allot

Cyber Threat Report H1 2026

When Kids Tap, Risk Follows

Kids Online

Executive Summary

Did you notice? Kids and teens are growing up inside apps.

They watch, play, chat, learn, and explore almost entirely on trusted platforms such as YouTube, TikTok, WhatsApp, Roblox, and gaming apps. Their digital behavior is fast, intuitive, and emotionally driven. They tap quickly, follow rewards instantly, and rarely pause to verify what sits behind a link.

This behavior makes young users a uniquely vulnerable online segment. Criminals understand this dynamic and actively exploit it. Fake rewards, cloned logins, free downloads, and deceptive ads are deliberately designed to look like familiar in-app content. One tap is often enough to expose children to phishing, scams, data harvesting, or malicious downloads, often without ever opening a traditional browser.

This report analyzes how children and teens behave online today, which apps and searches dominate their digital lives, and how those habits translate into real risks, blocked by ALLOT across four of the most frequent areas: gaming, streaming, online spending, and education.

Using real protection data, the report demonstrates a critical insight: even app-centric behavior repeatedly exposes children to external links, some of which lead to deceptive, unsafe, or malicious websites through ads, redirects, and embedded browsers

Allot Network-based protection plays a decisive role at this exact moment, intercepting risky connections in real time, before harm occurs.
For Telco Service Providers, this segment represents both a responsibility and a powerful opportunity to protect one of the most exposed user segments, automatically and at scale.

Table of Content

Children's Psychological Aspects to consider.

Why Kids Click First and Think Later

Kids and teens don't approach the digital world cautiously; they move through it instinctively, emotionally, and at speed.

Their online decisions are shaped by curiosity, social pressure, and the promise of instant rewards. In this environment, hesitation is rare. A tap often comes before evaluation, and familiarity is mistaken for safety.

Understanding these behaviors is crucial for assessing the risks outlined in this report and explaining why many threats succeed while seeming harmless.

When these factors combine, they create a recognizable pattern of online behavior. The six characteristics below describe how kids and teens typically engage with digital content.

These psychological traits are not flaws, they are normal aspects of how young minds learn, explore, and connect.

Impulsive Decision-Makers

Fast reactions → little time to assess what's behind a link

Always Connected, Always Responding

Fear of missing out drives constant engagement and rapid clicks

Instant Reward Seekers

Drawn to offers, challenges, and "tap-to-get" prompts

Overconfidence in Digital Skills

Believe they "know what they're doing," even when they don't

High Trust in Familiar Platforms

Assume that anything inside their favorite app is safe.

Limited Risk Anticipation

Underdeveloped ability to detect deception or hidden signals.

How's Life for Children in the Digital Age?

Being online is now a normal part of childhood. Drawing on OECD 2025 research, these figures illustrate how early kids get connected, how much time they spend online, and the activities that shape their daily digital lives.

71% of 10-year-olds already own a smartphone
Rising to **99%** at 15 years old.

What do they do online?

96%
Browse social networks

89%
Learn online (outside the school)

86%
Practical usage:
- Find a place
- Book a train ticket
- Buy a product

80%
Play video games

allot

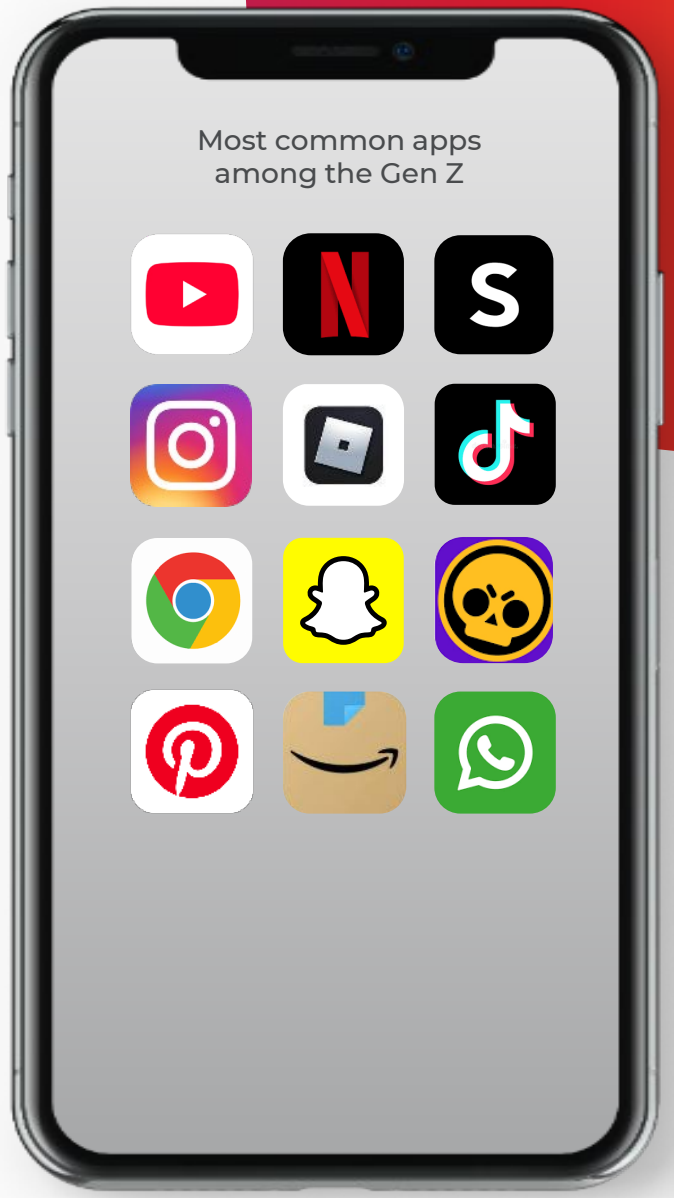
Where do kids spend time online?

A Few Apps Shape Most of Kids' Online Time

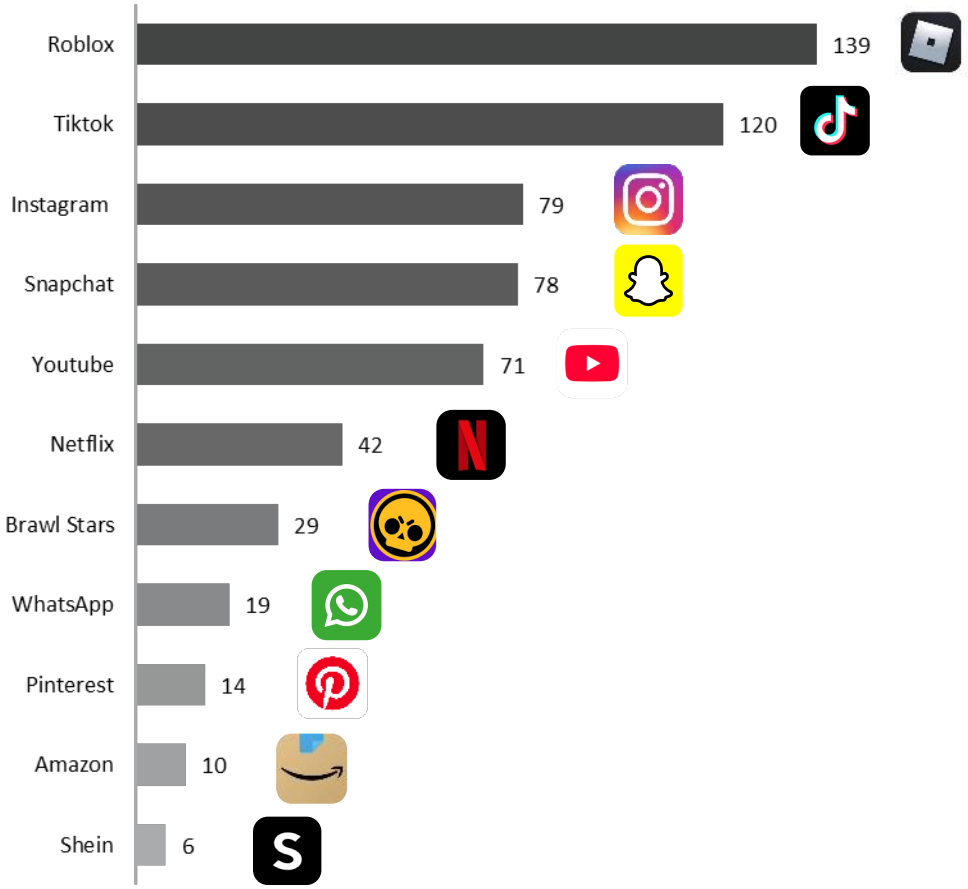
Children's digital activity is highly concentrated. Research indicates that most screen time is spent within a limited set of apps—video platforms, social media, messaging, games, and educational tools.

This concentration increases efficiency not only for content delivery, but also for exposure. When most activity happens inside a few environments, any risk introduced through those channels can reach many users quickly.

Importantly, kids don't distinguish between "app content" and "web content." Ads, links, and recommendations blend seamlessly into the experience.



Average daily minutes spent online by kids



Why is exposure inevitable?

Risk Finds Kids...
Kids Don't Look for Risk

Children rarely intentionally navigate to risky websites. Most exposure happens passively — as a side effect of normal app usage.

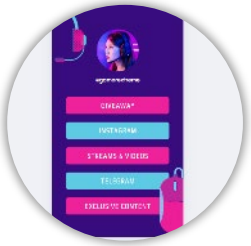
Content discovery, promotions, recommendations, and shared links are woven into everyday digital experiences. Kids interact with what feels familiar, relevant, and safe, without stopping to question where it leads.

Because trust is based on context rather than verification, exposure becomes predictable and repeatable. The more time children spend within a small set of apps, the more often they are quietly routed beyond them, without realizing it.

What Happens After the Tap?

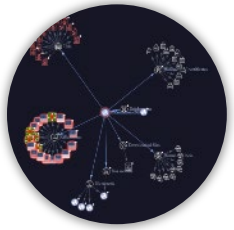
In-App Promos Can Redirect to Deceptive Pages

Ads, rewards, and "limited offers" embedded in apps are often powered by external ad networks. When a child taps, the app doesn't just show more content; it may automatically open web pages hosted outside the platform, beyond the app's control.



Links Open Without Clear User Intent

Links embedded in comments, messages, bios, and stories can open automatically inside apps. Without a visible browser or clear confirmation step, kids may reach external websites without realizing they left the app at all.



Redirect Chains Are Invisible to Users

Behind a single tap, multiple background redirects may occur, passing through tracking links, affiliate networks, or malicious intermediaries. Kids see only the first action, not the hidden journey that follows.

Ad Networks Introduce Risk at Scale

Games, videos, and social media platforms frequently rely on third-party advertising. These ad networks dynamically rotate destinations, meaning the same tap can lead to different external websites over time — including deceptive shopping pages, fake offers, or other unsafe destinations.

System Alerts and Pop-Ups Imitate Trusted Messages

Some pages triggered by apps display urgent warnings such as "update required" or "device issue detected." These messages mimic system alerts, pushing kids to act quickly without questioning the source.

Why This Matters?

These mechanisms mean risk doesn't require curiosity or mistakes. It can be triggered by normal, everyday app Interactions with a single tap.

Use cases from Allot during the last quarter

Where These Risks Actually Appear

The mechanisms described on the previous page are not theoretical. They surface repeatedly in the apps, platforms, and services kids use most; often disguised as fun, convenience, or opportunity. The following sections show how the same technical pathways play out across four everyday digital contexts.

Blocked Threats by Allot around Gaming

The Gaming World that Kids Love, and Criminals Exploit

Kids and teens move fast in gaming environments, claiming rewards, logging in, downloading add-ons, or chasing free items. Criminals exploit this instinct with look-alike pages, fake giveaways, and mod tools that promise shortcuts. What feels like a harmless gaming action can expose them to account theft, scams, or harmful software.

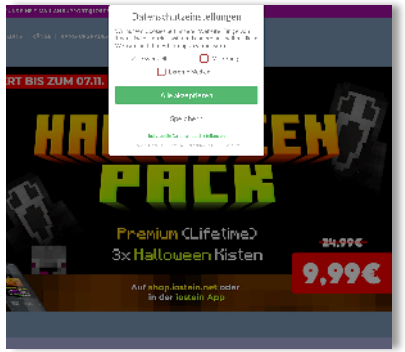
Fake Steam Storefront

Teens trust Steam and often log in quickly to check games or offers.

A cloned login page exploits that reflex, capturing credentials instantly.

Criminals use stolen accounts to resell items, lock players out, or access linked payment methods—turning a familiar interface into a high-impact phishing trap.

Minecraft Event Pack Lure

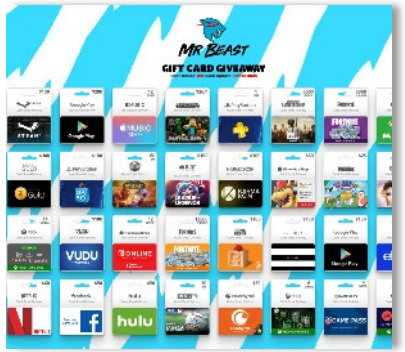


Seasonal offers feel exciting and urgent for young gamers.

Fake promo overlays mimic official events and push users to click or install add-ons.

These pages often hide tracking redirects, force unwanted permissions, or lead to scam purchases, turning a fun Halloween offer into a risky interaction.

Fake Gift Card Rewards Hub

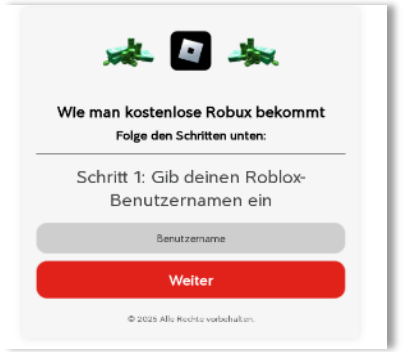


Teens click on “free gift cards” in hopes of easy wins or gaming credits.

These pages funnel users through deceptive forms, aggressive ad redirects, or fake surveys.

Criminals harvest personal data, force sign-ups, or lead kids to malicious downloads—while the promised rewards never exist.

Free Robux Phishing Step



Free Robux offers are extremely tempting to kids eager to upgrade avatars or buy items.

This fake page mimics Roblox visuals and asks for a username to begin a supposed reward process.

Scammers use this first step to guide children into deeper phishing flows, collect credentials, or redirect them to harmful pages disguised as reward verification.

Blocked Threats by Allot around Streaming

Entertainment Masks the Web's Darker Corners

Streaming is a daily habit for young users, making them quick to tap on "free movies," anime platforms, music apps, or exciting offers tied to popular shows. Scammers imitate these experiences with APK downloads, fake portals, and job scams. One tap can expose teens to malware, data theft, or deceptive sign-ups disguised as entertainment.

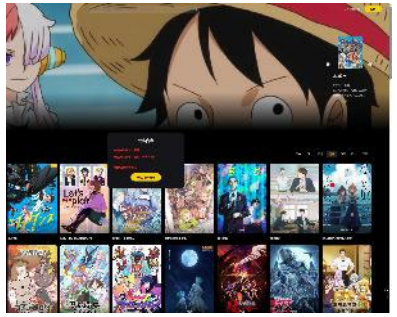
Streaming Login Phish

Login walls promise access to popular movies and shows, tempting teens to sign in quickly.

Fake platforms use these screens to harvest emails and passwords.

Stolen credentials can be reused across services, leading to account takeovers, spam campaigns, or further targeted scams

Anime Stream Login Scam



Anime content has a strong youth appeal, making clone platforms believable.

Fake sites mimic real streaming portals and ask users to log in or create accounts. These pages typically harvest credentials or redirect to unsafe ads.

Teens risk exposing email, passwords, and personal info through accounts they think are harmless.

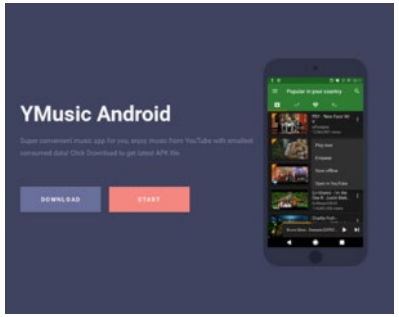
Sports App Aggregator Trap

Major sports events like the World Cup strongly attract teens looking for live matches, highlights, or insider access.

Aggregator pages list multiple apps that appear official and trustworthy.

These hubs often redirect users to betting platforms, unsafe apps, or downloads that expose devices to malware, gambling content, or data harvesting.

Free Music APK Lure



Teens searching for free music or background-play versions of YouTube apps are quick to tap on simple "Start" or "Download" buttons.

APK-based music apps often bundle hidden malware, intrusive permissions, or tracking components.

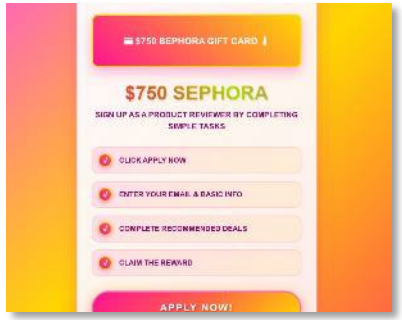
Kids may install unsafe software without understanding the risks to their device or accounts.

Blocked Threats by Allot around Online spending

The Illusion of Free Stuff

From coins and cosmetics to gift cards and gadgets, young users are drawn to offers that feel easy, instant, and harmless. Criminals mimic popular brands to harvest emails, passwords, and personal details. What seems like a quick win can expose kids to data theft and long-term online risks.

Sephora Gift Card Bait

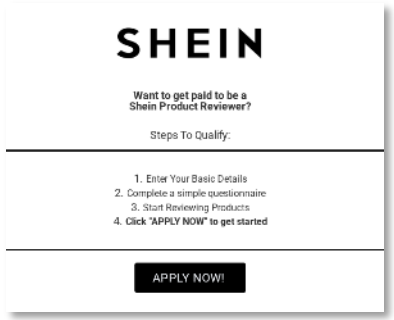


Big-brand beauty rewards draw teens looking for free makeup or trendy products.

Scammers exploit this with fake "reviewer programs" that require sign-ups or task completions.

Kids are funneled into data-harvesting schemes, aggressive ad redirects, or subscription traps with no real gift card.

SHEIN Tester Enrollment Scam

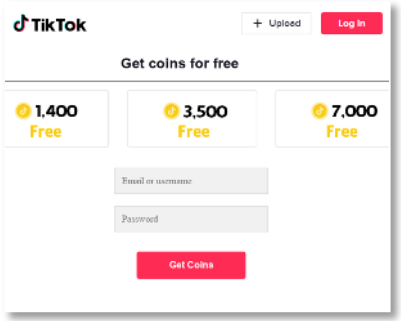


Teens are eager to get free clothes or influencer-style perks, making "tester" programs extremely attractive.

Fake application flows collect personal info, addresses, and survey data.

These pages often resell the data, enroll users in unwanted subscriptions, or lead to more deceptive offers.

TikTok Coins Login Trap



Free coins are highly appealing to teens who want status boosts or features inside TikTok.

These clone sites ask for usernames and passwords, harvesting credentials instantly.

Criminals gain access to accounts, personal messages, and linked profiles, putting identity and privacy at risk.

Xbox Email Collection Scam

A free Xbox is irresistible to younger gamers.

These giveaway pages collect emails and personal info under the promise of winning a high-value prize.

Criminals use the data for spam campaigns, credential stuffing, or selling it to third parties. The prize doesn't exist, only the risk does.

Blocked Threats by Allot around Education

Education Tools Targeted by Deceptive Pages

Young learners explore the web for answers, tools, and inspiration. Their trust in educational resources makes them easy targets for fake study sites, cloned portals, or risky downloads. What appears to be a shortcut for homework can expose them to scams and malicious content.

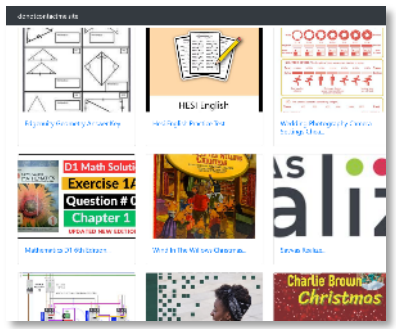
EdTech Skill-Building Lure

Teens interested in coding or AI may click on sites promising beginner guides or tutorials.

Scammers copy educational platforms to harvest emails, push intrusive ads, or serve infected “course downloads.”

Curious learners risk exposing personal data while believing they’re accessing safe study materials.

Textbook Download Scam

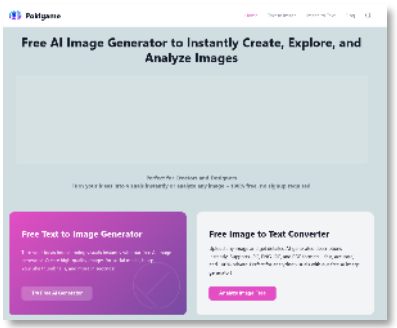


Free worksheets and textbook downloads are extremely tempting for students.

Criminals imitate resource libraries to lure users into downloading files laced with malware or clicking deceptive links.

Kids may unintentionally install harmful software or submit personal details on fake “unlock” pages.

AI Tool Freebie Trap

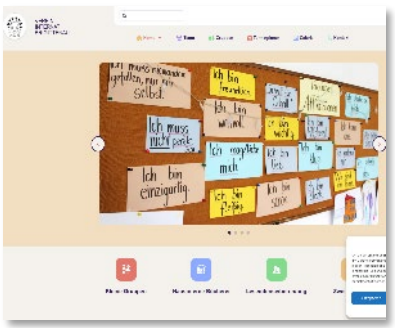


AI tools offering free images or text summaries appeal to teens looking for quick homework shortcuts.

Fake AI pages often redirect through ad networks, collect data through forms, or push unsafe downloads disguised as “AI installers.”

Kids risk malware exposure or leaking personal info when trying to save time.

Fake School Portal Lookalike



Pages mimicking real schools or student portals attract young users searching for schedules, group info, or assignments.

Criminals duplicate layouts to phish for login credentials or serve malicious pop-ups.

Teens may hand over school account details without realizing the site is fake.

Key Takeaways and Conclusions

01

Kids don’t browse; they tap

App-based behavior creates constant exposure to external websites through ads, links, and redirects.

02

One click is enough

Most threats require no technical skill — only curiosity, speed, and trust.

03

Trust is the attack surface

Familiar brands, games, and platforms are deliberately cloned to deceive young users.

04

Protection must act before awareness

Education matters, but it cannot prevent split-second decisions.

05

Network-based protection fills the critical gap

It works invisibly, instantly, and independently of apps, devices, or user behavior.

To Wrap Up

Kids and teens are among the most exposed digital audiences today; not because they behave recklessly, but because the online world is engineered for speed, rewards, and constant interaction.

This report shows that the greatest risks don't come from obscure corners of the web, but from places that feel familiar: games, videos, messages, offers, and learning tools. Criminals exploit trust, not ignorance.

In this environment, protection cannot rely solely on user awareness or parental control. It must operate at the moment of risk: between tap and page load.

Network-based cybersecurity provides the missing layer: automatic, real-time protection that shields young users across apps, platforms, and behaviors.

For Telco Service Providers, protecting kids and teens is not only a safety obligation, but a powerful way to demonstrate tangible value, trust, and long-term customer care.

References

I. OECD (2025), How's Life for Children in the Digital Age?, OECD Publishing, Paris, How's Life for Children in the Digital Age?

II. Qustodio (2024), The Digital Dilemma. Childhood at a Crossroads. Digital_Dilemma_2024_Qustodio_Data_Report.pdf

III. Qustodio (2024), Apps Through the Ages. 2024-06_PR-Gen-AlpaZ_US.pdf

IV. Radesky, J., Weeks, H.M., Schaller, A., Robb, M., Mann, S., and Lenhart, A. (2023). Constant Companion: A Week in the Life of a Young Person's Smartphone Use. San Francisco, CA: Common Sense. 2023-cs-smartphone-research-report_final-for-web.pdf

V. Analyzify (2024), Shein Statistics. Shein Statistics

VI. Numerator (2024), Anticipating Generation Alpha. Anticipating Generation Alpha

VII. The Annie E. Casey Foundation (2025) Social Media Safety For Teens, Blog. Social Media Safety for Teens

About Allot

Allot (NASDAQ & TASE: ALLT) makes networks safer, smarter and more valuable. We make it our mission to help telcos and enterprises gain deep network insight, defend against evolving cyber threats, and unlock new value for their customers. At the core of Allot's solutions is Deep Network Intelligence, powered by advanced AI/ML technologies, enabling unmatched app-aware visibility, even when traffic is encrypted. The same intelligence that drives precise traffic control and Quality of Experience (QoE) optimization enables real-time protection against DDoS and cyber threats, and the market's only comprehensive network-native platform that turns security into revenue-generating services. Through these services, we enable telecom providers to offer accessible and affordable cybersecurity protection services to their consumer and small business customers who do not have the resources or expertise to protect themselves otherwise. Leveraging 30 years of advanced telecom and enterprise network expertise, Allot partners with more than 500 communication service providers, including many of the world's top 10 telcos, and over 1,000 enterprises. Recognized by top analysts and trusted globally, Allot is at the forefront of secure, intelligent network experiences.

For more information about how Allot Secure can protect communication service provider's consumer and SMB customers, visit Allot Security Solutions