INDUSTRY OVERVIEW

Healthcare

A recent study reports that on average, healthcare organizations experience a monthly attack[1]. In an effort to protect patients and professionals, healthcare spending on data security and HIPAA compliance is at an all-time high.

Why Should Cybersecurity Be a Top Priority For You?

Your assets are valuable

Healthcare records are viewed as a high value target for cybercriminals given that they often include multiple data points such as social insurance and credit card numbers.

Growing reliance on information technology

The transition to electronic health records (EHRs) brings a host of challenges. From managing the various third party applications to continual software updates, many IT departments struggle to address the complexities.

Your employees can be your greatest risk

Cybercriminals look for gaps in your security posture, which oftentimes can be your own employees. Education and training are required to ensure that employees are aware of the unique hallmarks and key indicators of sophisticated attacks.

HIPAA audits are coming your way

The Office of Civil Rights (OCR) recently conducted its second phase of HIPAA audits. HIPAA requires that all organizations managing health records regularly review their administrative, technical and physical safeguards to ensure this sensitive information is protected. Failing to do so can result in significant reputational damage and financial loss as a result of fines.

Is Your Current Approach to Cybersecurity Working?

Firewalls, anti-virus, and other traditional technologies fail to detect new threats.

These automated, and largely signature-based, technologies only protect against threats that they already know about leaving your business vulnerable to new, unknown attacks.

Traditional technologies are noisy and challenging to manage.

They generate thousands of alerts, including false positives, and leave it to your IT team to figure out what's a real attack and then determine how to clean it up.

Skilled analysts coupled with advanced tools actively watch your network to hunt, investigate, and remediate attacks.

Without them, ongoing real-time forensic investigation fails and as a result, you're at an extremely high risk of a business impacting breach.

Traditional prevention technologies don't meet compliance and due diligence requirements.

HIPAA and HITECH regulators demand next generation solutions that go beyond preventative technologies to include the processes and policies to protect EHRs.

Healthcare

At eSentire, our 24X7 team of elite security analysts live inside the technology, knowing where and what to look for when it comes to the latest cyber threats. Using highly sophisticated leading-edge forensics tools, they are able to investigate and respond to odd or suspicious behavior and lock-it-down – within seconds. Our team of security analysts do all of the work, from forensic investigation to incident response, so you can focus on your business instead of managing cybersecurity.

We have been delivering our unique cybersecurity-as-a-service for 15 years to organizations across some of the most heavily regulated and cyber-targeted industries including healthcare. Our clients rely on our experience, technology and people to monitor, hunt, investigate, and remediate cyber attacks targeting their networks on a 24X7 basis.

Dramatically enhance your defense with best-in-class threat detection

Our proprietary threat detection technologies monitor your network and trigger real-time human forensic investigation to protect you from the advanced attacks that make the news headlines, and those that have gone unnoticed.

Rest assured with rapid threat response time

We respond to threats in seconds, contain them and then work with you to remediate them. Unlike other vendors, we don't have "tiers" of service or different SLA's determined by price because we believe that response times should never be compromised.

Take a proactive approach to regulatory requirements

Going beyond threat detection and response, we perform ongoing risk assessments and deliver training to help you understand and address the gaps in your security approach.

Sleep at night – because we don't

We actively monitor, hunt, investigate and remediate threats on your behalf around-the-clock, 24X7.

[1] Ponemon Institute, The State of Cybersecurity in Healthcare Organizations, 2016