CYWARE™ | zscaler™ | Solution Brief

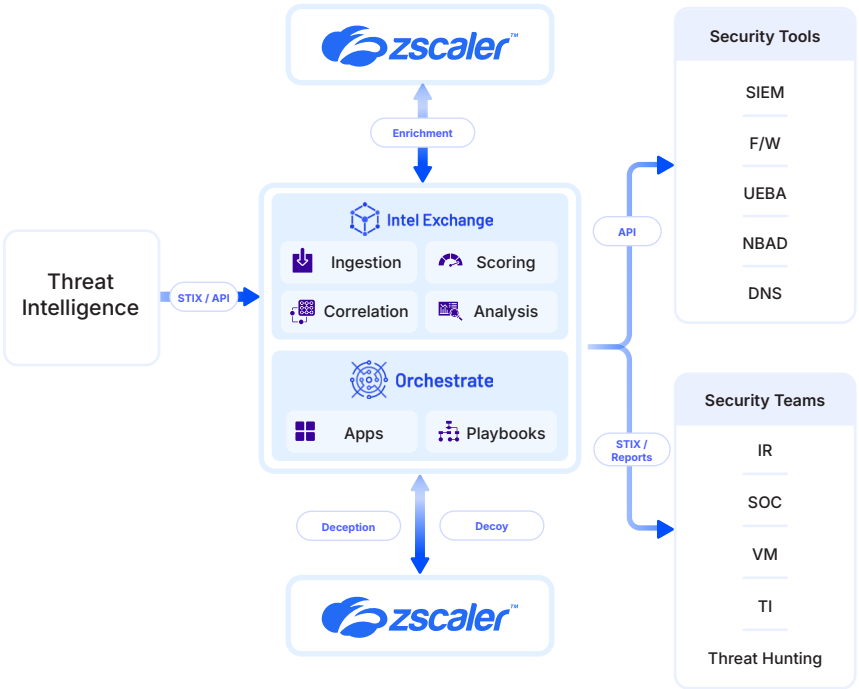
Enrich and Automate Threat Intelligence, and Accelerate Incident Response

A Partnership between Zscaler and Cyware

Cyware Intel Exchange is a purpose-built Threat Intelligence Platform (TIP) that automates ingestion, enrichment, analysis, prioritization, actioning, and bidirectional sharing of threat data. By integrating with **Zscaler Internet Access (ZIA)**, organizations gain high-quality threat intelligence enrichment that equips security teams with the insights needed to proactively detect, prioritize, and block threats before they escalate into attacks.

Through this integration, security teams can obtain clear, contextualized intelligence on suspicious Indicators of Compromise (IOCs) including IPs, domains, and URLs that have been flagged as malicious or linked to security events, and then automatically block them to protect critical digital assets.

Complementing this, **Cyware Orchestrate** extends the value by delivering low-code/no-code security automation. With its in-built **Zscaler Internet Access** app and support for **Zscaler Deception**, Orchestrate empowers SOC teams to automate actions across their security ecosystem, streamline incident response, and neutralize threats faster and at scale.



Integration Highlights

Threat Intelligence Enrichment: Automatically enrich domains, URLs, and IPs with Zscaler verdicts in Cyware Intel Exchange to improve confidence scoring and analyst decisions.

Automated Policy Enforcement: Query Zscaler for URL categories, identify malicious indicators, and update allowlists and denylists directly from Cyware rules.

Deception Technology: Zscaler deception decoys with Cyware Orchestrate for early attacker detection and rapid investigation.

Zero Trust Alignment: Zero Trust Exchange with Cyware orchestration to reduce dwell time and accelerate response.

Scalable Orchestration: Orchestrate playbooks with Zscaler apps to block URLs, fetch sandbox reports, perform lookups, and update policies automatically.

With this integration, organizations can:

- Improve security posture with proactive detection and automated response.
- Reduce mean time to detect (MTTD) and respond (MTTR).
- Eliminate manual overhead by automating enrichment and enforcement.
- Achieve consistent protection across cloud, endpoints, and users.

Key Use Cases

Threat Data Enrichment:
Perform real-time lookups from Cyware Intel Exchange to Zscaler to enrich investigations with IPs, URLs, and domains, improving confidence and decision-making.

Dynamic Allowlist and Denylist Management:
Automate URL and domain blocklists and allowlists in Zscaler based on Cyware rules to proactively stop threats.

Proactive Threat Detection:
Detect insider threats and lateral movement through Zscaler Deception, fully orchestrated in Cyware for faster response.

Contextualized Threat Intelligence:
Correlate IOCs with Zscaler insights to add context, categorize websites, and strengthen URL filtering and access control policies.

Automated SOC Workflows:
Use Cyware Orchestrate playbooks to automate actions such as URL lookups, sandbox analysis, scoring of threat intel, and response actions across 375+ SOC tools, reducing analyst fatigue.

Comprehensive Internet Security:
Enforce firewall, DLP, sandbox, filetype, SSL, and URL filtering policies through Zscaler Secure Internet Access, powered by Cyware orchestration.

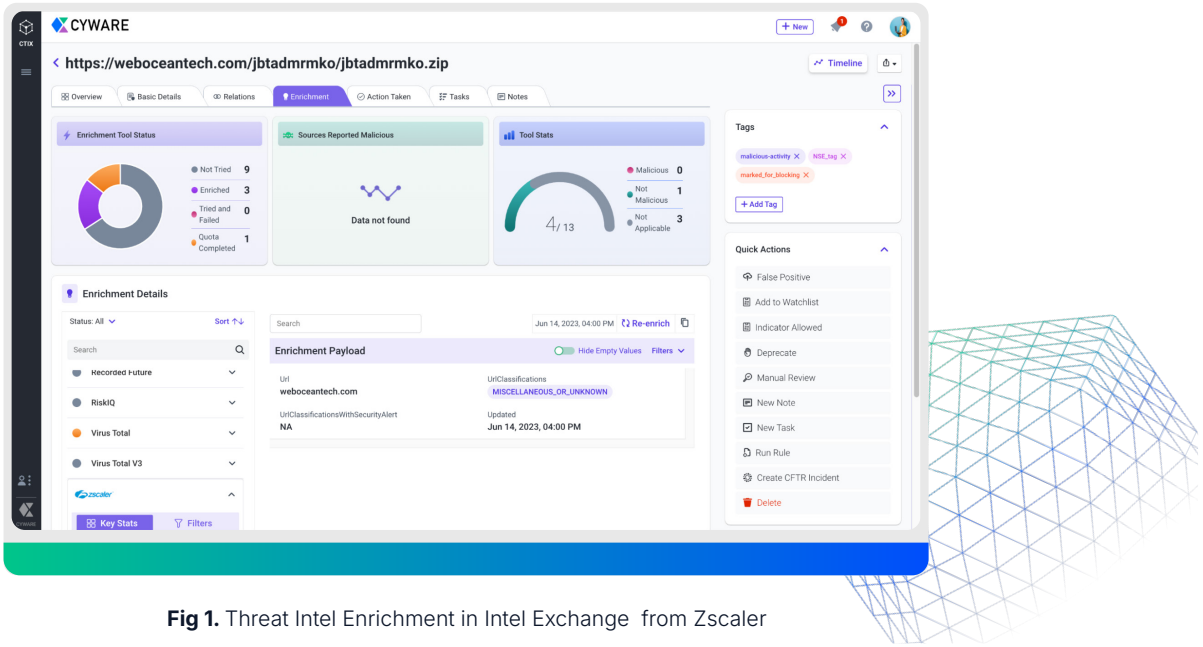


Fig 1. Threat Intel Enrichment in Intel Exchange from Zscaler

About Cyware

Cyware helps enterprises transform security operations while breaking through silos for threat intelligence sharing, collaboration, and automated threat response. Its unique Cyber Fusion solutions enable lean security teams to proactively stop threats, connect the dots on security incidents, dramatically reduce response time, and reduce analyst burnout from repetitive tasks. Cyware improves security outcomes for enterprises, government agencies, and MSSPs, and provides threat intelligence sharing platforms for the majority of ISAC/ISAO information-sharing communities globally.

Learn more at **www.cyware.com**

Cyware
111 Town Square Place Suite 1203, #4
Jersey City, NJ 07310
855-MY-CYWARE

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

Learn more at **www.zscaler.com**

Zscaler
120 Holger Way
San Jose, CA 95134
+1 408 533 0288