WebSafe Business 🔒

Security as a Service for Businesses

Allot WebSafe Business enables managed security service providers to protect the digital experience of business customers whose applications are migrating to the cloud and whose employees are increasingly mobile. With Allot WebSafe Business you can provide effective and flexible Security as a Service to small and medium business (SMB) customers who need protection from online threats and network abuse. Allot's multi-tenant web security services include web (URL) filtering, anti-malware, application control and mail security that protect your business customers and allow them to use Internet and cloud resources safely and productively.

Benefits

Security revenue and intelligence
- Deliver essential web security at affordable price points
- Address business mobility needs with security as a service
- Gain valuable insight on threats and usage trends

Transparency and accuracy
- Per tenant Acceptable Use Policy
- Per tenant application control
- Per tenant visibility and reporting
- Per tenant protection including off-network usage

Flexibility and scalability
- Reduce the complexity of multi-tenant operations
- Scale to support millions of business users
- Accelerate ROI through full integration in Allot Service Gateway

ALLOT
communications

Web Security, Visibility, Control

Businesses are concerned about falling victim to online cyber threats and are struggling to keep malicious malware attacks at bay. Those who lack the knowledge, expertise and stamina to protect their business properly, rely on your managed security services.

Unlike security technologies that were developed for perimeter and on-premise protection, Allot WebSafe Business is engineered to provide a flexible platform for delivering Security as a Service to millions of business users.

Network-based security is ideally suited to mobility needs, enabling you to offer flexible and effective security services at attractive price points for small and medium businesses.

Usage Visibility 👁	Get a clear picture of online usage and understand how Internet security threats are impacting business productivity and viability.
Web Filtering	Assure safe Internet browsing and prevent employee exposure to illegal or inappropriate content in the workplace.
Anti-Malware	Prevent malware threats from damaging mobile devices and causing loss of business data.
Application Control	Define and enforce the Acceptable Use Policy (AUP) that matches business needs.
Mail Security	Stop email spam from threatening business productivity by accurately filtering spam emails without over-blocking.
Ads Free	Reduce productivity distractions and exposure to risky links by blocking popup ads, animated gifs, and banners.

Web Filtering

URL Filter: customers select the content categories and URLs they want to filter per group, user profile, or device.

Browse Time: allows businesses to limit online access to specific hours and/or to maximum hours per day per application, device, group, or user profile.

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

Alerts: administrators receive SMS and/or email notification when attempts are made to access blocked content.

Anti-Malware

Allot WebSafe Business protects SMBs against all kinds of malware that can damage mobile devices and cause the loss of business data. The service 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's anti-malware as a service 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.

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.

Network-based Protection Against

- 🦠 Viruses
- 🐛 Worms
- 🐴 Trojans
- 😎 Spyware
- ⚠ Adware
- ✖ Rootkit
- ⌨ Keylogger
- 🎣 Phishing
- ✔ Others

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.

Reputation Filters → Content Filters → Context Filters
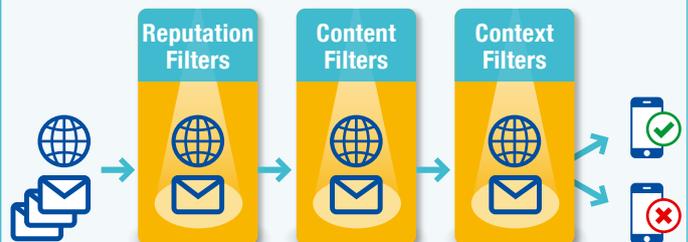
Simple end-user interface is easily customized to reflect your managed services brand and offering.

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.

Application Visibility and Control

Allot WebSafe Business is fully integrated with Allot Service Gateway, which provides Layer-7 visibility of application traffic, enabling business tenants to provision and enforce the Acceptable Use Policy that is right for their organization. Customers can limit access to "risky" applications such as P2P and anonymizers based on their Layer-7 protocol and get proactive alerts on blocking events.

Mail Security

Allot's optional anti-spam filtering 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.
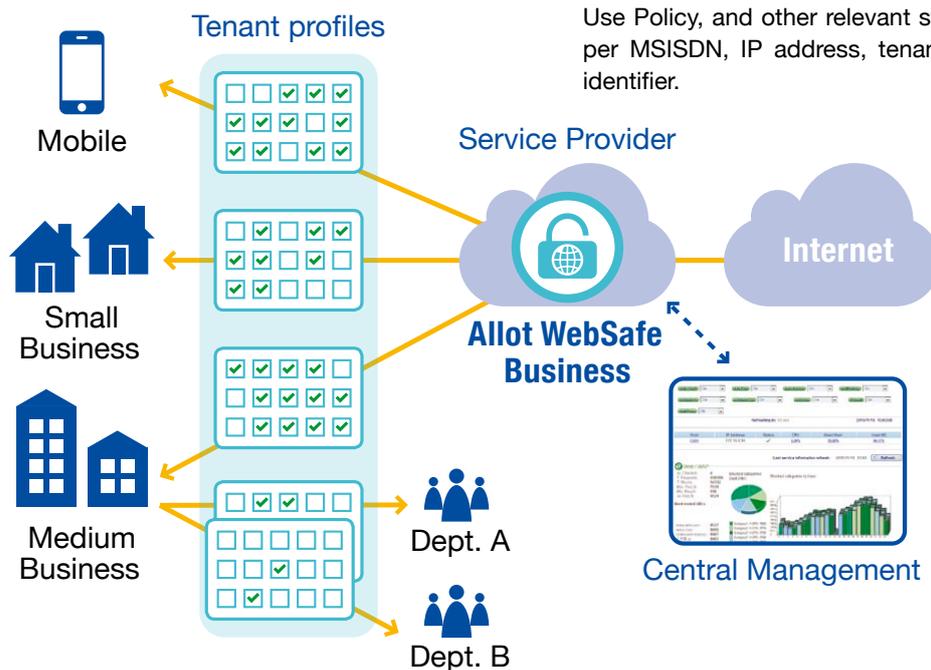
Ads Free

Popup ads, animated gifs and banners often link to risky URLs and expose employees to viruses, spybots, and other infections. Allot's optional Ads Free service effectively blocks these insertions.

Scalable Security as a Service

Flexbile Multi-tenancy

Allot's flexible, multi-tenant architecture allows you to offer a predefined set of web security features for business customers, as well as the ability for SMBs to customize their own web filtering, mail security, anti-malware, and application control settings. Allot supports millions of tenants and lets you manage them via a unified management console. Your managed services customers get a simple and intuitive interface suited to their different requirements for flexibility and security. Allot supports central and distributed tenant control with easy self-management of:

✔ Navigation Groups
✔ Black List Groups
✔ White List Groups
✔ User Profiles
✔ Tenant Policy Control

Network Security Services
Enjoy maximum security as you browse!

Make the most of your security service options
• Customize security settings according to user needs
• For all your connected devices
• Activate/Deactivate the service
• Go Antiphishing!
• And much more

For ADSL and Fiber-Optic Customers only.

Tenant Management and Reporting

With Allot's Security as a Service, business customers receive secure access to your business portal, where they can set up and manage their security service. Allot's numerous out-of-the-box reports feature easy-to-read graphs showing all malware blocking events, frequently accessed categories and URLs, enforcement events triggered by the customer's Acceptable Use Policy, and other relevant statistics that may be presented per MSISDN, IP address, tenant group, user profile, or other identifier.

Tenant profiles

Mobile

Small Business

Medium Business

Service Provider

Allot WebSafe Business

Internet

Dept. A

Dept. B

Central Management

Allot WebSafe Business supports millions of tenants and lets you manage them via a unified management console

Off-Net Service Continuity

As business users 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 Business 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 Business 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.

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 security risks and higher latencies that are inherent in typical cloud-based datacenter solutions. Moreover, Allot gives you complete visibility of online user behavior, enabling you to analyze and refine your managed services accordingly.

Unified Management

Allot WebSafe Business is part of the growing portfolio of Allot's pre-integrated security services designed to protect the digital experience of your consumer and business customers. Additional security products such WebSafe Personal, 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 business customers and to add value to their digital experience.