flare

Flare MSSP Partner Program

INCREASE MARGINS | ACCELERATE REVENUE | EMPOWER YOUR TEAM

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

Cyber Threat Intelligence • Dark web monitoring • Threat actor profiling • Supply chain exposures	**The Why** of a threat Flare has repeatedly demonstrated its ability to surface emergent threat from deep cybercrime expertise
Digital Risk Protection • Identity intelligence (credentials, infostealer data) • Brand monitoring • Domain monitoring • Takedown services	**The What** to protect Flare tracks digital assets and breached identities and makes informed risk decisions and impact analysis
Attack Surface Management • Exposed data • Exposed cloud services • Open ports • External vulnerabilities	**The How** to breach By identifying the attack surface, we are able to prioritize remediation actions to prevent breaches before they happen

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

> Flare is an **easy to set, easy to use and easy to sell** product.
>
> – Director of Sales, MSSP

Challenges Solved	
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.

MSSP Tenant Program Summary

MSSPs must purchase the Base Provider License before purchasing additional tenants for each of their end-customers. The license must be purchased as a standalone for one year. Renewal of the second year's subscription requires the addition of at least 1 tenant.

The Base Provider License includes the Global Search Bar (limited to 100 searches per month) and 100 identifiers for the MSSP's internal use and for pre-sales.* This provides MSSPs with a powerful pre-sales tool to perform initial pentests to showcase Flare data and findings. The license also includes the following features, available to the users (employees, consultants) of the MSSP.

Base Provider License Breakdown	
	FP-BASE-PROVIDER
Full Threat Exposure Management Platform (All Data Sources)	✓
SSO & MFA	✓
In-App, co-branded Reporting	✓
Global Search Bar and Search API	100 searches / month*
Threat Flow Custom Reports	✓
Supply Chain Exposure	✓
Deal Registration	✓
Alerts: Email, Slack, Teams, Webhooks	✓
Multitenancy	✓
SIEM/SOAR Integrations	✓
Custom Logo in portal	✓
Partner Marketing Portal and Content	✓
Exclusive Webinars and Co-Marketing Deliverables	✓
Platform API (incl. identifier data feeds)	✓
Threat Flow	
Threat Flow Generated Intelligence	✓
Threat Flow Custom Generated Intelligence and Threat Flow Explorer	✓
Takedowns	See add ons
Identifiers**	100

* Flare reserves the right to remove any pre-sales identifiers that have been in place on the MSSP's portal for more than 60 days.
** 1 search includes up to 100 results, in the UI or in the API. Additional results available via pagination.

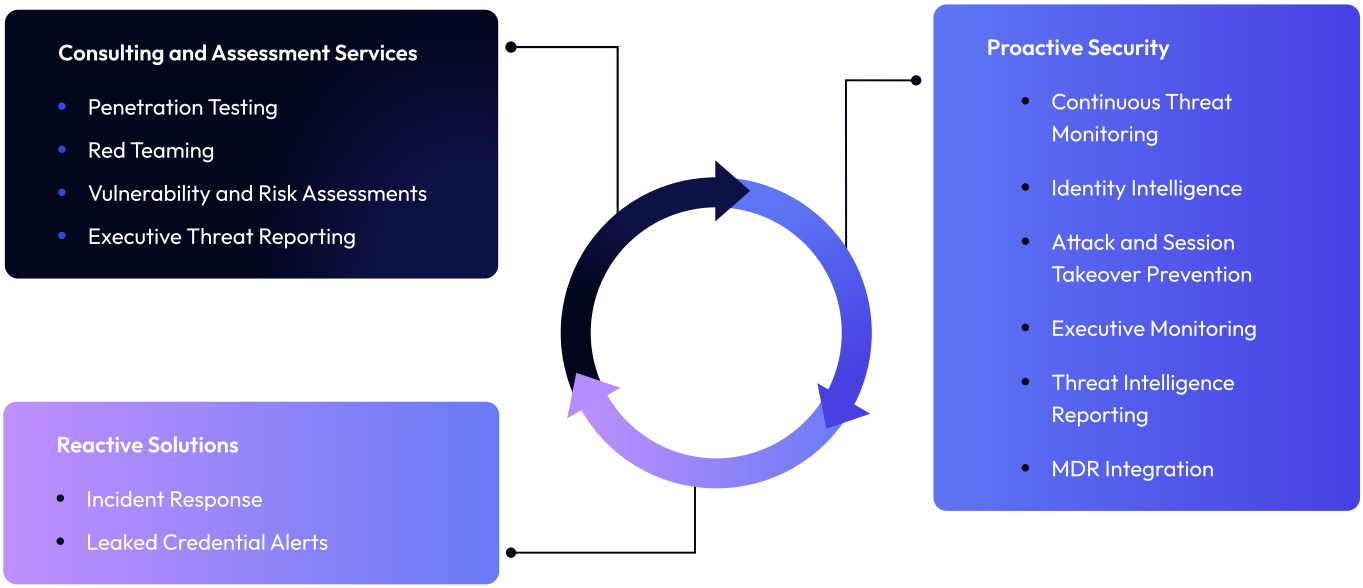
The following tenant bundles are available for each customer onboarded:

Tiers	Micro (MSSP Only)	Starter	Essentials	Core	Enterprise
All Data Sources	✓	✓	✓	✓	✓
Alerts: Email, Slack, Teams, Webhooks	✓	✓	✓	✓	✓
In-App Reporting	✓	✓	✓	✓	✓
Basic Alert Integrations in End-Customer's systems			✓	✓	✓
Identifiers (up to)	25	100	400	1000	4000

Add-Ons	
Takedowns	Flare enables the response to external threats via takedowns of malicious domains, code repository leaks, social media threats, and more.
Additional Searches	Global Search allows you to query Flare's entire cybercrime database regardless of identifiers.

Applying Flare to Multiple Managed Security Service Models

Where does Flare fit in your services?



Tenants are designed to align with the size, relative security maturity, and budget of prospective clients. The Micro Tenant is best suited for SMBs with limited cybersecurity budgets, while the Essentials and up include additional alert integrations in the end-customer's system with increased identifier counts more suited for mature organizations with larger cybersecurity budgets.

For MSSP Customers that would like access to their own Flare tenant, they will be subject to standard package costs and add-ons. Contact your CSM or CAM for the full price list.

MSSP Use Case - Continuous Assessment & Offensive Security

Best practices in penetration testing are shifting from traditional “point-in-time” assessments to continuous models that deliver stronger security outcomes. Flare supports this evolution by reducing barriers to threat exposure data, enabling continuous exposure monitoring, and providing actionable reporting—giving partners a distinct edge in the fast-moving offensive security 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

Challenge		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		What it Means
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 multi-tennant platform makes it easy to configure and support continuous offensive security service models

MSSP Use Case - Threat Detection and Response Services

For most customers already invested in MDR, Managed SOC, or related threat detection and response services, expanding their coverage to include coverage of external threats . With integration into core continuous services such as threat exposure management, incident response, MDR, and identity intelligence, Flare offers clear paths for growth and upsell notions for MSSPs.

Threat Exposure Management is the top emerging security category for MSSPs. What this means:

Challenge		Solution
Blind Spots Modern work dynamics (work from home, personal device use, etc.) introduce new risks and blind spots for MDR services.	→	**External Risk Coverage** Detect stealer logs, leaked credentials, technical exposures, lookalike domains, and third-party ransomware risks.
Limited Visibility Most MDR solutions focus on endpoint and SIEM telemetry and lack visibility into external threat exposures.	→	**Identity Threat Detection and Response** Uncover identity-based threats and provide actionable intelligence for remediation.
No External Response MDR platforms generally cannot take action against external threats like leaked credentials or malicious infrastructure.	→	**Takedown Capabilities** Enable active response to external threats, including phishing domain takedowns, impersonations, and more.

Challenge		Solution
50%+ expected gross margin on a typical end customer annual contract	→	A flexible path to annual recurring revenue
66% expected reduction in client breaches by 2026 by implementing CTEM (Gartner 2024)	→	A logical expansion of MDR/XDR solutions

Resources Available for Partners

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 client base, 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.

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.

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, case studies, and in-person event support, reach out to your Flare representative to explore further collaboration opportunities.