CYWARE

Cyware for Enterprise

Adopt next-gen security with threat intelligence analysis, security automation, and threat response.

Current Status of Security Threat Landscape

An increase in sophisticated cyberattacks has exposed the weaknesses of the obsolete security strategies used by enterprises worldwide. Enterprises are struggling to keep up with the pace of cyber threats. The deployment of numerous disparate security tools has made it difficult for enterprises to operationalize threat intelligence and make sense of a deluge of threat alerts. Security operations are siloed, skewed, and asymmetric, rendering incident response incomplete and ineffective. Enterprises need to move away from a reactive approach to a more proactive, collaborative, and intelligence-driven security strategy.

A Paradigm Shift Towards Cyber Fusion

Cyware's cyber fusion-powered modular approach to threat intelligence, security automation, and threat response offers an innovative approach to tackle these problems. Enterprises of all sizes have now adopted Cyware's solutions to aggregate and analyze threat intelligence from multiple internal and external sources, operationalize it through orchestration and automation playbooks, and bring together all internal security teams on a common cyber fusion-powered platform to deliver a comprehensive threat response. Cyware's solutions enable enterprises to move beyond their traditional boundaries of security operations and collaborate with their vendors, information sharing communities (ISACs/ISAOs), and other third-party entities for synergizing their strengths and protecting their extended security perimeter.

Cyware's Solution for Enterprises

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

CSAP

Cyware Situational Awareness Platform

Automated threat alert aggregation and information sharing platform

CTIX

Cyware Threat Intelligence eXchange

Intelligent bi-directional TIP that automates intelligence collection, analysis, and sharing

CFTR

Cyware Fusion & Threat Response

A threat response automation platform that combines cyber fusion and incident management

CSOL

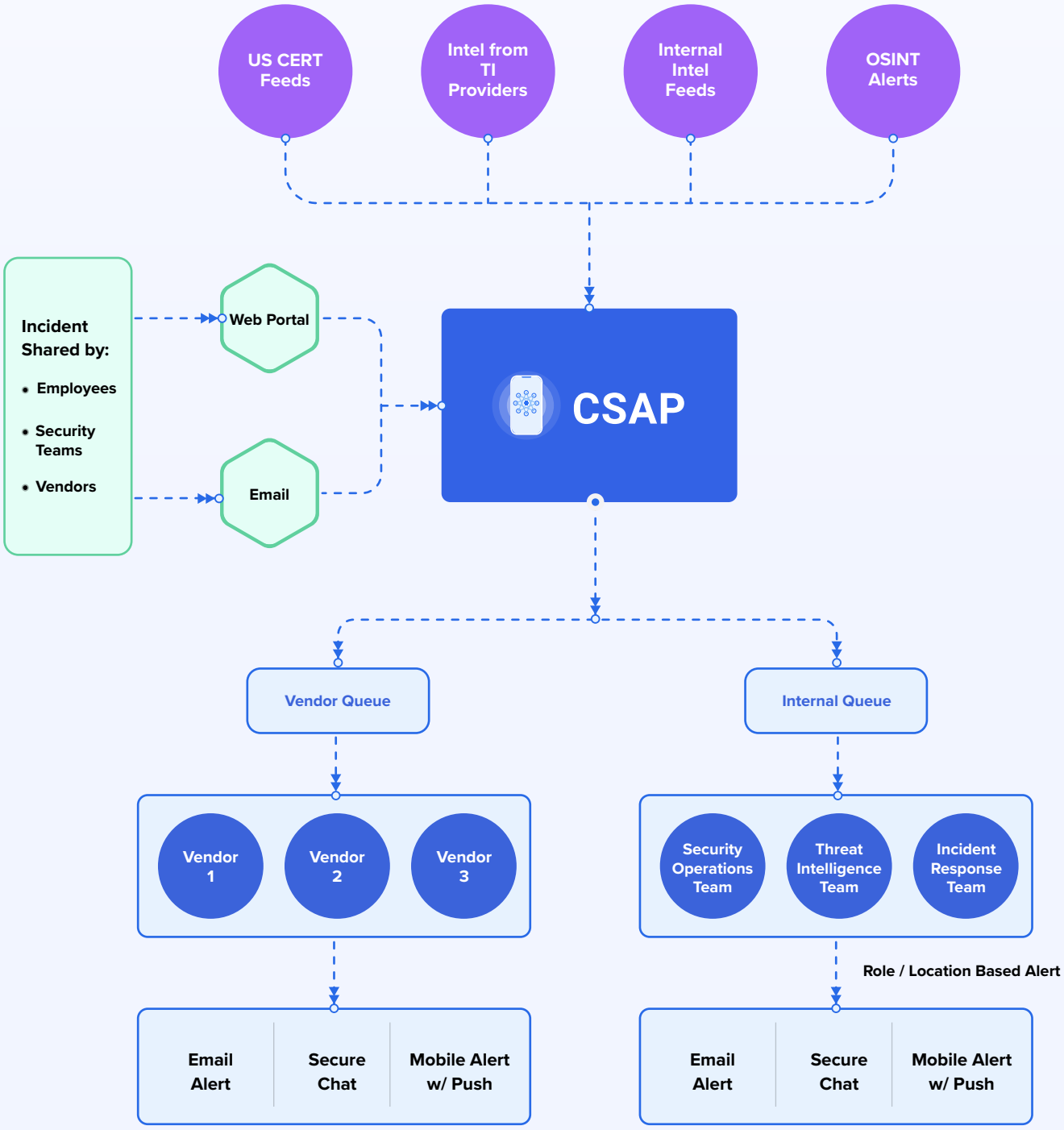
Cyware Security Orchestration Gateway

A universal, security orchestration gateway for executing automated playbooks

Cyware's solutions fit perfectly into the next-generation security needs of enterprises and they cover four critical and widely-adopted security scenarios.

Scenario 1: Strategic Intel Sharing and Alerting Model for Enterprises

In this scenario, enterprises are collecting strategic threat intelligence and security alerts from several internal and external sources including internal intel feeds, commercial TI providers, CERTs, OSINT alerts, and intel submissions from employees, security teams, and vendors with whom they share information. The security alerts are analyzed and shared as human-readable alerts over the **Cyware Situational Awareness Platform (CSAP)** web portal, mobile app, and email with all stakeholders based on their role, location, and business alignment.

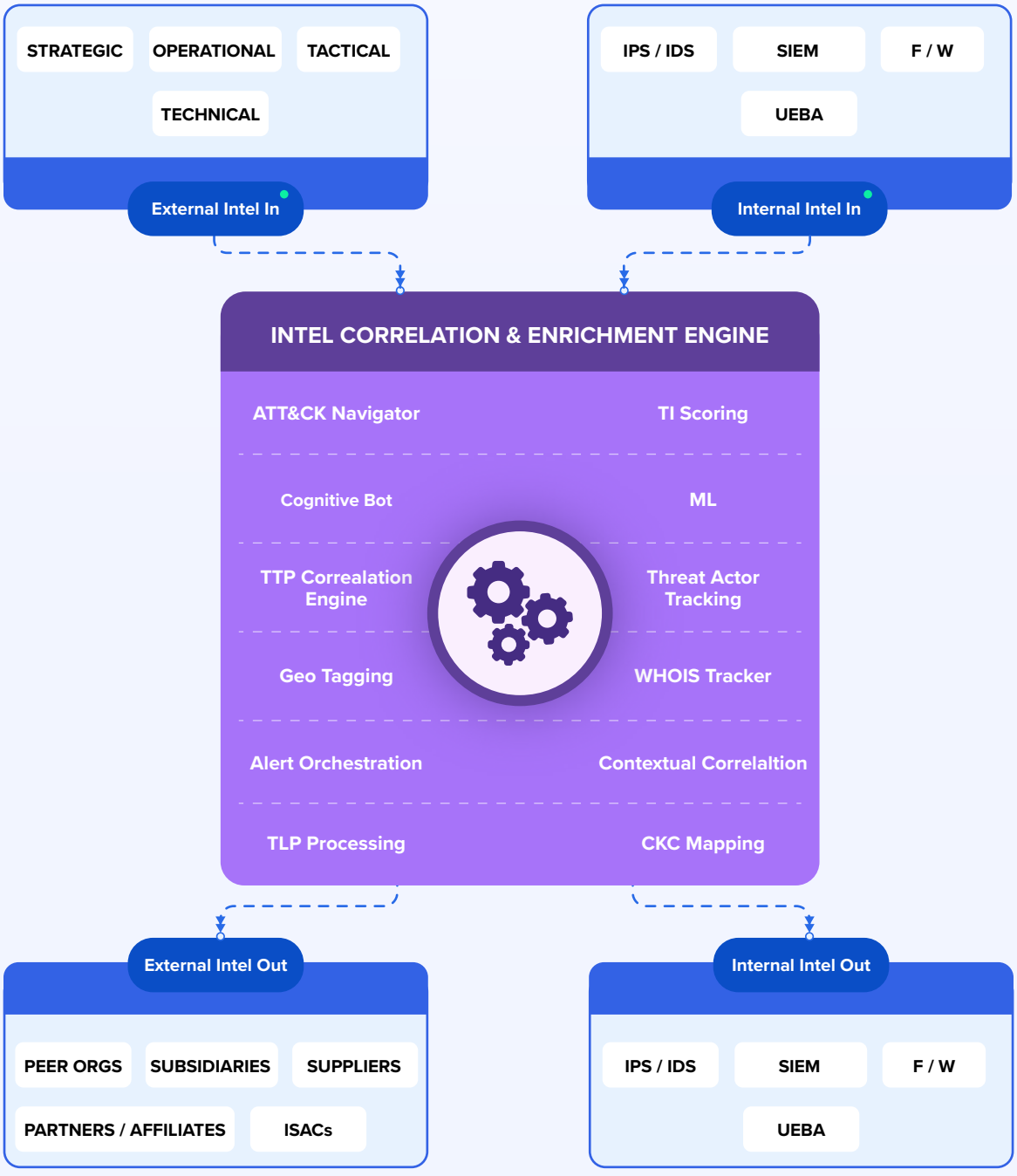


Scenario 1:
Use Cases and Benefits

1. Aggregate Threat Alerts and Strategic Intel from Security Tools and External Sources
2. Enable Security Teams and Vendors to Share Threat Intelligence
3. Alert Security Teams and Vendors in Real-Time (<30 seconds)
4. Foster Discussion-Driven Collaboration within Security Teams
5. Indicate Early Warning Threat Levels to Security Teams and Vendors

Scenario 2: Technical Threat Intelligence Automation Model for Enterprises

In this scenario, enterprises are involved in collecting technical threat intelligence including threat indicators of compromise from several external and internal sources. The structured and unstructured threat data is automatically ingested and normalized using the **Cyware Threat Intelligence eXchange (CTIX)** platform in a format-agnostic manner. The normalization process is followed by automated enrichment and analysis before updating it automatically in internal security tools including firewalls, EDR, IDS/IPS, etc., or sharing ahead with industry peers and vendors as STIX collections.

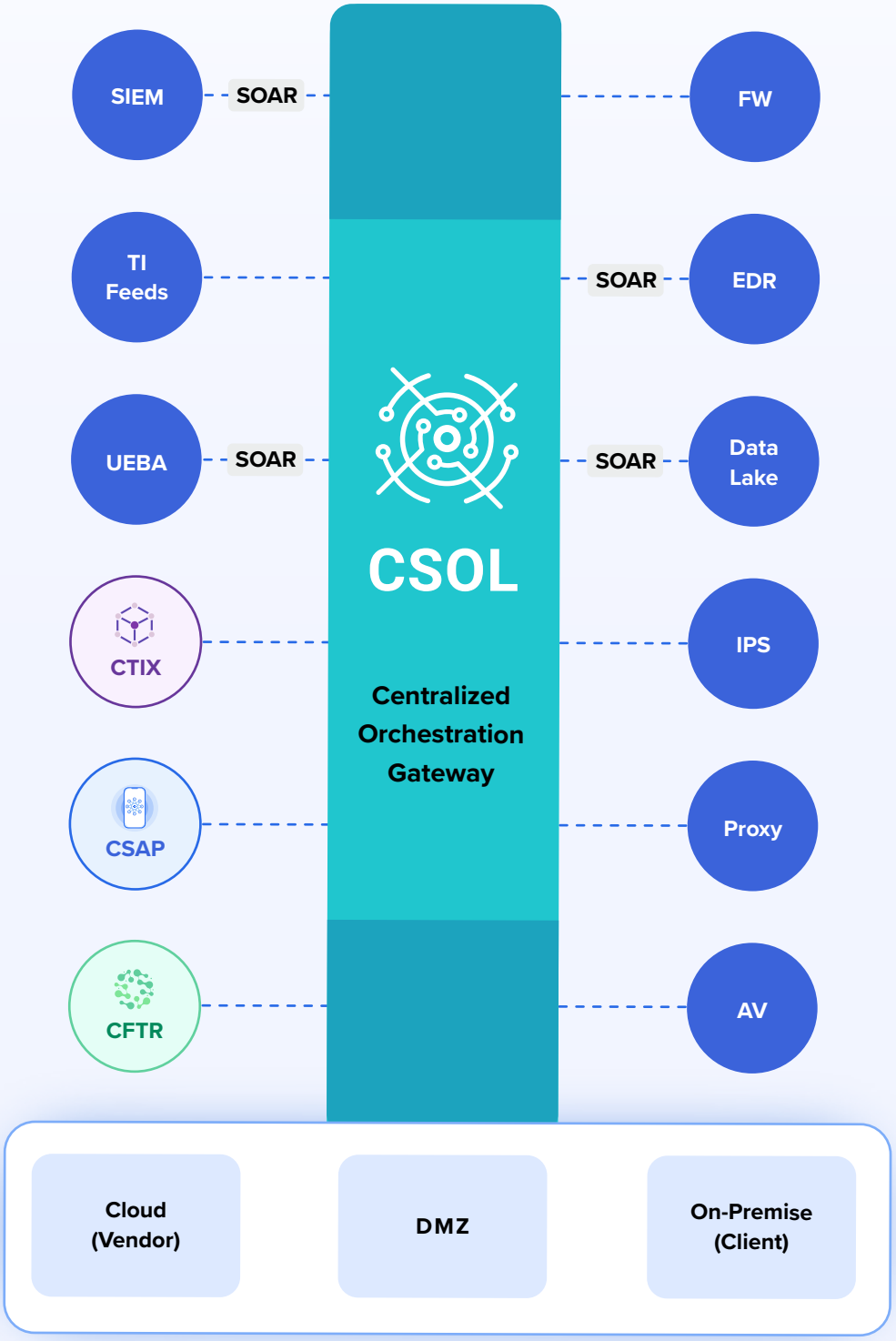


Scenario 2:
Use Cases and Benefits

1. Ingest Technical Intelligence including IOCs from Multiple Sources
2. Normalize Structured and Unstructured Intelligence
3. Automatically Enrich and Analyze Threat Intelligence
4. Automatically Update Enriched and Analyzed Threat Data in Security Tools
5. Validate Intel through Fully Configurable Automated Confidence Scoring
6. Share STIX-based Intel Collections with Industry Peers and Vendors

Scenario 3: Security Orchestration Gateway Model for Enterprises

In this scenario, enterprises are increasing efficiency and effectiveness by running orchestration playbooks to automate processes and workflows using the **Cyware Security Orchestration Layer (CSOL).** The scenario involves enterprises orchestrating threat data using a single orchestration layer that connects to all of their deployed security tools.

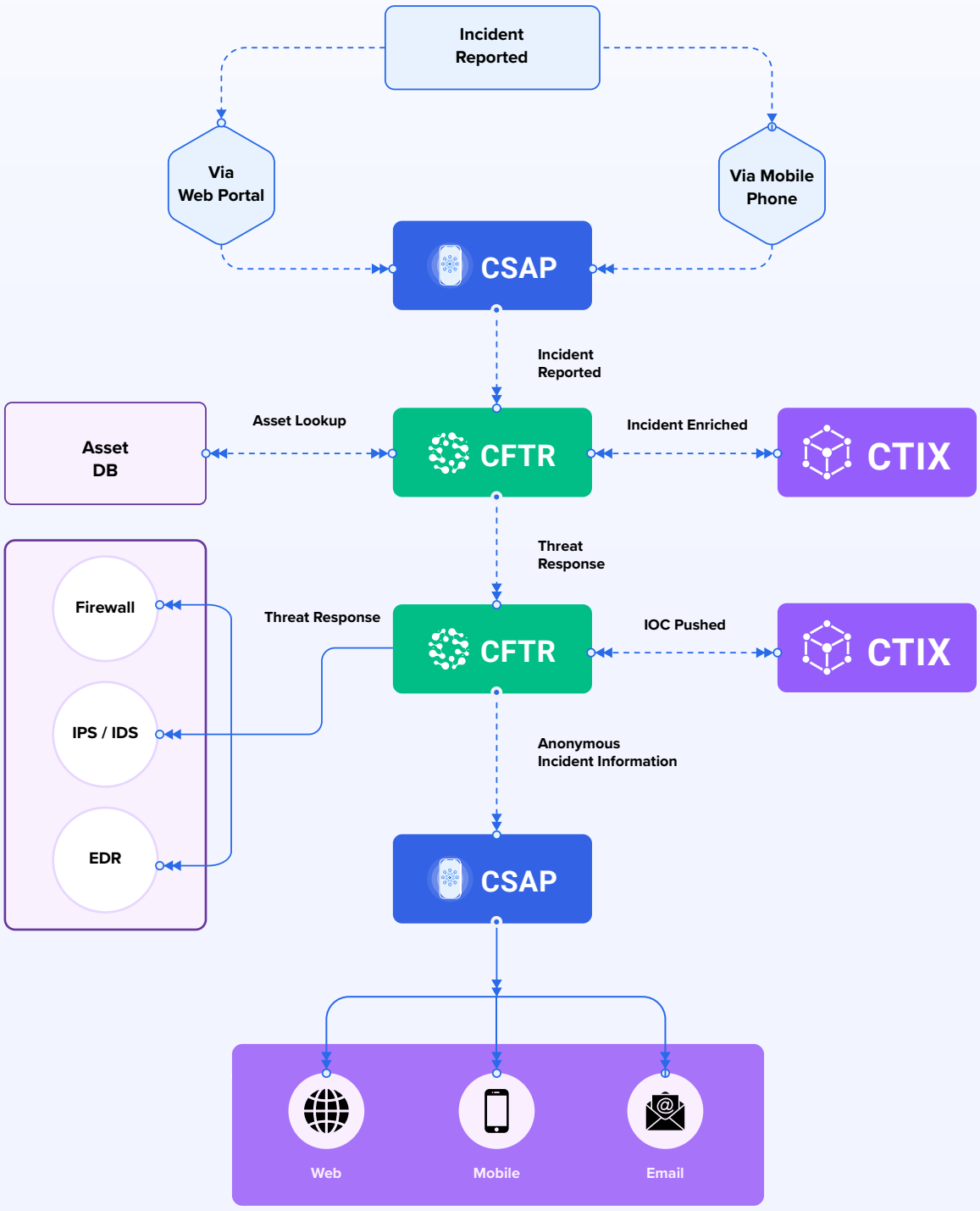


Scenario 3:
Use Cases and Benefits

1. Centralize Your Playbook Creation with Security Automation Gateway
2. Orchestrate Security Tools Deployed within Internal Perimeter and on External Cloud
3. Leverage Unlimited Pre-Built and Custom Playbooks
4. Automate Manual Security Processes, Procedures, and Workflows
5. Create Custom Connectors and Actions

Scenario 4: Threat Response Automation Model for Enterprises

In this scenario, enterprises are automating incident and threat response workflows using the **Cyware Fusion and Threat Response (CFTR)** platform. The scenario also includes enterprises leveraging the cyber fusion capabilities of the CFTR platform to bring together all internal security teams on a common platform to deliver a comprehensive, intelligence-driven, and collaborative response.



Scenario 4:
Use Cases and Benefits

1. Automate Case and Workflow Management Processes
2. Automate Incident Investigation, Triaging, & Response
3. Respond to Malware, Vulnerabilities, Threat Actors, and Incidents
4. Draw Contextual Intelligence by Connecting-the-Dots between Security Threats
5. Reduce Incident Costs through Effective Tracking & Metrics
6. Foster Collaboration between Security Teams through Cyber Fusion

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

1460 Broadway
New York, NY 10036

cyware.com | sales@cyware.com

855-MY-CYWARE