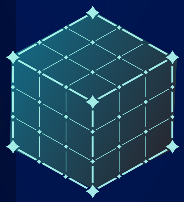
DATASHEET

# Security in an Air-Gapped Environment



Classified or offline networks that are not connected to the internet are an essential part of the US Government's national security and defense. The goal of establishing classified environments is to work with the sensitive information protected from access by the greater internet. In turn, classified environments are traditionally forced to operate with access to a fraction of the information accessible by internet facing networks. This practice results in a number of challenges including:

- Disconnected networks lead to relevant cyber threat intel being isolated in silos.
- The threat context required for decision making on classified and tactical networks is delayed due to cumbersome processes for providing data across domains.
- Relevant and valuable Sec Ops work is difficult to leverage across both unclassified and classified networks.
- Extended Detection and Response (XDR) is limited to the connected infrastructure on a single network, and cannot easily be transferred over to additional networks.

When it comes to cybersecurity, in both offensive and defensive efforts, context is key. Providing access to this context is a challenging request for most threat intelligence feeds and platforms as these capabilities typically require an internet connection to work correctly or to operate at their fullest capability. Analysts and security operators are forced to undertake cumbersome manual tasks to compile and extract relevant information in order to move it into their classified settings to make use of it. By the time they accomplish this task, the information can be dated and there is often new information to assess and investigate.

## The ThreatQ Platform

The ThreatQ platform accelerates security operations through streamlined threat operations and management. The integrated, self-tuning Threat Library, Adaptive Workbench, and Open Exchange allow organizations to aggregate data, quickly understand and prioritize threats, make better decisions and automate the right intelligence to the right tools at the right time to accelerate detection and response. ThreatQ Data Exchange makes it easy to implement bidirectional sharing of any and all intelligence data within the ThreatQ platform and scale sharing across many teams and locations. ThreatQ Investigations serves as a virtual cybersecurity situation room designed for collaborative threat analysis, shared understanding and coordinated response.

### BENEFITS OF THREATQ AIR-GAP DATA SYNC (AGDS)

Maintain network integrity through true air-gap deployment

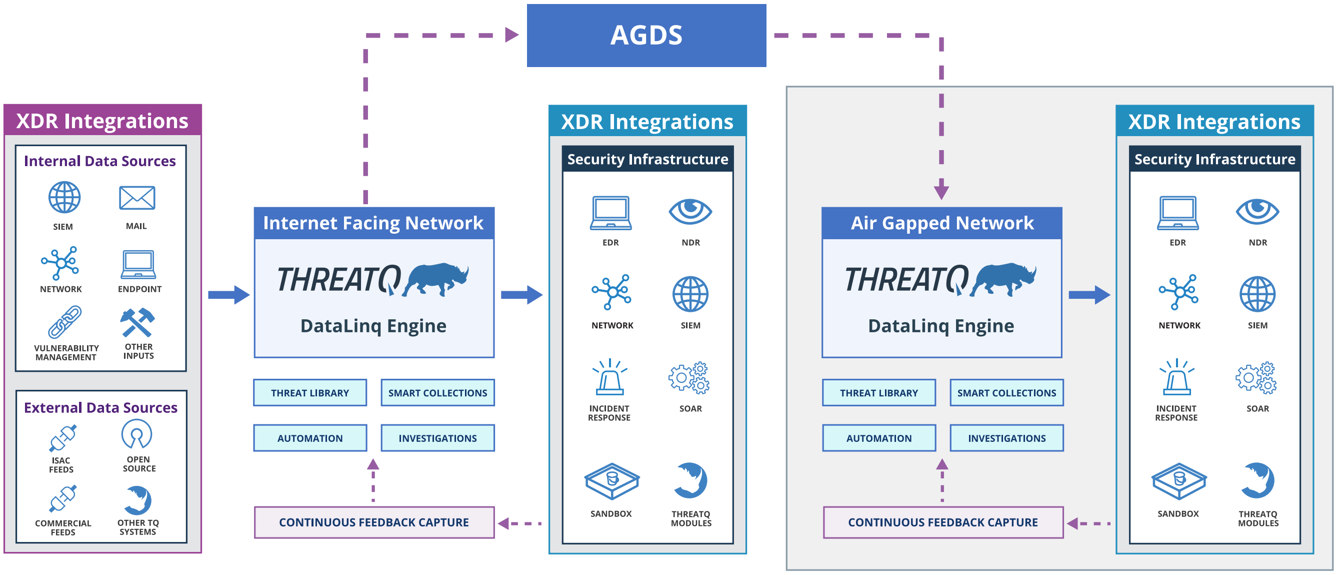
The control, flexibility, and integration capabilities to operationalize threat data available on the low side, can be leveraged by security infrastructure across network classification levels

Securely share unclass, enriched threat intelligence to classified networks through multiple transport methods

The ThreatQ platform works with existing processes and technologies and applies a data-centric approach to security operations to support a variety of use cases beyond threat intelligence management, including threat hunting, incident response, spear phishing, alert triage and vulnerability management. Having been granted Authority to Operate (ATO) by the Defense Information Systems Agency (DISA) at the Department of Defense Information Network (DoDIN) level as part of the Endpoint Security Solutions (ESS) Infrastructure, allows the ThreatQ platform to be deployed more swiftly by the DoD to meet their cybersecurity challenges.

**Air-Gap Data Sync (AGDS)** effectively transfers threat data between two ThreatQ instances, the online internet facing instance and the offline or disconnected instance. ThreatQ AGDS is designed to support air-gapped environments and has been implemented with both data diodes and manual transfer approaches.

As depicted in the diagram, ThreatQ AGDS uses an architecture that supports a one-way flow of data between the Internet facing instance and the air-gapped instance of the threat intelligence platform. The architecture enables data to be exported from instance 1 and passed to the transfer mechanism. The transfer mechanism, which is a one way diode or high speed guard, will enable the date to be transferred to the air-gapped environment. Once the data successfully transferred, ThreatQ AGDS will then upload the new data into the Threat Library of instance 2.



For a more in-depth analysis of the considerations influencing the design and implementation of a threat intelligence platform in an air-gapped environment, download the companion document titled: Using ThreatQ in Air-Gapped Environments.

DOWNLOAD NOW

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations 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 and APAC.

For more information, visit www.threatquotient.com.

THREATQUOTIENT

Sales@ThreatQ.com • 703.574.9885