Delivering Security as a Service to SMB Customers
Solution Brief
Contents

1 Introduction ...................................................................................................................... 1
2 The Market Opportunity .................................................................................................. 2
   2.1 Market Requirements .......................................................................................... 2
3 Allot Security as a Service solutions for MSSPs ................................................................. 4
   3.1 Benefits ................................................................................................................ 4
   3.2 Threat Prevention ................................................................................................. 5
   3.3 Application Visibility and Control ......................................................................... 6
   3.4 Multi-Tenant Security .......................................................................................... 7
   3.5 Tenant Management and Reporting .................................................................... 7
   3.6 Security Customer Engagement .......................................................................... 8
   3.7 Flexible Deployment ............................................................................................ 8
4 Summary .......................................................................................................................... 9
5 Why Allot ........................................................................................................................ 10
1 Introduction

The Managed Security Service Provider (MSSP) market is fast evolving with increasing number of customers looking to acquire security services. This trend is fueled by increased reliance on the Internet to conduct business as well as the growing awareness on the part of SMBs to the threat landscape, and the lack of in-house IT and security knowledge to protect against the growing complexity of attacks. Workforce mobility and applications transitioning from on-premise to the cloud further drive business customers to re-architect their security solutions and acquire security services from cloud security providers, MSSPs and ISPs.

Like most MSSPs, you rely on security technology developed for the enterprise. However, these technologies are far from adequate for you to deliver security services at an affordable cost with reduced operations complexity in a multi-tenant environment that scale to support hundreds of thousands SMB customers.

Allot’s Security-as-a-Service solutions are engineered from the ground up to provide security, visibility and control to millions of tenants. Based on Allot’s experience in the Service Provider market, your MSSP business can benefit from a carrier-class solution that integrates seamlessly in the MSSP and ISP infrastructure and generates ongoing revenue from essential security services.
2 The Market Opportunity

Over the last decade, large enterprises have made considerable investment both in technology and people to secure their key assets, detect breaches and respond to incidents. The threat landscape has become more sophisticated and although the rewards of attacking large enterprises are high, the level of sophistication and cost required is also high. Successful, high end attacks typically employ multiple vectors including social engineering, spear phishing, specifically crafted malware and advanced hacking skills.

On the other hand, “connected” SMBs face the same security threats as larger organizations, but have considerably fewer resources to protect themselves. SMBs present significantly easier targets, and with automation, modern cyber criminals are able to mass produce attacks for little investment. Security vendor, Kaspersky, has noted that “larger enterprises have become better defended so cybercriminals are moving down the business food chain.” With limited resources to address growing security concerns, the vast majority of these businesses will rely on a security service provider. In fact by 2018, Infonetics/IHS expects cloud security services to surpass CPE-based security services.¹ Smaller companies will typically approach their ISP while small to mid-size companies will also seek dedicated cloud security service providers.

<table>
<thead>
<tr>
<th>Cloud-based security</th>
<th>CPE based security</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ No deployment required by SMB</td>
<td>- Physical rollout on premise</td>
</tr>
<tr>
<td>+ Fewer calls to service center</td>
<td>- Technician to deploy and troubleshoot</td>
</tr>
<tr>
<td>+ Always up-to-date, everywhere</td>
<td>- Updates required per site</td>
</tr>
<tr>
<td>+ Bandwidth independent</td>
<td>- Will require a physical upgrade</td>
</tr>
<tr>
<td>+ Security for mobile workforce</td>
<td>- Security for on-premise assets only</td>
</tr>
<tr>
<td>+ Hassle-free, reliable service</td>
<td>- “Yet another box” to manage</td>
</tr>
</tbody>
</table>

2.1 Market Requirements

As an MSSP who wants to take advantage of this market, you are required to provide affordable security that is simple to understand and use and can cost-effectively scale to address a large customer base.

The service should cater for businesses that have no IT staff, providing zero-touch security that does not require software installation and configuration and yet provides the capability to customize through simple controls for those customers that want to. The service should be visible to the tenant, providing both real time notifications and reports that describe the shielding actions that the service has taken to protect him.

In order to address this market, your MSSP business needs a massively scalable solution that provides:

1. Effective threat prevention
2. Out-of-the-box Acceptable Use Policy (AUP) and Application Controls that are easily customized by the SMB
3. Rich out-of-the-box reporting capabilities and real-time alerting to security events and risky behavior
4. Multi-tenancy that supports millions of customers
5. Simple, scalable security management
6. Integration with existing customer management systems
3 Allot Security as a Service solutions for MSSPs

Allot WebSafe Business empowers you to scale your Security as a Service offering to small and mid-size businesses and provide the three pillars of a security service: security, visibility and control.

Allot WebSafe Business provides multi-tenant web security services for both encrypted and clear-text flows, including web filtering, anti-malware, application control and mail security that enable businesses of all sizes to use the Internet safely and more productively.

Effective threat prevention, per tenant acceptable use policy and application control are available in both pre-configured and customizable self-managed options that scale to millions of end users. Allot web security solutions are network-based, so they have no dependency on the customer’s infrastructure or endpoints and no impact on their performance. Activation of the service does not necessitate client installation and configuration by the tenant, which answers the need for simplicity and results in high customer satisfaction. With Allot’s Security as a Service, your SMB tenants get full visibility, real time notifications and reports that describe the shielding actions that the service has taken to protect their business, and delivering ongoing value to this important segment.

3.1 Benefits

For the Service Provider

- Broaden your ISP offering and increase ARPU from revenue-generating security services
- Address the growing market for SMB managed security services in a scalable, cost effective fashion
Enabling Security as a Service for the SMB Market

- Leverage network-based security that is ideally suited to mobility needs and results in high customer satisfaction and increased adoption rates.
- Strengthen customer engagement with regular reports on resource usage and blocked threats.

For the SMB

- Flexible service packages suited to meet various tenant requirements
- Effective threat prevention and peace of mind
- Self-managed and à la carte Acceptable Use Policies and application control
- Canned and customized reporting for security incidents, application and web usage
- Simple to activate and no maintenance

3.2 Threat Prevention

Viruses, spam, spyware, phishing, and Trojans are among the many malware threats that Internet users face every day. Allot WebSafe Business provides network-based anti-malware that protects your customers against all kinds of malware that can cause damage and loss of data. 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.

**Anti-Virus:** powered by Kaspersky Lab, Sophos, and Bitdefender technologies, providing industry-leading response time to new malware outbreaks. Device-agnostic protection 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 malicious sites.

**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.

**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.
Multilayer Detection:
patented heuristic methods 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.

### 3.3 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 that can be used to deliver infected files such as Peer-to-Peer and Anonymizers based on Layer-7 identification and get proactive alerts on blocking events. The solution monitors all traffic and provides complete visibility of application usage and online user behavior, it can also be used to prioritize business related applications. In addition advanced detection capabilities extend enforcement and reporting of the acceptable use policy to HTTPS encrypted flows.

- Rich reporting capabilities enable your managed services to provide additional value per tenant, including:
- Real-time application-based reporting provides granular statistics and analysis of Internet and business applications usage.
- Real-time alerts on use of risky applications and other high risk activity
- Historical reports on application usage and resource consumption
- Scheduled reports for automatic generation and distribution showing all malware blocking events, frequently accessed categories and web activity, enforcement events triggered by the customer’s Acceptable Use Policy, and other relevant statistics
3.4 Multi-Tenant Security

Allot WebSafe Business enables MSSPs to cater for different customer segments that will require different levels of management and reporting capabilities. Central and distributed tenant control enables customers to manage their own Internet security policy, and to define rules based on end users and/or user groups and can also be integrated with Active Directory. Allot’s flexible multi-tenancy enables you to fine-tune your Security as a Service offering to the needs of small and mid-size businesses for both management and reporting per tenant, per users and per user groups with complete tenant segregation.

3.5 Tenant Management and Reporting

Integration of the Multi-Tenant management interface through a REST API enables your business customers 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.
3.6 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 integrates easily with existing VPN or MDM platforms.

3.7 Flexible Deployment

Allot WebSafe Business is a software solution that can be deployed as a standalone service or can be integrated into an NFV service fabric. The solution enables unlimited scalability and cost-efficient deployment in Service Provider networks. When deployed in conjunction with high-performance Allot Service Gateway platforms the solution monitors all network traffic and can provide per-tenant service chaining capabilities to enable additional extensibility to other Service Provider offerings.
4 Summary

SMBs have caught the attention of cyber criminals and are considered low hanging fruit for targeted and automated mass-malware attacks. Security awareness in this market is growing, driven by high profile attacks that are frequently announced in the media. Allot’s solution is designed from the ground up to provide scalable cost-effective security as a service. The solution meets the growing demand to provide security, visibility and control for both the simple and more demanding environments, providing businesses a cloud based web security solution that is simple to activate and utilize. Allot solutions are deployed globally in hundreds of service provider networks where they are seamlessly integrated with existing customer management systems in both tier-one operator networks and cloud service providers, providing Security as a Service for all.
5 Why Allot

We could sum it up in three words: **Visibility**, **Control** and **Security**. But there is much more:

**Customers:** proven results enabling value added services in 1000’s of service provider networks

**Scalability:** Largest customer with over 7,000,000 individual customers in a paid security value add service.

**Superior Technology:** Extensible platform supporting best-in-class security solutions

**Reliability:** Allot expertise in applying carrier-class network know-how to Cloud solutions

**Support:** 24/7 worldwide support.

Your innovative, customer-centric and results-oriented solutions partner

Contact [sales@allot.com](mailto:sales@allot.com) or your Allot representative to find out more.
Enabling Security as a Service for the SMB Market