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.

674 healthcare breaches leaked over

40 million records[1]

> “With the shift to electronic health records and digital technology, cybersecurity is a strategic priority for the healthcare industry. Ransomware is the largest cyber threat, resulting in data theft and the disruption of healthcare services.”

The Center for Internet Security (CIS)[2]

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 safeguard 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 caused 39% of healthcare breaches while 61% were external threat actors.
- HIPAA Journal April 2021[3]
- Healthcare communities are increasingly challenged by trying to maintain HIPAA compliance.

Healthcare data breaches cost highest of any industry and costlier in the U.S.[4]

Healthcare organizations paid **$14 million** in HIPAA fines in 2020[5]

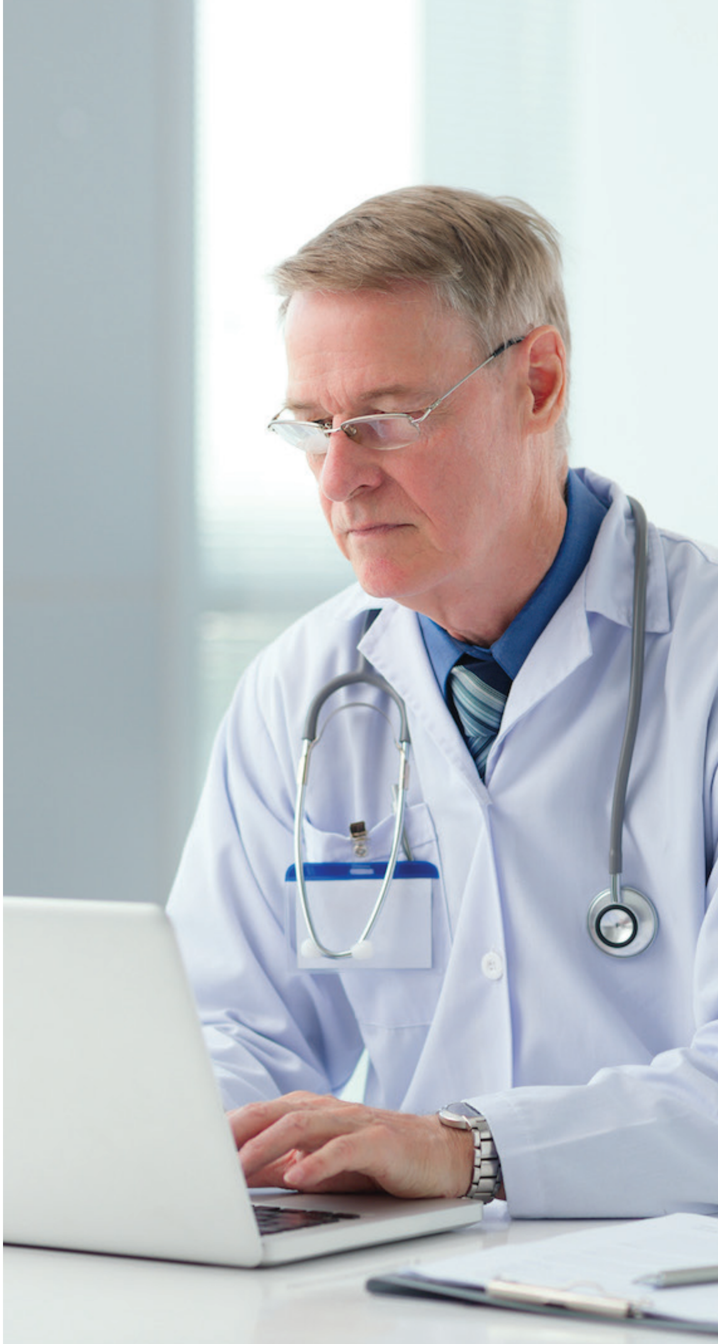
Obstacles

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 solution allows you to augment cybersecurity expertise and staff while retaining control of the infrastructure. A 24/7 Security Operations Center (SOC) provides remediation recommendations with full context that minimize false positives.

A Managed Service

Security experts

People with the right skills are critical to success in thwarting security breaches, and are often the hardest to recruit, 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 a "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 solution allows you to leverage a team of highly-skilled experts.

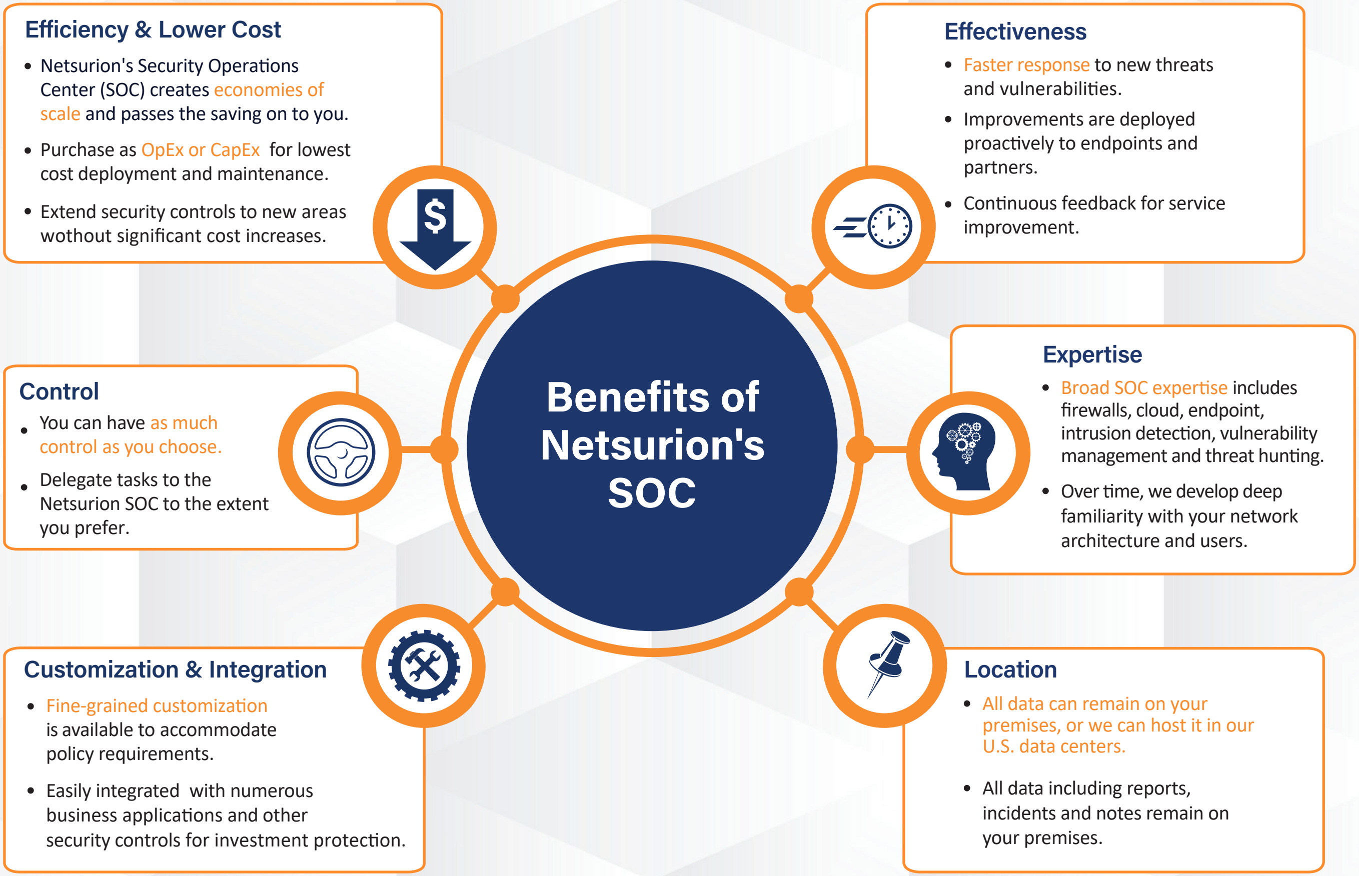
Managed Threat Protection

Comprehensive security coverage

A complete 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 a single easy-to-use dashboard.

Benefits



Benefits of Netsurion's SOC

Efficiency & Lower Cost

- Netsurion's 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 Netsurion SOC to the extent you prefer.

Expertise

- Broad SOC expertise includes firewalls, cloud, endpoint, intrusion detection, vulnerability management and threat hunting.
- 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 for investment protection.

Location

- All data can remain on your premises, or we can host it in our U.S. data centers.
- All data including reports, incidents and notes remain on your premises.

Managed SIEM

How we help

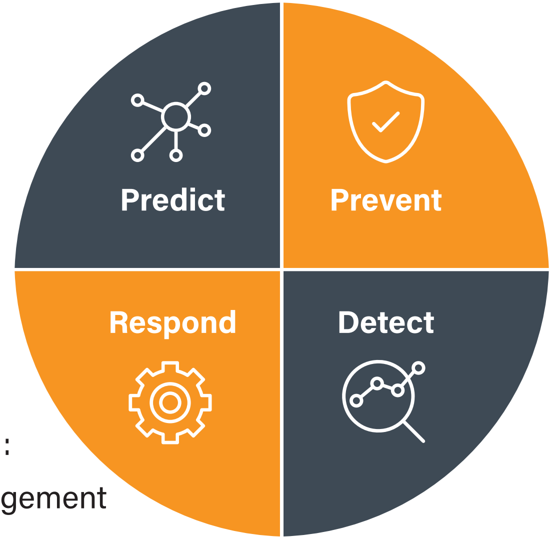
Netsurion's Managed Threat Protection, EventTracker, provides experts that work with your team to plan, scope, and install the implementation, then run, watch, and tune the implementation on your behalf. These cybersecurity actions ensure you derive the required data protection and compliance.

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

Capabilities

We provide technology and expertise that helps you get back to business.

- Comprehensive defense-in-depth protection: predict, prevent, detect, and respond to escalating threats.
- 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 operational: threat intel feeds, intrusion detection, vulnerability management
- Deliver comprehensive remediation recommendations as well as executive dashboards
- Maintain audit-ready artifacts - always be ready for a healthcare audit



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's managed platform approach of combining purpose-built technology and a team of cybersecurity experts gives customers and partners the ultimate flexibility to adapt and grow while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

1. https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/
2. https://www.cisecurity.org/hospitals/
3. https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/
4. https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/
5. https://www.hipaajournal.com/2020-hipaa-violation-cases-and-penalties/