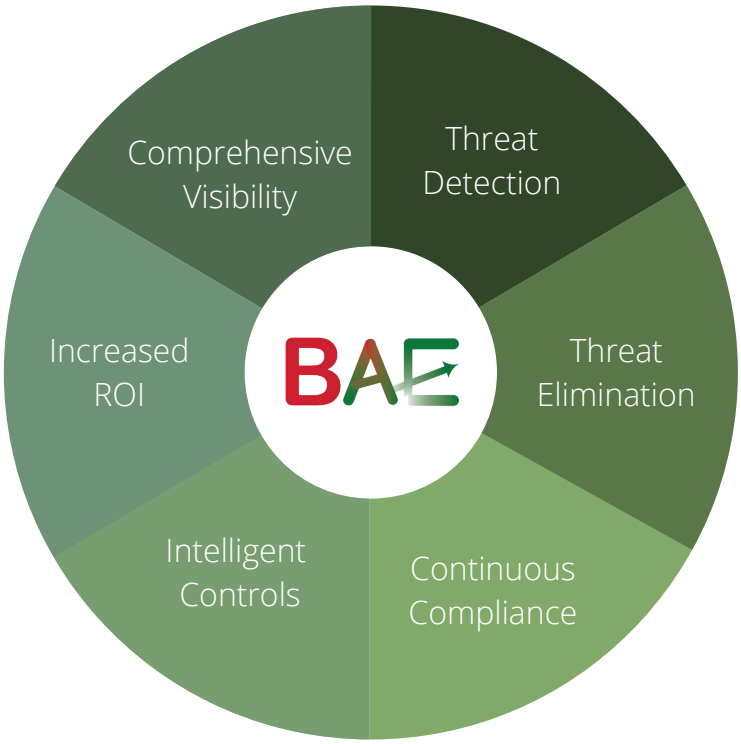
HEALTHCARE USE CASES

THE THREAT.

THE QUICK RISE OF RANSOMWARE.

Healthcare became the number one targeted vertical for cybercrime in 2015 and has held this title ever since. It's time to stop ransomware from holding your files and business operations hostage. This type of cyber attack can cause downtime, data loss, reputation loss, fines from authorities (under HIPAA), and intellectual property theft. This vicious malware locks you out of your devices or blocks access to files until a sum of money, or ransom, is paid.



THE CHALLENGE.

RAPIDLY, EVER-CHANGING THREAT VECTORS.

Ransomware attack typically involves multiple stages and each stage can be usually detected as a suspicious threat indicator leading to a potential ransomware attack by different security products. However, the challenges with detecting and preventing the ransomware with the existing security tools include: 1) Increased number of false positives because of limited visibility of each security tool which most of the times results in alert fatigue. 2) Misdetection because of lack of advanced correlation across the multiple security tools. 3) Delayed response because of more reliance on expert security analysts to correlate multiple suspicious activities in order to confirm attack and act on it.

THE SOLUTION.

COMPREHENSIVE CYBERSECURITY.

Seceon aiSIEM can detect ransomware at each stage of its development with much better accuracy. The advanced correlation engine can help minimize the false positives and focus on real Ransomware attack and detect it at the earliest stage with a high confidence. The AI based actionable intelligence pinpoints the recommendation, which is exact set of policies to push in order to stop the attack and its proliferation. The auto-remediation engine takes this action automatically without waiting for security analyst.