allot
See. Control. Secure.

Success Story

Swiftel Networks

Swiftel Networks Improves Business by Protecting Downstream Networks from DDoS Threats

About Swiftel Networks

Swiftel Networks sells wholesale products, technology, services, systems and processes to a wide variety of organizations so that they can operate as network providers, offering phone and internet connectivity to their users. It provides network services, end-user billing, payment processing and support to carriers, ISPs and virtual operators. Their clientele includes SMBs and enterprises as well as Communication Service Providers (CSP) and Internet Service Providers (ISP).

Challenge

Swiftel Networks wanted to develop its business as a provider of cloud-based CSP and ISP networks by creating a value-added-service offering for their consumer and Enterprise customers. The ideal offering would boost revenue in two ways; consumer services were meant to assure subscriber QoE and grow ARPU, while enterprise services were meant to allow downstream business customers to offload their infrastructure and reduce their operational costs.

These business plans were threatened when customers experienced massive DDoS attacks, mainly UDP floods and amplified reflection attacks using SSDP, LDAP and CLDA. They brought the wholesaler's infrastructure to a halt and resulted in significant damage to both reputation and service level agreements (SLAs).

Due to the nature of the wholesale business, they needed a network-level solution that would protect their valuable infrastructure and could also be sold to multiple downstream service providers. Scalability was essential to ensure protection could handle the expected increases in network users, bandwidth demand, application proliferation, and the growing number of threats that are constantly emerging.

SWIFTEL NETWORKS

Vertical | Service Provider

Industry | Fixed

Region | EMEA

Solution | DDoS Protection

Challenge

- Massive DDoS attacks from compromised IoT devices
- Halted business development due to damaged reputation
- Need to secure the network and add value to network service offering

Solution

Allot's DDoS Secure solution was designed specifically to meet the kind of requirements Swiftel, an Australian broadband wholesaler, faced. Using our Service Gateway, we were able to provide DDoS protection to Swiftel Networks infrastructure and enable them to offer DDoS protection to their own customers in the form of security-as-a-service. Allot DDoS Secure addressed their challenges and added a new source of revenue.

Benefits

- Partnering with Allot allowed Swiftel Networks to offer credible, proven solutions to their customers
- Gain full visibility of DDoS attacks and valuable threat intelligence
- Assure service availability and maintain high QoE
- New revenue from Allot-powered security-as-a-service

Above all, the urgency of addressing these issues meant that the solution needed to be credible, proven, and with fast ROI, especially for downstream CSPs who planned to offer DDoS Protection as a service to their enterprise customers.

> Allot enabled us to offer greater security to high-value customers and attract larger businesses and service providers."
>
> Ahad Aboss,
> Solution Architect

Solution

While some solutions were able to target and mitigate large attacks, few could handle large combinations of small DDoS attacks and at the same time mitigate these damaging volumetric attacks in seconds before any damage occurred. The combined volume of many smaller attacks caused many problems, including network congestion and the blacklisting of IP networks which would be devastating for downstream CSPs. The failure of traditional security approaches meant that behavior-based detection and mitigation was required.
Swiftel Networks looked for a solution with the following key elements:

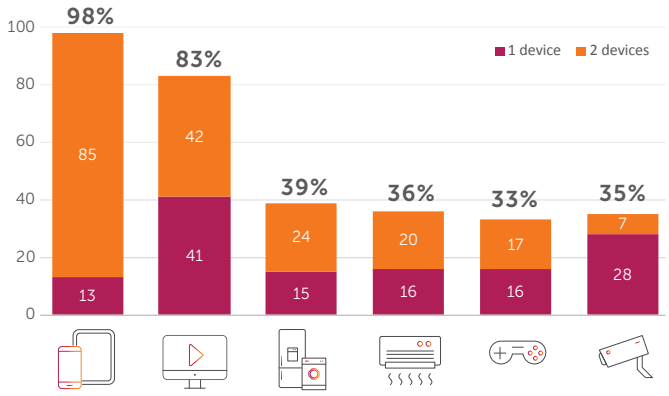
- DDoS Protection to secure the network against attacks and assure service availability
- Fast and complete mitigation that would handle small attacks and massive "hit-and-run" attacks
- Inbound and Outbound protection that will cover vulnerable IoT networks.
- Ability for downstream ISPs to prioritize application delivery to ensure subscriber quality of experience
- Captive Portal Redirection to induce out-of-quota subscribers to top up immediately rather than wait for the next billing cycle

The Allot Service Gateway was already installed by Swiftel Networks to provide DPI-based Traffic Management for application prioritization as well as captive portal redirection, a solution that they intend to offer their downstream CSP and ISP customers. Following the DDoS attack and after considering a variety of other options, Allot DDoS Protection and Bot Containment services were enabled in the same Allot Service Gateway platform via Allot DDoS Secure licenses. The ability to deploy multiple services in a single platform made the upgrade easy and provided the speed, versatility and security that the wholesaler needed.
By deploying these services across the primary network, Swiftel Networks can support the development of its business by offering similar security services to their own CSP and ISP customers as well. This opened new streams of revenue to achieve a higher ROI, which was a welcome byproduct of Allot's solution.

Benefits

- Added Value; Increased Revenue
- Assure Service Availability and QoE
- Multiservice value in one scalable solution
- Multi-tenancy capability

Percentage of Types of Devices in Connected Homes



Resources

About DDoS Secure

About Service Aware DDoS Mitigation

Frost & Sullivan DDoS Mitigation Whitepaper

Learn more about Allot's Solutions »