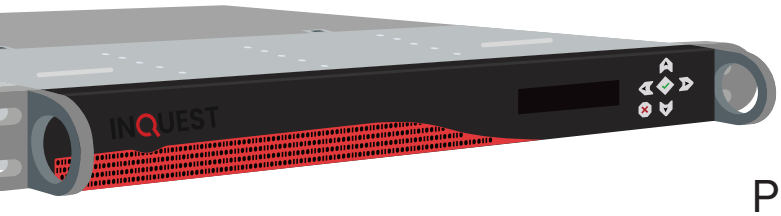
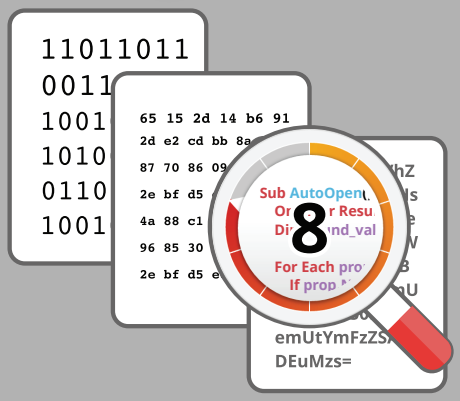
INQUEST



Prevent malicious application-logic and sensitive data-leaks as they pass through your traditional security defenses



- Founded in 2013 by seasoned veterans
- Trusted by the US Department of Defense
- Patented Deep File Inspection™ (DFI)
- Driven by unique threat intelligence sources
- Actively integrated with dozens of security vendors
- Deployed in over 25 SOCs worldwide
- Protecting 2M+ users and 5M+ endpoints
- Consuming over 2Tb/sec traffic globally
- Ingestion rates up to 40Gb/sec in 1U
- Inspecting data-in-motion, at-rest, and in-use
- Analyzing in real-time, hunting retrospectively
- Human-level scrutiny at multi-gigabit rates
- Reducing analyst frustration, improving ROI

All-encompassing, cloud-native, network threat eradication platform built by SOC Analysts for SOC Analysts that orchestrates your workflow and provides a variety of tools to assist with collaboration, investigation, and reporting.

INQUEST

SESSION ANALYSIS & DEEP FILE INSPECTION (DFI)

BACKGROUND

InQuest hails from the public sector and provides a cloud-native, network-based threat prevention platform. The solution leverages our research team's extensive knowledge of real-world attack campaigns and employs a variety of patented techniques to prevent elusive attack methodologies that would otherwise go unnoticed.

SOLVING THE ISSUE OF EMBEDDED CONTENT

InQuest focuses its scrutiny to identify, process, and inspect files downloaded over the web or received via email to prevent malicious code in transit. Innovative inspection techniques are applied to live monitored network traffic providing insights into even the most creative combinations of obfuscation.

This raw network data is fed through a gauntlet of proprietary security checks and is also made available for integration with your existing security infrastructure. There are currently integrations available for a variety of antimalware and sandbox technologies that serve in a complementary capacity to the analysis that InQuest is performing.

Most modern malware prevention solutions have limitations around the detection, inspection, and mitigation of embedded file content. Malware is commonly nested in multiple levels of compression, embedded in complex PDF object streams or buried within archive files.

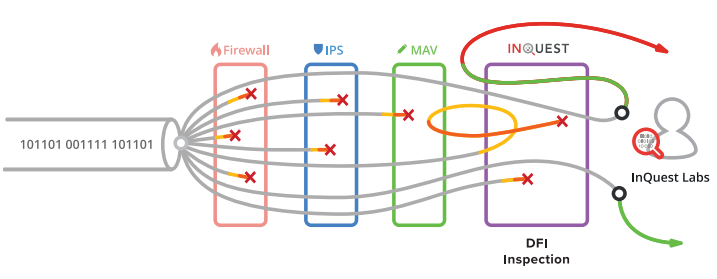


Figure 1

Our platform applies considerable resources and ingenuity towards the task of unmasking the malware within.

These typically hidden layers are analyzed by InQuest's threat prevention capabilities and, at times, in tandem with other third party security solutions as depicted in Figure 1 to reveal true positives. The InQuest platform also applies these unraveling techniques to prevent sensitive data-in-motion including confidential documents and personal identifiable information. Furthermore, InQuest leverages the advantages of hindsight by cataloguing and rescanning artifacts through our historical threat detection engine known as RetroHunting™.

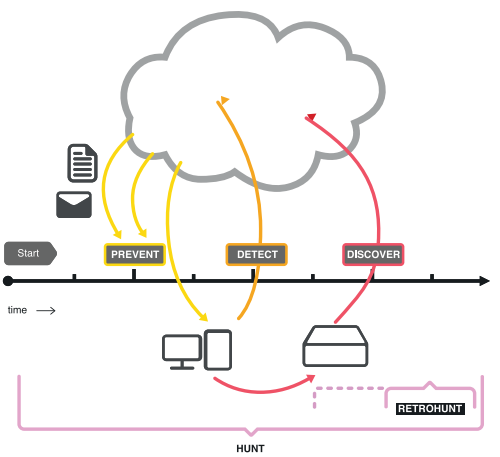


Figure 2

The InQuest platform empowers its users by providing them with the ability to create and apply custom signatures which run with the same performance and deep analytics benefits as the rest of the platform. Following in that model, InQuest augments its cataloguing, trending, and reporting capabilities with SIEM integration.

Supporting a variety of deployment configurations, InQuest provides value in attack prevention, breach detection, data leakage discovery, and threat hunting. In addition to our real-time analytics, our weekly threat intelligence updates trigger an automated retrospective analysis leveraging the power of hindsight to detect threats that may have previously traversed your network undetected. Analysts can also manually launch RetroHunting™ to pivot on any data exposed from our Deep File Inspection™ (DFI) stack.