



Case Study



CyFlare Scales SOC-as-a-Service Across MSPs and Enterprises

CyFlare is a Top 100 global Managed Security Services Provider (MSSP) based near Rochester, New York that delivers SOC-as-a-Service to VARs, MSPs, and MSSPs. CyFlare's mission is to empower partners to offer complete security operations without forcing clients to rip and replace existing security tools. To accomplish this, CyFlare built a wholesale SOC-as-a-Service offering that scales from the smallest MSP clients to large enterprise accounts.

CyFlare focused on solving common MSSP challenges: fragmented infrastructure, high costs, and difficulty identifying true threats among noise. Its strategy centered on using a unified SecOps platform to power consistent, context-rich security services for customers of any size.

Life Before Unified SecOps

CyFlare's analysts previously had to manage multiple disconnected security tools to deliver services. This meant juggling alerts from different consoles, manually correlating activity, and spending time troubleshooting context rather than resolving threats.

The lack of centralized visibility reduced efficiency, limited scalability, and made it hard to differentiate real incidents from false positives.

Before



Scattered Security Stack

Multiple products used together, but no centralized analysis or context.



High Cost & Complexity

Legacy SIEM and disparate tools were expensive and hard to maintain.



Limited Threat Context

Alerts lacked correlation across domains, slowing understanding of real incidents.



Manual Investigation Workflows

Analysts manually gathered and stitched together logs.



Hard to Scale

Security operations were difficult to expand across many client environments.

With Stellar Cyber



Unified Operational View

One platform ingests all signals for consistent, high-confidence insights.



Lower Total Cost of Ownership

Scalable, efficient managed services reduce overhead and licensing complexity.



Automatic Triage & Correlation

Multi-Layer AI™ groups related signals into prioritized, actionable incidents.



Faster Incident Response

Analysts act on contextual incidents with integrated timelines and full context.



Multi-Tenant Scale

Platform scales from small MSP customers to large enterprise accounts with ease.

Why CyFlare Built on a Unified SecOps Platform

CyFlare evaluated alternatives—including traditional SIEMs and point solutions—but found they were too costly, rigid, and lacked built-in multi-tenant support. The platform CyFlare chose offered key advantages:

- **Vendor-agnostic integration** with existing customer security tools so clients could retain investments.
- **Scalability** from small MSP client environments to large enterprise deployments.
- **Multi-Layer AI™** to automate triage and correlate weak signals into contextual incidents.
- **Unified dashboards** that enable both analysts and clients to understand threats and trends quickly.

This approach reduced platform complexity and allowed CyFlare to standardize service delivery across its entire customer base.

Security Operations After Platform Deployment

With the new SecOps foundation deployed, CyFlare transformed how it delivers managed services:

- **Automatic Triage:** Multi-Layer AI™ groups related signals into high-confidence incidents, dramatically reducing false positives and noise.
- **Faster Detection:** Analysts quickly spot meaningful threats that were previously buried in alert noise.
- **Scalable Service Delivery:** Built-in multi-tenant capabilities let CyFlare onboard and manage hundreds of client environments without proportional increases in staff.
- **Better Client Experience:** Unified dashboards, actionable incidents, and clear context help CyFlare deliver compelling customer demonstrations and reports.

CyFlare also found the platform vendor to be responsive to feature needs, evolving capabilities in parallel with CyFlare's service model—a key factor in long-term operational success.

Outcome

CyFlare now serves hundreds of active customers with consistent managed security outcomes. Adoption of the unified SecOps platform brought measurable improvements:

- **Higher Analyst Efficiency:** Analysts spend more time on real threat triage and response instead of manual investigation.
- **Broader Market Reach:** Platform scalability makes it possible to offer affordable SOC-as-a-Service to small MSPs and large enterprises alike.
- **Unified Detection and Response:** Correlated incidents enable rapid identification and remediation across the attack surface.
- **Improved Customer Confidence:** Clear dashboards and aggregated insights help partners and end customers understand risk and resilience.

CyFlare expects continued growth in customer accounts and plans to further integrate incident telemetry into broader automation and orchestration workflows to produce measurable security performance metrics for clients.



“By unifying telemetry and automating threat triage, we make it easier for MSPs and MSSPs to deliver consistent, high-value security services across any client environment,” said Joe Morin, CEO and co-founder of CyFlare.



Stellar Cyber’s open and unifying SecOps platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments.

With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley.