allot
See. Control. Secure.

Position Paper

Converged Customer Security Services for CSPs

February 2024

Contents

Executive Summary

In the world of telecommunications, convergence is a word that has many meanings. In this paper, we will stick to a single definition. At Allot, we refer to convergence when we talk about the integration of cybersecurity services for mobile and fixed broadband customers. This can be for both consumer and small business customers in the realm in which we operate.

Telecom operators that are also ISPs have been chasing after convergence solutions for a decade. For the sake of simplicity, we refer to these service providers with the umbrella term of Communication Service Providers (CSPs). Now that converged customer security services are available, CSPs can enjoy the many business benefits that they offer compared with standalone services. These include lower implementation, provisioning and maintenance costs, improved customer experience and brand differentiation.

Converged security solutions go hand in hand with network-native approach to customer security. 'Network-native' refers to services that are provided from within the CSP's network. While these services can be offered as standalone mobile or fixed services, their full value is released when they are implemented as a unified solution for both mobile and fixed customers. In this paper, we will briefly discuss the challenges that CSPs face in implementing customer security services and will address the advantages that converged security services grant CSPs who embrace them.

Challenges – CSPs and Siloed Security Solutions

CSPs are saddled with traditional IT and implementation challenges which lead to a sub-par customer experience and a long time-to-market for launching new solutions. Convergence fundamentally addresses these problems.

For a long time now, CSPs have been offering security solutions to their consumer and small business customers. These markets, according to Allot research, are primed for security services from their CSPs. However, because of the challenges, CSPs are often reticent to implement security solutions beyond standalone endpoint solutions.

When a CSP implements diverse security solutions for different types of customers (that is mobile and fixed), the CSP needs to monitor, maintain and support each solution separately, and each solution requires its own IT stack. This leads to additional resource expenditure which can be reduced with converged security solutions.

When a CSP wants to implement a security solution for mobile customers from one vendor and a solution for fixed customers from a different vendor, the CSP is left with two disparate solutions that require separate provisioning and monitoring. This is often true when both solutions are provided by the same vendor, as well. Disparate solutions increase the resources that the CSP needs to expend for security provisioning, sales and support, making both solutions less attractive. Endpoint solutions also offer limited monetization opportunities, with the majority share of revenues being taken by the endpoint solution vendor.

Beyond the direct financial factors, standalone endpoint solutions traditionally suffer from low adoption rates, often below 5%. This is a result of the downloading, installation, configuration, operation and maintenance processes being more complex than end users are comfortable with. Customers want a hassle-free security experience that standalone endpoint solutions do not offer. These issues are mitigated with converged security solutions, which, by definition need to be network-native solutions in order to be converged. This will be explained in more detail below.

The Solution – Converged Customer Security Services

By merging Customer Premises Equipment (CPE) client and network-based security into a unified, CSP-branded service, the customer enjoys a seamless, personalized experience that protects end-user devices and data.

Once, there were dramatic differences between fixed and wireless infrastructure. Now with software-defined networks, microservices and the like, fixed and mobile networks are more similar to one another. This convergence of network technologies makes convergence of network services, from billing to customer-facing services such as security, more achievable and more cost-effective.

For example, in a mostly-hardware network, the hardware needs to be upgraded from time to time, making service changes more complicated and expensive. That makes converged services even more of a challenge to maintain, leading to telcos making difficult decisions when it comes to the adoption of converged services, even when they know that they would benefit their customers. But today, with software-defined network infrastructure, where changes are predominantly software changes, the benefits of converged services, and particularly converged security services, are easier to achieve.

One good reason to converge mobile and fixed security services into a unified solution is that security simply works better and is more efficient when network data is not siloed. Greater efficiencies arise when both networks use the same threat database. But there are a lot of other good reasons for CSPs to implement converged security platforms, and CSPs know it.

In a global survey by Coleman Parkes Research, 94% of MNOs answered that they are interested in Converged Security – an integrated and unified approach of implementing comprehensive security measures across services, networks, and platforms. Their top criteria for convergence solutions included comprehensive threat detection, compatibility with existing security offerings, product portfolio and future roadmap, and scalability across fixed and wireless portfolios.

They indicated that the building blocks for a converged security solution included identity and access management, unified threat management, and centralized monitoring and management. Critical features for a positive customer experience with converged security included consistent and robust security, transparent security updates, reduced customer involvement, and easy setup and configuration. These are all good reasons to move to converged security.

In the survey mentioned, CSPs related that their expectations from converged security solutions included consistent and robust security across fixed-line, mobile, IoT, and digital services, transparent security updates and patches, reducing the need for customer involvement in managing security and easy setup and configuration.

In addition to improved efficiency and customer experience, converged security can deliver a marked boost in ARPA (Average Revenue Per Account) and improved customer retention among a list of benefits.

Operations

Convergence enables consolidated management across the account, centralized provisioning and service, reduced need for multiple parallel systems for different services, and a consolidated support platform and call center. Benefits include reduced operational cost (fewer tickets per account), reduced time to troubleshoot and resolve problems, improved automation, and improved self-service.

Sales and Marketing

Convergence, combined with a 360-degree offering, provides the ability to own the whole account, contributing to revenue opportunities in wireless, fixed, media, home security, consumer IoT, security, and other value-added services. The CSP can cross-sell, up and-sell future services (e.g., 5G, fiber, IoT services), improve profitability, and reduce Customer Acquisition Cost.

Accelerating Net-Adds

From experience with customer and prospect interactions, Allot estimates that CSPs can improve their net adds, via a converged security offering, by an average of 6-7%. This can have significant impact on revenue. For example, for a hypothetical CSP with 10M subscribers and average annual growth rate of 100,000 net

adds, 6% represents an additional 6,000 net-adds. Multiplied by an estimated monthly ARPU of $35, over the course of 3 years, this yields an additional $7.5M in revenue.

CSP Differentiation

Converged security is a core service application along with all of the primary CSP services on the network such as voice and data. It helps to differentiate the CSP's offering with an easy-to-onboard, easy-to-use service that provides a basic need to the customer. It also creates a more sticky relationship with customers.

Customer Experience

Security convergence also contributes to a better customer experience in a number of ways including a single Telco for all network service needs, enhanced customer plans and offers, easy account management for all services and users and better self service. These advantages lead to improved service experience and customer satisfaction, better value for converged bundles, better customer support and easier management of the services e.g., billing, setup and support.

How Converged Security Solutions Are Implemented

As mentioned earlier, converged security solutions are, by definition, network-native solutions. That means that they are integrated into the CSP network. This creates a situation where cybersecurity threats are blocked inside the network instead of on each individual device. Connect a device, be it a mobile phone or a CPE, to the network and it is protected from threats before they even reach the device. This situation offers a host of benefits to the CSP and to the end user. These benefits are described in more detail in an Allot Position Paper titled WORLD-LEADING NETWORK-NATIVE SECURITY.

Whether the mobile and fixed security services solutions come from a single vendor or different vendors, the CSP can use an umbrella platform that bridges the onboarding, configuration and reporting of different network-native solutions into a single, unified solution. When an Allot security solution is implemented, for example, the CSP can also deploy ASM, or Allot Security Management, platform. Telecom networks are not inherently designed with security in mind, let alone converged security. Platforms such as ASM give telecom networks the ability to deliver converged security services, with all the benefits they provide.

Conclusion

CSPs stand to reap numerous benefits from embracing converged security solutions. Considering the challenges associated with siloed security solutions and the complexities of implementation, the advantages of converged security solutions, facilitated by network-native approaches, are becoming increasingly compelling. Through a unified approach to security provisioning, monitoring, and support, CSPs can streamline operations, boost sales and marketing results, accelerate net-adds, and significantly enhance the overall customer experience.