Rampart AI™

RAMPART AI™

CASE STUDY

Rampart AI™'s Zero-Trust Security Approach Helps JournalDoc Protect Sensitive Medical Information

Challenges

- Availability and integrity of its application are of paramount importance.
- Security tool should detect and protect against breaches in real-time.
- Needs true Zero-trust protection

Resiliency

Rampart™'s zero-trust security approach provided JournalDoc with a competitive edge in the cybersecurity domain.

Reliability

Rampart™'s application protection tool ensured the resiliency of JournalDoc's solution, enabling customers to rely on the application's availability and integrity.

Revolutionary

Rampart™'s zero-trust security approach and dashboard provided JournalDoc with a competitive edge in the cybersecurity domain.

Client

JournalDoc, a search system that uses medical experts, patented algorithms, and machine intelligence to access and retrieve the most relevant medical information from accredited and authoritative databases.

Objectives

As JournalDoc deals with medical information, the availability and integrity of its application are of paramount importance. With the increasing prevalence of cyber-attacks, JournalDoc needed a security tool that could detect and protect against breaches in real-time while ensuring the availability and integrity of its application.

Solutions

Rampart AI™, a leader in the application security sector, provided JournalDoc with a next-generation application protection tool that uses a new-age zero-trust security approach. Rampart™ integrates directly into JournalDoc's DevOps pipeline and applies zero-trust security principles during testing, blocking all anomalies that stray from the learned baseline. Rampart™ ensures that only authorized behaviors are allowed, reducing false positives and false negatives. By adopting Rampart™, JournalDoc could focus on its primary objective of providing medical information to its customers while Rampart™ handled the cybersecurity aspect of the application.