USE CASE

THREATQUOTIENT

THREAT INTELLIGENCE SHARING

THE CHALLENGE ORGANIZATIONS FACE

When managing threat intelligence, organizations face a number of challenges protecting sensitive internal operations while engaging in necessary collaboration with external partners. Companies must maintain sovereignty over their data, ensuring it is owned, controlled, and housed within a private instance that can operate with autonomy and confidentiality. At the same time, they require a platform that allows for controlled access to this intelligence by external entities, such as federated operations and dealer networks, ensuring that collaboration does not compromise security.

The complexity of modern cybersecurity demands support for diverse sharing models, from machine-to-machine exchanges accommodating various languages and formats, including STIX, to the distribution of human-readable data. Access to user-centric dashboards, comprehensive reports, and sophisticated analytical tools is crucial for actionable intelligence.

The platform must also cater to the varying maturity levels of external teams, ensuring usability and accessibility regardless of their expertise. It must also seamlessly integrate with different infrastructures and architectures, enabling a versatile and inclusive approach to threat intelligence sharing across the cybersecurity ecosystem.

Empowering Secure, Flexible, and Collaborative Defense with ThreatQ

The ThreatQ Threat Intelligence Platform (TIP) is the leading solution for enabling and managing intelligence collaboration within and across organizations of any size and complexity. Combining the principles of a flexible data model and adherence to open intelligence sharing standards, the platform is crafted for both customization and seamless cooperation. It is designed to not only meet but enhance the cybersecurity measures of diverse organizations, facilitating secure and efficient internal and external collaboration.

ThreatQ is vendor-neutral, assuring bi-directional integration with a range of technologies and operational maturity levels, ensuring that teams can share intelligence extensively without the risk of exposing sensitive data. ThreatQ empowers teams to operate with autonomy while engaging in a broad, collaborative security network.

ThreatQ Sharing Highlights

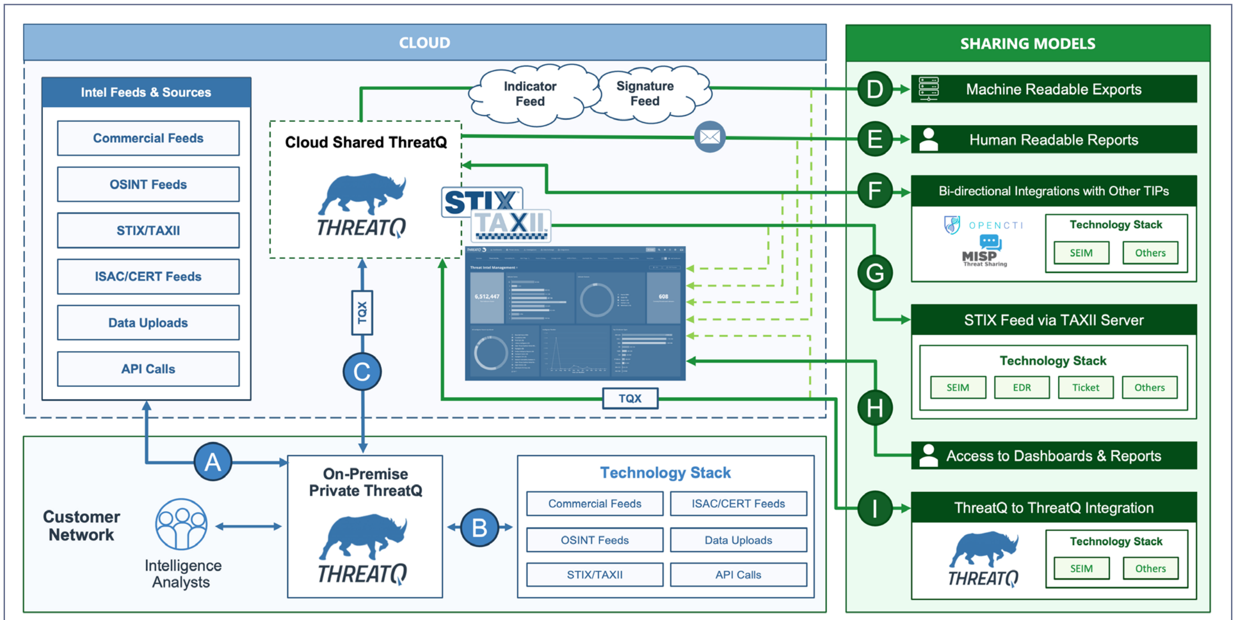
1. Vendor Agnosticism: the ThreatQ open exchange platform supports integration with a wide range of technologies, fostering collaboration without restrictions.

2. Segregated Environments: ThreatQ ensures the physical separation of internal and external intelligence sharing, maintaining privacy and data integrity across distinct instances with equal feature parity.

3. Deployment Flexibility: Customers can opt for on-premise, AWS cloud-hosted, or alternative cloud provider solutions, giving them control over their deployment strategy.

Representative Deployment

A leading organization in the Financial Services sector, utilized the ThreatQ collaborative architecture to maintain an on-premise platform for internal operations and a cloud-hosted platform for collaborating with external financial institutions. As depicted in the diagram below, the on-premise platform integrates directly with the organization's security stack, ensuring that intelligence feeds are collected without intermediary manipulation. The cloud instance, optionally hosted on AWS, serves as a community platform, allowing the organization to share intelligence securely with peers. The deployment underscores the ThreatQ commitment to security, operational independence, and collaborative defense strategies.



INTEGRATIONS

A. External intelligence ingestion and enrichment.
B. Internal integrations & intelligence collection.
C. Transfer data to Customer's shared cloud instance of ThreatQ. Ingest 'community' data on this instance.

SHARING

D. Delivery of curated intelligence via Exports in machine readable specific formats – Text, JSON, CSV, etc.
E. Human-readable intelligence reports via email.
F. Bi-directional integration with alternate TIPs such as MISP and OpenCTI
G. Collection of STIX feed via TAXII server ThreatQ.
H. Access to ThreatQ UI for Dashboards, reports, etc.
I. Native ThreatQ-ThreatQ integration via TQX for feed delivery (between ThreatQ users).

Benefits of ThreatQ Customers:

- For Large Organizations and Subsidiaries: The ThreatQ Platform allows for centralized control of threat intelligence while supporting autonomous operations across different business units or geographical locations.
- For MSSPs: Service providers can manage threat intelligence for multiple customers, maintaining strict data segregation and providing tailored threat intelligence as a value-added service.
- For ISACs: Information Sharing and Analysis Centers (ISACs) can leverage the ThreatQ secure exchange technology to distribute intelligence across their network, enhancing the collective defense.

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven threat intelligence platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit **www.threatquotient.com**.

THREATQUOTIENT

Sales@ThreatQ.com • 703.574.9885