INQUEST®

Ransomware

Threat actor groups regularly launch sophisticated email campaigns to lure employees into downloading malicious file attachments that contain embedded ransomware. Successful campaigns lead to a demand for a ransom to be paid to regain access to sensitive material in addition to compromising your organization's reputation. Despite the most sophisticated email application security controls, advanced threats can still get through to your users' inboxes.

InQuest's Integrated Cloud Email Security (ICES) solution, leveraging our patented Deep File Inspection® (DFI), goes to unparalleled levels of scrutiny to analyze, identify, and ultimately prevent malware, ransomware, and more from being delivered to your users.

CORE COMPETENCIES

- File Detection and Response (FDR)
- Threat Prevention
- Threat Hunting via RetroHunt®
- Deep File Inspection (DFI)
- Actionable and Automated Threat Intelligence

FEATURES & BENEFITS

- DFI rapidly dissects files to expose evasions and malicious content
- Dozens of Optical Character Recognition (OCR) / Computer Vision / Natural Language Processing (NLP) models automatically inspect all emails
- Complementary Integrations (MultiAV / Sandbox)

DIFFERENTIATORS

- Decorated emails with banners that clearly indicate the level of threat of that email
- Email inspected well beyond OSI layer 7 – dissecting common ransomware carriers
- Automate the task of discovering ransomware attacks through the continuous analysis of messages and other proprietary analytics of email content
- Easily integrate with existing Microsoft Exchange, Google Workspace or Microsoft Office 365 deployments in minutes