THREATQUOTIENT

AT A GLANCE

ThreatQ TDR Orchestrator Deployment Models

Complete deployment flexibility:
Choosing a deployment model that's right for your organization

A threat intelligence platform is the heart of any cybersecurity program. The best way to deploy that platform depends on your needs as an organization. In order to determine the right deployment for you, ask questions like...

- **What is your cloud strategy?**
- **Where do you see your infrastructure in 3 years time?**
- **Do you have a virtual private cloud in Amazon?**
- **Are you looking to host top secret information?**
- **Do you need to air-gap the platform for security reasons?**

ThreatQ TDR Orchestrator

ThreatQ TDR Orchestrator is the industry's first solution to introduce a simplified, data-driven approach to Security Automation, TIP, and TDIR that accelerates threat detection and response across disparate systems, resulting in more efficient and effective security operations.

ThreatQ TDR Orchestrator can be deployed multiple ways in order to suit a customers' needs. On-premise, air-gapped and cloud hosted.

On-Premises

- For maximum data governance under your control, ThreatQ TDR Orchestrator can be deployed solely on-premises, providing you complete control over your data and remain cost-efficient.

Private cloud Instance in your own AWS VPC (Virtual Private Cloud)

- ThreatQ TDR Orchestrator is available as an AMI (Amazon Machine Image) for deployment within your own private AWS cloud, managed by your own devops team.
- This gives the option to run in a cloud computing environment being both flexible and scalable.

Air-Gapped

- ThreatQ can be deployed in a secure, air-gapped environment to protect your systems and data as well as meeting any compliance requirements.
- Effective Placement within the architecture.
- Architecture Of The Threat Intelligence Platform - an 'on-premises' solution that will work effectively in an air-gapped environment.
- Platform Updates - receive updates on a regular and timely basis and should involve simple installs that keep the entire architecture in line with custom functionality.

- Enrichment And Analysis Sources - This capability offers enrichment of threat data from both internal and external sources; it avoids compromising the security of the wider environment.
- Integrations - Out of the box, ThreatQ's Open Exchange provides the largest and most adaptable set of integrations in the industry. The ThreatQ ecosystem supports a wide array of products today – including commercial, industry, private and custom solutions – and is growing rapidly.
- Split Threat Intelligence Platform Functions.

Cloud Hosted

- Simplistic deployment and on-boarding process.
- Private access to your own private data-store.
- Customer administration of user accounts and access.
- Highly reliable environment with SLA Ingest threat data from a large number of feed sources including open source, industry and paid feeds.
- Integrate with a variety of SIEMs, Ticketing Systems, Endpoint Detection and Response tools, and more…
- 24/7 customer support option available.

CREATING A LEADING DATA-DRIVEN SECURITY OPERATION

Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. Automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to share curated threat intelligence, advisories and reports with a range of internal and external stakeholders, including critical infrastructure sectors, quickly.

Achieve more with the ThreatQ Platform:

- **CONSOLIDATE** and normalize all sources of external (e.g., commercial feeds, MITRE ATT&CK) and internal threat intelligence and vulnerability data in a central repository
- **AUTOMATE** enrichment actions in bulk, including correlating data, building relationships, and adding more attributes and context for a deeper understanding of threats and trend analysis
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities
- **SCORE** threat intelligence sources and manage expiration automatically based on your requirements to produce high-fidelity intelligence
- **PRIORITIZE** data based on what matters most for different stakeholders and reprioritize automatically as new data and learnings are available
- **INTEGRATE** with existing tools and threat intelligence sources via a comprehensive library of APIs and custom connectors
- **SHARE** intelligence and respond to requests for intelligence from the SOC and other internal entities right away
- **ACCELERATE ANALYSIS** of attacks and reduce time to create reports and advisories from days to hours

Request a live demo of the ThreatQ Platform at threatq.com/demo

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection, investigation and response (TDIR). ThreatQ is the first purpose-built, data-driven threat intelligence platform that 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 integration marketplace, data management, orchestration and automation capabilities support multiple use cases including threat intelligence management and sharing, incident response, threat hunting, spear phishing, alert triage and vulnerability management. For more information, visit www.threatquotient.com.