

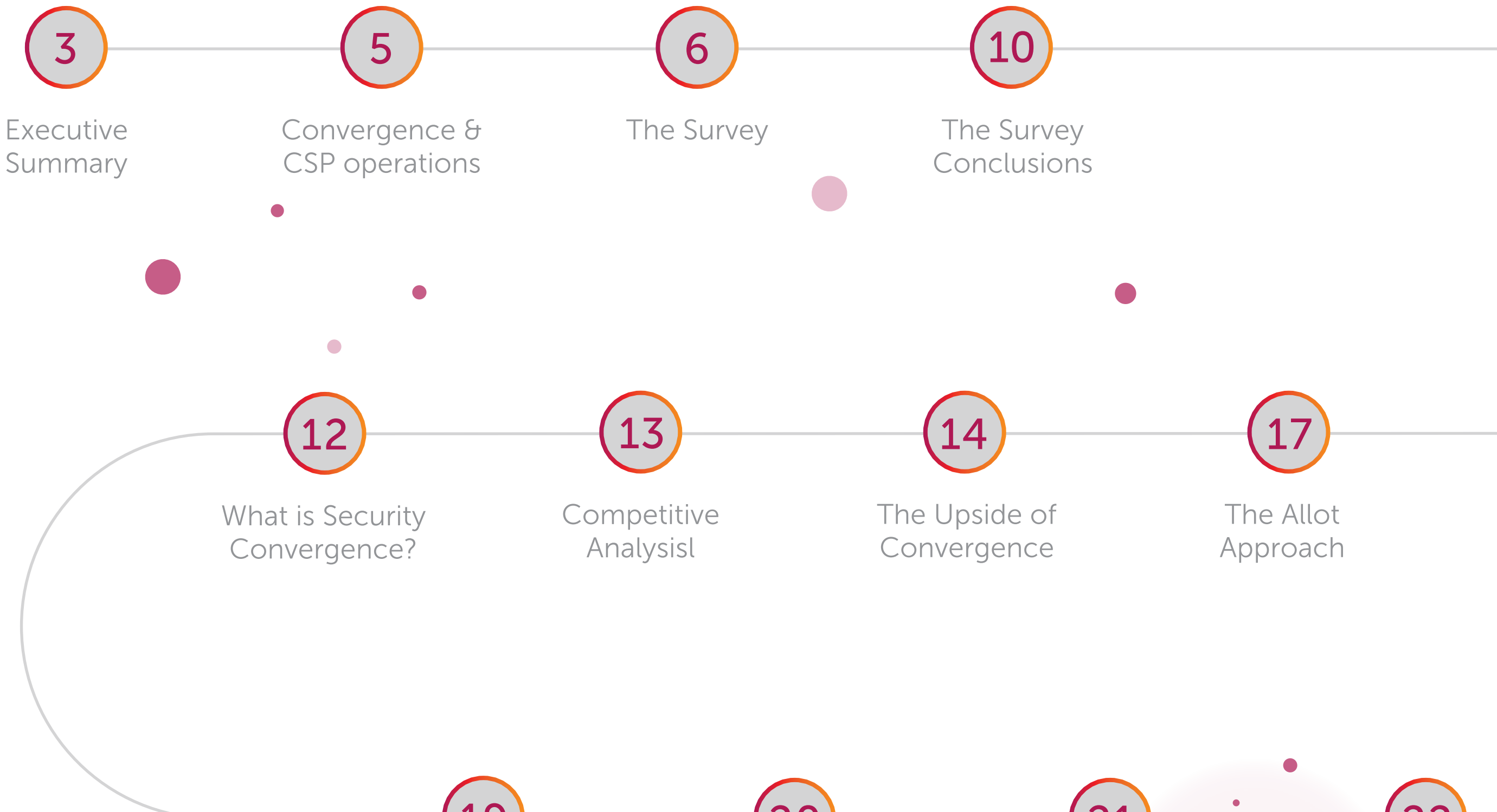
Cybersecurity Convergence

How to Orchestrate Synchronized Network Security

Telco Security Trends, H1 2024



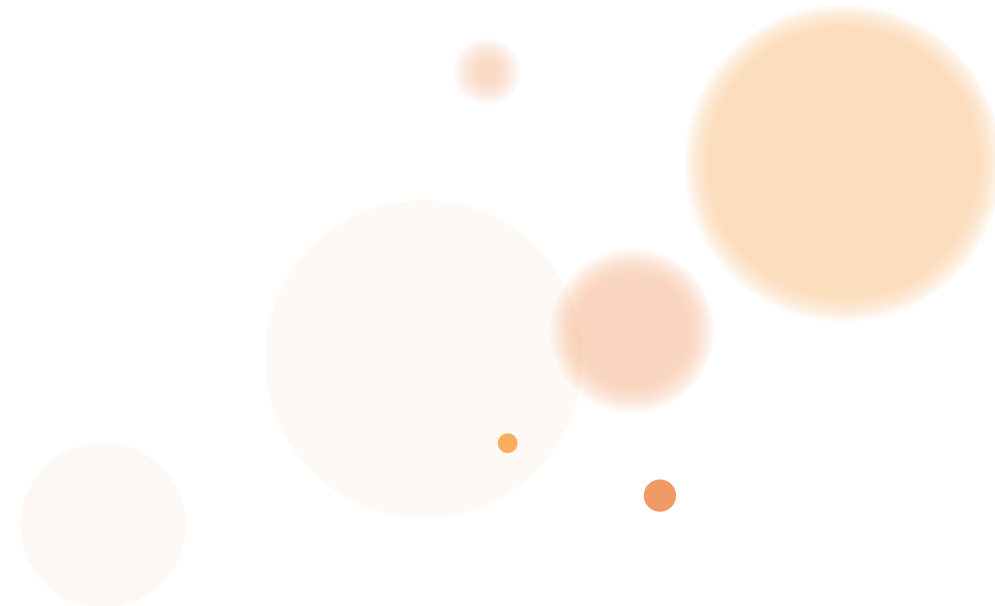
Table of Contents



3	Executive Summary
5	Convergence & CSP operations
6	The Survey
10	The Survey Conclusions
12	What is Security Convergence?
13	Competitive Analysisl
14	The Upside of Convergence
17	The Allot Approach
19	Allot HomeSecure Protection
20	Key Takeaways
21	Survey Methodology
22	Resources

Executive Summary

What are the critical building blocks needed for a comprehensive solution for Communication Service Providers?



The concept of convergence is not new in the world of telecommunications. As far back as 2004, the world's leading telecommunications operators formed an alliance to market fixed-mobile convergence products to millions of customers. At the time, it was anticipated that the Alliance would encourage major telecommunications operators around the world to drive the development of convergence services.

However, this did not include cybersecurity services.

Over time, as phishing, ransomware, trojans, and other cyberthreats posed a growing threat to the welfare of communication service provider (CSP) customers, the need for cybersecurity services grew dramatically. To answer this need, some CSPs offer different cybersecurity solutions, including endpoint security, firewalls, and DNS-based products. In many cases, these third-party solutions were resold to customers as a "hodgepodge" cybersecurity offering.

94%
of Telcos are interested in Converged Security as an integrated and unified approach

To get a better understanding of the current state of CSP cybersecurity offerings, Allot commissioned an independent survey of Tier 1 CSPs in North America, Europe, and Australia.

Through the survey, these CSPs weigh-in on cybersecurity convergence and the results uncover some new insight that point toward a growing trend in the industry.

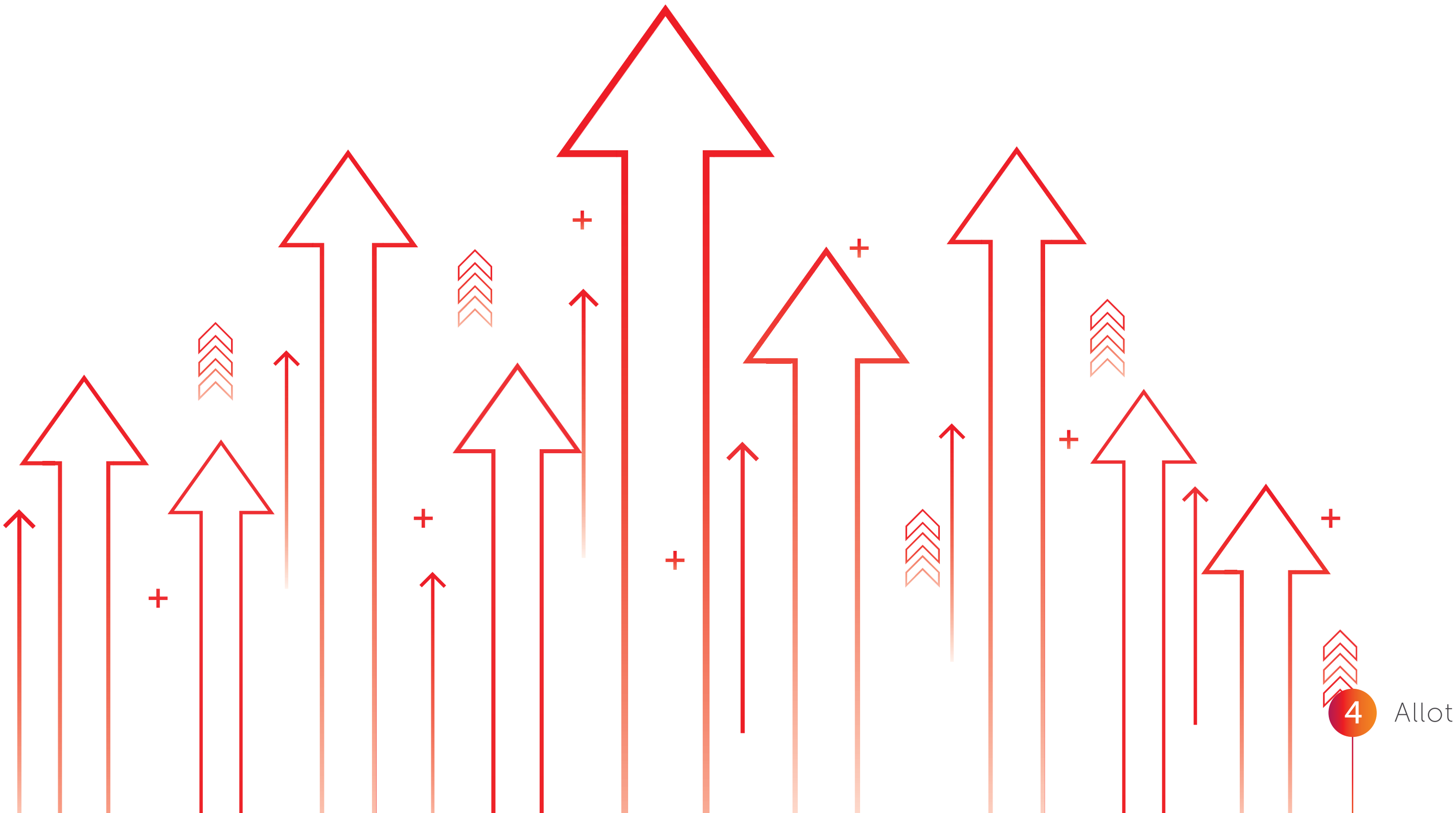
Growing cyber threats

Phishing, ransomware, trojans, and other cyberthreats are posing a growing threat to the welfare of communication service provider (CSP) customers. The need for cybersecurity services is growing dramatically.

Security solutions offered by CSPs

To answer the need for cyber security, some CSPs offer different cybersecurity solutions, including endpoint security, firewalls, and DNS-based products. In many cases, these third-party solutions were resold to customers as a “hodgepodge” cybersecurity offering.

Many CSPs are selling a variety of third-party cybersecurity products bundled together as an offering to their customers



Convergence & CSP operations

While CSPs and the industry at large works to implement a variety of solutions to confront the growing problem of cyber threats, a more organized approach has already been implemented in other aspects of CSP operations...

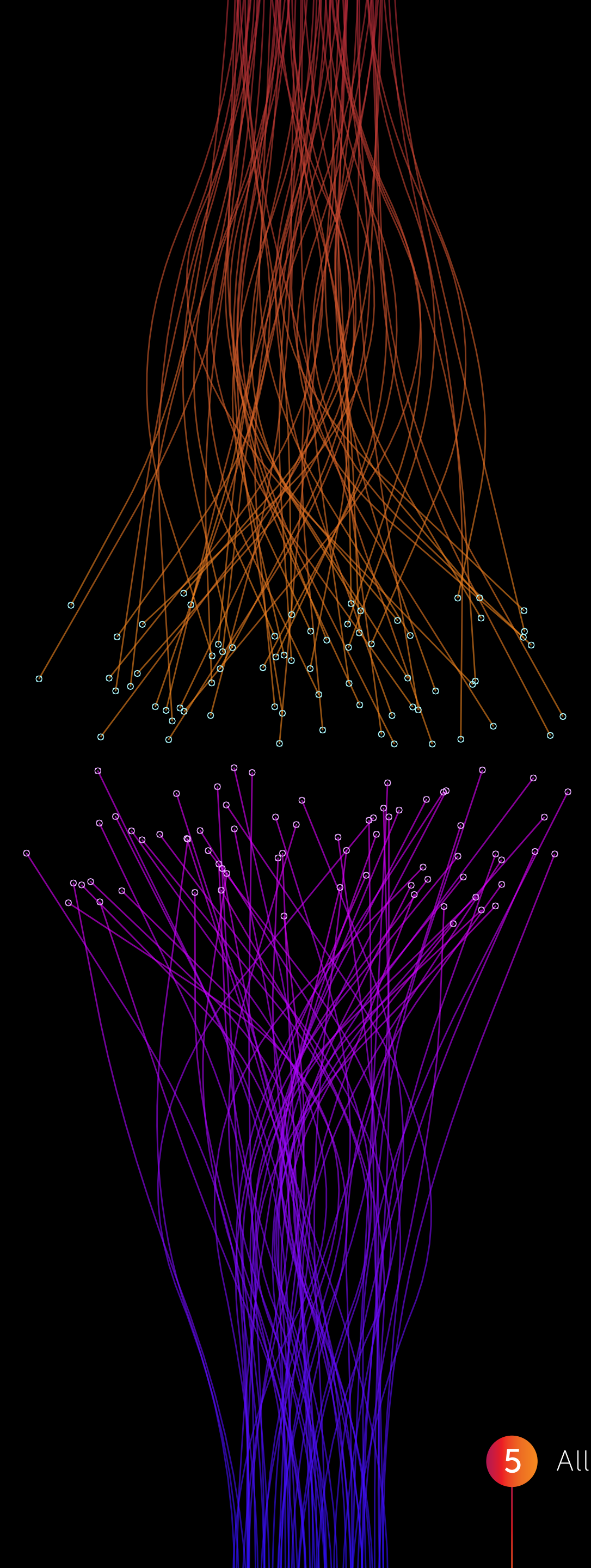
Fixed-Mobile Convergence (FMC)

Convergence in relation to FMC is already the norm in the world of telecommunications.

As far back as 2004, the world's leading telecommunications operators formed an alliance to market fixed-mobile convergence products to millions of customers.

At the time, it was anticipated that the Alliance would encourage major telecommunications operators around the world to drive the development of convergence services.

Allot commissioned an independent survey of Tier 1 CSPs in North America, Europe, and Australia for deeper insight into the issue.



The Survey

To get a better understanding of the current state of CSP cybersecurity offerings, Allot commissioned an independent survey of Tier 1 CSPs in North America, Europe, and Australia.

During July and August of 2023, Coleman Parkes Research conducted an anonymous research project on behalf of Allot. 109 Tier 1 CSPs, offering both fixed and wireless services, were surveyed.

Through the survey, these CSPs were able to weigh-in on cybersecurity convergence, too.

The Communication Service Providers (CSPs) were asked, "How interested is your organization in the different types of converged solutions initiatives?"

Globally, 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.



The Top 4

CSPs were also asked, "What are your key criteria for convergence solutions for security products?"

According to the survey, when considering converged security, CSPs rank these criteria at the top of their lists:



3 Top Building Blocks

When asked, "What are the important building blocks for a converged security solution?" CSPs replied with an interesting list of answers.

In addition to robustness, CSPs listed these other building blocks as important for a converged security solution:



Included "Identify and access management across any device type (e.g., mobile, fixed, IoT)"

Included "Unified threat management & reporting"

Included "Centralized monitoring and management for end user (e.g., permissions and user profiles)"

4 Top CX Features

Converged Security must deliver a positive customer experience to be a viable offering for CSPs.

When thinking about customer experience, CSPs ranked these features as critical for a converged security solution they would consider:

98%

included "Ensuring consistent and robust security across fixed-line, mobile, IoT, and digital services"

93%

included "Transparent security updates and patches"

91%

included "Reducing the need for customer involvement in managing security"

89%

included "Easy setup and configuration"

The Survey Conclusions

A converged security offering is the right/only choice for CSPs

CSP Interest in and Adoption of Convergence

- At least 1 in 4 CSPs rank ability to apply unified cyber security across all services as number 1 benefit, highlighting the growing concern for safeguarding customer data and network integrity.
- Cost savings from operational efficiency and opportunities to lock consumers into more services are the top benefit of converged approach.

Main benefits of Converged Solutions

- At least 1 in 4 CSPs rank ability to apply unified cyber security across all services as number 1 benefit, highlighting the growing concern for safeguarding customer data and network integrity.
- Choice of Converged Solutions provider is cost-driven for 2 in 3 as its main benefit is to save costs for the CSP business.

Saving costs must be balanced with incurring costs

- Choice of Converged Solutions provider is cost-driven for 2 in 3 as its main benefit is to save costs for the CSP business.

Measuring Success

- Despite focus on costs the main KPI for success of converged services is Cross-Platform adoption.
- This aligns with the telecom industry's shift towards offering seamless and consistent services across various devices and channels.

Barriers to adoption of Convergence by CSPs

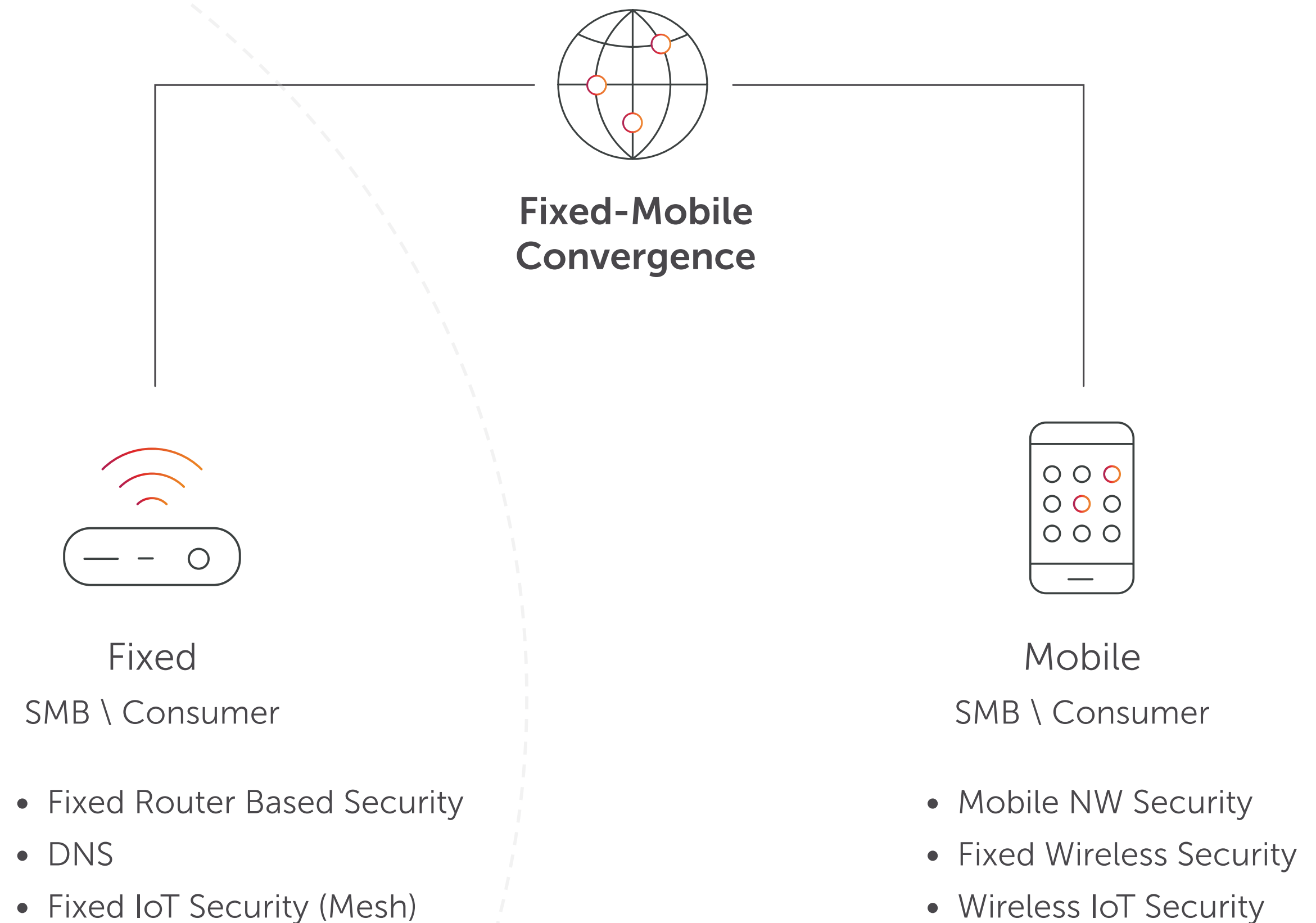
- Globally, the main barrier on the convergence journey is legacy systems – 3 in 4 CSPs are struggling with this.

Converged Security Focus

- When choosing Converged Security, CSPs rank comprehensive threat detection and compatibility with existing security among top 3 criteria.
- This is a key priority given that sensitivity of data accessed online / on mobile devices.
- Robustness is important for converged security solutions.
- However, given the competitiveness of the telecoms market, Converged Security still must tick all the boxes of customer experience to be an attractive offering.

What is Security Convergence?

Security solutions in the Telco portfolio are seamlessly offered as a unified experience across Fixed & Wireless, IoT; i.e., Unified Management, Reporting, UX/UI, Service bundles & Support



Competitive Analysis

How does Converged Security compare to other solutions?

Standalone/EP Security Offering

Poor Adoption Rate (EP)

- CSP just one of Many channels
- Difficult to Set-up & Ongoing Management (App based)
- Fragmented experience across Fixed-Wireless
- Limited Monetization
- Residual Margin: EP takes away majority share
- Price Takers: pricing dictated by the market
- High Operational Cost
- Cost of Provisioning
- High Touch Sales & Support (call center calls)
- High IT Enablement Cost
- Custom IT- Dev for Fixed-Wireless Convergence
- High cost of managing independent IT stacks (Fixed & Wireless)
- CSP Exclusivity
- None, just another commoditized solution
- No/limited control on UI/UX

Converged Security

High Adoption Rate

- CSP exclusive channels
- Easy Zero-Touch Onboarding & Management
- Unified experience across Fixed-Wireless security products
- High Monetization
- High Margins- Allot takes a fixed-minority share
- Price Setters: pricing dictated by the CSP
- Low Operational Cost
- Minimal cost of Provisioning
- Low-Touch Sales & Support (supported by Allot)
- Low IT Enablement Cost per solution
- One Platform- Multiple lines of revenue
- Reduce cost of supporting multiple IT Stacks
- CSP Exclusivity
- Exclusive to CSP (white labeled) -CSP branded UI/UX
- Complete control on Bundling & Customization capabilities

The Upside of Convergence

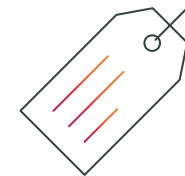
Convergence Contributes to Better Business for the CSP



Operations

Convergence enables consolidated management across the account, centralized provisioning & servicing, reduced need for multiple parallel systems for different services, and a consolidated support platform & call center.

Benefits include reduced operational cost (fewer tickets per account), reduced time to troubleshoot and resolve problems, improved automation, and improved self-service.

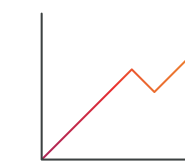


Sales and Marketing

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.

Consumer market - unified acquisition, custom bundling.

The CSP can cross sell, up-sell future services (e.g., 5G, fiber, IoT services), improve wallet share/profitability, and reduce CAC.



Accelerating Net-Adds

From other 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 of 100,000 net ads, 6% represents an additional 6000 net-adds. Multiplied by an estimated monthly ARPU of \$35, over the course of 3 years, yields an additional \$7.5M in revenue.

The Upside of Convergence

Convergence Contributes to a Better Customer Experience

Features

- One Telco for all network service needs
- Service continuity (e.g., preferences/settings Mobile > Fixed SSO / Common UI/UX for Support
- Customer Plans & Offers
- Easy Account Management for all Services & Users
- Improved On-Demand consumption (Service Sharing - data, media, etc.)
- Better Self Service

Business Value

- Improve Service Experience & Customer Satisfaction
- Better Value for converged bundles (get more for less, family sharing)
- Better Customer Support
- Ease of Management (billing, setup, service)

The Upside of Convergence

Convergence Contributes to Better Security

(via better CSP operations and better adoption among customers)

Leading APAC CSP provides zero-touch protection for SMBs

Allot NetworkSecure providing CSP-branded network-based security protection to wireless and fixed wireless SMB and IoT customers.

Benefits



- Fast time to market – PO to go live took 4 months.
- CSP-grade scalability
- Configuration changes don't require vendor involvement
- Bandwidth independent – pricing not tied to bandwidth tier
- Protects against latest cybersecurity threats across the network, including IoT devices

A leading player in the telecommunications industry enhancing the subscriber experience with Allot cybersecurity solutions

The results were remarkable. Within the first three months of launch, the Allot security solution achieved impressive performance metrics:

Benefits



- Over 50M cyber threats blocked, safeguarding subscribers from malicious online activities.
- A rapid adoption rate, with more than 200K subscribers embracing the solution only 3 months from launch.
- These numbers reflect the telecom's dedication to delivering a service that truly resonates with its customers' needs.

By partnering with Allot, the telecom has strengthened its position in the market and set a new standard for internet security.

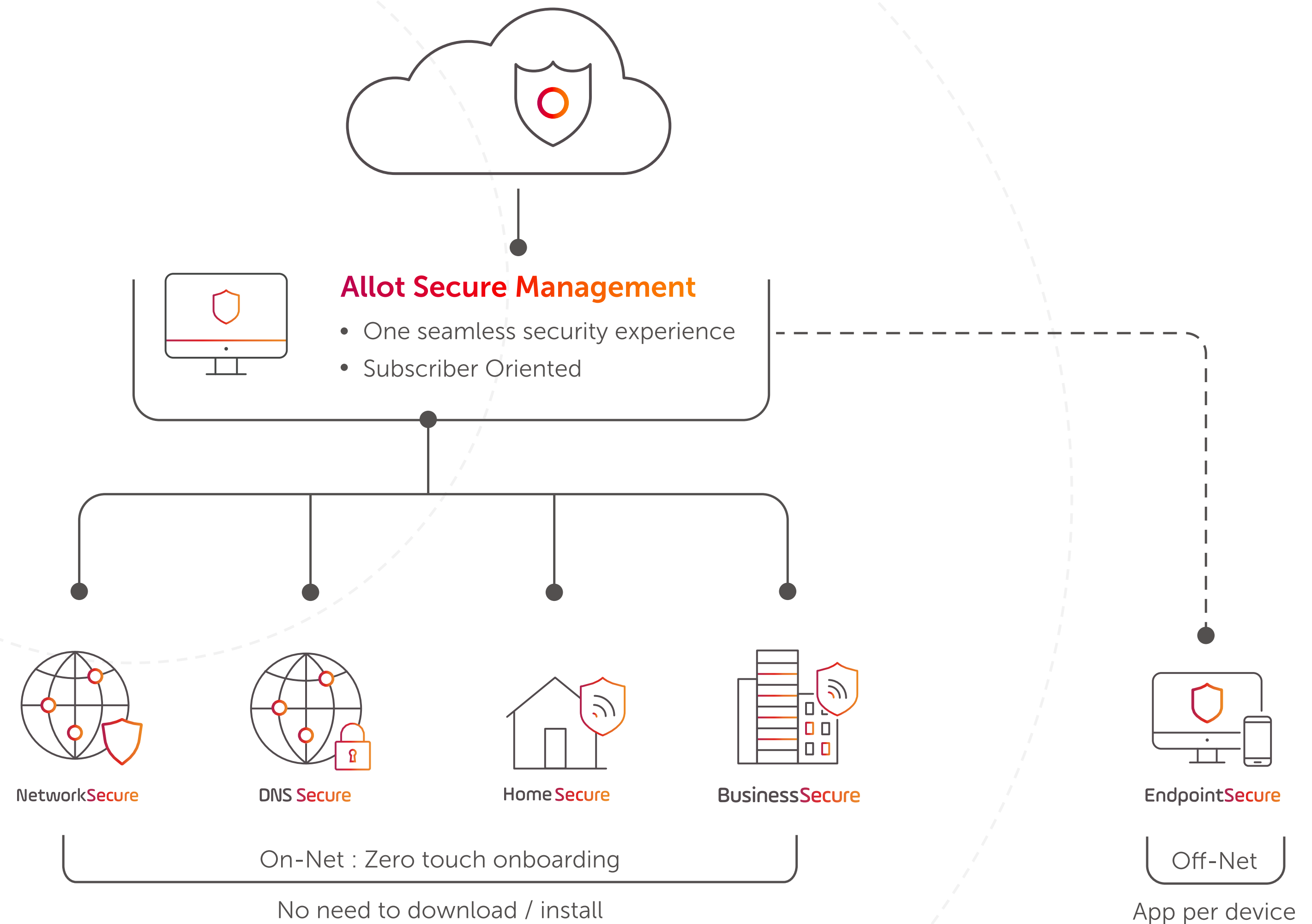
The Allot Approach

In a world where cyberattacks have become a clear threat to our everyday lives, providing security to customers who want to protect their families and businesses from cyber threats and exposure to intrusive sites with inappropriate content, is an important role for service providers to fill. Allot Secure provides 360-degree end to end protection, anywhere, any time and on any device. All products within the Allot Secure portfolio enjoy unified provisioning and a management system including network-based security – through NetworkSecure, home gateway and business router-based security through HomeSecure and BusinessSecure respectively, and endpoint-based security through EndpointSecure. Thus, customers are protected at all times, whether they are on the mobile network, at home using an IoT device, or on Wi-Fi at the local café, with easily managed parental controls for all connected devices, wherever they may be.



Allot Secure enables mobile, fixed, and converged network operators to secure their customers. 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.

- Network-based solution
- Mass consumer and SMB markets
- Any device, anywhere, any threat
- Unified management system
- A converged security offering



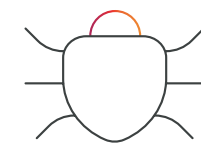
Allot HomeSecure Protection

As connected devices proliferate, home networks become the foundation of the connected home. Yet they are increasingly more difficult to manage, and attacks are much more common.

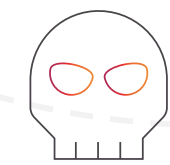
Allot HomeSecure is a simple, reliable solution that guarantees a secure network for the connected home. This is achieved through a small agent, remotely deployed on the home router, that provides unprecedented visibility into the network. Using Machine Learning technology and network visibility, Allot HomeSecure identifies all devices in the home network and allows parents to assign devices to the relevant user and automatically apply the most suitable security policy.

Benefits

Allot HomeSecure protection includes a simple and intuitive portal to control and manage your home network providing:



Threat Protection: Multiple security layers protecting home devices from the latest threats, including different types of malware such as ransomware, trojans, adware, viruses, bots, as well as phishing attempts.



Internal Protection: Detect potentially malicious network activities and weaknesses including port scans, brute force attacks, common device passwords usage, lateral movement from IoT devices and others.



CPE Protection: Prevent communication with unsafe destinations, prevent DNS tampering and identify weak Wi-Fi passwords.



Parental Control: User-specific filtering, based on categories, allows Internet access to be limited, according to content, schedules and more.

Key Takeaways

Across the world, the need for cybersecurity is growing.

Tier 1 CSPs in North America, Europe, and Australia are interested in converged solutions that include cybersecurity.

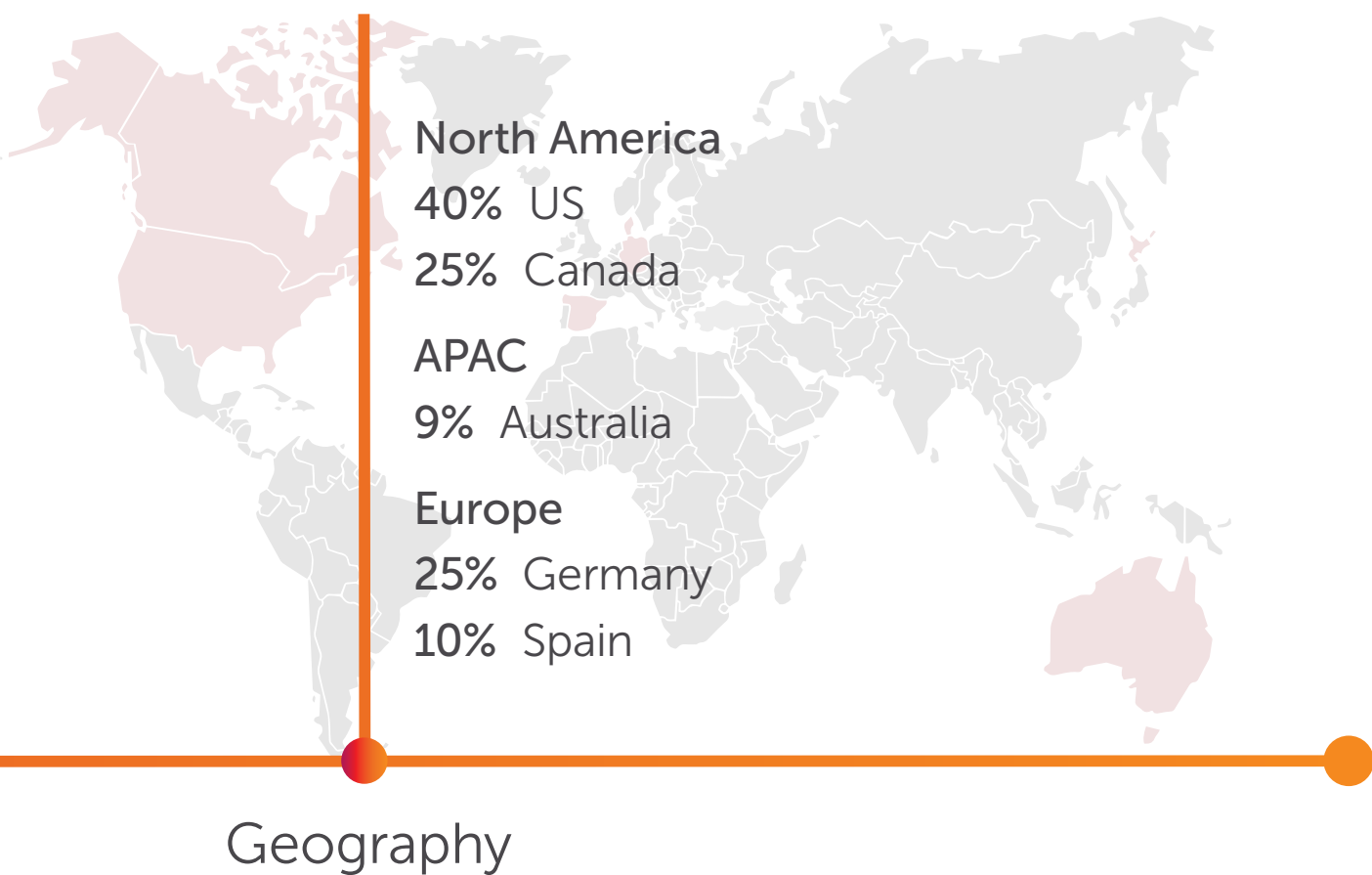
Service providers that offer converged security – across fixed, mobile, and converged networks – have additional opportunities to stand out from the competition.

Allot offers a converged cybersecurity solution designed specifically for CSPs that brings substantial benefits to operations, sales & marketing, and the user experience, with all the necessary building blocks for a truly comprehensive solution.

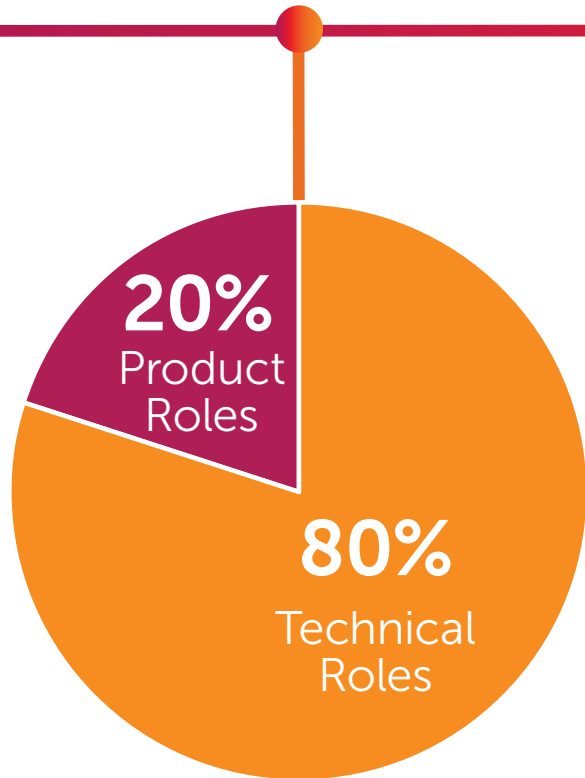
Survey Methodology

During July and August of 2023, Coleman Parkes Research conducted an anonymous research project on behalf of Allot. 109 Tie wireless services, were surveyed.

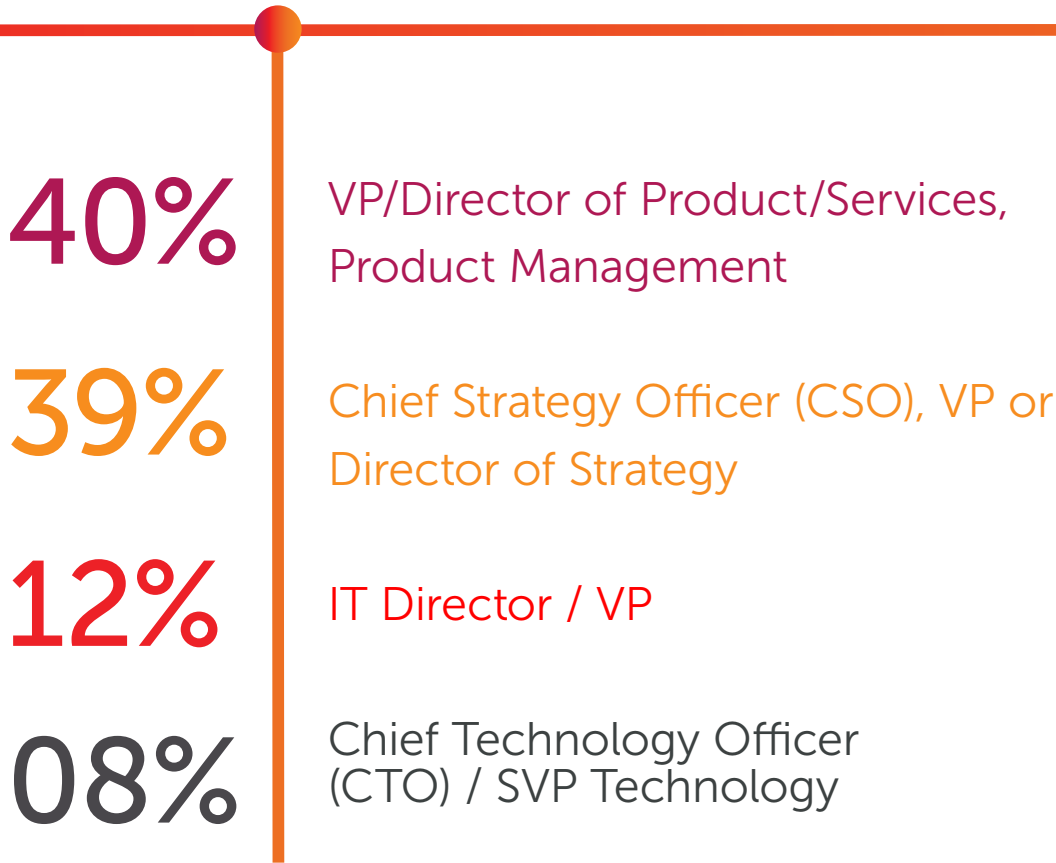
99% of those surveyed were either the lead decision maker, or part of the decision-making team.



No. of respondents



Job function



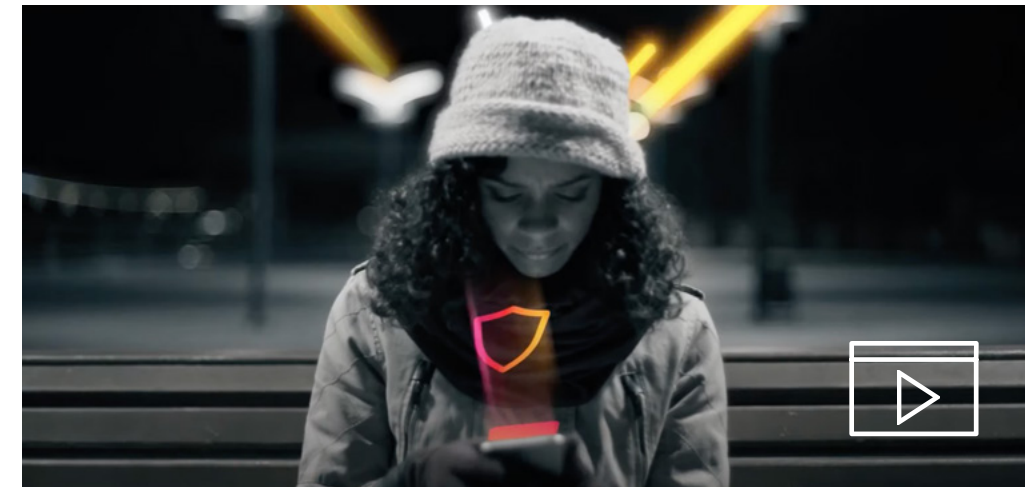
Resources

The following resources provide additional insight to CSPs considering converged security solutions for their customers.



Podcast – How could operators protect subscribers from cyber risks?

[Learn more](#)



Cyber Security Services for Communication Service Providers

[Learn more](#)



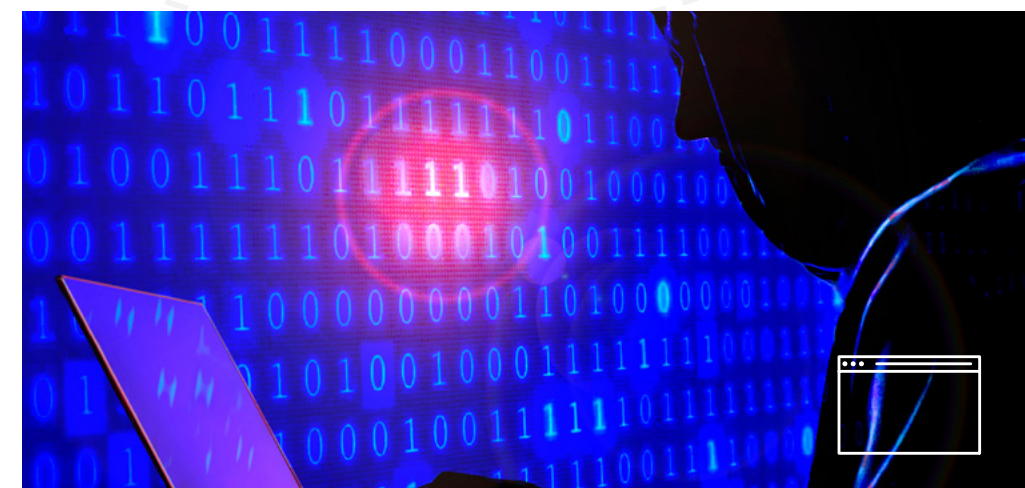
Service Provider Security

[Learn more](#)



Security for connected home & mobile devices

[Learn more](#)



Top Cybersecurity Terms

[Learn more](#)



Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed, and converged service providers and over 1000 enterprises. Our industry-leading network-based security as a service solution is already used by over 20 million subscribers globally.

Allot. See. Control. Secure.

To learn how CSPs can protect their business subscribers, visit

www.allot.com »



© 2024 Allot Ltd. All rights reserved. Specifications subject to change without notice. Allot and the Allot logo are registered trademarks of Allot. All other brand or product names are trademarks of their respective holders. www.allot.com