CYWARE™

# Cyware for Managed Security Service Providers (MSSPs)

Automate Security Monitoring and Response for Your Clients

# Current Status of Managed Security Services

The increases in technology costs and a general shortage of skilled security staff have led to more and more organizations partnering with managed security service providers (MSSPs) for handling their threat detection and response activities. However, the present framework of managed security services falls short of the demands posed by the evolving security threat landscape.

The increase in the variety of security tools and technologies deployed within client environments has made it significantly more challenging for MSSPs to optimize their services and meet their service level agreements (SLAs). An inability to fully automate the threat lifecycle process makes it difficult for MSSPs to cope with the wide variety of data coming in disparate formats from different security tools.

To combat these challenges, MSSPs are now leveraging Cyware to effectively integrate with client tools, automate threat data enrichment, and provide detailed incident investigation and response capabilities. Cyware's security solutions for MSSPs leverage advanced threat investigation, response, security automation, and notification capabilities that allow MSSPs to effectively manage security and provide more value to all their clients.

# Cyware's Solutions for Managed Security Service Providers (MSSPs)

Cyware's solutions facilitate scalable and integrated management of all client security operations. The modular platform works in an integrated manner to link threat investigation, triaging and client alerting through an efficient, automated process. The solution comes with a multi-delivery alerting mechanism and advanced automation capabilities to ensure real-time notification and alerting on security threats.

**Cyware's modular approach comprises of the following integrated platforms:**

## Cyware Situational Awareness Platform (CSAP)

An automated threat alert aggregation and information sharing platform that equips key security personnel with information to improve situational awareness and resilience.

## Cyware Threat Intelligence eXchange (CTIX)

A smart, client-server threat intelligence platform (TIP) for ingestion, enrichment, analysis, and bi-directional sharing of threat data within your client network.

## Cyware Fusion and Threat Response (CFTR)

A threat response automation platform that combines cyber fusion and automation to stay ahead of increasingly sophisticated cyber threats in real-time.

## Cyware Security Orchestration Layer (CSOL)

A universal, security orchestration gateway for executing on-demand or event-triggered tasks across deployment environments at machine speeds.

Cyware enables MSSPs to modularize the entire solution across different clients by deploying separate, integrated modules for incident response and orchestration. With Cyware, MSSPs are not required to have a full orchestration (SOAR) layer installed for all clients. Instead, MSSPs can cut down their high operational costs by deploying Cyware's lightweight and cost-effective orchestration gateway based on the client requirements.

Cyware's solutions fit perfectly into the client-centric security needs of any MSSP and they cover three critical and widely-adopted managed security scenarios.

## Scenario 1

Scenario 1 covers the threat detection and client notification use cases of the MSSPs. In this scenario, a managed security provider goes beyond just managed detection to share the role, location, and sector-based security alerts with the clients over multiple delivery channels.

## Scenario 2

Scenario 2 builds on the basic managed detection services to provide direct action taking capabilities. By connecting the client's security tools to an advanced threat response and automation platform, MSSPs can leverage real-time threat intelligence for faster and more informed threat management and response.

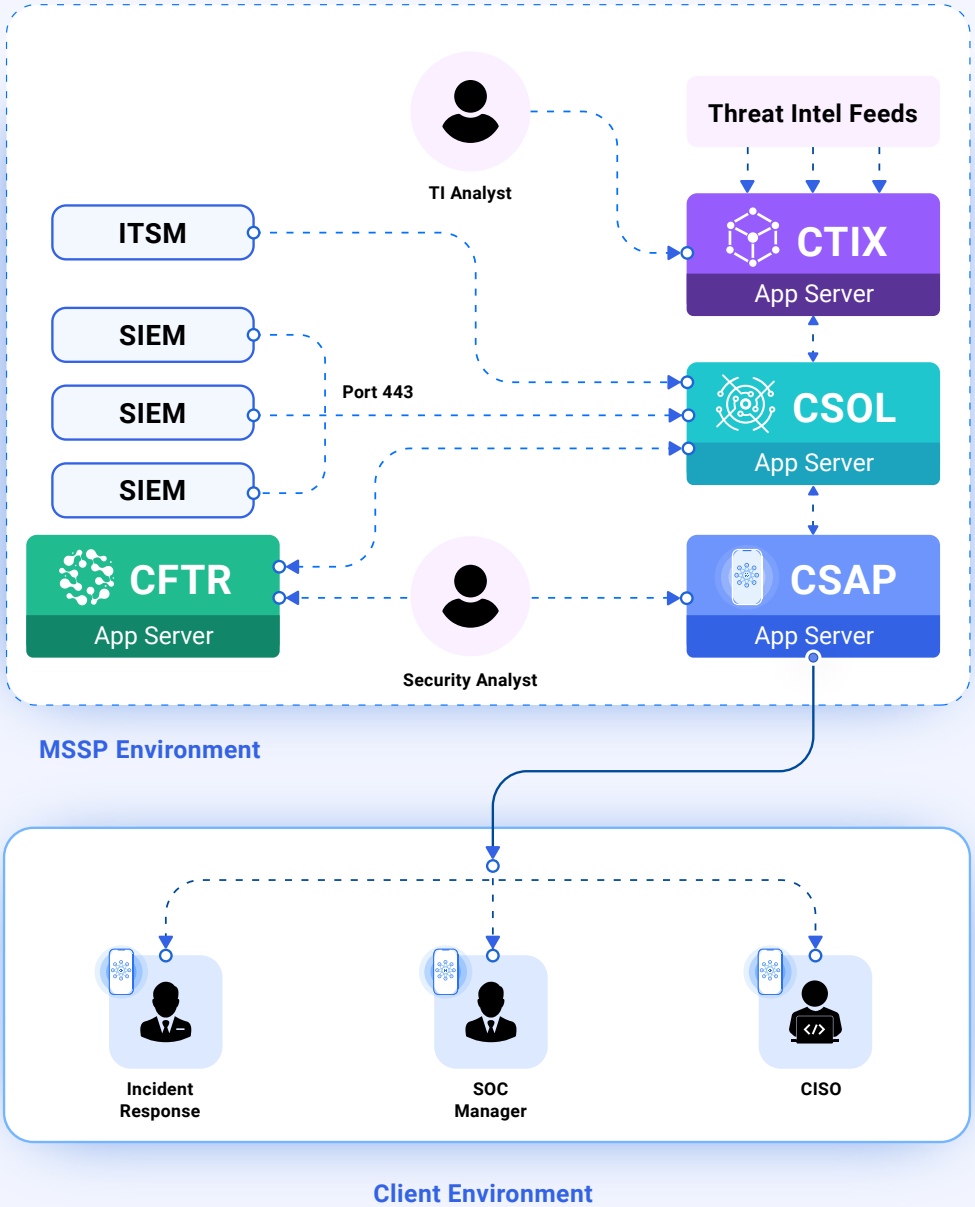
## Scenario 3

Scenario 3 covers the advanced levels of managed security services involving a large number of clients. In addition to the threat response, security automation, and threat intelligence platforms being hosted within the MSSP's environment, an additional lightweight orchestration layer is deployed within each client's environment. This lightweight integrator (size less than 20 Mb) known as CSOL Agent helps automate process workflows between the cloud applications and on-premise deployed security solutions. This allows for faster and easier orchestration of threat data from disparate security tools complemented by automation-driven actioning that strengthens an organization's defense posture and accelerates the response to cyber threats.

# Scenario 1

In Scenario 1, a managed security provider goes beyond just managed detection to share the role, location, and sector-based security alerts with the clients over multiple delivery channels. In addition to email, MSSPs can leverage Cyware Situational Awareness Platform (CSAP) as an additional interactive medium to disseminate the incident from MSSP to clients to enable efficient bi-directional communication. With Cyware, MSSPs can automate the entire threat detection workflow. Cyware Security Orchestration Layer (CSOL) is an advanced security automation tool that orchestrates the collection of threat data from SIEM and ITSM tools deployed in the MSSP environment. CSOL also connects with Cyware Fusion and Threat Response Platform (CFTR) to deliver automated alert triaging at machine speeds thereby eliminating the entire manual effort and reducing the overall costs for MSSPs.

**Served Client Base: Tier 0: Small size: No Orchestration: Narrow technology landscape**
MSSP clients who do not requireany direct orchestration and want to receive notification for any incident/alert and act on it on their own.



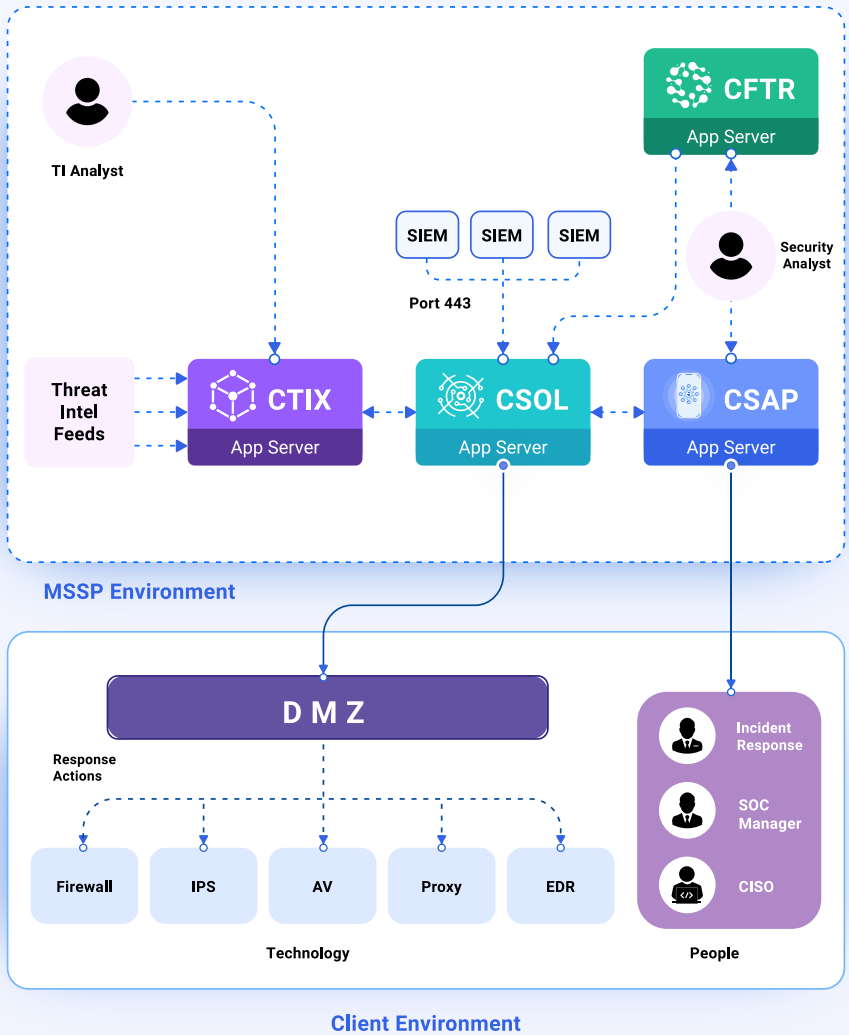
# Scenario 1:
# Use Cases and Benefits for MSSPs

1. Manage Detection Services with Automation
2. Share Alerts with Clients in Real-Time (<30 seconds)
3. Acknowledge Alerts and Assign Actions
4. Share Early Warning Threat Levels with Clients
5. Enrich Threat Intelligence from Trusted Sources
6. Enable Clients to Share Advisories / Threat Intelligence with MSSP
7. Foster Discussion-Driven Collaboration between Clients
8. Threat Data Knowledge Sharing Between MSSP Clients

# Scenario 2

Scenario 2 goes beyond the basic managed detection services to provide direct action taking capabilities in the client's security tools to the MSSPs by hosting an advanced threat response and automation platform in the MSSP's environment. **Cyware's Fusion** and **Threat Response Platform (CFTR)** offers advanced levels of incident investigation, triaging, and workflow management capabilities for MSSPs. With **CFTR**, MSSPs can streamline post-detection and incident triaging, followed by data enhancement, incident correlation, and intel enrichment processes. MSSPs can also leverage several key metrics within **CFTR** including average incident cost, cost per incident type, the average cost per analyst, etc. to quantify incident costs across the line of clients. With Cyware, MSSPs can use the automation and orchestration capabilities of **Cyware Security Orchestration Layer (CSOL)** to take direct actions in the security tools, including firewall, IDS/IPS, EDR, etc. deployed in the client's environment to proactively block malicious threats.

**Served Client Base: Tier 1: Medium size: No Orchestration: Well Developed Technology Landscape**
MSSP clients who want to orchestrate security tools deployed in the client environment that can be managed through an orchestration layer deployed in the MSSP environment. This enables MSSPs to take direct response action in their environment while also separately receiving threat and incident alerts for their clients.



# Scenario 2:
# Use Cases and Benefits for MSSPs

**Note:** In addition to the ones listed below, this scenario includes all the use cases and benefits from Scenario 1.

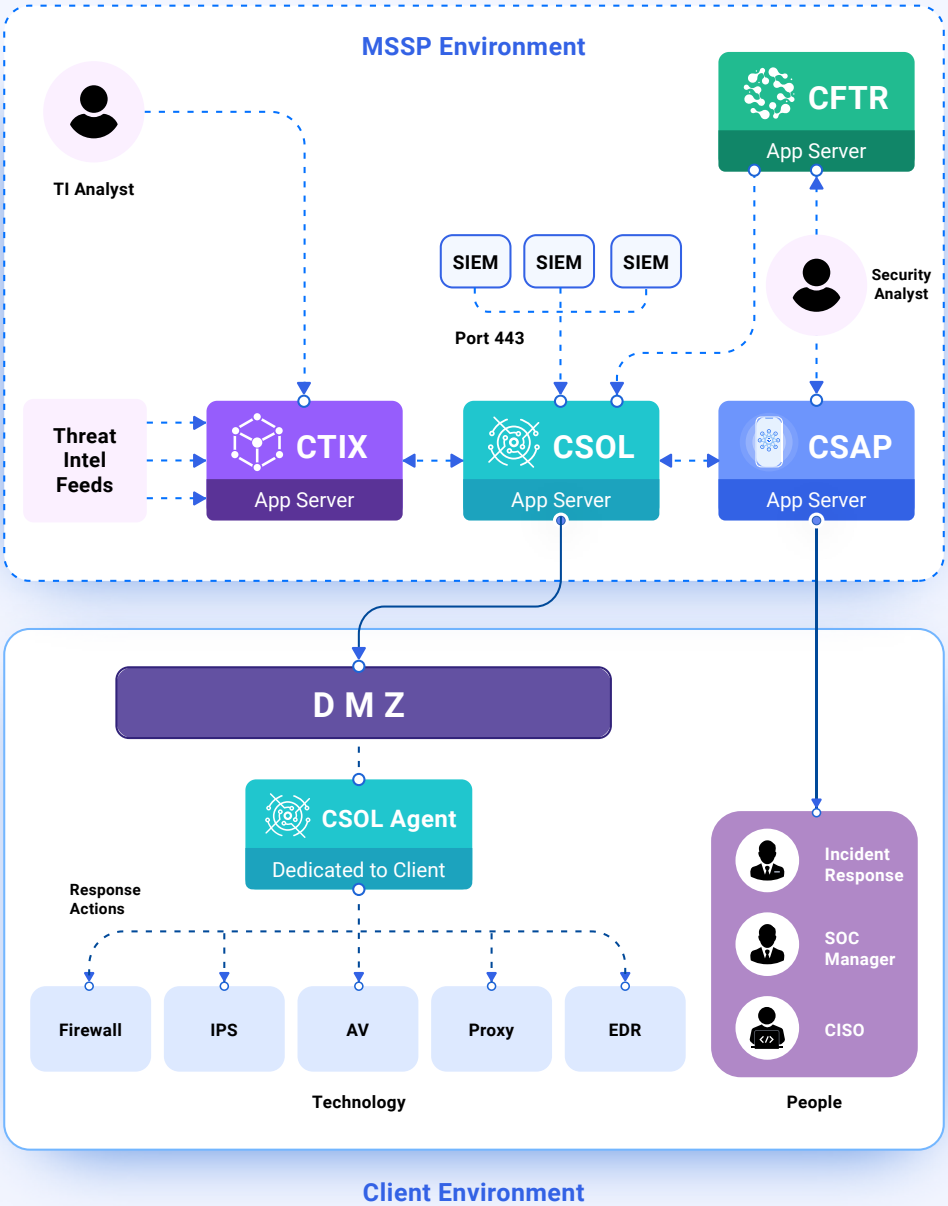
1. Automate Incident Investigation, Triaging & Response
2. Reduce Client Incident Costs through Effective Tracking & Metrics
3. Take Actions Directly within the Client's Environment
4. Reduce Response Times with Unlimited Brand-Agnostic Playbooks

# Scenario 3

Scenario 3 covers the advanced levels of managed security services involving a large number of clients. In addition to the threat response, security automation, and threat intelligence platforms being hosted within the MSSP's environment, an additional lightweight orchestration layer called **CSOL Agent** is deployed within each client's environment for faster and easier orchestration of threat data from on-premise deployed security tools. The **CSOL Agent** facilitates the orchestration of threat data to MSSP's environment for managing detection, notification, investigation, and response tasks. The dedicated orchestration layer in each client's deployment environment makes incident triaging, threat data correlation, and automated actioning precise and relevant to each client.

**Served Client Base: Tier 2: Large size: No Orchestration: Wide Technology landscape**

MSSP clients who want to deploy a dedicated orchestration layer in the client environment to orchestrate threat data from their disparate security tools. This is done using CSOL Agent, a lightweight integrator, with a size less than 20 Mb, that enables MSSPs to take direct response action in their environment while also separately receiving threat and incident alerts.



# Scenario 3:
# Use Cases and Benefits for MSSPs

**Note:** In addition to the ones listed below, this scenario includes all the use cases and benefits from Scenario 1 and Scenario 2.

1. Foster Collaboration through Cyber Fusion
2. Connect-the-dots between Security Threats
3. Deploy a Dedicated Automation Layer within the Client's Environment
4. Enable Cross-Environment Automation without Exposing On-Premise Networks

# An Essential Overview

| Capability | Scenario 1 | Scenario 2 | Scenario 3 |
|---|---|---|---|
| Manage detection services with automation | ✓ | ✓ | ✓ |
| Share alerts with clients in real-time (<30 seconds) | ✓ | ✓ | ✓ |
| Acknowledge alerts and assign actions | ✓ | ✓ | ✓ |
| Share early warning threat levels with clients | ✓ | ✓ | ✓ |
| Enrich threat intelligence from trusted sources | ✓ | ✓ | ✓ |
| Enable clients to share advisories/threat intelligence with MSSP | ✓ | ✓ | ✓ |
| Foster discussion-driven collaboration between clients | ✓ | ✓ | ✓ |
| Threat data knowledge sharing between MSSP clients | ✓ | ✓ | ✓ |
| Multiple alerting and notification channels | ✓ | ✓ | ✓ |
| Automate incident investigation, triaging, & response | — | ✓ | ✓ |
| Reduce client incident costs through effective tracking & metrics | — | ✓ | ✓ |
| Take actions directly within the client's environment | — | ✓ | ✓ |
| Reduce response times with unlimited brand-agnostic playbooks | — | ✓ | ✓ |
| Foster collaboration through cyber fusion | — | — | ✓ |
| Connect-the-dots between security threats | — | — | ✓ |
| Deploy a dedicated automation layer within the client's environment | — | — | ✓ |
| Enable cross-environment automation without exposing on-premise networks | — | — | ✓ |

**Email us at sales@cyware.com to get started.**

CYWARE™

228 Park Ave S #77147 New York,
New York 10003-1502

cyware.com | sales@cyware.com

855-MY-CYWARE