StingBox HoneyPot

Sales Enablement Guide: StingBox

StingBox Sales Enablement Guide

Leveraging Deception Technology for Modern Managed Services

This guide is designed to help MSP sales and account management teams position **StingBox Deception Technology** as a critical layer in a modern security stack.

What Makes Stingbox Different?

Keep these three (3) **"StingBox Truths"** in mind to differentiate the solution from standard EDR/MDR:

- **Deployment in Minutes:** Whether it's a physical "StingBox" hardware unit, a virtual machine, or an external cloud monitor, it requires zero complex configuration or "tuning" periods.
- **The "Blind Spot" Filler:** Most security tools look for signatures or behaviors. StingBox looks for presence. It catches attackers during the reconnaissance phase—before the ransomware is even deployed.
- **Near-Zero False Positives:** Unlike AI-driven tools that guess, StingBox is binary. If a "StingBox" is touched, it is extremely likely to be a malicious actor or a policy violation.

SECTION 1 — Core Framing (The Universal Pitch)

Use these points to set the stage with any C-suite or technical decision-maker.

- **The "Tripwire" Concept:** "We install digital tripwires across your internal and cloud networks. These systems have no business purpose, so they should never be touched by a legitimate user."
- **High Fidelity, Low Noise:** "Our team doesn't have to sift through thousands of logs to find a threat. If StingBox alerts us, we know with 100% certainty that someone is poking around where they don't belong."
- **Catching Lateral Movement:** "Traditional security focuses on the 'front door.' StingBox catches attackers once they are inside and trying to move from one computer to another."

SECTION 2 — Strategic Persona Talking Points

Persona A: The Generalist / IT-Focused MSP

Focus: Operational efficiency and "proving" the value of the seat price.

- **The Insurance Policy:** "StingBox validates that our other tools are doing their job. It's the final safety net that ensures nothing slips through the cracks."
- **Efficiency:** "Because it generates near-zero false positives, our engineers only respond to 'smoking guns.' This allows us to provide elite-level security monitoring without bloated overhead costs."
- **Visible Value:** "In our quarterly reviews, we can show you exactly how we are monitoring the 'dark corners' of your network that standard antivirus and other tools don't even see."

Persona B: The Scaling / Operationally Mature MSP

Focus: Risk mitigation, SLA adherence, and standardized security stacks.

- **Closing the Detection Gap:** "Standard EDR can be bypassed by sophisticated fileless malware. Deception technology is the industry standard for catching 'living-off-the-land' attacks."
- **Rapid Incident Response:** "StingBox gives us the earliest possible warning. We can isolate a threat during the discovery phase, often hours or days before a breach becomes a crisis."
- **Compliance & Cyber Insurance:** "Insurance carriers are increasingly looking for proactive detection. Adding deception technology puts our clients in a superior risk category, making renewals easier and premiums lower."

Persona C: The Security-First MSP (MSSP)

Focus: High-level telemetry, threat hunting, and sophisticated defense.

- **Enhanced Telemetry:** "StingBox provides high-confidence signals that enrich our entire SOC workflow. It's the 'signal' in a world of 'noise.'"
- **Attacker Deception:** "By deploying honey-services with StingBox, we force the attacker to reveal their intent and tools without risking your actual production data."
- **Cost-Effective Deception:** "Enterprise-grade deception used to cost six figures and require a dedicated analyst. StingBox allows us to provide that same level of protection at a mid-market price point."

SECTION 3 — Objection Handling

Objection	The "StingBox" Rebuttal
"We already have EDR/MDR."	"EDR is great at watching processes. StingBox is great at watching people. If an attacker uses stolen credentials, EDR thinks it's a normal user. StingBox catches them when they touch the 'forbidden' honey-pot."
"I don't want more alerts."	"You won't get more; you'll get better ones. StingBox is silent for months until there is a real problem. It's the only alert in your stack that guarantees a high-priority response."
"Is this just a honeypot?"	"It's a managed deception network. Unlike old-school honeypots that were hard to maintain, this is a cloud-coordinated system that monitors your internal LAN and your cloud environment simultaneously."

SECTION 4 — Closing & Next Steps

The "Peace of Mind" Close:

- "By adding StingBox, we aren't just adding another software agent; we're adding a 24/7 silent sentry. It's the most cost-effective way to ensure that if a breach does happen, it's detected quickly."
- "This gives us early visibility without operational overhead."
- "It strengthens your security posture in a measurable way."
- "It complements what you already have in place."

Next Step Framing:

- "I'd like to include a 'StingBox' in our next site audit so you can see the type of data it gathers."
- "If something does happen, we'll know immediately."
- "We typically deploy it quietly and let it do its job."
- "If nothing happens, that's still valuable."

For further information regarding this Document or StingBox products, please contact us at:

- Email: support@stingbox.com
- Phone: (561) 203-8594
- Website: www.stingbox.com
- Mailing Address: StingBox LLC 7190
  SE Federal Hwy Ste 3 Stuart, FL 34997-8693, USA