ABSOLUTE®

TECHNOBIND

ABSOLUTE SECURITY FOR PARTNERS:

SALES GUIDE & PITCH FRAMEWORK

Are your customers truly protected even when their security tools fail?

Most organizations believe that once they deploy endpoint security, they are fully protected. But here's the reality: Security tools don't always stay active on 100% of devices. And that's where the real risk begins.

The Problem Customers Don't See:

Today, enterprises invest heavily in EDR / XDR solutions, Antivirus, Endpoint protection and these tools are designed to Detect threats, Block attacks, and Monitor suspicious activity. But all of this depends on one thing: **The agent on the device must be working.**

What can go wrong?

- Agents crash or get corrupted
- Updates break functionality
- Users uninstall or disable them
- Malware shuts them down

Result:

- Devices become invisible to IT
- Threats go undetected
- Policies are not enforced

In large environments, this happens more often than expected.

The Risk: When Security Stops Working

During advanced attacks like ransomware:

- Security tools are often targeted first
- Communication with IT is blocked
- Monitoring stops silently

This creates a dangerous situation:

- The device is compromised
- IT doesn't know
- The threat spreads

And when disruption happens, the real challenge isn't just detection—it's how quickly you can recover and restore operations remotely.

The Concept: Endpoint Resilience

Traditional security = Protection
Endpoint resilience = Assurance that protection is always working

This is the gap most organizations are unaware of.

Where Absolute Fits:

Absolute delivers two critical capabilities:

Resilience:

- Continuous device visibility
- Automatic recovery of security agents
- Persistent control—even after OS reinstall or tampering
- Real-time assurance of endpoint compliance

Recovery with Absolute Rehydrate:

- Restore devices even if the OS is compromised
- Recover endpoints remotely without physical access
- Execute recovery at scale across environments
- Maintain control and communication during incidents
- Reduce downtime significantly

"We don't replace your security. We make sure it never stops working. And when things break, we help you recover—fast, remotely, and at scale"

Why This Matters:

Indian enterprises face unique challenges:

- Distributed and hybrid workforce
- Large endpoint fleets
- Limited IT bandwidth
- Increasing compliance pressure (DPDP, RBI, BFSI norms)

Resulting gaps:

- Silent agent failures
- Visibility blind spots
- Compliance risks

In distributed environments, physically accessing compromised devices is slow and impractical—making remote recovery capabilities critical for maintaining business continuity

The Partner Opportunity:

This is where it gets interesting for you as a partner.

1. **Sell Into Existing Installed Base, Your customers already use:**

- Microsoft Defender
- CrowdStrike
- SentinelOne
- Sophos

You're not replacing anything. You're enhancing what they already have.

This means: Faster sales cycles, Lower resistance, Easier conversations.

2. **Increase Deal Size (15–30%), Attach Absolute to:**

- EDR deals
- UEM deployments
- Device refresh projects
- Managed services

Turn a ₹1 Cr deal into ₹1.15–1.3 Cr deal

3. Open New "Recovery & Downtime" Conversations

- Move from security spend → business continuity discussions
- Position around: Downtime reduction, Faster recovery SLAs, Operational resilience

4. High-Margin, Low Competition

- Not a crowded category
- Not price-sensitive like AV/EDR
- Strong differentiation

5. Build Recurring Revenue

- Subscription-based model
- Predictable renewals
- Cross-sell and upsell opportunities

6. Access CXO-Level Conversations, Sell to:

- CIO
- CISO
- Risk & Compliance leaders

Move from reseller → strategic advisor

Where to Spot Opportunities (Sales Triggers)

Ask your customers:

- "How do you ensure your security tools are working on 100% of devices?"
- "What happens if your EDR agent stops reporting?"
- "Do you have visibility into agent health across all endpoints?"
- "How do you handle devices that go offline or get tampered with?"
- "If a device is fully compromised, how quickly can you recover it remotely?"
- "How long would it take to restore operations across hundreds or thousands of devices after an attack?"

If they don't have clear answers — you have an opportunity

Target Segments:

Highest potential:

- BFSI (compliance-driven)
- Government & PSU
- IT/ITES (remote workforce)
- Enterprises with 5,000+ endpoints

Final Takeaway:

With this solution, You can:

- Monetize the existing security installed base
- Differentiate in competitive deals
- Increase deal size and margins
- Enter compliance-driven conversations
- Build long-term recurring revenue

"Because in today's threat landscape, it's not just about protecting devices—it's about ensuring you can recover them, anytime, from anywhere."

Get in Touch Today to Know More.

+91 – XXXXXX

XXXXXX@technobind.com

www.technobind.com