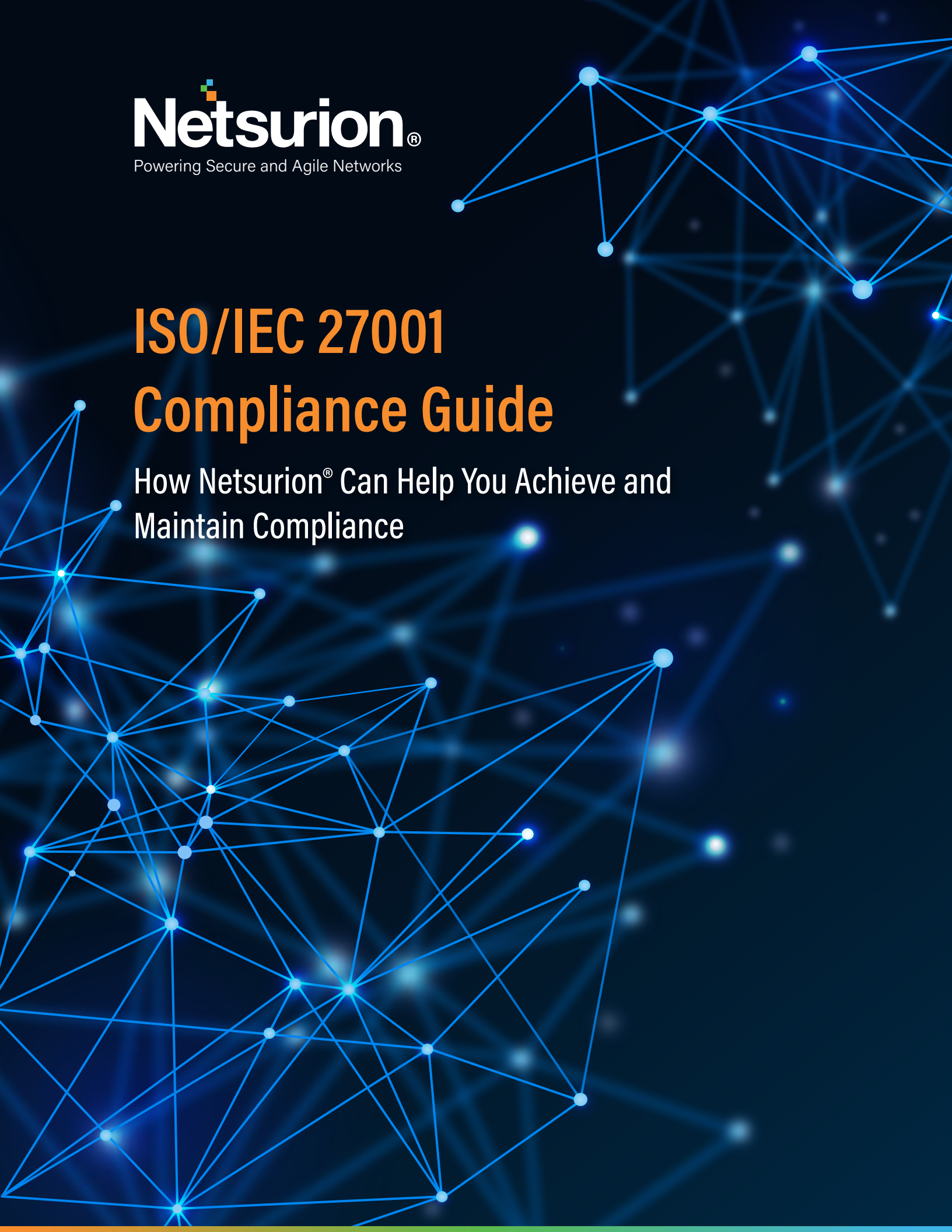
Netsurion®

Powering Secure and Agile Networks

ISO/IEC 27001 Compliance Guide

How Netsurion® Can Help You Achieve and Maintain Compliance



ISO/IEC 27001 Overview

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts — an important aspect in such a dynamic field, and a key advantage of ISO 2700's flexible risk-driven approach as compared to, say, PCI-DSS.

The standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profits), all sizes (from micro-businesses to huge multinationals), and all industries or markets (e.g. retail, banking, defense, healthcare, education and government). This is clearly a very wide brief.

EventTracker Provides a Full View of the Entire IT Infrastructure

Netsurion improves security, helps organizations demonstrate compliance and increases operational efficiencies. EventTracker SIEM enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced, minimizing potential exposure and costs.

Netsurion's Managed Threat Protection is our managed services offerings to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM-related tasks, including system management, incident reviews, daily/weekly log reviews, configuration assessments, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by EventTracker's built-in manufacturers Knowledge Base, which contains log definitions for thousands of types of log events, and automatically identifies which events are critical to security standard.

EventTracker provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, Windows, Linux/Unix, VMware ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Ease of Deployment and Scalability

EventTracker is available "on premises" or as a highly scalable cloud-based SIEM and Log Management solution. It offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for MSSP organizations serving the needs of smaller customers.

ISO/IEC 27001 Compliance Requirements

Human Resource Security

Control Description	Netsurion Capability
Control: A.8.3.3 Removal of Access Rights The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	EventTracker collects all account management activities. EventTracker reports provide easy and standard review of all account management activity.

Communications and Operations Management

Control Description	Netsurion Capability
Control: A.10.1.2 Change Management Changes to information processing facilities and systems shall be controlled.	EventTracker's Change Audit capability can be used to detect additions, modifications and deletions to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.
Control: A.10.3.1 Capacity Management The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	EventTracker provides central, secure, and independent audit log storage. EventTracker's central and extensible storage of audit log data ensures capacity will not be exceeded. EventTracker can collect logs from hosts, network devices, IDS/IPS systems, A/V systems, firewalls and other security devices. EventTracker provides central analysis and monitoring of network and host activity across the IT infrastructure. EventTracker's alarming capability can be used to independently detect and alert on threshold violations.
Control: A.10.3.2 System Acceptance Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.	EventTracker can track and report on when patches are installed on devices, showing which systems have had patching within the past month, or any other time frame as dictated by organizational policy.
Control: A.10.4.1 Controls against Malicious Code Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	EventTracker detects and alerts on any error conditions originating from anti-virus applications, when the services are started and stopped, as well as identifies when new signatures are installed. Alarming can be configured to inform the custodian(s) of when any malware is detected inside the environment.

Control Description	Netsurion Capability
Control: A.10.5.1 Information Backup Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	EventTracker can track and report on when backups are performed within the past month, or any other time frame as dictated by organizational policy.
Control: A.10.6.1 Network Controls Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	EventTracker can collect logs from hosts, network devices, IDS/ IPS systems, A/V systems, firewalls, and other security devices. EventTracker provides central analysis and monitoring of network and host activity across the IT infrastructure. EventTracker can correlate activity across user, origin host, impacted host, application and more. EventTracker can be configured to identify known bad hosts and networks. EventTracker's alarming capability can be used to independently detect and alert on network and host based anomalies via sophisticated filtering, correlation and threshold violations.
Control: A.10.9.3 Publicly Available Information The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.	EventTracker's file integrity monitoring capability can be used to detect additions, modifications, deletions, and permission changes to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.
Control: A.10.10.1 Audit Logging Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	EventTracker's monitoring, analysis, archiving, alerting, auditing and reporting capabilities provide for continuous monitoring of access points across the Electronic Security Perimeter(s). For instance, EventTracker monitors unauthorized access for auditing, logging, archiving and alerting.
Control: A.10.10.3 Protection of Log Information Logging facilities and log information shall be protected against tampering and unauthorized access.	Using EventTracker helps ensure audit trails are protected from unauthorized modification. EventTracker collects logs immediately after they are generated and stores them in a secure repository. EventTracker servers utilize access controls at the operating system and application level to ensure that log data cannot be modified or deleted.
Control: A.10.10.5 Fault Logging Faults shall be logged, analyzed and appropriate action taken.	EventTracker collects logs continuously and real-time in the organizational IT environment. The logs are analyzed and presented in the EventTracker Dashboard for real-time review. Alarms are activated on critical events that will cause immediate and direct notification to the administration. Reports and investigations for compliance are available at all times.

Access Control

Control Description	Netsurion Capability
Control: A.11.2.1 User Registration There shall be a formal user registration and deregistration procedure in place for granting and revoking access to all information systems and services.	EventTracker collects all account management and account usage activity. Changes to accounts, usage of default accounts and the full range of authorization and permissions related activity are automatically monitored and can be easily alerted on when unauthorized activity is detected. Preconfigred reports are provided to supply full account of all account usage and change history.
Control: A.11.5.1 Secure Log-on Procedures Access to operating systems shall be controlled by a secure log-on procedure.	EventTracker collects all account management and account usage activity. Changes to accounts, usage of default accounts and the full range of authorization and permissions related activity are automatically monitored and can be easily alerted on when unauthorized activity is detected. Preconfigred reports are provided to supply full account of all account usage and change history.
Control: A.11.5.4 Use of System Utilities The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	EventTracker can collect audit logs reporting on the access and use of utilities on hosts for monitoring and reporting. Additionally, EventTracker's file integrity monitoring capability can be used to independently detect access and use of utilities.
Control: A.11.6.1 Information Access Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	EventTracker supplies a one stop repository from which to review log data from across the entire IT infrastructure. Reports can be generated and distributed automatically on a daily basis. EventTracker provides an audit trail of who did what within EventTracker and a report which can be provided to show proof of log data review.

Information System Acquisition, Development and Maintenance

Control Description	Netsurion Capability
Control: A.12.4.2 Protection of System Test Data Test data shall be selected carefully, and protected and controlled.	EventTracker's Change Audit capability can be used to detect additions, modifications and deletions to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.
Control: A.12.4.3 Access Control to Program Source Code Access to program source code shall be restricted.	EventTracker's Change Audit capability can be used to detect additions, modifications and deletions to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.
Control: A.12.5.1 Change Control Procedures The implementation of changes shall be controlled by the use of formal change control procedures.	EventTracker monitors for proper operations and configuration changes that may put at risk the security of the system.
Control: A.12.5.2 Technical Review of Applications after Operating System Changes When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	EventTracker monitors for proper operations and configuration changes that may put at risk the security of cardholder data.
Control: A.12.5.3 Restrictions on Changes to Software Packages Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	EventTracker monitors for proper operations and configuration changes that may put at risk the security of cardholder data.
Control: A.12.5.4 Information Leakage Opportunities for information leakage shall be prevented.	EventTracker can monitor and logs the connection and disconnection of external data devices to the host computer where the Agent is running. It also monitors and logs the transmission of files to an external storage device.
Control: A.12.6.1 Control of Technical Vulnerabilities Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	Vulnerabilities can be detected by real-time examination tools or by using ETVAS vulnerability scanning systems.

Information Security Incident Management

Control Description	Netsurion Capability
Control: A.13.1.1 Reporting Information Security Events Information security events shall be reported through appropriate management channels as quickly as possible.	Vulnerabilities can be detected by real-time examination tools or by using EventTracker Vulnerability Management's scanning systems.
Control: A.13.1.2 Reporting Security Weaknesses All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	EventTracker documents alarm and response activities such as 'responsible parties notified'; alarm status such as 'working, escalated, and resolved'; and what actions were taken.
Control: A.13.2.1 Responsibilities and Procedures Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	EventTracker documents alarm and response activities such as 'responsible parties notified'; alarm status such as 'working, escalated, and resolved'; and what actions were taken.
Control: A.13.2.2 Learning from Information Security Incidents There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	EventTracker completely automates the process and requirement of collecting and retaining security event logs. EventTracker retains logs in compressed archive files for cost effective, easy to-manage long-term storage. Log archives can be restored quickly and easily months or years later in support of after-the-fact investigations.
Control: A.13.2.3 Collection of Evidence Where a follow-up action against a person or organization after an information security incident involves legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant authority(s).	EventTracker documents alarm and response activities such as 'responsible parties notified'; alarm status such as 'working, escalated, and resolved'; and what actions were taken.

Business Continuity Management

Control Description	Netsurion Capability
Control: A.14.1.2 Business Continuity and Risk Assessment Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	EventTracker collects logs continuously and real-time in the organizational IT environment. The logs are normalized, analyzed and presented in the EventTracker Dashboard for real-time review. Alarms are activated on critical events that will cause immediate and direct notification to the administration. Reports and investigations for compliance are available at all times.

Compliance

Control Description	Netsurion Capability
Control: A.15.1.3 Protection of Organizational Records Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	EventTracker's Change Audit capability can be used to detect additions, modifications and deletions to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.
Control: A.15.3.2 Protection of Information Systems Audit Tools Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	EventTracker's Change Audit capability can be used to detect additions, modifications and deletions to the file system. Analysis & reporting capabilities can be used for monitoring configuration changes. Real-time alerting can be utilized to detect and notify of changes to specific configurations.

Reference

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

How Netsurion Can Help

Not sure where to begin? Netsurion helps you reduce cyber risk, augment your IT team's skills, and spend less time on documentation and compliance readiness. Contact us and our experts can advise you on the path to achieve ISO/IEC 27001 preparedness.

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.