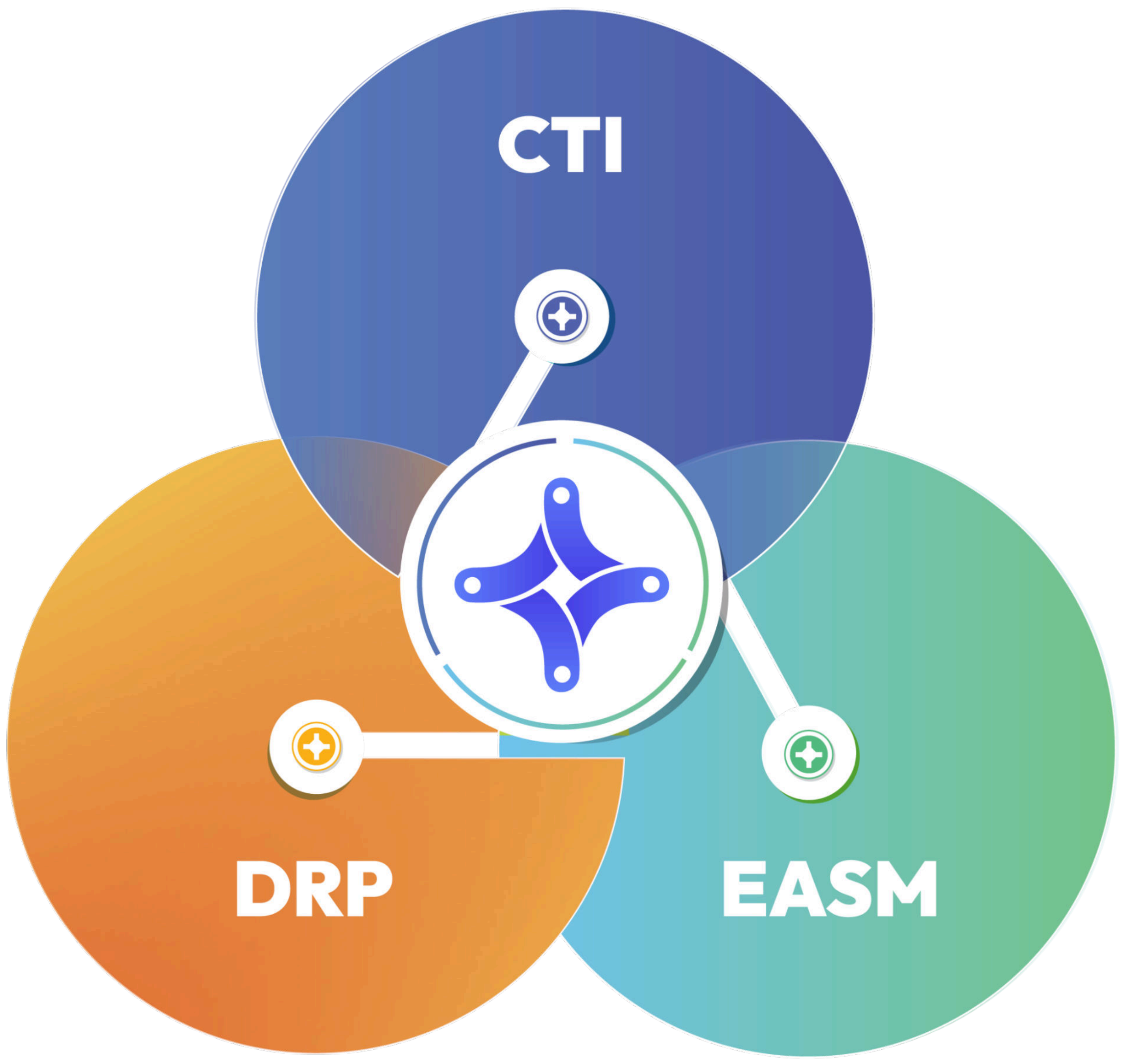
flare

Flare MSSP Partner Program

REDUCE COSTS | ACCELERATE REVENUE | EMPOWER YOUR TEAM

What is Continuous Threat Exposure Management?

Continuous Threat Exposure Management (CTEM) is an emerging strategic security program that integrates cyber threat intelligence (CTI), digital risk protection (DRP), external attack surface management (EASM) and other functions. This convergence enables organizations to proactively identify, prioritize, and respond to the types of exposure threat actors most commonly leverage to attack companies. A CTEM platform serves as the focal point for integrating exposure management throughout security functions, creating continuous risk reduction.



"By 2026, organizations prioritizing their security investments, based on a continuous threat exposure management program, will realize **a two-thirds reduction in breaches.**"

- Gartner eBook, Top Strategic Technology Trends 2024

Key Flare Platform Features That Enable CTEM	Benefits
Unified CTI, DRP, and EASM	Increased efficiency by consolidating siloed security functions
AI-Powered Reporting	Generate actionable and contextual intelligence at scale
Robust API and Integrations	Seamlessly integrate with core security systems and improve ROI on existing investments
Takedowns	Take remediation actions against external threats and reduce risk

Managed Security Partner Program Pricing Summary

Identifiers	200	400	600
Full Threat Exposure Management Platform	✓	✓	✓
Platform API	✓	✓	✓
Global Search Bar	—	—	✓
Customer Success & Support	**Limited** Onboarding Bi-annual review	**Limited** Onboarding Bi-annual review	**Standard** Onboarding Monthly reviews

Add Ons	
Global Search Bar	A popular (and powerful) feature within the Flare app that allows you to query Flare's entire security intelligence and exposure management database regardless of your identifiers.
Threat Flow Custom and Explorer	Threat Flow is Flare's AI application that enables the delivery of timely, relevant, and trustworthy summaries of threat actor chatter on the dark web.
Takedowns	Flare enables the response to external threats via takedowns of malicious domains, code repository leaks, social media threats, and more.
Quarterly Threat Exposure Report	Prepared by a Flare Analyst, quarterly reports provide a convenient summary of your most noteworthy threat exposures from the previous quarter.
Global Search API	Available as a consumption-based add on, the Global Search API lets you query Flare's entire cybercrime database regardless of the identifiers
Additional Identifiers	Identifiers are the way you can apply your context to Flare's threat intelligence database. Some examples of identifiers include domains, keywords, executive names, and email addresses.

MSSP Partner Program Use Case - Pen Testing

The Flare platform originated as a tool built by red teamers, for red teamers. By reducing barriers to threat exposure data, facilitating more efficient assessments, and offering valuable reporting capabilities, Flare provides unique advantages to partners in the highly competitive security testing market.

> **“What used to take about 1500 hours to complete can now be done in 1 week.**
> Flare allows me to empower junior analysts to do dark web investigations that were previously impossible, hence liberating bandwidth.”
>
> - CTI Director, Large MSSP

Challenges Solved

Challenges	Solution
Use of multiple open source and/or limited tools for OSINT	Consolidate OSINT workflows in a single, easy to use platform
Limited external exposure visibility	Leverage a vast dataset that includes diverse sources like dark web marketplaces, GitHub repos, open ports, cloud buckets, and more
Limited time and resources to dedicate to implementing new security tools	Genuinely intuitive, flexible, and easy to use with minimal training required

Opportunities	Solution
Improved margins	Reduce investigation time by 10x and free up time for your security experts to concentrate their expertise where it's most impactful
Better results for your customers	By automating the discovery, enrichment, and prioritization of data for remediation, it puts your security experts in a better position to deliver valuable outcomes to your customers
A path to recurring revenue models	Flare’s platform is easily scaled and applied to an ongoing Threat Exposure Management (TEM) recurring revenue service

MSSP Partner Program - Managed Services

Flare provides MSSPs with a streamlined path to growth in the competitive cybersecurity landscape through its Threat Exposure Management (TEM) platform. Flare simplifies the delivery of TEM services—such as dark web monitoring, credential monitoring, and threat intelligence—which typically compliment security monitoring services like managed detection and response (MDR). Additional offerings from Flare such as threat analyst prepared reporting and takedown services can further extend your operational capabilities and enable you to deliver high-value security outcomes to customers.

> “Flare.io is an **easy to set, easy to use and easy to sell** product.”
>
> - Director of Sales, MSSP

Challenges Solved

Challenges	Solution
Limited external visibility and response capabilities	Flare unifies the core elements of a Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management to monitor and respond to external threats
Limited managed security resources	Flare's flexible system and support options adapt to partner demands, enabling MSSPs to expand service offerings and capture new revenue
Effectively communicating risk to customers	AI-powered reporting capabilities enable you to quickly and effectively communicate complex technical exposures to your clients

Opportunities	Solution
Alignment with cybersecurity market trends	CTEM and cybersecurity consolidation motions are here to stay. Strategically position your business with these trends and pass the benefits on to your customers
Annual Recurring Revenue	By adopting CTEM, MSSPs can position themselves at the forefront of the security industry and create new revenue streams
Competitive Differentiation	With simplified licensing, quick time-to-value, and alignment to CTEM, Flare are provides unique advantages to MSSP partners in the complex cybersecurity market

Example Threat Exposure Management Service Model

Flare's platform simplifies the delivery of Continuous Threat Exposure Management services, integrating seamlessly with core security systems such as SIEM, SOAR, and ticketing technologies. Additional threat analyst-supported reporting and takedown services further enhance managed service capabilities. The following is a high-level service model overview that partners can reference to get a sense of what a Threat Exposure Management service could look like.

Function	Flare	MSSP	End Customer
Flare CTEM Platform • Cyber Threat Intelligence • Digital Risk Protection • External Attack Surface Management	✓	—	—
Alerting	✓	✓	—
Threat Investigation	—	✓	✓
Threat Mitigation	—	✓	✓
Threat Mitigation (Takedowns) • Look-alike domains • GitHub code leaks • Social media	✓	—	—
Quarterly Reporting • Prepared by Flare Threat Analyst	✓	—	—

Partner Portal and Resources

Single Sign On

Once you have been onboarded to the Flare platform, you will have access to Flare's partner portal via SSO at https://partner.flare.io.

Deal Registration

If you have a new opportunity in your clientbase, deal registration is the fastest way to get Flare sales support. Simply fill in the registration form and a Flare representative will be in touch with you!

Branding

Here you will find documents such as Flare's brand guidelines, logos, press releases, banners, and more.

Demand Generation

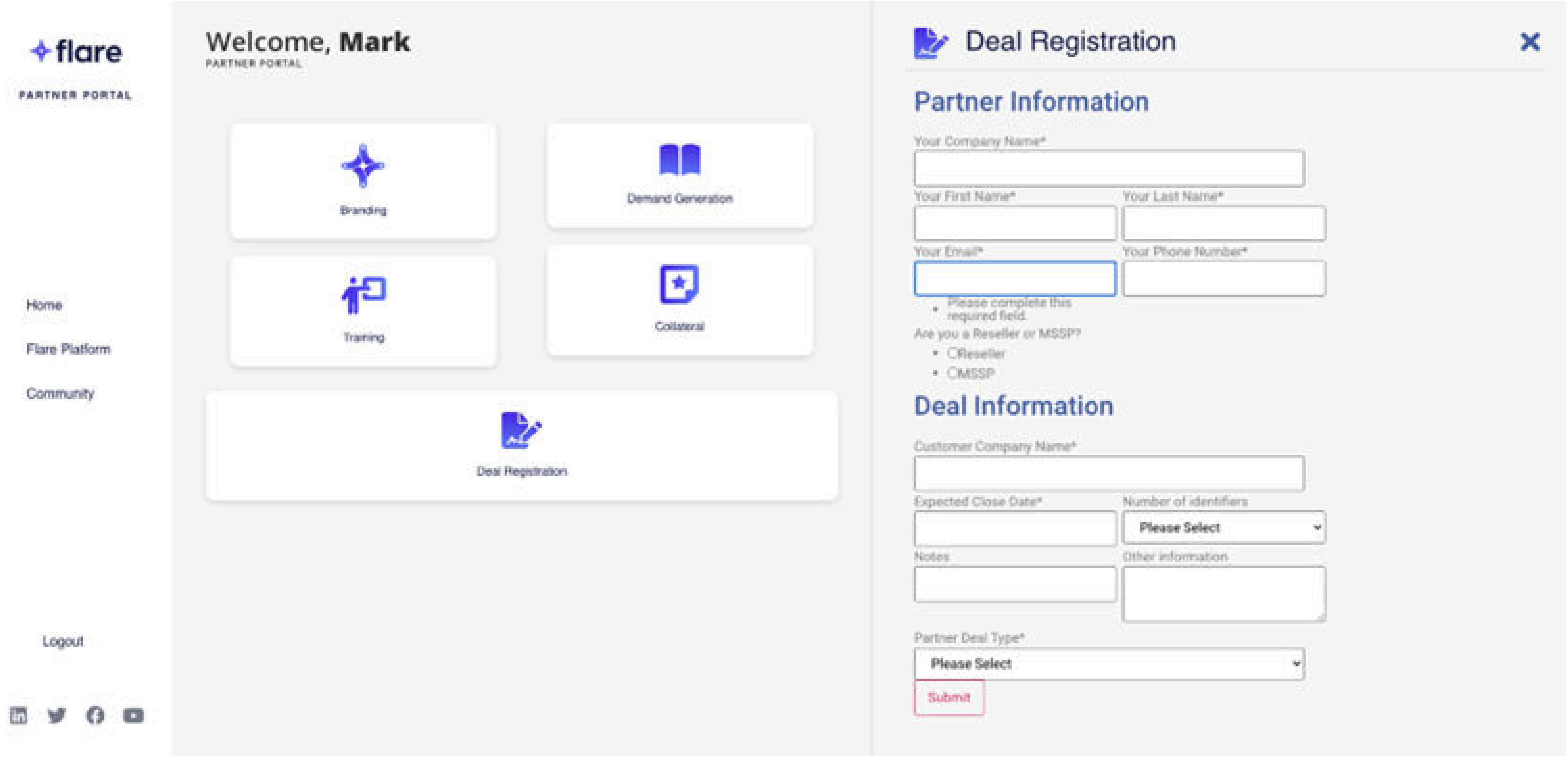
Discover and participate in Flare's latest demand generation campaigns. This section will be updated with email templates, webinar links, social media post templates, and more.

Training

Watch recorded enablement webinars, product training videos, and influencer-created content to keep you up to date on the latest Flare platform features.

Collateral

Read the latest data sheets, white papers, and customer success stories to help you demonstrate Flare's value and make progress in your deal cycles.



Welcome, **Mark**
PARTNER PORTAL

Deal Registration

Partner Information

Your Company Name*

Your First Name* | Your Last Name*

Your Email* | Your Phone Number*

- Please complete this required field.

Are you a Reseller or MSSP?

- ○Reseller
- ○MSSP

Deal Information

Customer Company Name*

Expected Close Date* | Number of identifiers: Please Select

Notes | Other information

Partner Deal Type*: Please Select

Figure 1 - Flare Partner Portal

FAQ

How is Flare different from competitors?

Flare stands out with an intuitive platform, seamless UX, and an "ungated" approach to threat intelligence, making it easy for MSSP partners to deliver services efficiently. Unlike competitors, Flare provides high-fidelity intelligence tailored to each client, minimizing noise and unnecessary alerts to enhance security operations. Additionally, our platform leverages advanced data science and machine learning across unique datasets, enabling MSSPs to uncover deeper insights, accelerate threat detection, and deliver more impactful outcomes.

How much coverage does an identifier provide my end customers?

Coverage varies depending on each customer's unique attack surface and risk profile. Generally, the larger and more complex the attack surface, the more identifiers are needed for effective coverage. All customers benefit from assigning identifiers to their domains and subdomains. From there, identifiers can be extended to specific keywords, names, IPs, or queries, complementing domain-based monitoring for more comprehensive protection.

Tell me more about "Identifier Rotation."

Flare allows MSSP partners to rotate up to twice their paid identifier count each month. This flexibility supports penetration testing, business development, and research efforts, ensuring partners can dynamically adapt monitoring to their evolving needs.

What is the difference between the Global Search Bar and the Global Search API?

The Global Search Bar within the Flare platform lets users search the entire cybercrime database without relying on predefined identifiers. The Global Search API offers programmatic access to the same database, allowing partners to integrate advanced search queries into their workflows. This API requires a premium, as it provides flexibility beyond the standard identifier-based pricing model, enabling complex, scalable workflows.

What marketing support can I expect from Flare?

Flare provides co-branded marketing assets, product training, and sales enablement resources via the Partner Portal. For additional marketing activities such as joint webinars and case studies, reach out to your Flare representative to explore further collaboration opportunities.

Learn more about joining the Flare MSSP Partner Program →

flare.io/partner-program

✉ partners@flare.io

flare