



CYWAREone

Global Partner Program



“
Cyware enables smarter and more
effective security through cyber fusion.”
”



Anuj Goel
CEO

Welcome to **CYWAREone**

Global Partner Program.

“
There is a growing demand for Shareable, Actionable, and Relevant Threat Intelligence. This is the time to partner with Cyware.”



Matt Courchesne

Head of Channel, North America

Index

01	Cyware-at-a-Glance	01
02	Our Partner Program for Channel & MSSPs	10
03	Why Cyware One?	18
04	Benefits of Partnering with Cyware	19
05	How To Become A Partner And Sell Cyware	20

Cyware-at-a-Glance



Industry-leading TIP and SOAR platforms



Unique Collaboration Tools for Intel Sharing



Orchestration Beyond Incident Response



Complete Visibility to Connect the Dots and Turn Threat Intel into Intelligent Action



Powerful Modules that Combine into a Complete Cyber Fusion Center

KEY HIGHLIGHTS

Enterprise Customers

Fortune 500 customers from Financial Services, Healthcare, Government, Manufacturing, Supply Chain, Aerospace and other sectors



Leading ISACs and ISAOs

Powering threat intel sharing for >85% of ISACs and ISAOs



Award Winning Team

More than 50% in engineering. Global teams and award-winning support



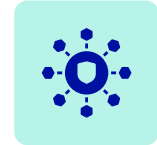
Critical Certifications

FedRAMP Ready, SOC 2 Type 2, ISO 27001



Cyber Fusion

Next Generation SOAR & Threat Intelligence Solved



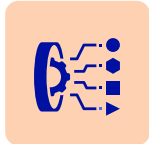
Information Sharing



Threat Intelligence



Orchestration / Automation



Incident / Threat Response



What Sets Cyware Apart

Capability

Threat Intelligence

- Unidirectional Sharing
- Manual Intel Analysis
- Technical Intel Ingestion

Incident Response

- Focus on "Managing Incidents"
- Case Management Workflow
- Siloed Response

Security Automation

- Incident Response Orchestration
- Pay Per Automation
- Limited Alert Aggregation

What Market Offers

What Cyware Offers

- Bidirectional Intel Sharing and Collaboration
- Connected TIP: End-to-End Intel Automation and Mgmt
- Backbone of Intel Sharing for ISACs, ISAOs, CERTs
- Trusted User Generated Threat Intel Feeds

- Focus on "Managing Threats"
- Connect-the-dots / Contextual Intelligence
- Collective Defense / SecOps-IT Ops-DevOps Fusion
- Fabric or Glue Between Security Teams

- Any-to-any, Decoupled Orchestration Layer
- Unified, Low-Code Customization
- Unlimited Automation Playbooks / App Marketplace
- Multi-source Unlimited Alert Aggregation
- Secure Cloud-to-On Premise Orchestration

Cyware Suite Modules



Orchestrate

Centralized Decoupled Orchestration for Cyber, IT, and DevOps workflows across Cloud, On-Premise, and Hybrid environments.



Respond

Case Management and Incident Response

Integrated **threat response** with advanced **"Connect-the-dots" (correlation)** capabilities to unify Intel and SecOps.



Intel Exchange

Threat Intelligence Platform

Intelligent **bi-directional "Connected" TIP** for ingestion, analysis, and automated sharing.








Collaborate

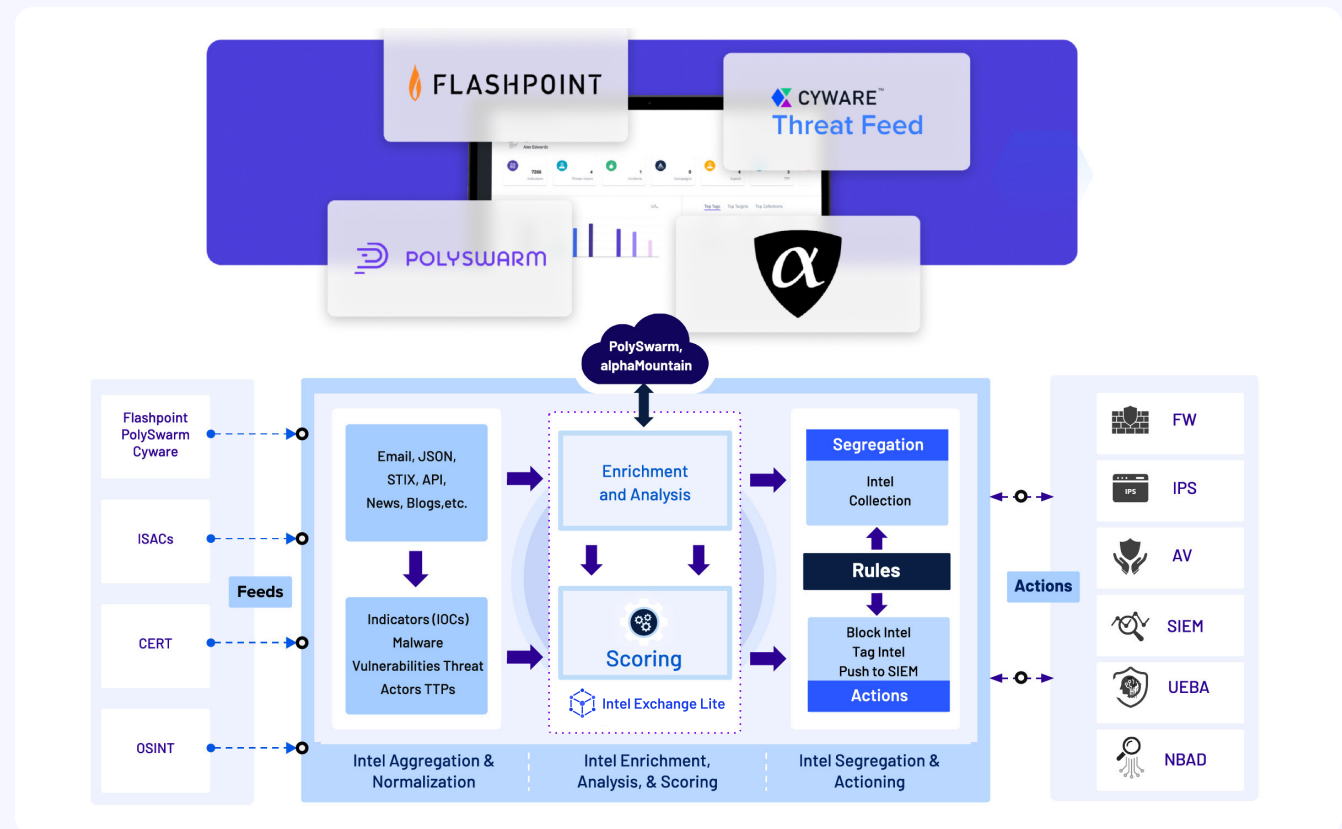
Security Alerts / Advisories

Mobile-enabled automated **alerts aggregation, storage and dissemination** for situational awareness.

Intel Exchange Lite Cloud Native, Automated TIP for Growing Teams

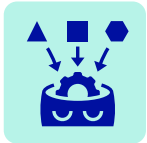
-  Built for **Mid-Market** with Small (or no) Intel Teams
-  **Cloud only**
-  **Integrates with On-Prem** SIEM, EDR, Firewall and other security technologies
-  Pre-packaged **Platform + Feeds + Enrichment**
-  List Price: **< \$100K**

Threat Intel Automation Platform Pre-Loaded with Premium Intelligence Feeds and Enrichment Sources



MSSPs & Cyware

Creating A Collective Defense Posture



Learn from **client incidents** and apply those learnings to proactively stop similar incidents for other clients.



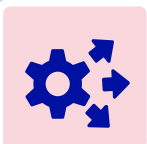
Adopt an **ISAC approach** with centralized intel collection (generated through internal monitoring), enrichment, contextualization, correlation, analysis and sharing.



Become an **Intel generator with relevant, actionable and timely intelligence** for your clients.



Enable proactive **orchestration using the collective intelligence** to stop the attacks on client networks at the earliest.



Deliver Orchestration-on-demand for clients for Incident Response, Intel Response or any other security response required at the client end without requiring multiple SOAR deployments.

MSSPs & Cyware Threat Intelligence-as-a-Service



Monitoring Intel Only



Provide Context



Shared Orchestration & Response



Dedicated Orchestration & Response



TlaaS (Cyware Hub & Spokes Model)

1

Get ROI on existing point solutions.

2

Easy path to additional services related revenues.

3

Vendor Agnostic modules, and 350+ integrations ensure interoperability.

4

Customized Spokes cater to your clients' unique threat intelligence needs.

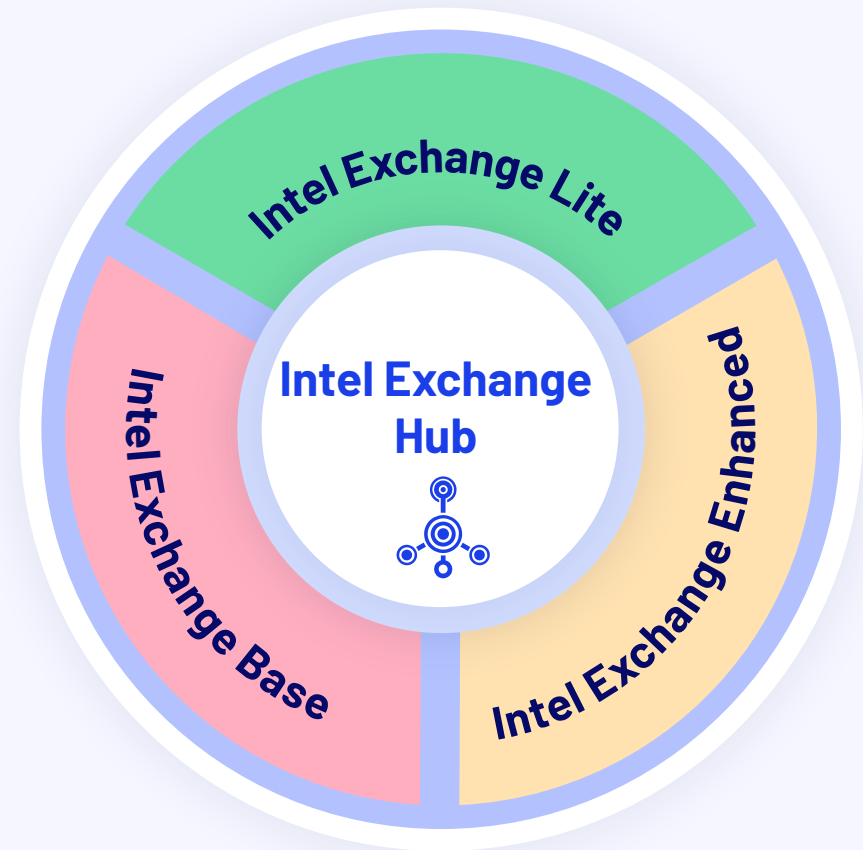
5

Cyware Collaborate Platform enables real time collaboration.

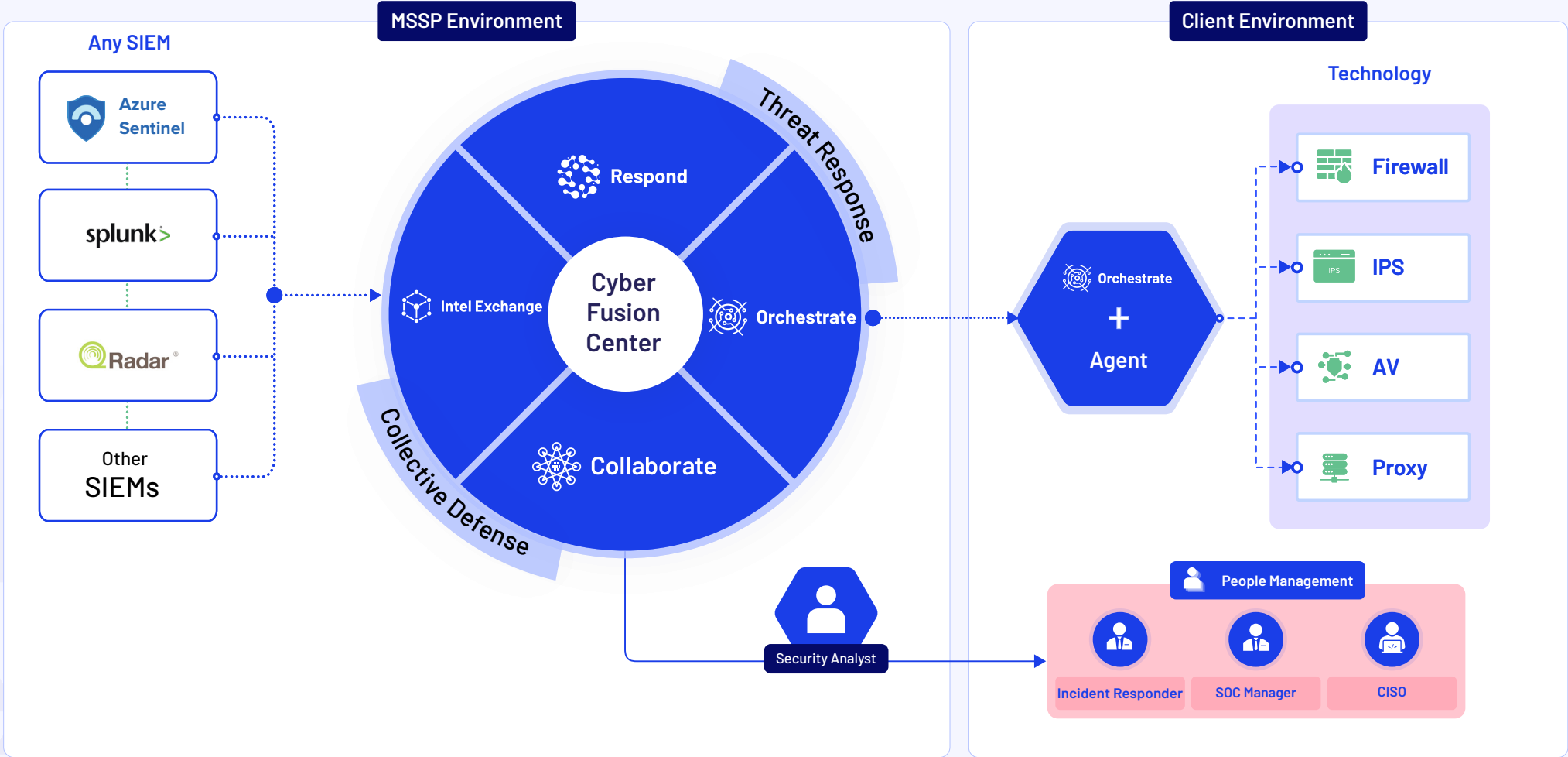
MSSPs & Cyware

Helping MSSPs Become Mini ISACs, One Spoke At A Time

Cyware's Hub & Spoke model allows MSSPs to create a collaborative **Threat Intelligence-as-a-Service (TlaaS)** network for their clients.

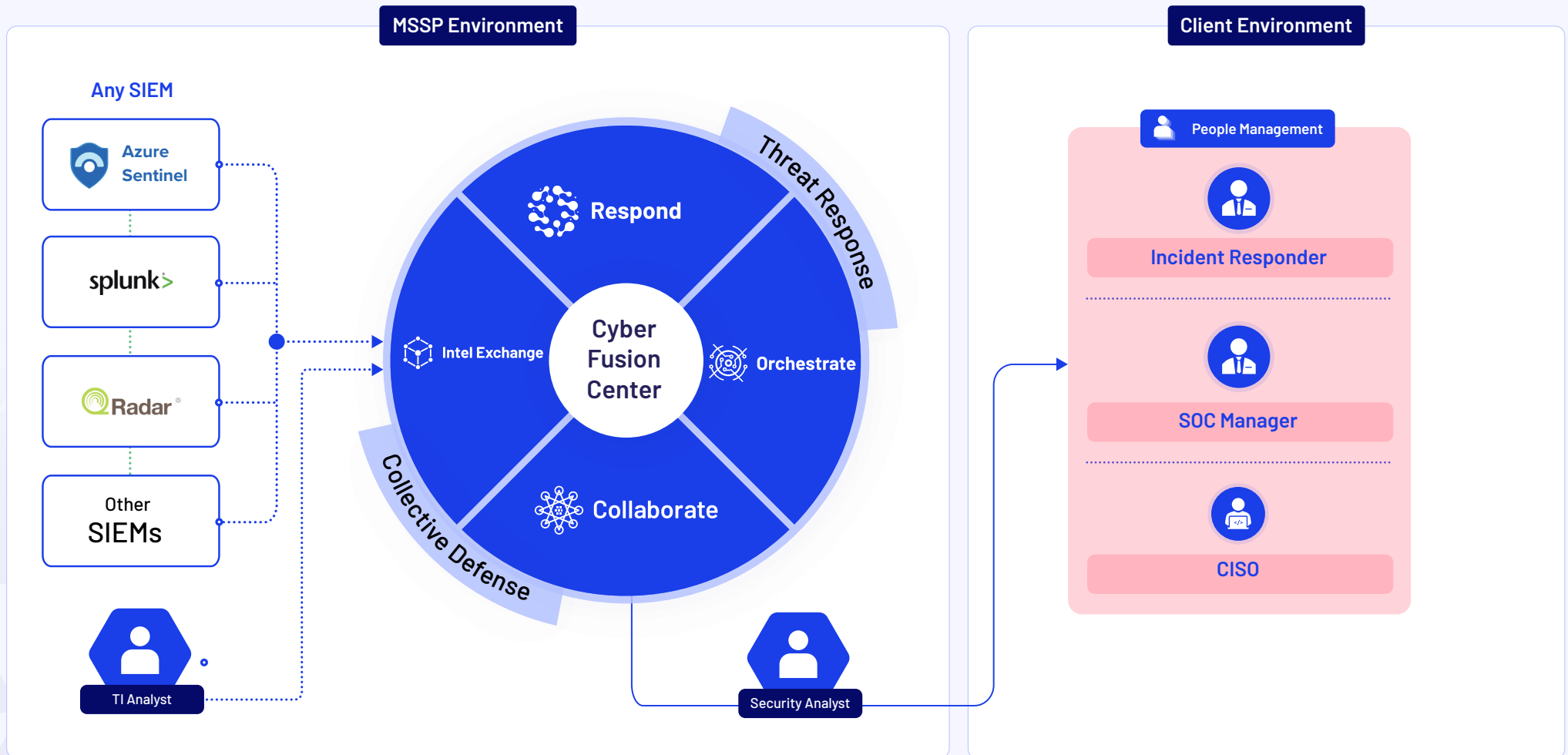


MSSPs & Cyware Cyber Fusion Center-as-a-Service



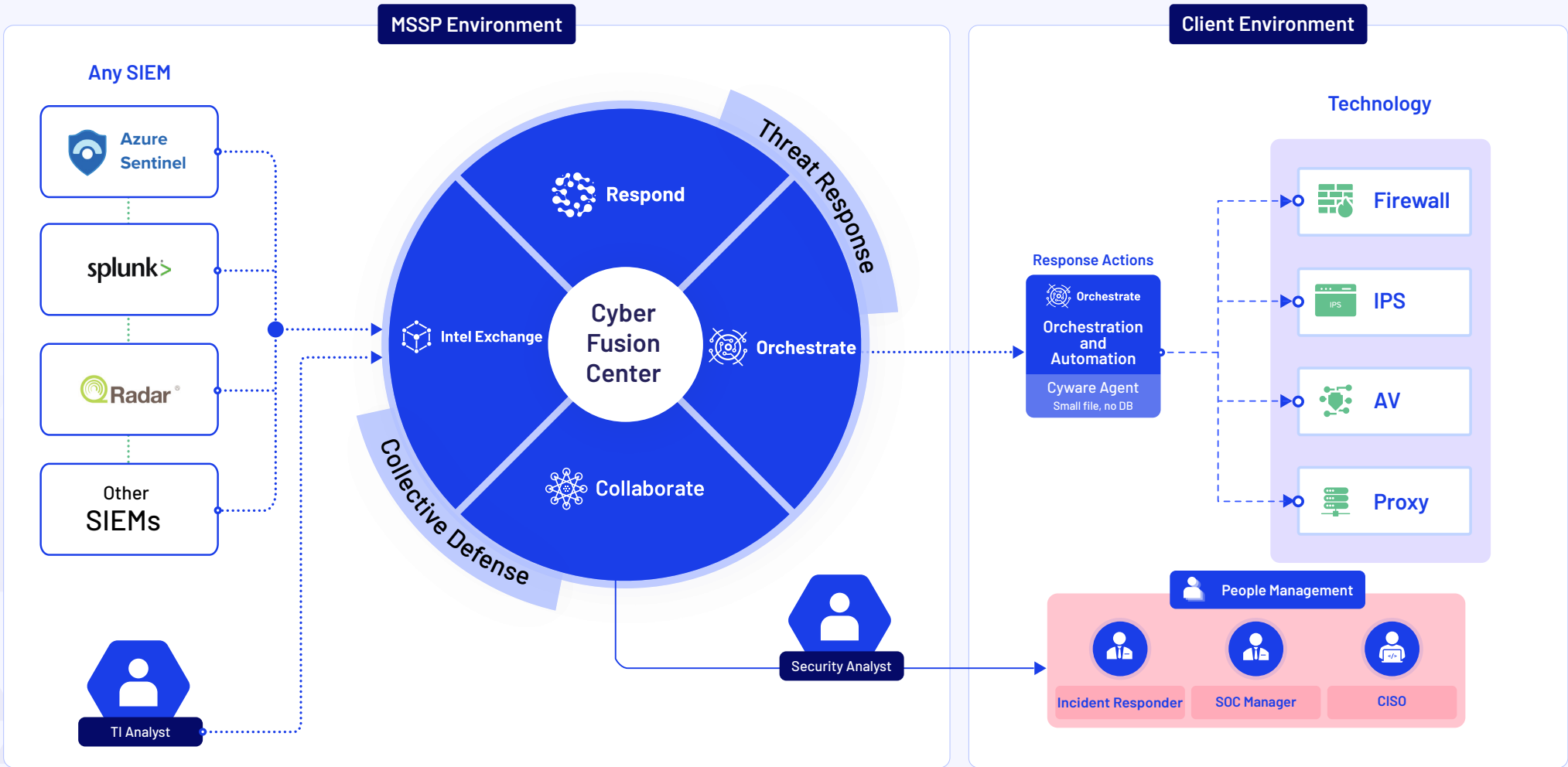
MSSPs can leverage Cyware's Fusion Center technology to provide services for organizations of any security maturity. This is possible through the modular structure of Cyware's Cyber Fusion Center. This document provides information on 3 prominent and widely used scenarios.

Scenario 1 Monitoring Only



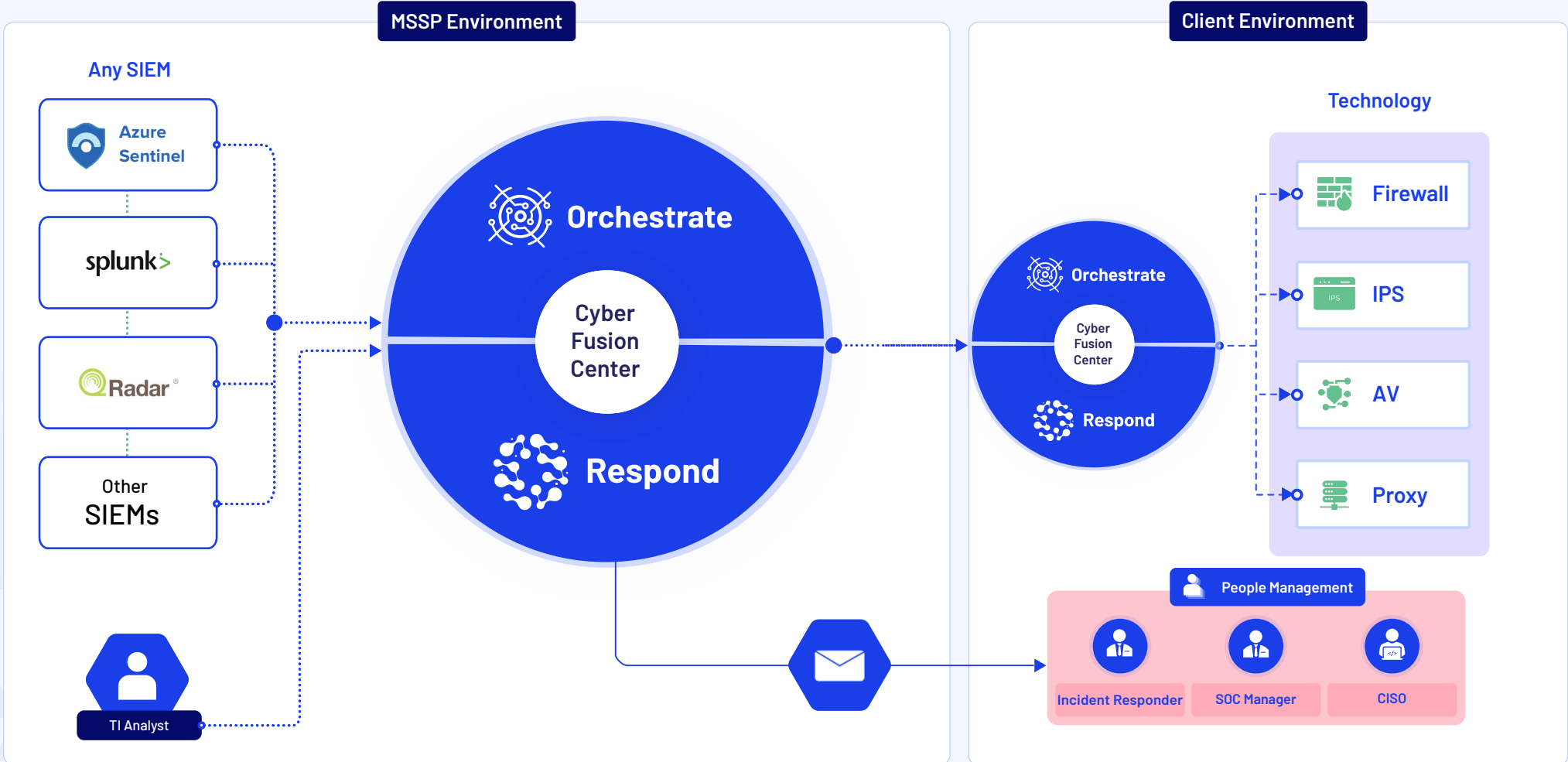
In this scenario, the MSSP does L1 monitoring and sends out alerts to the client via Collaborate's web app, mobile app, and email. MSSPs provide SOC-as-a-Service to their customers. There is zero infrastructure in the client's environment. Usually, events take up to 45-60 minutes of SOC L1/L2 analysts' time, and with Cyber Fusion Center, this can be reduced to 10 mins.

Scenario 2 Security Automation with Dedicated Cyware Orchestrate Instance



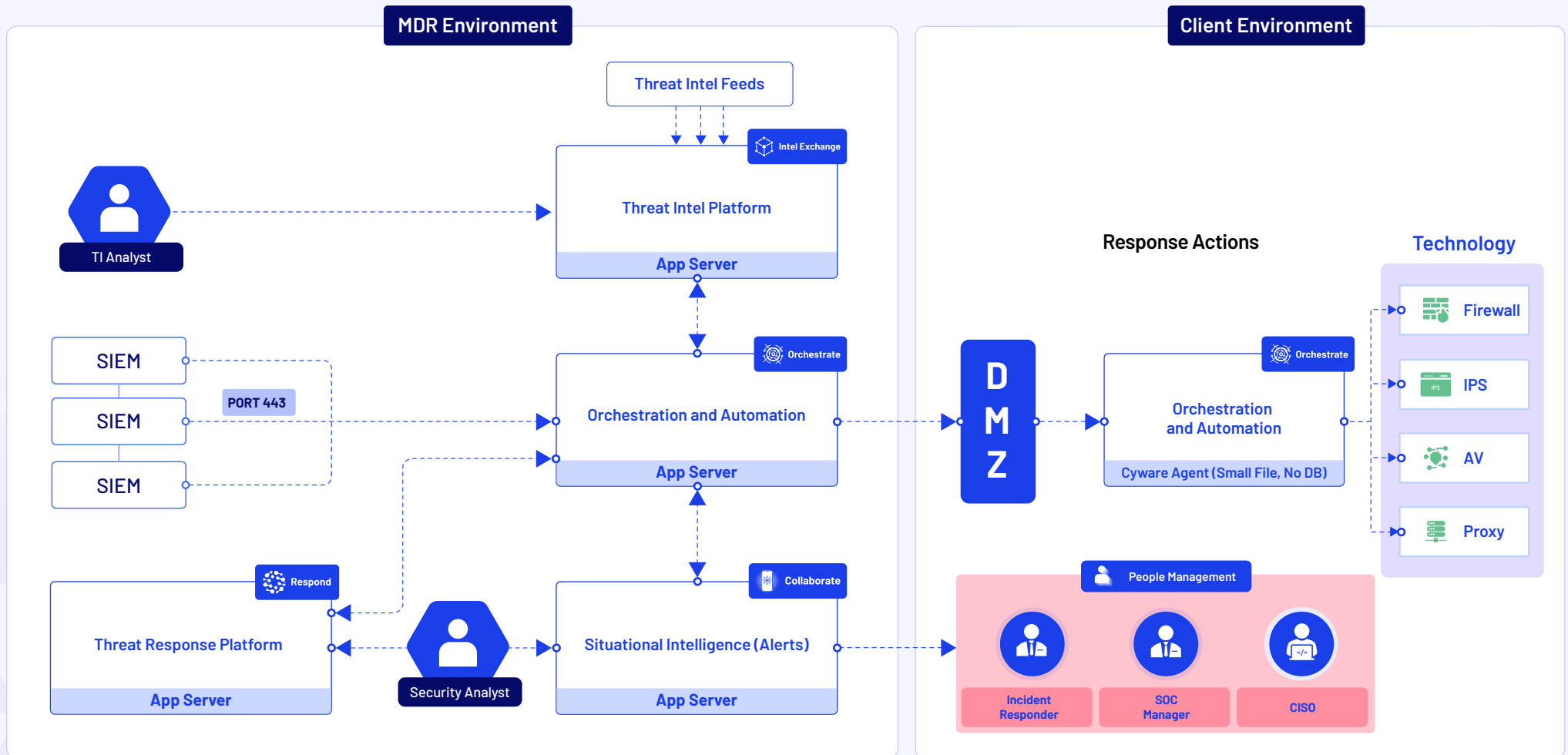
In this scenario, in addition to the benefits of Scenario 1, the customer gets access to a dedicated orchestration instance on the MSSP's environment.

Scenario 3 Security Automation with Dedicated Threat Response Instance

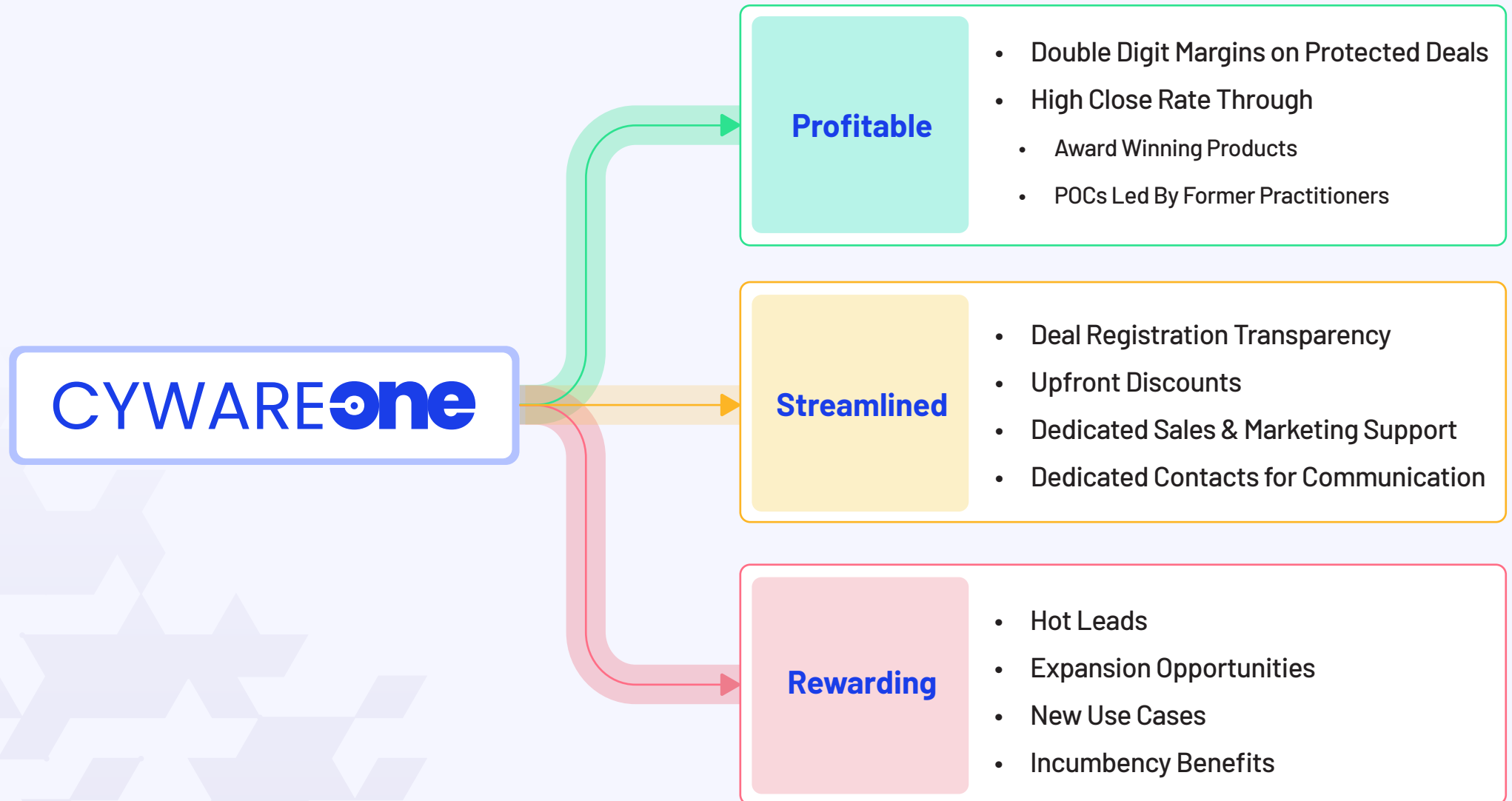


In this scenario, in addition to the benefits of Scenario 1 and 2, the customer gets access to dedicated orchestration and threat response instances on the MSSP's environment.

Scenario 4 Dedicated Orchestration and Response Service



Why Cyware One?



Benefits Of Partnering With Cyware

20% Protected Margin on Registered Deals

10% Pass Through Margin



Incumbency Protection for Partner of Record During Renewal



Expansion Opportunities with Modules



Hot Leads



How To Become A Partner And Sell Cyware

Apply

Click [here](#) if you are a Channel Business and click [here](#) if you are an MSSP.
Complete the application form and accept the terms and conditions.



Collaborate

- Contact your Cyware Channel Management Team to get introduced to the Cyware sellers in your region.
- Our expert sellers can help your team learn how to position Cyware.
- A well planned and executed account mapping will yield continued mutual success.



Sell

- Leverage the knowledge gained during Sales Enablement Sessions and Account Mappings to position Cyware with your customers and prospects.
- Once you gauge interest, engage your Cyware team immediately.
- Let our team to do the heavy lifting.



For more information you can reach us at:

111 Town Square Place Suite 1203, #4 Jersey City, NJ 07310

www.cyware.com