussions** and elite threat actor communities that are safely and securely viewable
- **Illicit shops & marketplaces** where goods and services can be tracked, viewed and analyzed
- **Actor tutorials & manuals** that teach agency teams what the threat actors learn, and better prepare for different types of attacks
- **Technical Intelligence** enables agencies to ingest high-signal indicators of compromise (IOCs) with turnkey integrations into existing workflows
- **Industry Alerting** delivers hand-curated alerts on industry-level threats from Flashpoint's Tactical Threat Monitoring Team
- **Automated Alerting** so that users can monitor and triage keyword alerts across Flashpoint collections

Extensible, Secure and Compliant

The Flashpoint API grants access to Flashpoint intelligence reports, technical data and uniquely sourced conversations from illicit threat actor communities. It enables users to enrich and enhance internal data with the Flashpoint targeted data acquired from these curated sources.

The platform is easily integrated into users' existing systems and platforms. It enables technology partner integrations, including threat intelligence platforms, security information & event management systems (SIEM) and link analysis tools.

Turnkey integrations include:

ThreatQuotient · Cortex XSOAR by Palo Alto Networks · RiskIQ · MISP Threat Sharing · IBM Security QRadar · splunk> phantom · Anomali · splunk> · Maltego · Silobreaker · ThreatConnect · servicenow

Flashpoint add-ons:

- **Threat Response and Readiness:** Helps teams prepare for, as well as quickly assess and respond to, a ransomware or cyber extortion attack
- **Data Exposure Alerting:** Identify sensitive data, source code, or vulnerable systems within open-source datasets and public-facing infrastructure
- **Compromised Credentials Monitoring:** Protect the agency, citizens and partners against account takeover and unauthorized access by threat actors
- **Payment and Credit Card Fraud Mitigation:** Detect stolen payment cards and block fraudulent transactions

Securely hosted on U.S. soil, the Flashpoint Intelligence Platform is compliant with General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), the European Union Privacy Shield and the U.S. Department of Justice Data Collection Guidelines from Illicit Sources. The Flashpoint Intelligence Platform operates as a push, therefore does not require FedRAMP authorization because it's not hosting agency data. The platform can be purchased in multiple configurations, tailored towards different agency teams and needs.

Flashpoint Services

Flashpoint knows that managing and predicting threats is a hands-on endeavor for public sector agencies and offers a selection of services that further augment agency intelligence teams.

- **Curated Alerting:** Receive customized hand-curated alerts from Flashpoint's Tactical Threat Monitoring Team
- **Tailored Reporting Service (TRS):** A tailored weekly deliverable that addresses specific intelligence requirements and highlights relevant threats with further assessments
- **Customer Success:** Partner with an expert industry practitioner to receive premium onboarding and rapid, dedicated support
- **Request For Information (RFI):** Submit requests directly to Flashpoint analysts for on-demand bespoke intelligence and analysis
- **Directed Actor Engagement:** Flashpoint is uniquely able to anonymously and securely engage with threat actors on a customer's behalf

Benefits of the Flashpoint solution set for public sector agencies

The combination of Flashpoint innovation, tradecraft and services delivers powerful benefits to public sector agency intelligence teams.

- **Safe Access to Extensive Stores of Publicly Available Information (PAI):** Every day, Flashpoint tracks and exposes data from thousands of data sources, analyzes and indexes it for delivery. It serves this enriched data through a robust, powerful and sanitary portal that safely allows users to view, analyze and live in the data from any device they choose.
- **Portable, Scalable, Extensible:** Flashpoint is a cloud-based service hosted in a secure CONUS environment and can be accessed from any device in any location. It can scale to thousands of users. Agencies can easily pull data from Flashpoint into a variety of other analytical engines via robust APIs.
- **Proven, Trusted and Evidentiary:** Flashpoint has collected and delivered trusted intelligence and context to government agencies for over 20 years. All Flashpoint data is collected passively within the U.S. and international privacy laws. It can be traced back to the source and can be used as evidence in hearings and trials.
- **Real-Time and Historical Context-on-Demand:** With stores that date back to the 1990s, agencies can gain full context in real-time for virtually any emerging threat indicator across application areas of national security, fraud, cyber threats or other illicit activities. Data collections are continuously monitored and evaluated by cultural, analytical and dialectical experts.
- **Fast Starts, Quick Turns, Proven Tradecraft and Processes:** Flashpoint provides agencies with speed and agility and the ability to spin up new connections and rich context in hours instead of months.

Flashpoint Competitive Advantages

Flashpoint's strategic advantage lies within its combination of cutting-edge technology, innovative process and growing stores of portable but secure data collections that can flexibly support and augment internal government agency operations.

Most commercial and closed, proprietary competitors to Flashpoint use openly sourced cyber intelligence, artificial intelligence and machine learning algorithms. There is limited tradecraft involved, and what is involved isn't seamlessly integrated with the technology. They can narrowly target specific and select sources and analyze those sources in a limited and singular fashion. Changing courses to incorporate new collections can be cumbersome, difficult and expensive to do. It can take months to develop the right levels of access within the illicit community. And, access to the intelligence once collected often requires teams to use specific systems tethered to internal agency networks.

BREADTH AND DEPTH OF SOURCES

Flashpoint sources include openly sourced cyber intelligence and layers in human and signals intelligence, all of which are backed by expert analysts who can be redeployed for on-the-fly support mission needs. Fueled and vetted by best-of-breed integration of technology, signals and human capabilities, Flashpoint can access the broadest available set of communities, assets, shops and evidentiary data sources and seamlessly scale access and analysis as needed. Flashpoint combines technology and tradecraft to access the broadest set of communities to source, collect, analyze and index threat intelligence. The depth and breadth of collections and analysis reach back almost two decades and grow daily, providing unparalleled context. And when pivots to new collections need to be made, Flashpoint has the connections and tradecraft to get them up and running in minutes.

UNPARALLELED TRADECRAFT AND EXPERTISE

Flashpoint solutions are hosted and staffed on U.S. soil with expert analysts. Flashpoint team members have cohort status within sites and global language expertise—where and how it counts.

A POWERFUL CLOUD-BASED PLATFORM THAT IS EASY TO USE

Flashpoint intelligence is portable. Users can safely and cleanly access the platform via any internet-enabled device in any location. The search and collaboration capabilities within the Flashpoint Intelligence Platform are robust, intuitive and fast. And, agencies can leverage the Flashpoint API to pull data into their internal systems.

SPEED TO CONTEXT AND INSIGHT THAT IS IMMEDIATELY ACTIONABLE, AT ALL LEVELS

Flashpoint solutions' intuitive and easy-to-use interface rapidly converts data to valuable and actionable context. They deliver actionable intelligence in ways that support the widest breadth of delivery needs: raw (conversation data), visualized (dashboard) or finished intelligence products that help everyone from the analyst to senior leadership.

Flashpoint delivers results and near 5x ROI

With Flashpoint, agencies can augment internal intelligence efforts with a powerful, web-based solution backed by expert tradecraft. The results are dramatically faster time to insight, proactive intelligence capabilities, better collaboration and more efficient internal intelligence teams. Agencies can duplicate the Flashpoint capabilities internally, but at high cost, training and the risks involved in first-person direct searches in illicit communities.

Beyond performance gains, the Flashpoint solution delivers a powerful Return-on-Investment (ROI). In a Total Economic Impact™ study performed by Forrester Consulting, there were several significant areas of savings over a projected three years that Flashpoint customers experienced, along with substantial ROI.

482% ROI

<3 Month Payback

Net Present Value of $1.9M

Forrester Total Economic Impact™ of Flashpoint

One key area of savings was increased productivity. Forrester estimates Flashpoint delivers over $650,000 in workforce savings over three years by supplying an expert analytical team to provide a wealth of custom-curated information. A public sector organization would have to invest at least that much in the dedicated workforce and training to achieve similar high-quality, custom-curated intelligence levels. Additionally, because Flashpoint uses advanced tradecraft and experts that assist security teams in determining the validity of intelligence, organizations can save over $204,000 in time by eliminating false reports.

Another area of savings was the reduction of risk due to insights and proactive protection capabilities. Forrester estimates that organizations who use Flashpoint solutions will save approximately $1.38M over three years between avoidance of data breach and reduced losses from fraud.

With an average savings of $2.2M against a subscription and training cost of $385,000, organizations that invest in Flashpoint solutions can expect to achieve an ROI of 482%. Forrester estimates that the complete payback of a three-year investment in Flashpoint can be made in less than three months of operations.

Flashpoint success in the public sector

Flashpoint's strategic advantage lies within its combination of cutting-edge technology, innovative process and growing stores of portable but secure data collections that can flexibly support and augment internal government agency operations.

Most commercial and closed, proprietary competitors to Flashpoint use openly sourced cyber intelligence, artificial intelligence and machine learning algorithms. There is limited tradecraft involved, and what is involved isn't seamlessly integrated with the technology. They can narrowly target specific and select sources and analyze those sources in a limited and singular fashion. Changing courses to incorporate new collections can be cumbersome, difficult and expensive to do. It can take months to develop the right levels of access within the illicit community. And, access to the intelligence once collected often requires teams to use specific systems tethered to internal agency networks.

Conclusion

Through a unique combination of technology and tradecraft, Flashpoint helps government agencies better focus their time, energy and resources by delivering unrivaled access to highly valued, expert-backed, openly sourced intelligence. With Flashpoint, public sector agencies can safely and accurately paint the picture of what the conversation looks like behind the threat indicator in a verifiable, evidentiary manner.

ABOUT FLASHPOINT

Flashpoint is the globally trusted leader in risk intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the private and public sectors to help them rapidly identify threats and mitigate their most critical security risks.

For more information, visit **www.flashpoint-intel.com** or follow us on Twitter at **@FlashpointIntel**