CYWARE™

Cyware for Information Sharing Communities

Anticipate, prevent, and respond to threats through bi-directional threat intelligence sharing and automation solutions for ISACs and ISAOs.

Current Status of Threat Intelligence Sharing in ISACs/ISAOs

The current security threat landscape has transformed the manner in which organizations are preparing and responding to security threats. More and more organizations are now joining threat information sharing communities such as **Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs)** to engage in bi-directional sharing of real-time threat intelligence against prevailing security threats.

Hundreds and thousands of cyberattacks carried out on a daily basis against the member organizations of these sharing communities are now putting immense pressure on their outdated threat information sharing solutions. Several large ISACs and ISAOs are now leveraging **Cyware** to outmaneuver security threats targeting their industries by sharing relevant and actionable threat intelligence with their member organizations in real-time.

Cyware's security solution leverages advanced, next-generation capabilities for real-time alerting and automated threat intelligence sharing to deliver a state-of-the-art information-sharing capability. Cyware has helped ISACs and ISAOs reduce the time it takes to ingest, enrich, and disseminate intel by as much as 98% while also seeing significant increases in the level of member collaboration.

Cyware's Solution for Sharing Communities (ISACs/ISAOs)

Cyware's threat intelligence sharing platforms - **Cyware Situational Awareness Platform (CSAP)** and **Cyware Threat Intelligence eXchange (CTIX)** leverage a "Hub and Spoke" model of information sharing to facilitate closer collaboration between ISACs/ISAOs and their member organizations. The two modular platforms can work together as an integrated solution to enable multi-source threat intelligence collection and bi-directional sharing between the member organizations. The solution comes with a multi-delivery alerting mechanism and advanced automation capabilities to ensure real-time actioning on security threats.

The solution fits perfectly into the intelligence sharing needs of ISACs and ISAOs. It covers two critical and widely-adopted information sharing scenarios of ISACs and ISAOs.

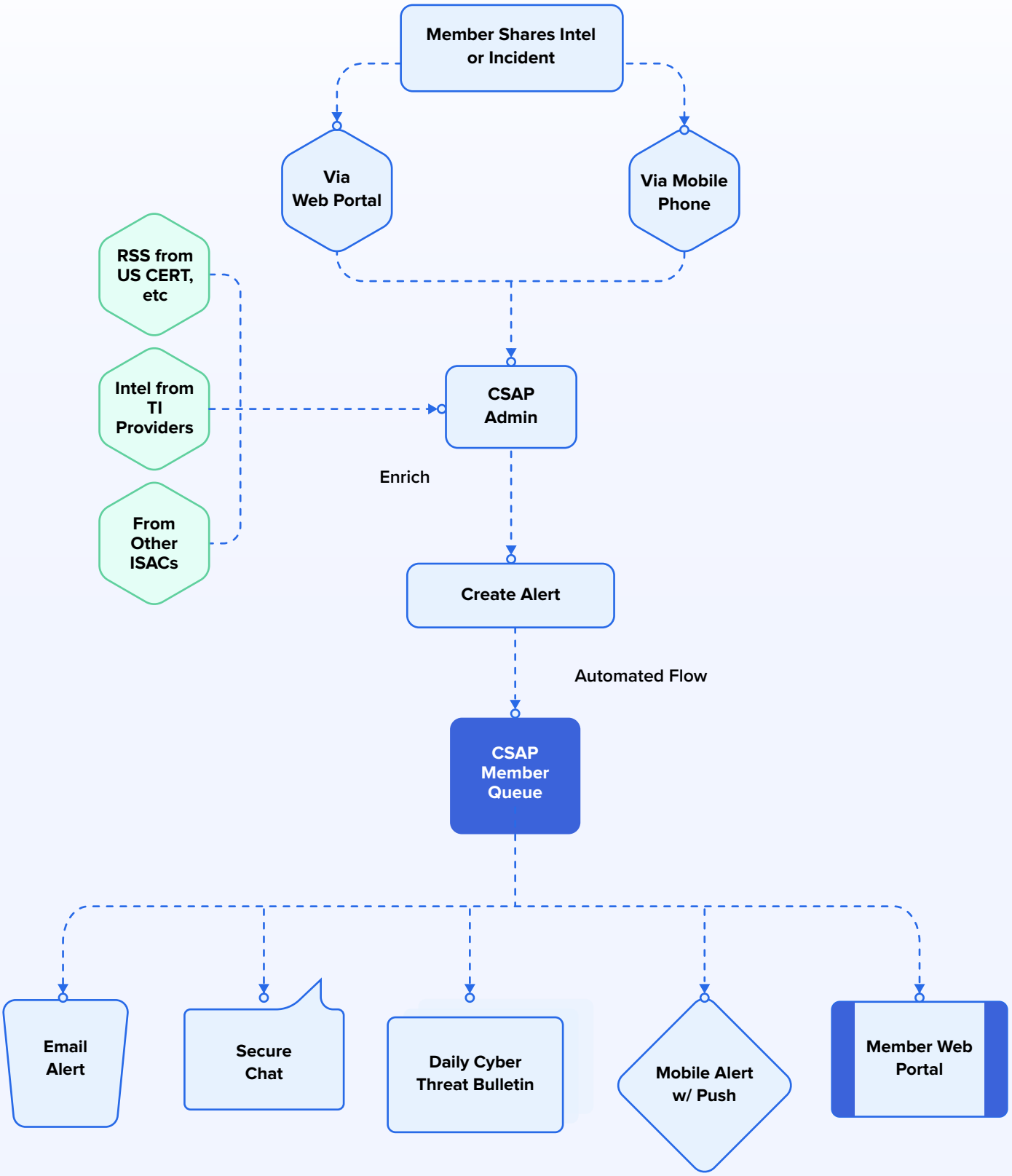
Scenario 1

This scenario is when information sharing in the ISAC/ISAO is largely focussed on the human-readable and manually shareable macro intelligence including indicators of compromise (IOCs), malware alerts, vulnerability advisories, security incidents, phishing, and spear-phishing attacks. This enables the ISAC/ISAO and their members to collect, share, and provide alerts from high-level information on the changing threat and risk landscape along with intelligence on specific attacks.

Scenario 2

This scenario is when information sharing in the ISAC/ISAO is fully automated and extends to include highly technical intelligence from additional external sources that can be operationalized. This includes multi-source intel collection, enrichment, analysis and bi-directional sharing of STIX-collections of threat indicators of compromise (IOCs), tactics and techniques (TTPs), kill chain mappings, exploitability mappings, artifacts, and logs with member organizations.
This allows for curation and enrichment of threat information that leads to more relevant and actionable intelligence.

Scenario 1: Strategic Threat Intelligence Sharing and Alerting Model for ISACs/ISAOs



Note: This model assumes that ISAC/ISAO member organizations do not have a pre-deployed threat intelligence platform.

Scenario 1: Strategic Threat Intelligence Sharing and Alerting Use Cases and Benefits for ISACs/ISAOs

1 Collect Member-Shared Strategic Threat Intelligence

Cyware's advanced threat intelligence sharing solution allows ISACs/ISAOs to collect threat intelligence on malware, phishing attacks, security incident information, etc. from their members. Member organizations can share threat intelligence anonymously or with due attribution, with their central ISAC/ISAO hub or directly with other member organizations without ISAC/ISAO analyst intervention using the **Cyware Situational Awareness Platform (CSAP).** The platform comes with multi-modal sharing channels including an advanced web portal, mobile app, and an email integration feature. Members can leverage the pre-configured TLP-based threat intelligence sharing templates in the web portal and the mobile app to share all relevant details in a detailed and structured format

2 Expand Scope by Collecting and Sharing Macro Intel

The multi-source threat intelligence ingestion capabilities of **Cyware Situational Awareness Platform (CSAP)** enables ISACs/ISAOs to expand their scope of intel sharing by collecting and sharing all types of macro intel including Cyware's premium strategic threat intelligence feed, regulatory alerts, finished intel reports, threat research reports, malware advisories, vulnerability reports, threat bulletins, and RSS feeds from national CERTs, commercial threat intelligence providers, open-source feeds, and other sharing communities. ISACs/ISAOs can create exclusive channels to ingest threat intelligence from these sources for focused automation-driven analysis and enrichment before sharing it with their members

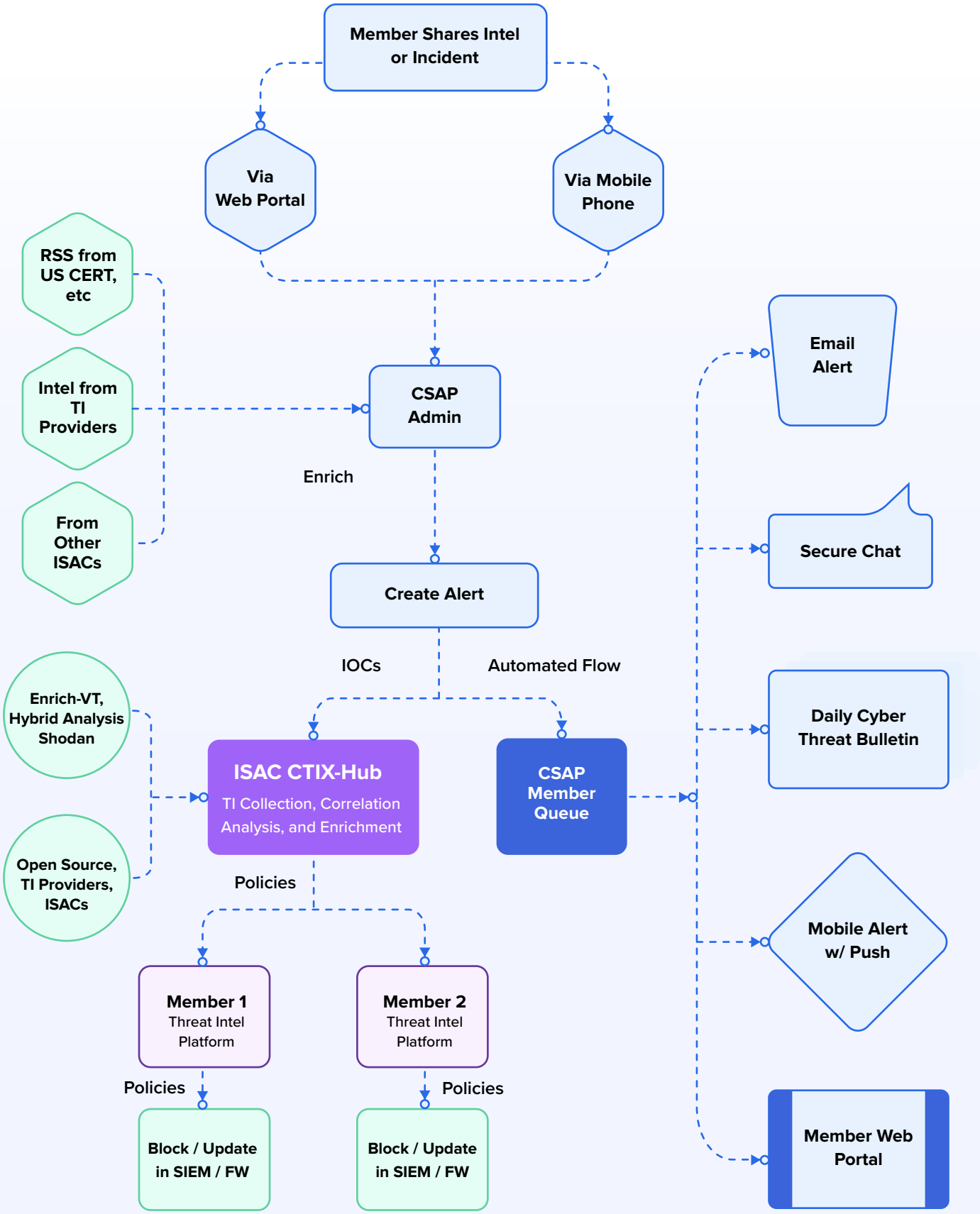
3 Alert Members in Real-Time (<30 seconds)

The underpinning of any threat intelligence sharing program is the ability to create actionable insights for member organizations to proactively act against security threats. With **Cyware Situational Awareness Platform (CSAP)**, ISACs/ISAOs can execute their collaboration-driven mission of sharing automated real-time alerts with their members based on their role, sector, and location. The alerting mechanism comes with a member-rating feature allowing members to provide feedback to the ISAC/ISAO hubs on the relevance and quality of each alert, making information sharing a calibrated and two-way interactive process for improved outcomes. Members who do not have a threat intelligence platform can receive threat indicators in CSV, XML and JSON formats.

4 Foster Discussion-Driven Collaboration with Members

Cyware's solution takes threat intelligence sharing to an altogether different level by delivering the discussion-driven collaboration capability to ISACs/ISAOs. Members can leverage a built-in, secure and encrypted messenger to directly initiate group-level or one-on-one direct discussions on threat alerts for brainstorming issues, outlining new sectoral threats and sharing learnings and mitigations. The solution also comes with an integrated and centralized document storage feature that ISACs/ISAOs can use for sharing threat response manuals, standard operating procedures, and other value-driven documents/handbooks with members for quick referencing and actioning.

Scenario 2: Technical Threat Intelligence Automation & Sharing Model for ISACs/ISAOs



Note: This model assumes that some ISAC/ISAO member organizations have a pre-deployed threat intelligence platform.

Scenario 2: Technical Threat Intelligence Automation and Sharing Use Cases and Benefits for ISACs/ISAOs

1 Enable Members To Share Custom Threat Indicators of Compromise (IOCs)

Cyware's threat intelligence solution allows ISAC/ISAO member organizations to share malicious threat indicators (IOCs) using a web portal and mobile app. The portal and mobile app come with pre-configured templates allowing members to share standard and sector-specific custom threat indicators in a detailed and structured format. The multi-modal sharing capability allows members to share indicators manually or leverage automation capability to parse threat indicators from any source URL with just one click. Alternatively, members can also integrate their email inbox with the solution and use email as an additional means of sharing threat indicators.

2 Ingest Micro Threat Intelligence from Trusted External Sources

The multi-source threat intelligence ingestion capabilities of **Cyware Threat Intelligence eXchange (CTIX)** enables ISACs/ISAOs to collect micro threat intelligence including indicators of compromise (IOCs), tactics and techniques (TTPs), exploit alerts, kill chain mapping, and ATT&CK mapping in machine-readable (STIX / TAXII) formats from several trusted external sources. With Cyware, ISACs/ISAOs can collect technical threat intelligence from commercial threat intelligence providers, CERTs, OSINT data sources, and other sharing communities. Cyware's solution also comes with MITRE ATT&CK Navigator allowing ISACs/ISAOs to map threat actor tactics and techniques against reported incidents to identify threats prevalent in their sector.

3 Normalize Structured and Unstructured Intel in Multiple Formats

ISAC/ISAO hubs can ingest threat intelligence from members and external sources in a format-agnostic manner without relying on manual effort for normalization. Cyware provides format-agnostic threat intelligence sharing capabilities with support for widely used standards such as STIX 1.x, STIX 2.0, MAEC, CSV, XML, PDF, YARA, Cybox, OpenIOC, MISP, etc. Cyware's threat intelligence solutions come with support for both structured and unstructured data handling and threat intelligence ingestion allowing the collection of threat intelligence also from the email. This means that any form of intelligence can be leveraged and operationalized by ISAC/ISACO member organizations.

4 Automatically Enrich, Analyze, and Share IOCs without Direct User Involvement

Cyware's solution allows ISACs/ISAOs to utilize the integrated capabilities of **Cyware Situational Awareness Platform (CSAP)** and **Cyware Threat Intelligence eXchange (CTIX)** to extract threat indicators (IOCs) from member-shared intel, automatically enrich it from trusted sources including Shodan, HybridAnalysis, VirusTotal, WHOIS, etc without any manual effort. In addition to sharing indicator-rich threat alerts with members on their web portal, mobile app, and emails, the ISAC/ISAO hubs can push enriched and analyzed intel feed STIX-collections to member organizations and leverage an advanced rule engine to automate mundane actions and speed up triage management. ISAC/ISAO hubs can leverage **Cyware Threat Intelligence eXchange (CTIX)** to share malicious emails, domains, hashes, IP addresses, artifacts and logs with member organizations. Members with pre-deployed TAXII-based threatintelligence platforms (TIPs) can receive enriched threat intelligence as a STIX collection which they can automatically feed into their security tools such as SIEM, firewalls, etc.

5

Validate Intel through Fully Configurable Automated Confidence Scoring

ISAC/ISAO member organizations can prioritize threat response with greater accuracy by identifying potential threats through confidence scoring-driven intel validation. ISAC/ISAO hubs can cross-correlate the malicious indicators with threat sightings by the member organizations to effectively calculate the risk posed by threats to the entire sector.

The analyzed and validated indicator is then shared with the member organizations who can automatically disseminate information to their deployed security tools such as firewalls and IDS/IPS systems to preempt any malicious intrusions by proactively blocking potential threats.

An Essential Overview

Capability	Scenario 1: Strategic Threat Intel Sharing Model	Scenario 2: Technical Threat Intel Automation & Sharing Model
Collect member-shared strategic threat intelligence	✓	✓
Expand scope by collecting and sharing macro intel	✓	✓
Alert members in real-time (<30 seconds)	✓	✓
Foster discussion-driven collaboration with members	✓	✓
Leverage multiple delivery channels (mobile app, web portal, and email) for seamless information sharing	✓	✓
Enable members to share custom threat indicators of compromise (IOCs)	—	✓
Ingest micro threat intelligence from trusted external sources	—	✓
Normalize structured and unstructured intel in multiple formats	—	✓
Automatically enrich, analyze, and share IOCs without direct user involvement	—	✓
Validate intel through fully configurable automated confidence scoring	—	✓

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