TAG

BUYER'S GUIDE FOR ENHANCED SECURITY SERVICES IN MOBILE AND CONVERGED TELECOM INFRASTRUCTURE

DR. EDWARD AMOROSO,
FOUNDER & CEO, TAG

allot

BUYER'S GUIDE FOR ENHANCED SECURITY SERVICES IN MOBILE AND CONVERGED TELECOM INFRASTRUCTURE

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG

This TAG Infosphere[1] buyer's guide addresses the need to embed security services into mobile networks. Direct buyers are the communication service providers (CSPs)[2] who need the ability to deliver increased security to their customers. The end-users are the consumers and small businesses who desire hassle-free security services from their provider. The Allot[3] NetworkSecure solution[4] is shown to address these requirements.

INTRODUCTION

A major challenge for CSPs involves providing a good balance between the need to support connectivity for customers to access the on-line services they desire, while also helping to maintain a safe and secure environment for consumers and small businesses. This goal demands at minimum the ability for CSPs to offer the option for buyers to obtain and self-manage new cybersecurity protections in their network services.

[1] *TAG Infosphere provides research and advisory in cybersecurity, artificial intelligence, and climate science/sustainability for enterprise teams, government agencies, public policy lawmakers, academic researchers, and commercial vendors. See* https://www.tag-infosphere.com.

[2] *Throughout this report, we refer to the communication service provider (CSP) as being essentially synonymous with the term Internet service provider (ISP), which is commonly used in the United States. In both cases, we assume the CSP or ISP to be the conduit for users to access the Internet. Obviously, this service is typically bundled with additional offerings for voice, video, and other commercial capabilities.*

[3] *Allot is a major global provider of leading innovative network intelligence and cybersecurity solutions for service providers and enterprises across the world. Additional detailed information on Allot can be obtained at* https://www.allot.com.

[4] *Allot NetworkSecure delivers robust and content filtering services to customers from within the communication service provider's network. Much of the information in this report is derived from* https://www.allot.com/network-security/network-security-services.

To achieve higher levels of cybersecurity for customers, CSPs can overlay the required capabilities onto their network at the application level, known informally as an over-the-top (OTT) approach. This might be useful for CSPs who would like to augment their cyber protections without burdening subscribers with the aggravation of software installation and maintenance. Such attention is driven by the increased threats that emerge for the end customers of CSPs.[5]

CSPs can also, however, seek to integrate such capabilities into their network infrastructure. Our focus here is on a streamlined strategy that involves the best elements of network integration with use of a third-party vendor. While there are pros and cons to any solution, we believe that the embedded strategy through vendor partnership results in a superior experience from a performance, security, and support perspective.

This TAG Infosphere report offers a practical buyer's guide for CSPs who choose to take this embedded approach toward increasing the cybersecurity options for their mass market customers. A set of criteria requirements is offered to guide buyers to the optimal functional capabilities and the Allot NetworkSecure product is used to demonstrate how a commercial solution can meet the desired requirements.

FUNCTIONAL REQUIREMENTS FOR BUYERS

Any CSP buyer who seeks to embed the ability to deliver security services into their infrastructure for mass market customers should review the functional requirements below for applicability to their circumstances. Each of the requirements is listed and explained briefly in the context of a CSP making design decisions for their own infrastructure. We then apply these requirements to the Allot NetworkSecure product to illustrate practical coverage.

NETWORK TECHNOLOGY REQUIREMENTS

R1.1 Mobile Networks: Integrating a security solution into the CSP infrastructure for mobile networks would involve deploying security measures specifically tailored to the unique challenges and characteristics of mobile communication, such as securing mobile devices and protecting against mobile-specific threats like mobile malware.

R1.2 Converged Networks: In converged networks where both mobile and fixed services are provided over a unified infrastructure, the security solution integration would need to address the security needs of both mobile and fixed services within the same network environment. This could involve implementing comprehensive security measures that cover all aspects of converged network traffic, from mobile data to fixed line Internet traffic.

DEPLOYMENT REQUIREMENTS

R2.1 Standalone Solution Support: The security solution should be capable of being deployed as a mostly standalone solution within the CSP infrastructure, providing dedicated security functionalities without relying on external systems or dependencies. (Obviously, any system deployed into CSP infrastructure cannot be fully standalone and will rely on updates from adjacent connected system.)

R2.2 Virtual and Cloud Functions: To support virtualized network environments, the security solution should be deployable as a Virtual Network Function (VNF) or Cloud-Native Function (CNF), allowing for flexible and scalable deployment within a virtualized network infrastructure.

---

[5] *Traveling executives and staff, for example, often must make use of foreign-owned networks that could be easily subjected to local laws (or lack of laws) that might be inconsistent with the organizational mission and goals. In these potentially hostile circumstances, OTT solutions at the application level (e.g., encryption) are highly recommended.*

R2.3 White Label Deployment: The solution should include the ability for CSPs to deploy the embedded cybersecurity services in a manner that is resold to their family and small business end-users in a so-called "white label" marketing arrangement.

R2.4 Zero Touch Management: The solution should provide a means for end-users to self-manage their policies and enforcement mechanisms in a zero-touch manner. This will help to simplify deployment and streamline management.

CORE SECURITY REQUIREMENTS

R3.1 Core Embedded Solution: The security solution should be integrated into the core infrastructure of the CSP, providing fundamental security capabilities at the network level to protect against a wide range of threats and vulnerabilities to end-users.

R3.2 Edge Embedded Solution: Similar to core security requirements, edge security solutions need to be integrated into the network infrastructure at the edge, where traffic enters and exits the CSP network, to provide effective protection against threats at the network perimeter to end-users.

POLICY REQUIREMENTS

R4.1 Malware Protection: The security solution should include robust malware protection mechanisms, such as antivirus scanning, to detect and mitigate malware threats targeting network endpoints and end-user system.

R4.2 Website Filtering: Implementing website filtering capabilities within the security solution allows for the enforcement of policies to block access to malicious or inappropriate websites, helping to prevent malware infections and protect users' privacy.

R4.3 Content Control: Integration of content control features enables CSPs to offer services that allow end-users to manage and monitor their Internet usage, including restricting access to certain content categories or setting usage limits.

R4.4 Device/IoT Protections: With the proliferation of connected devices and IoT (Internet of Things) devices, the security solution should provide protections against threats targeting these devices, such as certain types of IoT malware.

R4.5 Off-Net Security: Off-net security capabilities are necessary to extend security protections beyond the CSP's network boundaries, ensuring that users remain protected even when accessing external networks or services, such as public Wi-Fi hotspots.

CASE STUDY: ALLOT NETWORKSECURE

The Allot NetworkSecure product is a commercially available solution for CSPs that can be implemented as a standalone component, virtual network function (VNF), or cloud-native function (CNF) at the core or edge of the service provider's mobile network infrastructure. The solution is designed to attract CSP mass market customers to use the services to enforce customizable policies including content controls and malware avoidance.

Our observation is that the Allot NetworkSecure solution matches up well with the set of criteria shared above (R1.1 through R4.5) for CSP buyers seeking to augment their infrastructure with the ability to upsell additional cybersecurity solutions for consumers and small business. Below we review each of the requirements and show how the Allot solution offers effective functional support.

R1.1 Mobile Networks	The Allot NetworkSecure solution can be deployed into mobile (e.g., 4G/LTE, 5G) network infrastructure.
R1.2 Converged Networks	Converged mobile and broadband networks are also easily covered by the Allot Secure.
R2.1 Standalone Solution Support	Standalone software is often used by Allot customers, especially in traditional networks.
R2.2 Virtual and Cloud Functions	Virtual and cloud functional support are supported modes of deployment for Allot NetworkSecure.
R2.2 Virtual and Cloud Functions	The Allot NetworkSecure product should enable white label resale by CSPs.
R2.4 Zero Touch Management	The NetworkSecure product should support self-management with zero touch.
R3.1 Core Embedded	The Allot NetworkSecure solution can be embedded into the core network infrastructure.
R3.2 Edge Embedded	The Allot NetworkSecure solution can be embedded into the network infrastructure edge.
R4.1 Malware Protection	The Allot NetworkSecure solution is designed to detect and thwart malware traversing the network.
R4.2 URL Filtering	Threat-informed URL filtering capability is a key function supported in the Allot NetworkSecure solution.
R4.3 Content Controls	Configurable control filtering is a key function supported in the Allot NetworkSecure solution.
R4.4 Device/IoT Protection	In conjunction with Allot DNSSecure, devices including IoT can be protected from within the network.
R4.5 Off-Net Security	Allot partners with the best endpoint security providers to extend security off-net to the device.

Figure 1. Comparison of Allot NetworkSecure to Requirements Criteria

ACTION PLAN

The recommendation here is that CSPs should take a close look at the NetworkSecure capability for augmentation of their network infrastructure to provide new services. This will help to increase revenue opportunities and serve to reduce nagging cyber risks being addressed by consumers, and small business. These individuals and groups will value the opportunity to work with their provider to address their risk concerns such as parental control for minors.

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.