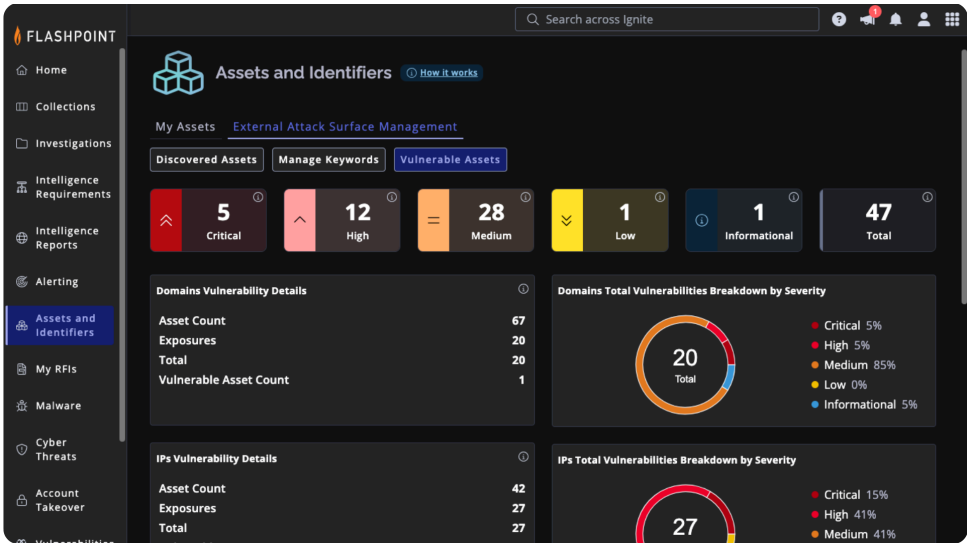
Flashpoint External Attack Surface Management (EASM)

Outpace threats with attacker-relevant context. Prioritize with intelligence-led EASM.

With **up to 95%** of an organization's assets changing each year, rapid infrastructure changes create blind spots and shadow assets for attackers to exploit. Most EASM tools respond with high volumes of alerts ranked by CVSS scores that don't reflect real-world attacker reachability. Flashpoint EASM takes a different approach. It continuously discovers your internet-facing assets and maps them directly to Flashpoint's industry-leading vulnerability intelligence, including **over 105,000 vulnerabilities** that public sources miss. The result is an attacker's-eye view of your perimeter, with the context to act on it.



Risk-Based Prioritization
Prioritize remediation based on asset exposure and real-world attacker behavior, rather than relying on CVSS scores that do not reflect real-world exploitability.

Unmatched Vulnerability Intelligence
Map assets to Flashpoint's Vulnerability Intelligence, including over 105,000 vulnerabilities public sources miss, pre-NVD findings, and Flashpoint's proprietary KEV list.

Unified Platform
Consolidate asset discovery, vulnerability intelligence, and alerting into a single workflow in Flashpoint Ignite, so you can move from discovery to remediation faster.

> “Flashpoint’s Vulnerability exploitability details have allowed us to prioritize risk remediation more effectively.”
> CISO, MANUFACTURING

How Flashpoint EASM Helps

- **Eliminate External Blind Spots.** Forgotten assets and shadow IT remain invisible to security teams, but not to attackers. Flashpoint EASM continuously scans domains, subdomains, and IP addresses, automatically flagging when a forgotten asset is running software actively targeted by malicious actors.
- **Connect Vulnerabilities to Exposed Assets.** Generic CVE feeds tell you what is broken in the world. They don't tell you what is broken on your perimeter. Flashpoint EASM maps discovered assets directly to Flashpoint's Vulnerability Intelligence and shows you which software component and version is responsible for each finding.
- **Cut Through Alert Fatigue.** Noise comes from everywhere. Scanners produce thousands of findings on known assets, intelligence feeds flag CVEs that may not exist on your perimeter, and AI-driven discovery compounds the volume. Flashpoint EASM maps its Vulnerability Intelligence to your exposed assets so your team can focus on actual risks.
- **Replace Manual Processes with Continuous Monitoring.** Stop relying on CSV uploads and stale CMDB exports. Flashpoint EASM actively monitors your external footprint and pushes alerts when a new vulnerable asset is discovered.
- **Stay Ahead of AI-Driven Vulnerability Volume.** AI models can find thousands of potential flaws in source code in a single week. Flashpoint EASM identifies which of those flaws exist on your internet-facing assets and provides the exploit maturity and active exploitation context needed to determine what actually requires a patch.

105,000+ Vulnerabilities tracked beyond public NVD sources

95% Of an organization's assets change each year

Key Features

Guided Asset Discovery	The setup wizard allows you to add known assets and continuously monitor domains, subdomains, and IP addresses with minimal configuration.
Automated Vulnerability Mapping	Flashpoint's proprietary vulnerability data is mapped to your asset inventory for contextual risk scores without manual enrichment.
Asset Triage Inbox	Triage statuses (discovered, owned, external, discarded) ensure your team only monitors what actually matters.
Proactive Alerting	Alerts are pushed to the Ignite Inbox or via email when new assets are discovered, or when a Known Exploited Vulnerability (KEV) is detected.
Asset Detail Page	A single pane of glass shows which software component and version is responsible for the vulnerability on a specific IP or domain, and shows exposed high-risk ports like RDP and SSH, vastly speeding up remediation efforts.

About Flashpoint

Flashpoint is the leader in threat data and intelligence. We empower mission-critical businesses and governments worldwide to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Through the Flashpoint Ignite platform, we deliver unparalleled depth, breadth and speed of data from highly relevant sources, enriched by human insights. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud and brand protection. The result: our customers safeguard critical assets, avoid financial loss, and protect lives. Discover more at **flashpoint.io**