THREATQUOTIENT™

THREATQ™ AND CISCO UMBRELLA

The joint solution of Cisco Umbrella and the ThreatQ Threat Intelligence Platform (TIP) provides the first line of defense against threats on the Internet.

With the combination of Cisco Umbrella and the ThreatQ Threat Intelligence Platform, organizations can uncover current and emerging threats and stop phishing, malware and ransomware earlier.

THREATQ BY THREATQUOTIENT™

ThreatQ is an open and extensible threat intelligence platform (TIP) to provide defenders the context, customization and collaboration needed for increased security effectiveness and efficient threat operations and management. ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders unmatched control through a Threat Library™, an Adaptive Workbench™ and an Open Exchange™ to ensure that intelligence is accurate, relevant and timely to their business. With ThreatQ, customers can automate much of what is manual today and get more out of existing security resources, both people and infrastructure.
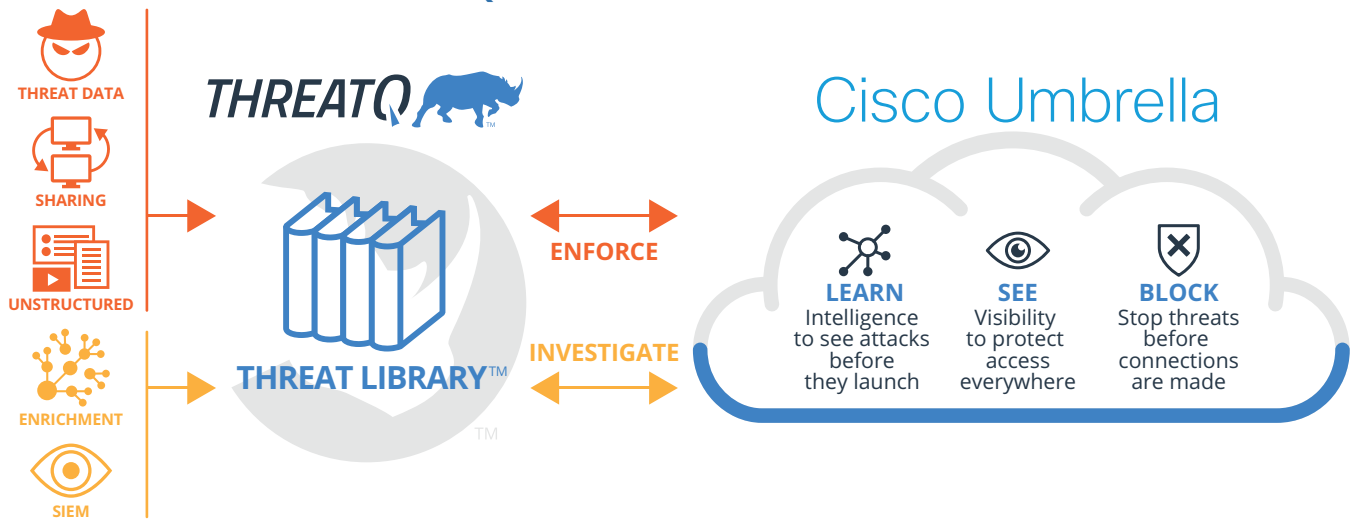
CISCO UMBRELLA

As the industry's leading Secure Internet Gateway, Cisco Umbrella provides the first line of defense against threats on the Internet wherever users go. Leveraging their global infrastructure, which resolves over 120 billion Internet requests a day, Umbrella is able to see where imminent attacks are being staged. It also delivers complete visibility into Internet activity across all locations, devices and users, and blocks threats before they ever reach your network or endpoints. Additionally, Umbrella is an open platform and integrates easily with your existing security stack and delivers live threat intelligence about current and emerging threats. By analyzing and learning from Internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for attacks, and proactively blocks requests to malicious destinations before a connection is even established — without adding any latency for users.

With Umbrella, you can stop phishing and malware infections earlier, identify already infected devices faster and prevent data exfiltration.

INTEGRATION HIGHLIGHTS

Provides threat analysts with detailed and historical indicator data

Deep visibility into traffic both on and off network

Helps security teams respond appropriately when investigating a threat

THREATQ / CISCO UMBRELLA ARCHITECTURE

THREAT DATA

SHARING

UNSTRUCTURED

ENRICHMENT

SIEM

THREATQ

THREAT LIBRARY™

ENFORCE

INVESTIGATE

Cisco Umbrella

LEARN
Intelligence to see attacks before they launch

SEE
Visibility to protect access everywhere

BLOCK
Stop threats before connections are made

INTEGRATION USE CASES

Add malicious domains curated by the ThreatQ platform to Umbrella domain lists for blocking

Use Umbrella's passive DNS data to query a domain or IP address' historical record

Use Umbrella Investigate's integration with Cisco Threat Grid to uncover file hashes associated with malware campaigns and build out a full view of an attacker's Internet infrastructure

Pull in domain tags, security scores and other metadata associated with domains and IP addresses

Automatically send IP Addresses, FQDNs and URLs to critical infrastructure for blocking.

OPEN EXCHANGE ARCHITECTURE

ThreatQ's Open Exchange provides an extensible and flexible environment for analysts to achieve the optimal balance between system automation and expert analysis. Because no single security solution provides a silver bullet against attacks, ThreatQ's Open Exchange architecture supports standard interfaces for ingestion and exporting, including STIX/TAXII, XML, JSON, PDF, email and other formats of structured and unstructured data, along with an SDK and APIs for custom connections.
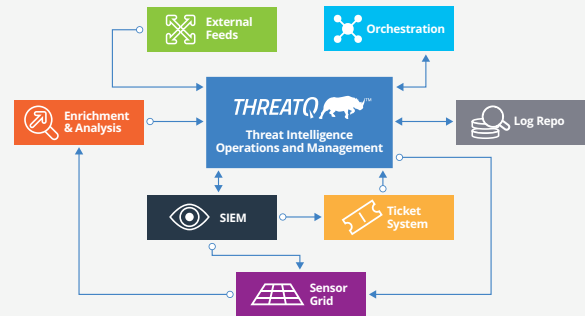
ABOUT THREATQUOTIENT™

ThreatQuotient understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, empowers defenders to ensure the right threat intelligence is utilized within the right tools, at the right time. Leading global companies are using ThreatQ as the cornerstone of their threat intelligence operations and management system, increasing security effectiveness and efficiency.

For additional information, please visit threatq.com.

ABOUT CISCO

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. At Cisco, customers come first and an integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success.

For more information, visit cisco.com.

TQ_ThreatQ-Cisco-Umbrella-Solution-Overview_Rev1

THREATQUOTIENT

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Sales and General Inquiries: +1 703 574-9885