Allot Secure

DDoS BusinessSecure (Network Protection-as-a-Service)

Cybersecurity Monetization

In today's digital landscape, medium-sized businesses (SMEs) are increasingly vulnerable to volumetric cyberattacks, such as Distributed Denial of Service (DDoS) and Botnet assaults. These attacks can cripple networks, halt operations, and lead to substantial financial losses. The high cost of on-premises security solutions and the need for specialized IT expertise often make robust defense measures unattainable for many SMEs. As a result, more businesses are turning to Managed Security Service Providers (MSSPs), Cloud Providers, and Application Service Providers (ASPs).

This scenario presents a lucrative opportunity for Communication Service Providers (CSPs) to monetize cybersecurity by offering comprehensive communications and security services. By positioning themselves as secure communications providers, CSPs can boost revenue from the business segment as well as enhance their reputation as reliable partners thus differentiating themselves from competitors.

Benefits

- Monetizing Network Protection

  By offering a subscription for Network Protection Services to business customers, CSP can create new revenue streams while optimizing the costs associated with protection efforts.

- Reinforce Your Brand Reputation

  By providing protection against DDoS attacks, blocking Command & Control communications, mitigating outgoing botnet-driven attacks, isolating weaponized IoT, and remediating infected users, CSPs demonstrate their commitment to their SME customers' business resilience. This not only strengthens brand reputation but also positions the CSP as a trusted provider.

- Drive SME Customers' Retention and Growth

  By offering full protection against inbound and outbound volumetric attacks, CSPs position themselves as comprehensive security providers. This assurance enables SMEs to operate with confidence, knowing they are shielded from various cyber risks by their CSP. Such comprehensive network protection is a compelling value proposition that drives customer retention and attracts new business.

Features

Real-time DDoS protection

Detect and block Denial of Service attacks within seconds, before they can threaten or disrupt your customer's network and communication services.

Distributed mitigation of DDoS attacks

World-wide deployment of the service is forming the Security Community. The Service Provider may decide to participate in the Community or not. If the Service Provider joint Security Community, attacks against it will be mitigated by community members by removing malicious traffic passing through their network. This can significantly reduce the load on peer-to-peer connections and avoid the need for a scrubbing center.

Botnet concealment

Automatically detects and quarantines infected endpoints. Proactively prevents botnet attacks.

Self-managed service

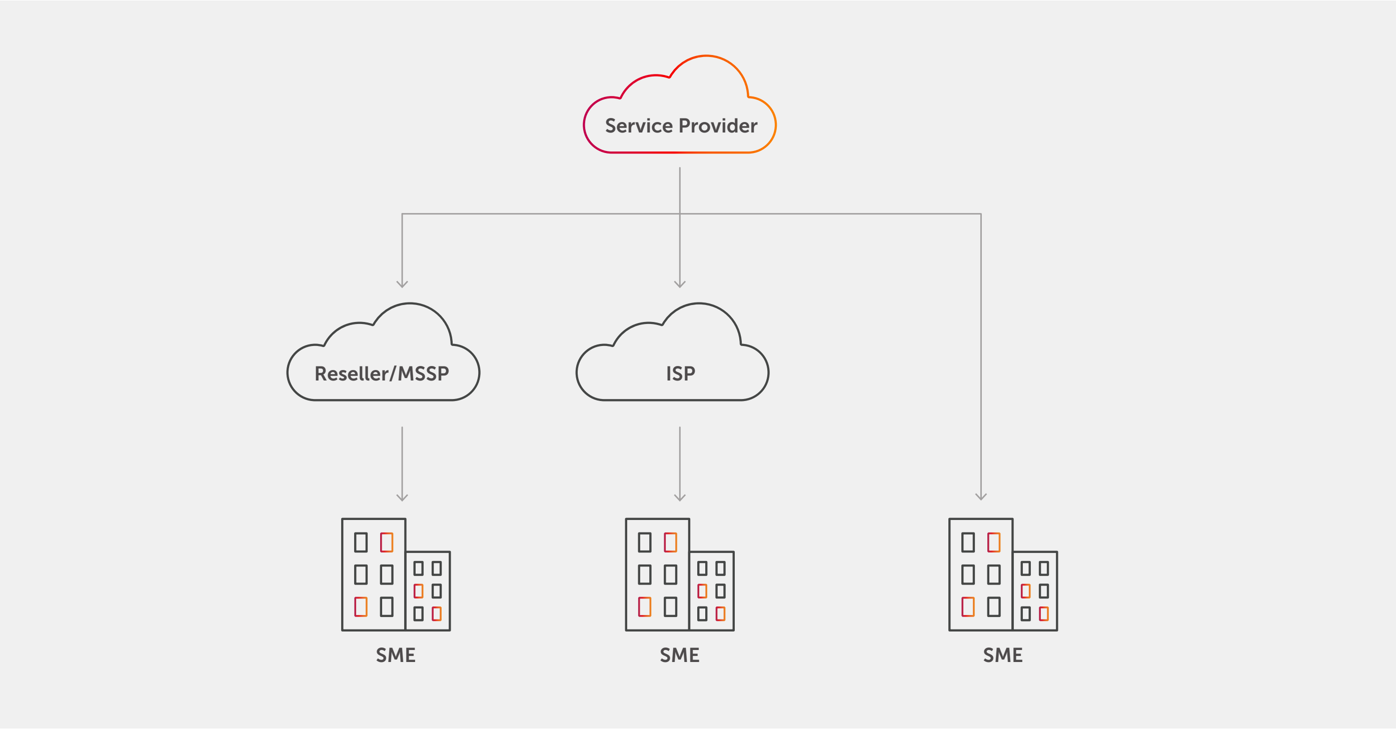
Business customer has a dedicated UI for monitoring network usage and managing the protection service. Two factor authentication can be applied to regulate user access to the system. User's rights to view and/or change system data are role-based.

Multi-level hierarchy

Service Provider can assign one of the following types to the business customer account:

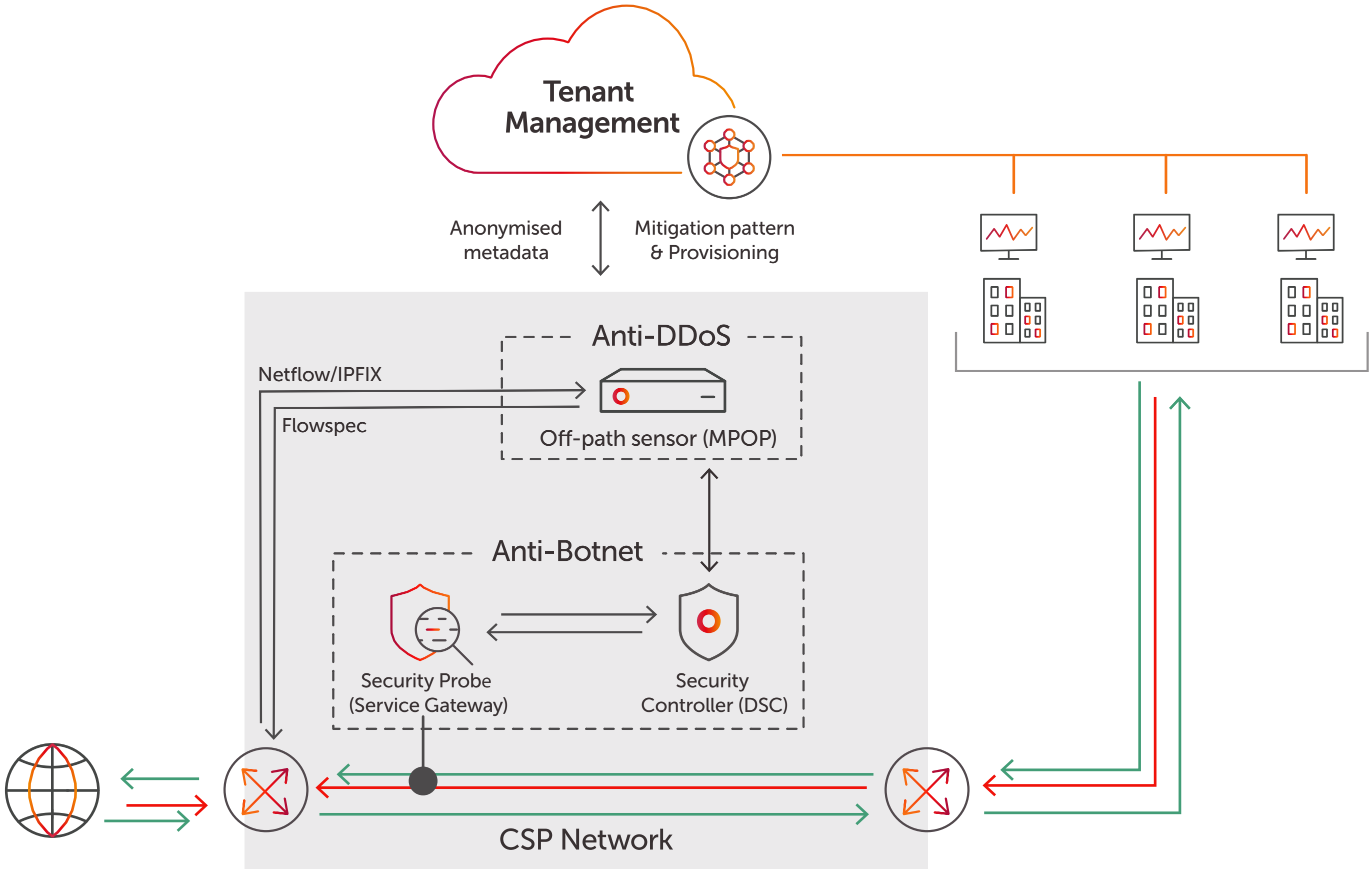
- MSSP – a reseller of the service with no own access or transport network
- ISP – a reseller of the service who also uses the service to protect their own network
- Business – the end-customer who uses the service to protect its network

Top-level users with the appropriate rights can view and/or change system data for lower-level accounts for which they are licensed.



DDoS BusinessSecure provides effective protection against the ever-growing number of inbound and Botnet cyber attacks that threaten your business customers: SME and Enterprise

Features



Cloud-based Tenant Management

- Support multi-layer tenant hierarchy
- 2-factor authentication
- Tenant provisioning

Off-path sensor

- Collects the tenant's traffic metrics from the routers
- Detects volumetric DDoS attacks
- Collects detected bot activity from the Security Probe, via the Security Controller
- Updates the multi-tenant portals

Security Probe

- Detects the Botnet activity
- Reports to the Off-path sensor
- Optional: Quarantines the infected end-points

On the above diagram, Security Probe and Security Controller are optional elements and are only required for detection and isolation of infected devices.

NOTE: Inline deployment option is available as well. Please approach Allot local sales team for more details.

Specifications

DDoS BusinessSecure comprises a cloud-based Tenant Management, an Off-path Sensor (MPOP), an optional Security Probe (SG), and an optional Security Controller (DSC).

Tenant Management

Provides CSPs with the ability to manage business accounts, analyze aggregated metadata to create mitigation patterns; and provides business accounts with a dedicated user interface to self-configure and manage protection in real time.

Off-path sensor

Collects traffic metrics from routers via Netflow or IPFIX. The metrics are aggregated, analyzed for attack detection, and forwarded to Tenant Management via IPsec VPN. If a DDoS attack is detected, the Off-path sensor requests traffic samples, anonymizes them, and sends them to Tenant Management to create mitigation pattern. The pattern is deployed to routers via Flowspec to remove malicious traffic or reduce its rate.

Security Probe

Uses all-packet inspection to detect abnormal endpoint behavior. Security Probe notifies the security controller of suspicious endpoints.

Security Controller

Evaluates the data it receives from the relevant Security Probe (there may be multiple Security Probes deployed in the network that can be managed by the same controller), applies policy using the Off-path Sensor to isolate the suspicious endpoint, and notifies tenant management of the detected bot and the corrective actions applied.

Feature	Network-layer DDoS Protection	Bot Containment
Detection		
Approach Technology	Off-path	TAP all-packet inspection
	Flow-based detection over • Netflow v9 • IPFIX • sFlow	Behavior analysis
Types of Threats	• High packet rate • Fan-in (many IPs to one IP) • Carpet bombing (many IPs to many IPs) • DoS (one IP to one IP) • TCP floods • UDP floods • ICMP floods • Malformed packet flood • Fragmented packet flood • DNS Flood	• Address scan • Port scan • Flow bomb • Mass SMTP • Mass DNS • Aggressive IP (too many sessions per IP) • C2 (communication with Command-and-Control Center)
Reporting	Attack pattern, details, and statistics	
Web UI	Supported browsers: Chrome, Firefox	
Notifications	E-mail, Syslog, REST API	
IP versions	IPv4, IPv6	
Asymmetric Traffic Inspection	Yes	
Number of protected accounts	No Limit	N/A
Mitigation		
Mitigation Time	18 Sec.	
Mitigation Action	• Block • Rate-limit • Alert	
BGP Blackholing (RTBH)	Yes	N/A
BGP Flowspec	Yes	N/A
Distribute mitigation	Via Security Community	N/A

Security Controller

	Physical Edition DSC-200	Virtual Edition DSC-VE (minimum configuration)	Containerized Edition DSC-CE (minimum configuration)
Capacity			
Probs per Controller	Up to 20		
Managed Throughput	Up to 10 Tbps		
Server Specification			
CPU/vCPU	Dual Intel Xeon Silver 4214 (12 Cores) 85W 2.2 GHz	8 vCPUs	
RAM/vRAM	64 GB	16 GB	
Storage/vStorage	2.8 TB	200 GB	
Hypervisor/Life Cycle Management	N/A	• VMWare vSphere 6.7+ • KVM RHEL 7.6+	• K8s • EKS • Robin.io
Management			
Traffic Encryption and Firewall Requirements	• User to Controller: HTTPS and SSH • Controller to Sensor: HTTP/HTTPS/Syslog • Controller to Prob: HTTP/HTTPS		
Management Traffic (maximum throughput)	• 1 Mbps per Sensor • 1 Mbps per Prob		
Mechanical and Environmental			
Form Factor	Standard 1U in 19" rack 43 mm x 434 mm x 715 mm (H x W x D)	N/A	
Weight	11.9-18.8 kg/26.2-41.4 lb		
Operating Temperature	• 50–95°F; 10–35°C (up to 3,000 ft/914.4 m); • 50–90°F; 10–32°C (3,000–7,000 ft/914.4–2,133 m)		
Power Consumption	750 W (per PSU)		
Power Supply	AC, dual redundant, hot swappable		
Certification and Safety	FCC (Part 15 of the FCC Rules, Class A), ICES-003 (issue 5, Class A), UL/IEC 60950-1 CSA C22.2 No. 60950-1, NOM-019, Argentina IEC60950-1, Japan VCCI, Class A, Australia/ New Zealand AS/NZS CISPR 22, Class A; AS/NZS 60950.1, China CCC GB4943.1, GB9254 Class A, GB17625.1, Taiwan BSMI CNS13438, Class A; CNS14336-1, Korea KN22, Class A; KN24, Russia, Belorussia and Kazakhstan, TR CU 020/2011 (for EMC) and TR CU 004/2011 (for safety), IEC 60950-1 (CB Certificate and CB Test Report), CE Mark (EN55022 Class A, EN60950-1, EN55024, EN61000-3-2, EN61000-3-3), CISPR 22, Class A, TUV-GS (EN60950-1/ IEC60950-1,EK1-ITB2000), RoHS Directive, Energy Star 2.0		

Specifications

Security Probe

Physical Editions

	SG-9100	SG-9700
Performance		
Max Throughput (PPS)	7 million	40 million
Max Throughput (Gbps)	50 Gbps	300 Gbps
Max Number of Connections/Flows	12,000,000/24,000,000	72,000,000/144,000,000
Max Number of Endpoints	1,500,000	9,000,000
Hardware Specification		
RAM	128 GB	586 GB
CPU	Intel Xeon-Gold 4210R (10 cores), 1.9 GHz	Dual Intel Xeon-Gold 6248R (24 cores) 3.0GHz
Operating System	Allot Common Platform (ACP)	
Interfaces		
Ethernet interfaces	16 x 1GE/10GE (SFP+)	40 x 10GE
Management	2 x 1GE	2 x 10GE or 2x 1GE
Mechanical and Environmental		
Form Factor	2U 19" rack mount	2U 19" rack mount
Dimensions	8.7 x 44.5 x 72 cm	8.73 x 44 .54 x 67.94 cm (3.44 x 17.54 x 26.75 in), dimensions without Bezel
Weight	20 kg	Min 32.75 lb (14.9 kg), Max 43 lbs (19.5 kg) per number of NIC interfaces
Operating Temperature	10°C to 35°C (50°F to 95°F)	
Operating Humidity	8% to 90% RH	
Power Supply	Dual Hot Plug 750 W 230/115 VAC or -48 VDC	Dual Hot Plug, Redundant 100/240VAC or -48VDC, efficiency of up to 94%, Energy star, 80PLUS
Max Power Consumption		800W
Certification and Safety	CE Conformity, EMC, RoHS, Safety (UL, EN), ISO 9001, ISO/IEC 90003, ISO 14001, SI ISO 27001	CE Conformity, EMC, RoHS, Safety (UL, EN), ISO 9001, ISO/IEC 90003, ISO 14001, SI ISO 27001

Virtual Edition

	SG-VE
Platform	
Hypervisor	VMWare vSphere 6.7 and above, KVM RHEL 7.6 and above
Minimum VM Requirements	vCPU: 4; vRAM: 10GB; vStorage: 100 GB
Max Throughput	4 Gbps/4 vCPU; 12 Gbps/8 vCPU; 24 Gbps/16 vCPU; 48 Gbps/32 vCPU

Off-path Sensor

Physical Editions

Physical Editions	MPOP-500	MPOP-1000
Performance		
Max Routers Throughput (Gbps)	500 Gbps	1,000 Gbps
Max Number of Flows	No Limit	No Limit
Max Number of Connected Routers	No Limit	No Limit
Max Number of Endpoints (IPs)	No Limit	No Limit
Management		
Traffic Encryption and Firewall Requirements	• User to Sensor: SSH • Controller to Sensor: HTTP/HTTPS/Syslog • Tenant Management to Sensor: HTTP/HTTPS	
Management Traffic (maximum throughput)	• Sensor to Routers: 500 Mbps in total • Sensor to Controller: 100 Mbps • Sensor to Tenant Management: 50 Mbps	• Sensor to Routers: 1 Gbps • Sensor to Controller: 100 Mbps • Sensor to Tenant Management: 50 Mbps
Hardware Specification		
CPU	Dual Intel Xeon Silver 4214 (12 Cores) 85W 2.2 GHz	Dual Intel Xeon Gold 6254 (18 Cores)
RAM	128 GB	256 GB
Storage	22 TB	32 TB
Interfaces		
Management	2 x 10 Gbps	
Mechanical and Environmental		
Form Factor	Standard 1U in 19" rack 43 mm x 434 mm x 715 mm (H x W x D)	
Weight	11.9-18.8 kg/26.2-41.4 lb	
Operating Temperature	50–95°F; 10–35°C (up to 3,000 ft/914.4 m); 50–90°F; 10–32°C (3,000–7,000 ft/914.4–2,133 m)	
Power Consumption	750 W (per PSU)	
Power Supply	AC, dual redundant, hot swappable	
Certification and Safety	FCC (Part 15 of the FCC Rules, Class A), ICES-003 (issue 5, Class A), UL/IEC 60950-1 CSA C22.2 No. 60950-1, NOM-019, Argentina IEC60950-1, Japan VCCI, Class A, Australia/ New Zealand AS/NZS CISPR 22, Class A; AS/NZS 60950.1, China CCC GB4943.1, GB9254 Class A, GB17625.1, Taiwan BSMI CNS13438, Class A; CNS14336-1, Korea KN22, Class A; KN24, Russia, Belorussia and Kazakhstan, TR CU 020/2011 (for EMC) and TR CU 004/2011 (for safety), IEC 60950-1 (CB Certificate and CB Test Report), CE Mark (EN55022 Class A, EN60950-1, EN55024, EN61000-3-2, EN61000-3-3), CISPR 22, Class A, TUV-GS (EN60950-1/IEC60950-1,EK1-ITB2000), RoHS Directive, Energy Star 2.0	

Virtual Edition

Virtual Edition	MPOP-VE
Platform	
Hypervisor	VMWare vSphere 6.7 and above, KVM RHEL 7.6 and above
Minimum VM Requirements	vCPU: 20; vRAM: 128 GB; vStorage: 16 TB
Max Throughput	500 Gbps
Max Number of Connected Routers	No Limit
Max Number of Handled Accounts (IPs)	No Limit

July 2025