DATASHEET

Build Effective Defense Against Threats Using Zscaler

Access clear insights about suspicious domains, URLs, and Hashes to block threats, associated with your digital assets, using Zscaler enrichment.

Cyware Threat Intelligence eXchange (CTIX) can automatically ingest threat data from a multitude of sources in different formats and allows analysts to get a holistic view of the threats relevant to the organization from a centralized point. Zscaler brings in threat intelligence feed enrichment and equips organizations with the protection they need to proactively detect, prioritize, and block emerging threats before they turn into attacks that disrupt business operations, compromise networks, and damage brand reputation.

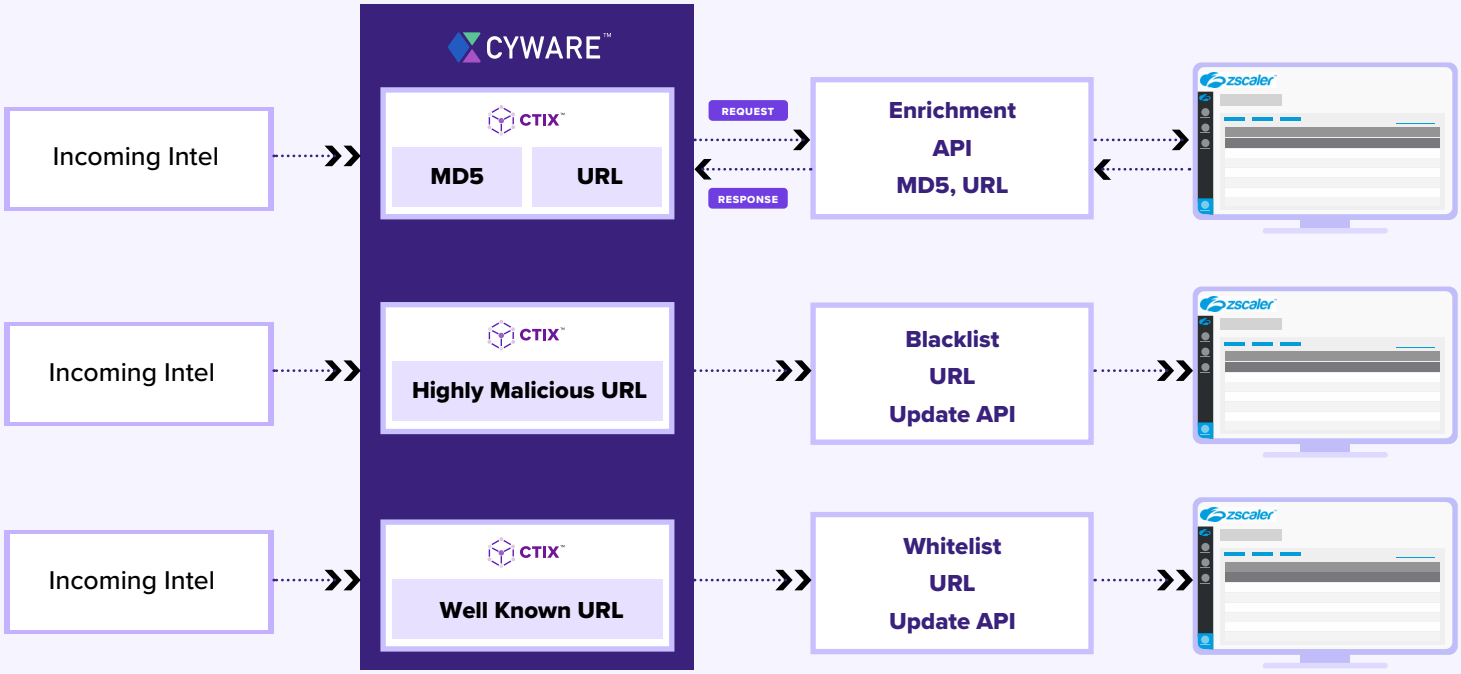
The integration

- Allows analysts to correlate threat data with additional insights and analyze vast amounts of external interactions and suspicious threat indicators targeting your organizations.
- Enhances and enriches internal intelligence and threat intelligence received from Zscaler sources, both manually and automatically, to add better context and allow analysts to make informed decisions.
- Investigates threats with better context by querying Zscaler for URL categories to identify the malicious nature of domains.
- Automatically updates the Zscaler database with blacklisted and whitelisted URLs using CTIX rules.
- Continuously evaluates confidence score for threat indicators and automates threat blocking by enriching and pushing IOCs and suspicious URLs, domains, and hashes to peer organizations.

Capabilities and Benefits

- Tailored threat intelligence feeds allow for the early detection and proactive mitigation of targeted attacks in your organization.
- Automatically update Zscaler with blacklisted and whitelisted URLs and allow securityteams to perform real-time actioning to enable proactive blocking of threats.
- Real-time threat investigation with the help of URL, Domain, and Hash threat data lookup.
- Security teams can add additional context to the threat data available in CTIX by correlating them with Zscaler to identify malicious URLs and investigate confidently.
- Security teams can perform contextual analysis with the help of high-quality indicator feeds and identify, prioritize, and mitigate risks that target their organization's network.
- Attribute confidence score to indicators and enable analysts to make informed decisions before executing actions to defend against threats.

Architecture



Orchestrate Intel with CSOL

Security teams can leverage Cyware Security Orchestration Layer (CSOL) as an end-to-end security orchestration layer and expand CTIX-Zscaler integration capabilities to create specialized threat intelligence workflows. These workflows can be created with the easy-to-use playbook builders or by modifying Cyware's existing pre-built playbooks. CSOL offers orchestration across deployment environments (cloud and on-premise) with automated playbooks, flexible APIs, and full customization capabilities.

The Zscaler connector app in CSOL allows your security team to communicate with the Zscaler application to perform a multitude of tasks and gain organization-wide visibility over malware threats.

About Zscaler

Zscaler is revolutionizing internet security with the industry's first security-as-a-service platform, used by more than 5,000 leading organizations, including 50 of the Fortune 500. Zscaler is a Gartner Magic Quadrant leader for Secure Web Gate ways and delivers a safe and productive internet experience for every user, from any device, and any location — 100% in the cloud. Zscaler delivers unified, carrier-grade internet security, next-generation firewall, web security, sandboxing/advanced persistent threat (APT) protection, data loss prevention, SSL inspection, traffic shaping, policy management, and threat intelligence — all without the need for on-premises hardware, appliances, or software.

CYWARE™

Cyware®

1460 Broadway New York NY 10036

cyware.com | sales@cyware.com

855-MY-CYWARE