

WebSafe Personal



Security as a Service for Consumers

Allot WebSafe Personal enables service providers to secure the digital experience by providing Security as a Service (SECaaS) to consumers who are concerned about exposure to online threats and harmful content. As a fully integrated service in Allot Service Gateway platforms, Allot WebSafe Personal is built for rapid rollout of personalized parental controls and anti-malware services that safeguard your customers, increase brand loyalty, and generate incremental revenue. Allot SECaaS solutions are network-based, so they can be used with any device without impacting performance or battery life. Moreover, your customers enjoy uniform setup options for all devices and hassle-free maintenance.

Benefits

Security revenue and intelligence

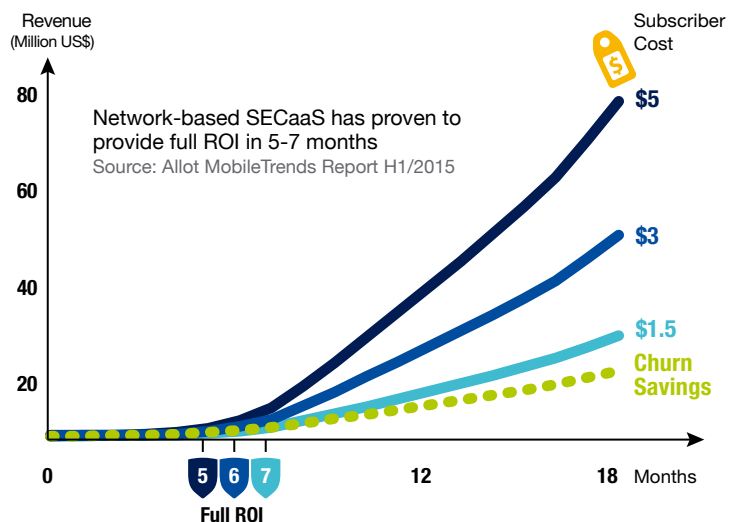
- Increase ARPU from consumer security services
- Leverage SECaaS, which is ideally suited to mobility needs
- Gain valuable intelligence on user profiles and online threats

Transparency and accuracy

- Transparent protection, including off-network usage
- Avoid over-blocking
- Strengthen customer loyalty with personalized threat reports

Flexibility and scalability

- Deploy flexibly with single tenant or multi-tenant operation
- Accelerate ROI through full integration in Allot Service Gateway
- Scale to support millions of users



Personal Parental Controls

Safe browsing for everyone in the family

With the proliferation of smartphones and tablets, online activity has increased dramatically among teens and children. Even at home, the screens-per-room count is growing, with households often using two or more Internet access devices in a room at any given time. Allot WebSafe Personal helps you provide peace of mind to parents who are concerned about the online activities of their children and want to protect them from harmful and inappropriate content.

Allot WebSafe Personal assures child-safe browsing by allowing parents to determine the websites and content that their children can access, as well as the hours and amount of time they spend online. Accurate web filtering techniques identify, classify, and control access in real-time according to individual user profiles, which the parent manages online.



Service Highlights

Personal Web Filters: allows parents to select the content categories and URLs they want to filter per device.

Personal Application Control: parents can limit access to “risky” applications based on their Layer-7 protocol such as P2P.

Personal Browse Time: allows parents to limit online access to specific hours and/or to maximum hours per day per device.

Personal Unblock: provides a channel for users to submit unblock requests and resolve blocking errors within minutes. User feedback is reviewed and incorporated into the filtering logic.

Personal Alerts: parents receive SMS or email notification when attempts are made to access blocked content.

Personal Ads Free: keep kids safe by blocking popup ads, animated gifs and banners.

The screenshot displays the Allot WebSafe Personal web interface. At the top left is the Allot Communications logo. The main header reads "WebSafe Personal" and includes navigation links for "Language", "Contact us", and "Log Out". Below the header is a menu with tabs for "GENERAL", "PARENTAL CONTROL", "AD \$ FREE", "ANTI-PHISHING", "FIREWALL", and "REPORTER". The "PARENTAL CONTROL" tab is active, showing "Options" for "Filter Configuration". Under "Filter Configuration", there are checkboxes for "Enable safe search" and "Enable password override". Below this is the "Categories to Block" section, which lists various content categories with checkboxes: anonymizers, anorexia and bulimia, banners, bombs, chat, dating, drugs, gambling, games, hackers, health, instant messaging, models, personal websites, pornography, racism, sects, sexuality, spyware, and violence. There are "Select all" and "Clear all" buttons for these categories. The "Files to Block" section shows two lists: "Not Selected" (Images, Music, Programs, Video) and "Selected" (Compressed Files, ARJ, RAR, ZIP). There are "Add" and "Delete" buttons between the lists, and an "Add" button for "Other extensions". At the bottom of the interface are "Accept" and "Cancel" buttons. On the left side of the interface, there is a sidebar with "OPTIONS" and a "Protected" status indicator with a green checkmark icon.

Allot's simple web-based GUI makes it easy for users to personalize their own web security settings

Personal Anti-Malware

24/7 protection from malicious online threats

Viruses, spam, spyware, phishing, and Trojans are among the many malware threats that Internet users face every day. Allot WebSafe Personal provides network-based anti-malware that protects your data consumers against all kinds of malware that can damage mobile devices and cause the loss of personal content. It also includes powerful anti-virus and anti-phishing for email (SMTP, POP3) and web traffic, which takes the worry out of engaging in online activity and transactions.

Allot anti-malware provides quick response to new threats, 24/7 updates and a wide protection net that requires no action from users and no resources from their devices.

Service Highlights

Anti-Virus: employs Kaspersky Lab, Sophos, and Bitdefender technologies to provide industry-leading response time to new malware outbreaks. Allot allows flexible customization of protection levels, quarantine, user notification, infected-file detection and on-demand reports.

Anti-Phishing: scans web and email traffic for telltale signs of phishing such as generic greetings, personalized greetings (spear phishing), suspicious links, threats, personal information requests, misspellings, bad grammar, and pharming attacks that redirect web traffic to bogus sites.

Anti-Spam: inspects inbound email for spam content and automatically blocks or quarantines spam-infected email messages coming into desktop clients through POP3, IMAP or SMTP servers. Allot integrates 16 leading technologies and 180 languages to detect spam, including analysis of email origin, destination, text, hyperlinks, and file attachments.



Network-based Protection Against

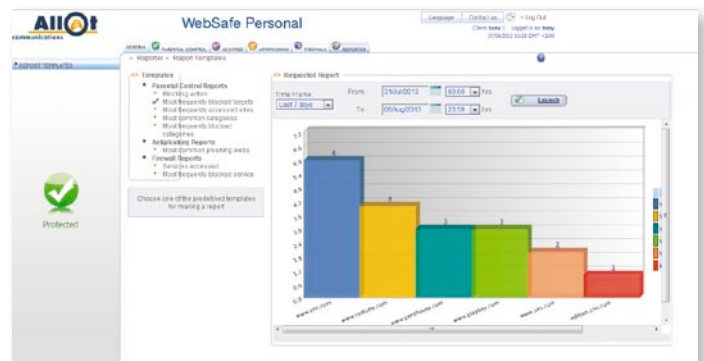
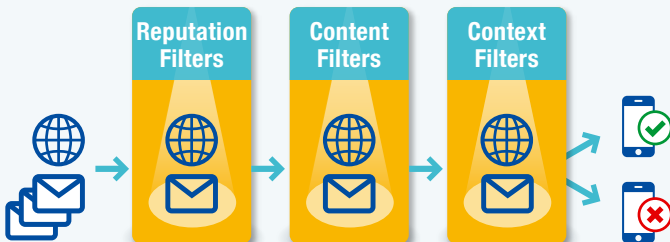
- Viruses
- Worms
- Trojans
- Spyware
- Adware
- Rootkit
- Keylogger
- Phishing
- Others

Personal Security Reports

With Allot WebSafe Personal, parents can get periodic reports detailing the online activity of their children and the malware threats they encounter. Easy-to-read graphs show the most frequently blocked targets; the most frequently accessed categories and sites; and other relevant statistics per MSISDN, per IP address, or other identifier. Anti-virus and anti-phishing activity reports are provided in condensed and detailed formats for both web and email traffic. All reports are accessible via standard web browsers from your customer service portal.

Multilayer Detection

Real-time multilayer detection employs patented heuristic methods to identify unregistered signs and mutations that use polymorphic codes to avoid detection. Allot inspects compressed files, images, and scripting files which are popular places to embed malware.

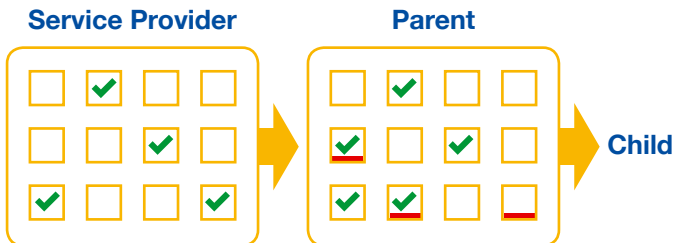


Personal security report showing the top targets blocked during the past 7 days on a specific device.



Single and Multi-Tenant Operation

Single and multi-tenancy operation allows you to offer a predefined set of web security features for all consumers, as well as the ability for customers to personalize their own parental control and anti-malware settings per device. Allot supports up to 50 million individual tenants and lets you manage them via a unified management console.



Off-Net Service Continuity



As your customers move between mobile and WiFi access zones, Allot Secure Dome provides seamless continuity of your web security services. Allot Secure Dome is a ready-to-use app for Android and iOS devices. The app is purpose-built to be easily customized to your brand and made available for download from Google Play and App Store. Once installed on a mobile device, Allot Secure Dome automatically detects when the user moves from RAN to WiFi (and vice versa) and opens a temporary VPN tunnel to route user traffic to your WebSafe Personal service for the duration of the off-network usage.

Configuration and provisioning of Secure Dome clients as well as in-app notification and customer engagement capabilities are managed by the Secure Dome Endpoint Manager within Allot's unified management console for web security services.

Scalable Service Delivery Framework

Allot WebSafe Personal software is fully integrated with Allot Service Gateway and Allot NetEnforcer platforms and may be hosted either on a blade in Allot Service Gateway or hosted externally on COTS hardware. This tight integration enables unlimited scalability and cost-efficient deployment in operator networks. Allot high-performance platforms monitor all network traffic and steer only the relevant flows to the security services, while a unified management console monitors and manages web security services for all customers across your entire network.

About Allot Communications

Allot Communications (NASDAQ, TASE: ALLT) is a leading provider of security and monetization solutions that enable network service providers to protect and personalize the digital experience. Allot's pre-integrated and highly scalable service delivery framework leverages the traffic intelligence in data networks to enable service providers to get closer to their customers; to safeguard network assets and users; and to accelerate time-to-revenue for value-added services. We employ innovative technology, proven know-how and a collaborative approach to provide the right solution for every network environment. Allot solutions are currently deployed at 5 of the top 10 global service providers and in thousands of CSP and enterprise networks worldwide.

www.allot.com info@allot.com

© 2016 Allot Communications Ltd. All rights reserved. Specifications are subject to change without notice. Allot Communications, Sigma and NetEnforcer and the Allot logo are trademarks of Allot Communications. All other brand or product names are the trademarks of their respective holders.

Visibility and Insight for Service Providers

Network-based Security as a Service means that you keep valuable threat-event data within your organization, thus avoiding the privacy risks and higher latencies that are inherent in typical cloud-based datacenter solutions. Moreover, Allot's SECaaS solution gives you complete visibility of network traffic and online user behavior, enabling you to analyze and refine data plans accordingly.

Unified Management

WebSafe Personal is part of the growing portfolio of Allot's pre-integrated security services designed to safeguard the digital experience of your consumer and business customers. Additional security products such WebSafe Business and WebSafe Enterprise can be co-deployed with ease and centrally provisioned by Allot's unified management console.



Security Customer Engagement

Nurture ongoing engagement with your Security-as-a-Service customers by sending them in-browser notifications. Notices to opt-in users are triggered automatically and may include text, images, video, banners, and animations. Automatic notifications provide a non-intrusive channel to keep in touch with customers and to add value to their digital experience.

sales@allot.com

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA Tel: +1 (781) 939-9300 Fax: +1 (781) 939-9393 Toll free: 877-255-6826 • **Europe:** NCI - Les Centres d'Affaires Village d'Entreprises 'Green Side', 400 Avenue Roumanille, BP309, 6906 Sophia Antipolis Cedex, France Tel: +33 (0) 4-93-001160, Fax: +33 (0) 4-93-001165 • **Asia Pacific:** 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104 Tel: +65 67490213 Fax: +65 68481015 • **Japan:** 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 Tel: +81 (3) 5297-7668 Fax: +81(3) 5297-7669 • **Middle East and Africa:** 22 Hanagar St., Industrial Zone B, Hod-Hasharon, 4501317, Israel, Tel: +972 (9) 761-9200, Fax: +972 (9) 744-3626

