TAG

THE ULTIMATE GUIDE TO SELLING DDOS PROTECTION SERVICE TO SMES

A SERVICE PROVIDER'S HANDBOOK

DR. EDWARD AMOROSO, CEO TAG,
FORMER CISO, AT&T

SPONSORED BY

allot

THE ULTIMATE GUIDE TO SELLING DDoS PROTECTION SERVICE TO SMEs

A SERVICE PROVIDER'S HANDBOOK

DR. EDWARD AMOROSO, CEO, TAG,
FORMER CISO, AT&T

EXECUTIVE SNAPSHOT

The small and medium-sized enterprise (SME) market is undergoing a critical shift in how it views cybersecurity, particularly the need to maintain business continuity in the face of cyberattacks. As volumetric and stealthy distributed denial of service (DDoS) attacks surge, SMEs find themselves increasingly in the crosshairs. Yet, unlike large enterprises with dedicated security operations centers (SOC) teams, SMEs often lack the resources or staff to respond effectively and frequently opt to outsource their cybersecurity needs.

This presents a timely and lucrative opportunity for service providers, as they already control the critical infrastructure, billing relationships, and customer trust necessary to deliver managed security services on scale. It allows service providers to offer DDoS and Botnet protection that is provisioned directly from their network, requires zero customer overhead, and adds immediate value. With such a protection, service providers are not only solving a security problem but also building stickier, higher-margin relationships.

The guide below offers practical advice on how to handle the sales process for SMEs who would like to add DDOS & Botnet protection service to their service provider relationship. The guide is written as advice to you the reader – who we will presume to be a principal within a communications service provider (CSP), Internet service provider (ISP), or telecommunications company. Our hope is that the advice below will help you to succeed in growing your revenue through your own service delivery infrastructure.

MARKET OPPORTUNITY

As every service provider no doubt knows, the demand for robust and frictionless DDoS protection among SMEs is growing, and this trend is driven by attack trends, compliance obligations, and shifting workplace behaviors. It is also driven, however, by the need for SMEs to ensure that their key information technology (IT) staff are not taken away from their normal work activities due to inconvenient DDOS attacks. Service providers can take advantage of this need by integrating DDoS protection service into broadband and business connectivity offers. The table below outlines the driver, the 2025-2026 trend, and the implications for service providers in delivering DDoS & Botnet protection services to SMEs.

Driver	2025–25 Trend	Implications for Providers
DDoS attacks	Up 20% YoY; millions mitigated in 2024, $20K-40K average cost of damage to a business, per hour	Providers need edge-level mitigation, embedded in the existing backbone
SME IT staff pressures	Managers must ensure that in-house support staff are not diverted from their regular work	Managed security with no setup burden becomes attractive
Compliance pressures	PCI DSS v4.0, NIS2, and sector-specific mandates	Meet regulatory needs such a solution
Back-to-office trends	SMEs increasing reliance on office Internet	Outages disrupt in-office operations; protection ensures continuity

This convergence of risk, regulation, and reliability makes the case for DDoS protection service adoption more compelling than ever. We strongly recommend that service providers review the above drivers to determine how well they map to their local sales and support environment. We suspect that the correlation will be obvious.

SME BUYER PERSONAS & PAIN POINTS

To effectively sell DDoS & Botnet protection services, service providers need to understand the varying priorities and concerns of SME decision-makers. Whether focused on operations, cost, compliance, or technology, each persona requires tailored messaging that connects the offering to their key goals and anxieties. The table below outlines how messaging can and should be tailored to the various personas that will emerge in the buying lifecycle for SMEs:

Understanding these people will enable your sales team to respond effectively to objections and build high-trust conversations with your SME customers.

Persona	Key Metric	Typical Objection	Messaging Hook
Owner/CEO	Revenue & business continuity	"We're too small"	"Over 50% of attacks target SMEs, so you should protect your business in one click."
IT Manager/ MSP	Uptime, SLA fulfillment	"Too much overhead"	"No software, no agents, and nothing for your team to install or manage."/ Zero-touch onboarding, immediate protection
CFO	Operational downtime	"Too expensive"	"One 45-minute attack costs more than two years of coverage."
Compliance Officer	Audit readiness	"We're cloud-based"	"Even cloud-first businesses are vulnerable at the access point, so such a solution can help."

VALUE PROPOSITION FRAMEWORK

The DDoS & Botnet protection service is an operational safeguard that removes pain points for SMEs while enabling new service revenue for providers. The key elements framework below outlines how it creates measurable value for both parties:

For SME:

1. Uninterrupted business continuity – Protecting business reputation and avoiding revenue loss.

2. Always-On Protection – Behavioral baselining and automated detection mitigate DDoS attacks from within the operator backbone before they impact customers.

3. Zero Customer Overhead – Unlike endpoint tools or third-party firewalls, such a solution should be zero-touch onboarding.

For CSP:

1. Frictionless Enrollment – Provisioning is embedded into the telecom service—no extra steps, hardware, or support tickets.

2. Flexible Monetization – Offer basic protection for all customers and upsell tiers that include SLAs, analytics, and traffic reporting.

3. Drive SMEs' retention and growth – CSP becomes a security partner for its SMEs' customers

This framework should guide how the solution is introduced in every pitch, briefing, and collateral document. During the sales engagement, the service provider team should use these points as collateral to help the buyer understand the overall value proposition for their team.

FINANCIAL IMPACTS

The financial advantages of using such a service for SMEs will be highly consistent and correlated to the size, scope, and scale of the buyer, so service providers are advised to ensure that all sales discussions take this relationship fully into account. That said, it is reasonable to guide a buyer that the following data be used to justify the purchase of such a service from a more financially quantified perspective:

1. The cost of a breach-related outage to an SME could result in days or weeks of downtime, during which orders, business, and revenue can be reduced. If a company under a DDOS attack operates, for example, at 50% capacity during a one-week attack, then it is conceivable that up to 50% of revenue for one week could be lost due to the attack.

2. The cost of a breach-related outage to an SME could also result in the time and wages of IT staff and consultants being allocated to DDOS detection, remediation, and recovery. It would not be unreasonable to expect that up to 100% of IT staff and consultant salaries could be allocated to the clean-up work for a one-week break.

As a simple case study example, let's assume that a mid-sized company that provides outsourced IT support is under a DDOS attack. We will also assume that the company's weekly revenue is $200K (a $10.4M annual revenue) and that three IT staff and one consultant have weekly salaries per individual of $1.5K (which implies $78K per year salaries).

Assuming these reasonable and representative estimates, the implication is that a one-week outage from a DDOS attack could thus have a financial impact of 50% of $200K, which is $100K plus an allocation of the four salaries, which is $6K. The effect of a single DDOS attack on this modest organization could be as high as $106K, which helps to explain why such a service will help buyers save money.

SUGGESTED PACKAGING & PRICING MODELS

Service providers can tailor such a solution's pricing models to align with the risk tolerance, connectivity usage, and budget flexibility of SME clients. Below are proven structures you can adopt or adapt when dealing with your potential customers. Remember that many of your SME customers will be prone to include such a solution if the price is reasonable, and the work required for installation and use is essentially zero.

Model	When to Use	Example Tier
Add-on Percentage	Bundle with business broadband	15-20% uplift on monthly internet bill per protected site
Consumption Blocks	Businesses with peak usage traffic	Tiered mitigation at 1, 5, or 10 Gbps
Included in Plan	Regulated sectors or competitive plays	Basic volumetric protection for all with upgrade options
Free Trial	New broadband customers	30-day free protection; includes emailed attack reports

It is highly recommended that a solution with high versatility in packaging be chosen to ensure that providers can hit price points across SME tiers, from budget-conscious startups to compliance-bound mid-market firms. This is a key point since SMEs will not have large security or IT budgets.

GO-TO-MARKET (GTM) PLAYBOOK

A successful rollout will depend heavily on aligning marketing efforts to each customer journey phase. Service providers can use a structured playbook to build a pipeline, convert interest, and grow long-term value. We presume that the funnel stages shown below will map to the specific approaches being taken by the sales team to engage SMEs in a deal:

Funnel Stage	Key Tactics	Metrics
Awareness	Webinars: "What is DDoS?" / Email campaigns to SME owners	Impressions
Consideration	ROI calculator; scenario-based outreach	Incident avoidance and IT staff rates
Purchase	Easy ordering (portal or sales desk); no-installation onboarding	Trial to paid conversion
Expansion/ Retention	Quarterly reviews, bundled with other managed services	Churn rate, ARPU uplift

Supporting content and tools should reinforce simplicity and business impact across each touchpoint.

MESSAGING PILLARS & SAMPLE COPY

The messaging pillars below are designed to resonate with SME buyers and simplify your go-to-market communications. We recommend using these messages consistently across web pages, sales decks, and account outreach.

Pillar	Proof Point	Sample Copy
Business Continuity	Losses per attack include revenue loss, lost hours/ time of IT staff	"Stay connected. One click shields your business from revenue loss & inconvenient outages."
Hands-Off Simplicity	No agent installs, no user actions required	"Nothing to install. Protection starts with your service."
Regulatory Alignment	PCI DSS, NIS2, ISO 27001	"Meets key availability mandates for SMEs"
Telco-Trusted Defense	Same filters protect Fortune 500 networks	"Carrier-grade DDoS protection is now available to every SME."

Where possible, reinforce these points with customer proof, demos, or risk reports. Remember that the SME team will not be security savvy and will not resonate with claims that a DDOS attack will cost them hundreds of thousands or millions of dollars. However, they will resonate with the claim that if the business office network is down, great inconvenience will follow, which could cost the company real time, effort, and dollars.

SALES ENABLEMENT TOOLKIT

To support internal teams and channel partners, equip your field force with the following turnkey resources, which can be developed and supported through your sales contact at Allot.

1. **Live Attack Simulator** – Real-time demo illustrating how the solution alerts and stops DDoS floods.
2. **Objection Handling Sheets** – Battlecards for retail, healthcare, and SaaS verticals with common SME concerns.
3. **ROI Calculator** – Translate downtime risk into economic value.
4. **Case Studies** – One-pagers from retail, healthcare, and SaaS verticals.
5. **Pitch Deck Template** – Modular deck walking from risk to solution to business impact.

The more easily your teams can show value, the faster adoption will grow. Just let our team at Allot know which sales enablement resources you would like to have, and we will ensure that you have tailored support to help engage your client with such a solution.

COMPLIANCE & REGULATORY SUPPORT

DDoS protection is now more than a nice-to-have. Instead, it's becoming a regulatory expectation and a requirement for many larger companies to hire smaller SMEs as suppliers, partners, or vendors. Such a solution helps SMEs satisfy multiple requirements, including the following everyday compliance demands:

- **PCI DSS v4.0 (Requirement 6.4.3)** – Availability controls for online merchants
- **NIS2 (EU Directive)** – Telecoms must secure critical digital infrastructure
- **Cyber Insurance** – Discounts available when telco DDoS protection is active

Again, we suggest that the service provider position the solution as a risk-mitigation and compliance-alignment solution. The solution should also be reinforced as helping to avoid the massive inconvenience of a DDOS attack on a business and its staff.

ALLOT DDoS SECURE

Allot DDoS Secure (a Network Protection as a Service solution) enables you to boost your security services revenue and position yourself as a trusted security partner for your business customers.

Allot DDoS Secure offers an affordable, branded DDoS and botnet protection service for your business customers that mitigates risk and enhances customer retention. It is ideally suited for business customers with fixed IP addresses who lack IT expertise or budget resources. Allot DDoS Secure offers these customers simplified cloud-based deployment and zero-touch onboarding.

Provide outstanding network protection services to your business customers, fostering growth, reducing churn, and enhancing their resilience!

OBJECTION HANDLING CHEAT SHEET

Our experience shows that service providers must be ready to answer common SME concerns with clear, non-technical language that reinforces value and simplicity. Below are some typical objections that we predict occurring during the sales engagement lifecycle, and we've listed some suggested responses.

Objection	Response
"Our firewall blocks DDoS"	"Allot DDoS Secure detects attacks before they reach your firewall. Volumetric floods bypass most edge tools."
"We use cloud apps"	"That's great, but outages at your office are still blocking access. Allot DDoS Secure keeps you online."
"It's too technical"	"There's nothing to configure. Protection is provisioned by your provider automatically."
Any expected delays in my internet traffic	No delays are expected since internet traffic will not be diverted, and no inline nodes are required.
"Why pay more?"	"One attack can cost more than a year of coverage, and the first month is often free."

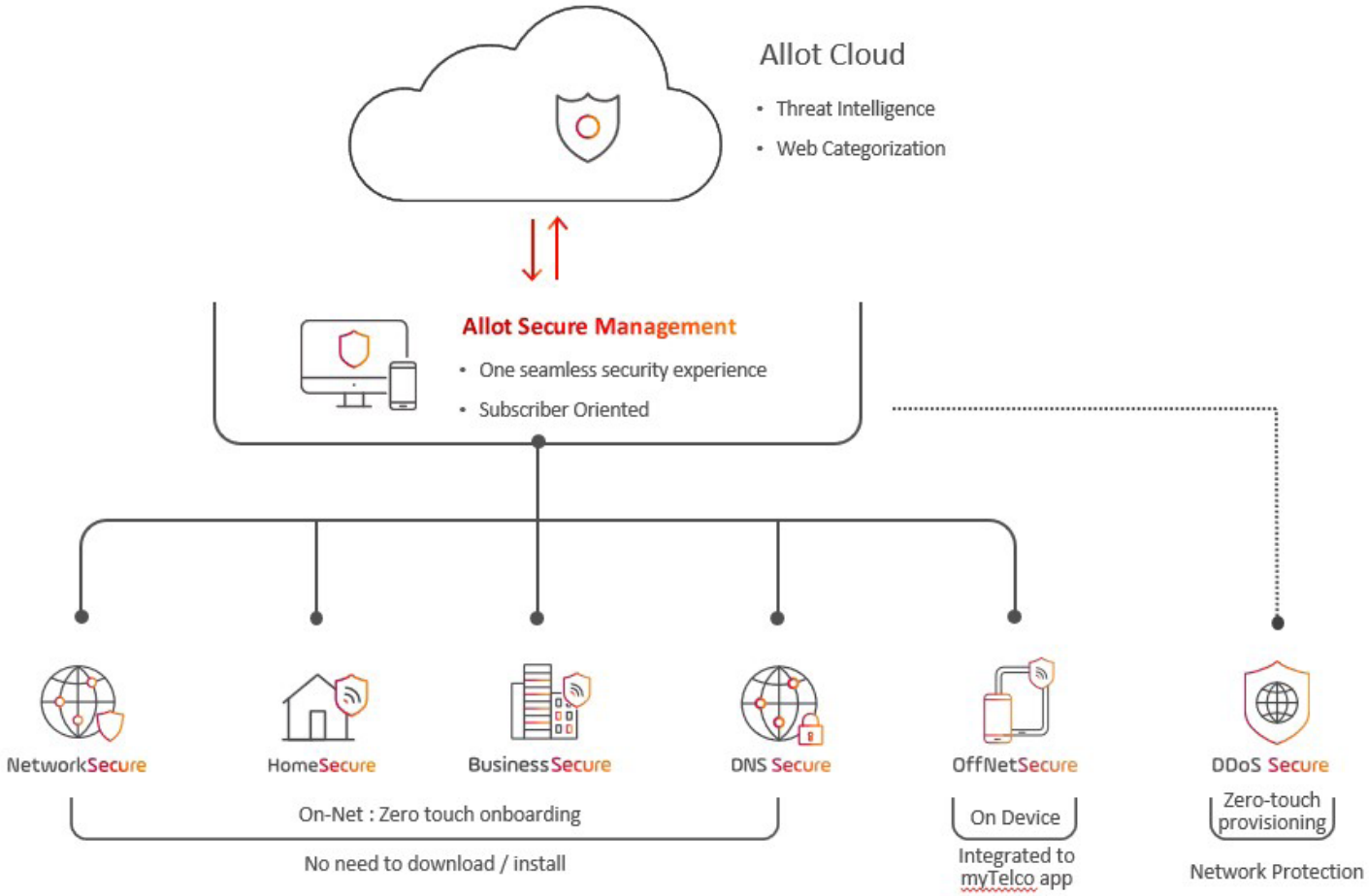
We recommend that service providers train their frontline teams to use these responses conversationally, not as scripts, but as part of their standard sales narrative, to build trust.

FINAL TAKEAWAY

Allot DDoS Secure represents a transformational opportunity for CSPs, ISPs, and telcos to deliver carrier-grade security service with consumer-grade simplicity. By packaging DDoS and Botnet protection as a frictionless add-on to broadband and connectivity, service providers can reduce churn, increase ARPU, and turn cybersecurity into a core differentiator. The time to act is now, before your SME customers face the next outage or your competitors move first.

Allot DDoS Secure is part of Allot's Secure monetization offering.

Allot is the leading provider of network-based cybersecurity solutions for service providers. Business customers, SMEs, and subscribers rely on their service provider to keep them secure. Service providers are ideally positioned to deliver comprehensive security across their business customers' networks and all devices, whether on or off the network. Allot Secure empowers providers to increase ARPU by offering security to their subscribers and business customers.



ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence,.