A Comprehensive Guide to

# Managed IT Security for Healthcare Organizations

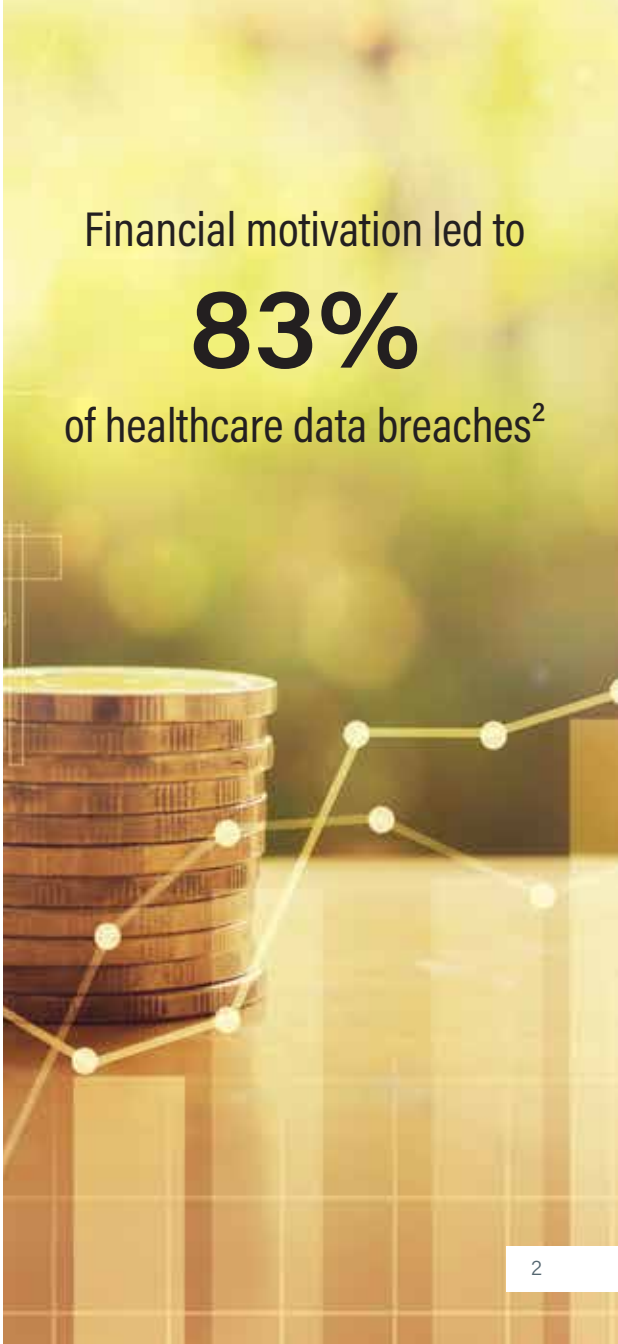
Netsurion™ | EventTracker®

# Introduction

Healthcare providers and payers have increased their use of IT to communicate with staff and patients, and to store and share sensitive patient data.

Healthcare providers must meet security requirements while meeting compliance with Health Insurance. Portability and Accountability (HIPAA) regulations. For many organizations, the geographically-dispersed locations of providers and facilities makes maintaining overall IT operations and security a complex and daunting task.

351 healthcare breaches leaked over
**13 million records**[1]



# Healthcare providers face unique IT security challenges

Electronic Health Records (EHR) and the ubiquity of mobile devices in healthcare increases risks of exposure to security breaches and many hospitals are unprepared. Ransomware has also become a challenge to health IT executives as they struggle to maintain confidentiality and to protect Protected Health Information (PHI).

- Many healthcare organizations lack the staff and expertise to defend against advanced cybersecurity threats.
- Dispersed locations and devices make safeguarding data a challenge. This requires a solution that can scale up and down with real-time 24/7 monitoring to protect sensitive data.
- Insiders accounted for 59% of recent healthcare data breaches - whether inadvertent or malicious.
- Healthcare communities are increasingly challenged by security breaches, malware, and ransomware in addition to trying to maintain HIPAA compliance.

Healthcare data breaches cost highest of any industry and costlier in the U.S.[3]

Healthcare organizations paid **$28 million** in HIPAA fines in 2018[4]

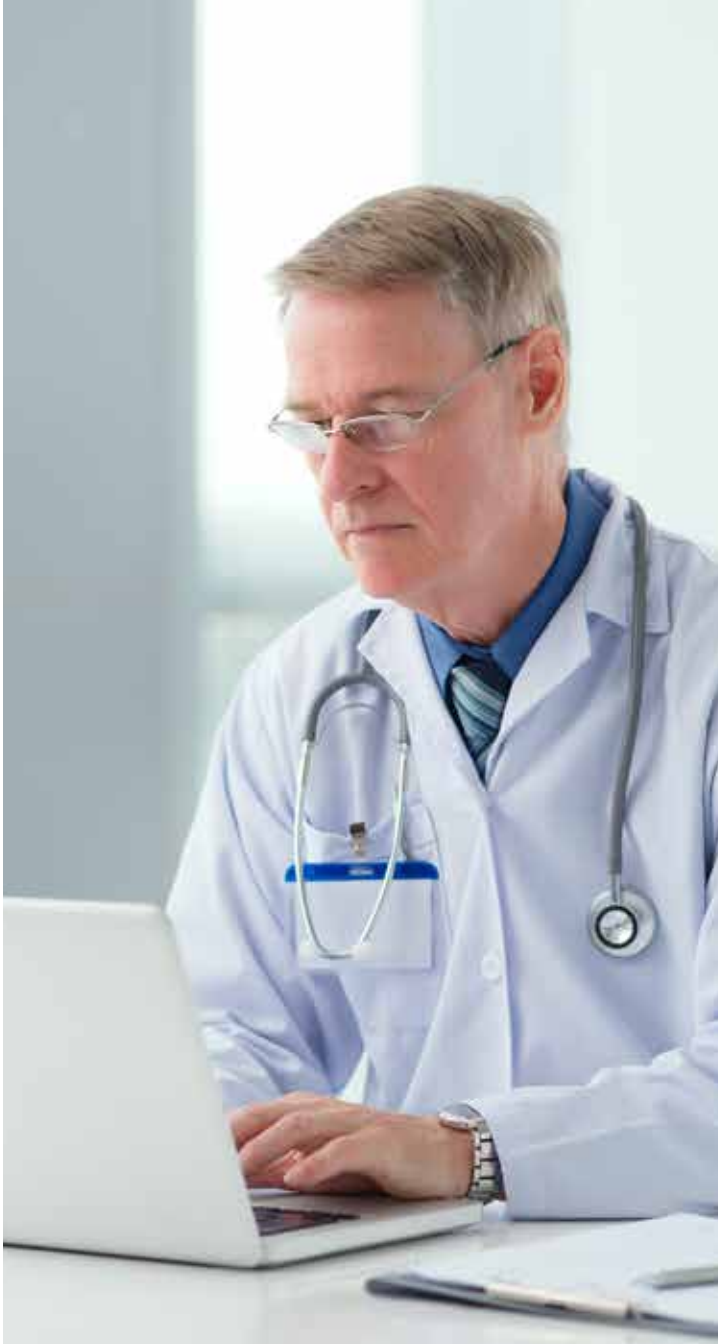
# Challenges

The biggest challenge is to find the most capable information security solution that can:

- Enhance operational efficiency
- Improve cybersecurity
- Simplify healthcare compliance

Experts to
manage it for you.

Netsurion™ | EventTracker®



# Managed SIEM

Security Information and Event Management (SIEM) centralizes log management and threat correlation via real-time analysis for rapid defense and incident recovery. The central repository also enables forensics, trend analysis, and automated compliance reporting.

Getting results from SIEM technology requires dedicated IT security expertise. A Managed SIEM allows organizations to leverage the expertise of the SIEM vendor, while retaining control of the network. A 24/7 Security Operations Center (SOC) provides remediation recommendations with full context that minimize false positives.

# Managed SIEM

## Security Experts

People with the right skills are critical to success in thwarting security breaches, and are often the hardest to assemble, train, and retain. Over 40% of organizations say they lack skilled/trained staff for security effectiveness, according to Cybersecurity Insiders.

Cyber attackers continue to elevate their capabilities; healthcare organizations must keep up with these advanced and mutating threats. It is challenging for a single organization to defend against "cybersecurity arms race". As a result, not every cybersecurity professional has, or needs to have, all of the relevant skills that a healthcare organization could need.

Unfortunately, the demand for cybersecurity professionals far outpaces the available supply. However, a Managed SIEM allows your organization to leverage a team of highly-skilled experts.

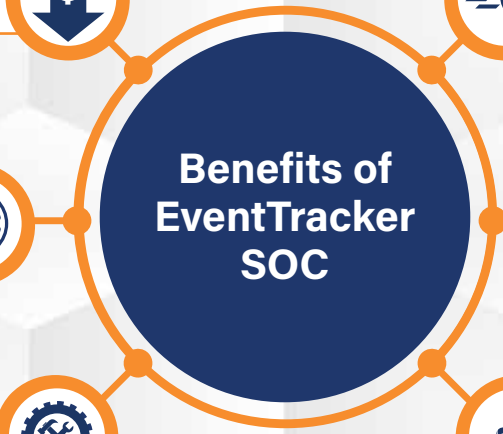
# Managed SIEM

## Comprehensive Security Technology

A complete SIEM platform with 24/7 SOC experts enables you to:

- Monitor your network for threats including malware, ransomware, advanced persistent threats, and phishing attacks.
- Assess internal and external threats.
- Detect insider threats, attack patterns, and data leaks.
- Review access to critical servers, workstations, network devices, applications, and databases.
- Simplify compliance with HIPAA, PCI DSS, and other regulations, all from an easy-to-use dashboard.

# Benefits




### Efficiency & Lower Cost

- EventTracker Security Operations Center(SOC) creates economies of scale and passes the saving on to you
- Purchase as OpEx or CapEx for lowest cost deployment and maintenance
- Extend security controls to new areas wothout significant cost increases

### Effectiveness

- Faster response to new threats and vulnerabilities
- Improvements are deployed proactively to endpoints and partners
- Continuous feedback for service improvement

### Control

- You can have as much control as you choose
- Delegate tasks to the EventTracker SOC to the extent you prefer

### Expertise

- SOC staff includes experts in popular technologies including MS Windows, RedHat, Cisco, VMware, Active Directory, Exchange, Oracle, Snort, Imperva, and McAfee ePO.
- Over time, we develop deep familiarity with your network architecture and users

### Customization & Integration

- Fine-grained customization is available to accommodate policy requirements
- Easily integrated with numerous business applications and other security controls

### Location

- All data can remain within your firewall, on your premises, oroptionally we can host it in our U.S. data center.
- SOC staff get limited audited access to EventTracker only
- All SIEM data including reports, incidents and notes remain on your premises

# Managed SIEM

## How We Help

Netsurion's co-managed SIEM, EventTracker SIEMphonic, provides experts that work with your team to plan, scope, and install the implementation, then run, watch, and tune the implementation on your behalf. These activities ensure that you realize the benefits of your SIEM platform, and derive the security protection and compliance you require.

The EventTracker SOC consults and coordinates with your healthcare IT team to configure and deploy EventTracker SIEMphonic to meet your needs. You can have as much of a hands-on role as you prefer.

# Features

EventTracker SIEM provides expertise that helps you get back to business.

- EventTracker software updates, services and knowledge packs, new release upgrades, licensing key installation
- System health checks, storage projections, and log volume/performance analysis
- Analyze changes in log collection for new systems and non-reporting systems
- EventTracker adminstration and configuration for users, standardized reports, dashboards, and alerts
- Confirm external/third party integrations are functioning normally: Threat Intel Feeds, ET-IDS, ET-VAS


- Deliver remediation recommendations via Critical Observation Report as well as executive dashboard report
- Maintain audit-ready artifacts - always be ready for a healthcare audit

# Why Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance. Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.


1. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/
2. https://www.cshub.com/attacks/articles/insiders-are-most-common-threat-actors-in-healthcare
3. https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/
4. https://www.modernhealthcare.com/article/20190208/NEWS/190209933/hipaa-enforcements-hit-record-28-million-in-2018