CYWARE™ | Solution Brief

Cyware for State, Local, Tribal, Territorial (SLTT) Governments

Strengthen Your Cyber Defenses with Unified Threat Intelligence Management

The Challenge

SLTT cyber threat intelligence (CTI) teams play a mission critical role in protecting sensitive data, ensuring seamless cyber operations across agencies, and leading efforts across governments to take actions to mitigate cyber threat risks. These teams work tirelessly to safeguard people, critical infrastructure, and government assets from cyber threats while ensuring a swift and coordinated response.

With increasingly sophisticated ransomware and denial-of-service attacks, diverse and disconnected technologies, a shortage of skilled cyber workforce, and tightening budgets, defending against cyber risks is more challenging than ever.

Threat intelligence management must evolve—it must transform intelligence into near real-time action, minimize manual effort, enhance cross-agency collaboration, and remain cost-effective to support mission-critical cybersecurity operations.

DISCOVER
Proactively detect threats with real-time intelligence and automated risk assessment.

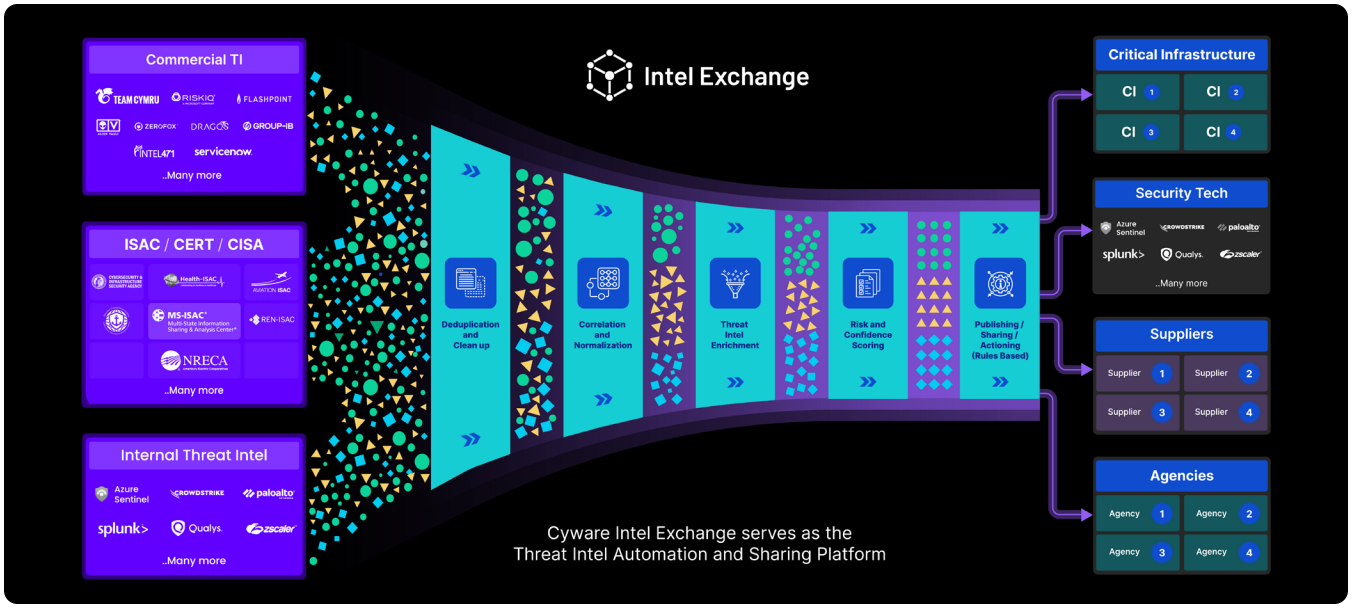
ACT
Automate threat response and orchestrate security actions for swift threat mitigation.

COLLABORATE
Share intelligence securely across agencies for a unified defense.

DEFEND
Enhance cyber resilience with proactive threat containment and defense.

How Cyware Transforms the Way SLTT Governments Defend Against Evolving Cyber Threats

Cyware's AI-powered solutions, deployable across cloud, on-premise, and hybrid environments, help SLTT Governments strengthen their cybersecurity posture as threats and regulations evolve. As a StateRAMP Readiness-in-Process platform, Cyware goes beyond monitoring — **it transforms cyber intelligence into actionable responses, streamlines security operations, fosters seamless cross-agency coordination, and delivers cost-efficient, mission-critical protection.**



Unified Threat Intelligence Management and Orchestration

Don't just monitor threats—gain real-time, actionable intelligence tailored to your needs with automated threat intelligence exchange and actioning. Adopt a Threat-Informed Cybersecurity approach to detect threats faster, collaborate efficiently, and stay compliant.

- **Reduced Alert Fatigue & Resource Optimization –** Automate threat intelligence processing to cut noise, reduce manual effort, and improve security team efficiency—maximizing ROI.
- **Real-Time Threat Sharing –** Streamline IOC and TTP exchange for faster detection and response, enhancing overall security effectiveness.
- **Actionable Intelligence –** Enrich, analyze, and prioritize threats to drive smarter security decisions.
- **Seamless Collaboration –** Securely share threat intelligence and defensive measures across agencies.
- **Bi-Directional Intelligence Ingestion –**Ingest, enrich, and operationalize threat data from any source, in any format.
- **Seamless integration with Public Sector ISACs:** Effortlessly integrate with CISA AIS, MS-ISAC, Aviation ISAC, Health ISAC, Maritime ISAC, Research & Education Network ISAC, and the National Rural Electric Cooperative.
- **Advanced Correlation & Scoring –** Leverage integrations with leading threat feed providers for automated enrichment and precise prioritization.

Seamless Collaboration & Information Sharing

A single agency can be secure, but only a unified ecosystem is truly resilient. Strengthening national security requires collective defense– proactively gathering, analyzing, and sharing threat intelligence and best practices to enable synchronized cyber defense, coordinated security planning, and rapid response.

- **Effortless Intelligence Sharing –** Access pre-analyzed threat advisories from top providers.
- **Stronger Collaboration –** Build trusted threat-sharing networks with other SLTT governments, critical infrastructure, vendors, and partners for better coordination.
- **Greater Threat Visibility –** Automate alert ingestion, enrichment, and sharing for a unified threat picture.
- **Access to Expertise –** Use the Threat Defender Library to create, collaborate, and share SIEM rules, detection files, and playbooks.
- **Faster Threat Response & Crisis Management –** Automate threat detection, enrich intelligence, and enable coordinated inter-agency response with other SLTT agencies with real-time alerts and joint mitigation.

Acquiring and Maximizing Cybersecurity Investments

Government agencies have varying levels of cybersecurity preparedness. Federal and state grants, including the IIJA SLCGP, offer funding to strengthen defenses. Assessing needs, planning strategically, and justifying ROI are key to maximizing these investments.

- **Assess & Plan –** Identify security gaps, align with key aspects of CISA's Cybersecurity Performance Goals (CPGs), and develop a roadmap for sustainable improvement.
- **Implement & Automate –** Deploy real-time threat intelligence sharing, automated response, and cross-agency collaboration to enhance defenses.
- **Scale & Sustain –** Future-proof cybersecurity investments with modular, scalable solutions that adapt to evolving threats.

Strengthen Cyber Defenses

Request a Demo Today

CYWARE™

Trusted Threat Intelligence Platform

Cyware seamlessly automates the entire threat management lifecycle, enabling real-time defense through AI-powered insights and orchestration for unmatched threat mitigation efficiency.

Proven Experience and Expertise

Trusted by SLTT Governments, Critical Infrastructure Organizations and ISACs for intel-driven security automation, delivering ROI within the first 90 days of deployment.

Comprehensive Security & Compliance Solutions

Strengthens collective defense by enabling seamless threat intelligence sharing across Federal Agencies and SLTT Governments.

Seamless Integration with Tools and Technologies

Enables smooth operationalization of threat intelligence across security, IT, and DevOps ecosystems.

Compliant & Secure Data Handling

Efficiently processes large volumes of structured and unstructured threat data while ensuring compliance.

StateRAMP · FedRAMP · Joint Cyber Defense Collaborative · NASCIO Representing Chief Information Officers of the States · AAPA Essential. Resilient. United. Seaports Deliver · Secure by Design Pledge · SOC 2 Type 2 · OASIS · OCA Open Cybersecurity Alliance · Cybersecurity & Infrastructure Security Agency · VPAT Compliance · Privacy Shield Certified · CoSAI Coalition for Secure AI

For more information:

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

cyware.com | government@cyware.com

CYWARE™