A Comprehensive Guide to Remote Managed IT Security for Law Firms
About 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.
Introduction

Law firms are increasingly being required by their clients to bolster IT security efforts to ensure the safety of restricted corporate data, and demonstrate compliance with the relevant industry requirements.

Failure to do so can be costly. Not only can you face fines for exfiltration of private information, but the violation of confidentiality and the loss of a client’s trust will do irreparable harm to your firm’s reputation.

80% of the largest law firms have experienced a digital data breach

95% of corporate counsel believe that cybersecurity breaches are becoming more frequent in their industries
Law firms face unique IT security challenges

• Many law firms lack the network security expertise and IT security resources they need to properly defend against advanced security threats.

• Firms with multiple locations have to safeguard all devices and data from cyber threats, on the interconnected network. This requires a solution that can scale up and down to large and small offices with real-time 24x7 monitoring to protect sensitive data.

  ▪ They are big targets for malware and ransomware, with attacks motivated by cyber espionage and monetary gain.

66% of law firms do not have staff dedicated exclusively to Information Security
Challenges

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

- create operational efficiency
- improve security
- meet compliance regulations

Someone to manage it for you.
Remote Managed SIEM

Security Information & Event Management (SIEM) centralizes the storage and interpretation of security data including logs and allows near real-time analysis for rapid defense and recovery. The central repository also enables forensics, trend analysis and automated compliance reporting.

Getting results from SIEM technology requires dedicated IT security expertise. A Remote Managed SIEM allows firms to leverage the expertise of the SIEM vendor, while retaining control of the network. The remote team escalates security incidents with context to the firm’s in-house IT team so they can perform remediation.
Remote 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. At the 2016 Gartner Risk & Security Summit, more than 75% of attendees agreed that they lacked the internal staff to manage all their security activities.

Cybersecurity is a complex and nuanced field, and legal organizations require different skills to achieve their unique goals. As a result, not every cybersecurity professional has, or needs to have, all of the relevant skills that a legal firm could need.

Unfortunately, the demand for cybersecurity professionals far outpaces the available supply. However, a Remote Managed SIEM allows your firm to leverage a team of highly skilled security experts.
Remote Managed SIEM
Comprehensive Security Technology

A scalable and comprehensive SIEM platform enables you to:

- Monitor your network for threats including malware, ransomware, advanced persistent threats or phishing attacks.
- Assess external and internal vulnerabilities
- Monitor network traffic for data leakage, attack patterns, etc.
- Review access to critical servers, workstations, network devices, applications, databases, etc.
- Demonstrate compliance with PCI-DSS, SOX 404, HIPAA, FFIEC and other regulations, all from a simple easy to use dashboard.
The EventTracker takes advantage of economies of scale and passes the savings on to you.

- Purchase as OpEx or CapEx for lowest cost deployment and maintenance.
- Extend security controls to new areas without significant cost increases.

Efficiency & Lower Cost

Effectiveness

- Faster response to new threats and vulnerabilities.
- Improvements are deployed to all customers, no action needed on your part.
- Continuous feedback for service improvement.

Control

- You can have as much control as you choose.
- Delegate tasks to the ECC to the extent you prefer.

Customization & Integration

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

Location

- All data remains within your firewall, on your premises, subject to your controls.
- ECC staff get limited, audited access to EventTracker only.
- All SIEM data including reports, incidents and notes remain on your premises.

Expertise

- ECC staff includes experts in popular technologies including MS Windows, RedHat, Cisco, VMware, Checkpoint, Exchange, Oracle, Snort, Imperva, McAfee ePO etc.
- Over time, we develop deep familiarity with your network architecture and users.
Remote Managed SIEM
What to Expect

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 value you want and expect with your initial purchase.

Netsurion will consult and coordinate with your team to configure and deploy Netsurion to meet your needs. Then the staff will assume as much or as little responsibility for all SIEM-related tasks as you require.
Features

EventTracker SOC provides expert EventTracker system administration including:

- 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 Administration and Configuration for Users, Standardized Reports, Dashboards and Alerts
  - Generate Weekly System Status Report
  - Confirm external/third party integrations are functioning normally: Threat Intel Feeds, ET-IDS, ET-VAS

- Analyze your Alerts, Incidents, Anomalies and Reports
  - Escalate as needed
  - Deliver Critical Observations Report
  - Deliver Monthly or Quarterly Management Executive Dashboard Powerpoint
Features

- Review Top Level Summary Reports for relevant frameworks
- Review Detailed Reports as necessary
- Annotate finding as needed
- Maintain auditor-ready artifacts – “always be ready for an IT audit”

The EventTracker SIEMphonicteam provides on-demand expert services on an annual retainer

- Advanced Correlation and Behavior Analysis Configuration
- Custom Alerts
- Custom Scripts
- Configuring FLEX Reports and Top Level Summaries