Visibility for Protecting Performance and Availability of Insurance Company Networks

Insurance companies exist to protect businesses and consumers from loss. Regardless of whether the calamities involve life, health, property, or auto, there is an associated insurance policy available to help compensate for that loss.

But how do insurance companies protect themselves from risks related to security threats? A successful breach can:

- Cause loss of client's private data
- Cause catastrophic damage to internal applications and databases
- Impede access to the company portal that is used by thousands of agents, affiliates, and customers to conduct business from volumetric or distributed denial of service (DDoS) attacks

These questions are top of mind at the executive level of many insurance companies today, in part because of their potential to cause financial and reputational damage to their own business. However, there are several additional factors that raise the stakes still higher. In particular, the rise of several new regulatory initiatives that now obligate insurance organizations to comply with specific security requirements has put a new light on the need to step up monitoring and preventive strategies.

Drivers for Improving Monitoring and Security Capabilities

The need to increase and improve monitoring and security capabilities in insurance companies is driven by the well-recognized gap in existing legacy security tools, the expanded role and influence of chief compliance officers (CCOs), and the increased importance of compliance with new regulations and periodic risk assessments. Investments in new digitally transformative technologies, advances in cloud solutions, and the adoption of Software-as-a-Service applications add even more complexity in protecting service delivery.

These issues include:

Gap in monitoring and security solutions. While cybercriminals constantly evolve and increase the sophistication of their security threats and attacks, the protection used by insurance companies is becoming outdated and increasingly ineffective. This gap in protection is well recognized at the highest levels of insurance company management and is one of the drivers that are prompting insurance organizations to upgrade and/or expand their security protection. Additionally, cybercriminals have become experts at lurking undetected inside company networks for extended periods of time before successfully executing their attacks. Broader visibility has never been more important, both internally and externally, to detect, investigate, and respond to potential risks and threats.

Expanding role and influence of Chief Compliance Officer. As one of the most highly regulated industries, insurance companies must comply with a host of complex regulations. Recently initiated regulations have compliance deadlines staggered between 2017 and 2021, which has elevated the role of Chief Compliance Officer to board-level visibility and influence. Meeting the deadlines for initial compliance and managing ongoing compliance processes requires oversight, strategy, planning, and execution expertise.

Increase in new regulations and periodic risk assessment and reporting. High-profile cybersecurity breaches in 2014 and 2015 have resulted in new legislation designed to strengthen security practices. At the center of this legislation is the National Institute of Standards and Technology (NIST) 800-53, a new standard for security and privacy controls for all U.S. federal information systems (except those pertaining to national security). A major element of this gold standard in cybersecurity calls for documenting cyber risks as part of annual or semi-annual certifications, putting responsibility for security squarely on leadership.

The Securities and Exchange Commission (SEC) has issued guidance calling for security breaches and service outages caused by cyberattacks material events to be disclosed within 72 hours. The SEC has gone so far as to make the board of directors and C-level executives of public companies accountable for risks stemming from cybersecurity, thereby exposing them to class action lawsuits.

Increased complexity from digital transformation. In a period when insurance companies have benefited from global economic growth, rising interest rates, and higher investment income, there has been higher spending on digitally transformative technologies, like cloud, SD-WAN, and mobile applications for customers. These technologies have created new complexities in assuring availability and security of application service delivery. Protecting legacy environments while innovating securely has been the challenge, leading insurers to acquire and implement targeted solutions for data security, data privacy, and cybersecurity.

These four influencers collectively drive the need for insurance organizations to improve their business assurance coverage with superior performance monitoring and security capabilities.

Our Approach for Gaining Monitoring and Security Visibility

NETSCOUT's approach to business assurance is built on a foundation of high-quality data and real-time analytics via monitoring and deciphering the actual communications traffic making it difficult, if not impossible, for bad actors to hide when we are monitoring the network. Based on network traffic, NETSCOUT's patented Adaptive Service Intelligence™ (ASI) technology provides the most robust data source available to ensure services are delivered by measuring the actual transactions and dependencies of the service.

NETSCOUT® analytics are the industry-leading standard for scalability and ease-of-use, enabling proactive service triage to keep all aspects of the insurance business running smoothly end-to-end. Leveraging ASI, the nGeniusONE® Service Assurance platform and Arbor Threat Analytics solution provide unmatched capabilities that ensure the reliable availability and uninterrupted delivery of critical networked application services, ensuring they do not cause process delays or quality issues.

Our Solutions

NETSCOUT delivers visibility to support insurance companies' security and performance requirements. Depending on the specific needs of your organization, NETSCOUT offers a number of cybersecurity solutions for insurance companies, including:

- nGeniusONE Service Assurance platform that leverages ASI data from packets monitored by InfiniStreamNG™ (ISNG) appliances and vSTREAM™ virtual appliances for real-time performance metrics. ASI generates Key Performance Indicators (KPIs) from analysis of traffic utilization, application, and database servers and network errors. Providing analysis of more than 1,000 voice, video, and data applications, nGeniusONE analytics can help triage issues related to either performance degradation or security risks to quickly put the right information in the hands of the right team at the right time for further investigation and resolution or mitigation.

Potential Penalties for Non-Compliance

Health insurers – Must meet Health Insurance Portability and Accountability Act (HIPAA) requirements noted in the Privacy Rule, Security Rule, the Omnibus Rule, and the HITECH Act (Updated between 2003 and 2013). These updates require notification of breaches to the Department of Health and Human Services, which can result in financial penalties for non-compliance of up to $250,000 and criminal penalties.

Insurance industry – The National Association of Insurance Commissioners (NAIC) passed an Insurance Data Security Model in 2017 that is the basis of multiple current state laws and is in legislatures of several others requiring the implementation of an information security program that covers data security, investigation, and notification to regulators of security breaches and events within 72 hours.

US financial companies – Financial companies must meet Gramm-Leach-Bliley Act requirements (Financial Services Modernization Act of 1999) for the secure handling of non-public personal and financial information.

Publicly traded companies – The Securities and Exchange Commission (SEC) updated guidance that requires companies to disclose security breaches and service outages caused by cyberattacks within 72 hours, holding board of directors and executives responsible for cybersecurity disclosures.

Companies that service the federal government – Companies in this sector must comply with the Federal Information Security Management Act (FISMA). Based on NIST 800 (see above), FISMA requires companies to self-assess and manage risks associated with cybersecurity, as well as perform annual audits and semi-annual risk assessments of insurance system and communications protection. Failure to comply can result in loss of government funding or participation in future contracts, as well as potential government hearings and reputational damage.

https://blog.rsisecurity.com/penalties-for-non-compliance-with-fisma-and-how-to-avoid-them/

Foreign companies processing data belonging to EU residents – The General Data Protection Regulation (GDPR) extends data protection laws and requires disclosure of breaches within 72 hours; otherwise, insurance companies risk fines ranging from 10,000,000EUR or 2% revenue for low-level failures to 20,000,000 EUR or 4% revenue for high-level failures.

All the above stipulations ultimately depend on reporting and that requires monitoring and detection.

- Arbor Threat Analytics (ATA) solution that leverages information from ISNG appliances and vSTREAM virtual appliances, providing valuable visibility to protect the insurance organization from enterprise-wide network threats to the business. With the ability to promptly and efficiently detect, validate, and respond to threats, ATA serves as an early warning system of damaging incidents. Leveraging the same ASI data for analytics, insurance organizations can reduce the time cybercriminals can lurk in the network, thus reducing exposure to risks associated with the company's resources and systems, customer data, reputation, and regulatory compliance directives.
- Arbor Edge Defense (AED) is a stateless packet processing engine that acts as a network perimeter enforcement point, detecting and blocking inbound cyberthreats such as DDoS attacks or other Indicators of Compromise (IoCs) as well as outbound malicious communications from compromised internal devices to known bad sites. Leveraging ATLAS global threat intelligence, AED is able to provide more context to blocked IoCs.

Depending on the specific insurance organization's security or performance management need, NETSCOUT offers several other solutions that can work in concert with those highlighted above to provide the right protection for the threats and risks facing their organization.

Value to Insurance Companies

For insurance companies, NETSCOUT solutions are designed to ensure IT services supporting business are available and performing as expected. With NETSCOUT cybersecurity and performance assurance solutions, insurance companies will benefit from:

- **Faster response to the most serious threats.** Leveraging powerful detection, investigative, and forensics analysis capabilities minimizes catastrophic impact to the business by blocking cybercriminals from dwelling in the environment over protracted periods of time.
- **Reduced financial loss.** Rapid, focused detection and logical, intuitive workflows for threat investigation minimize exposure to security threats and costly repercussions such as remediation costs, as well as damage to customer loyalty and reputation.
- **Improved collaboration with combined first and last line of defense.** AED has the ability to stop inbound DDoS attacks and IoCs as well as detect and block outbound communications from compromised internal devices to known bad sites.
- **More efficient, rapid security team response.** NETSCOUT's ATLAS® global threat intelligence drives faster risk analysis by providing teams with more context to blocked IoCs.
- **Extends value of investment across full complement of their security tools.** NETSCOUT cybersecurity solutions can be integrated existing security stacks, including robust TEST API and support for Syslog, CEF, LEEF, and STIX/TAXII.

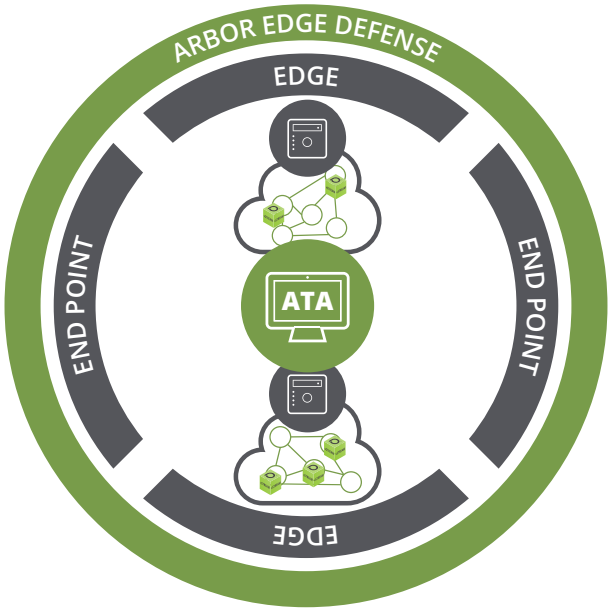

Figure 1: Arbor Threat Analytics (ATA) provides visibility deep inside data centers, between the edge and endpoints, for any infrastructure, any application, and anywhere for threat detection, incident response and forensic analysis, using the best data source for security and network operations. Arbor Edge Defense (AED) is focused on security for beyond the perimeter to detect and block both inbound cyberthreats, such as DDoS attacks or other IOCs, and outbound malicious communications from compromised internal devices to known bad sites.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

EFS_017_EN-1901 12/2019