CYWARE™

Collective Defense Intelligence Hub for State and Local Government

Powering a Whole-of-State Intel Sharing, Collaboration, and Actioning Ecosystem

Elevate the protection of state critical infrastructure with a whole-of-state collective defense intelligence hub that enables cybersecurity collaboration across public sector governments and private sector enterprises. The Cyware Threat Intelligence Hub serves as the central operational engine, enabling states to aggregate threat data, streamline multi-party communications, and orchestrate a synchronized, whole-of-state defense network that empowers every community stakeholder to respond to threats faster.

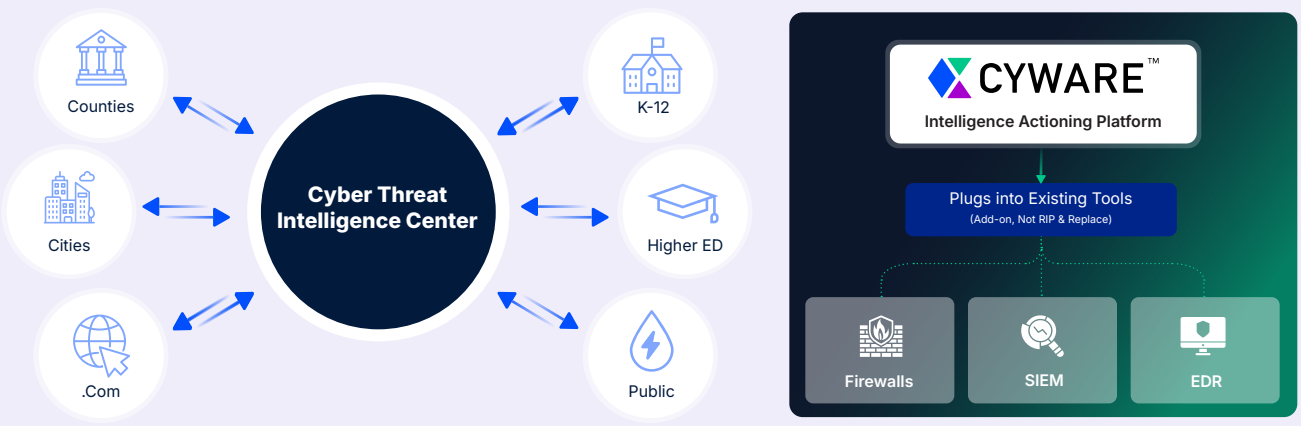
The Mission: A Whole-of-State Collective Cyber Defense

Establishing a strong central cybersecurity foundation is a critical first step for any state. A crucial first step is establishing a central threat intelligence hub foundation that extends statewide, empowering a collective defense ecosystem for every stakeholder from the most sophisticated state agency to the smallest local municipality. As AI-generated threats emerge at unprecedented speed, true whole-of-state resilience requires a synchronized community front where a threat detected at one endpoint instantly informs the defense of the entire network.

The Strategy: Build a Unified Ecosystem with Cyware

Cyware is the industry-recognized leader in cyber collective defense systems for critical infrastructure. For example, Cyware is deployed in a large state to connect thousands of state and local organizations, municipal utilities, and hospitals into a single intelligence sharing, collaboration, and action network. This whole-of-state defense ecosystem eliminates the traditional state-to-local gap, enabling all covered stakeholders to collaborate and act in real time against AI-accelerated threats.

State Intelligence Sharing and Actioning Architecture



CYWARE™

Technical Framework:

From Threat Intelligence to Action

Cyware is designed to replace manual data entry with an automated platform for threat actioning .

- **Consolidated Hub Operations:** Reduce community operational headaches and costs by consolidating disparate community functions into a single application. This approach eliminates the “leaky data bucket,” significantly improving data retention, historical intelligence usage, and overall administrative experience.
- **High-Speed Interoperability:** Accelerate actioning speed for sophisticated community organizations by enabling seamless, machine-to-machine bi-directional connectivity. The hub fully supports open sharing standards, instantly connecting environments using any STIX (1.0, 1.1, 2.0, 2.1) or MISP formats.

Why Cyware:

Automated Connectivity

Promote seamless connection with any technology asset or framework, driving real-time whole-of-state threat intelligence sharing across all stakeholders.

Proven Industry Leadership

Recognized as the industry leader in cyber collective defense systems for critical infrastructure, Cyware is trusted and used by 85% of major ISACs

Workforce Readiness

RSOC-trained analysts familiar with Cyware workflows help reduce onboarding time, optimize operational efficiency, and strengthen whole-of-state cyber operations.

U.S. Based Support

Cyware is U.S. headquartered, with all support delivered by U.S. citizens from within the United States.

Dedicated Sovereign Infrastructure

A dedicated state-level multi-tenant environment ensures secure, sovereign handling of public sector data across all covered community stakeholders.

Strengthen cyber readiness and accelerate coordinated response across your state with Cyware.

Book Your Demo Today!

For more information:

111 Town Square Palace Suite 1203 #4 Jersey City, NJ 07310 cyware.com | sales@cyware.com

CYWARE™