LogMeIn Resolve

Datasheet

Data Protection for MSPs: How You Should Sell it to your Customers

Data protection services is no longer a "nice-to-have" for businesses aiming to maintain agility, reduce downtime, and ensure data security. For Managed Service Providers (MSPs), data protection represents an opportunity to elevate client operations while diversifying service offerings for improved profitability.

The Opportunity for Data Protection from MSPs

Key Challenges Businesses Face Without Data Protection

Without proper data protection strategies, businesses face significant risks that can threaten their operations and long-term success. Data loss from cyberattacks, hardware failures, or accidental deletion can disrupt operations entirely.

The resulting downtime can lead to substantial financial losses, particularly for small to medium-sized businesses. Additionally, failing to comply with industry regulations such as HIPAA or GDPR can result in heavy penalties and legal troubles, further compounding the challenges businesses face.

Data Protection Services are a Business Enabler

Investing in a robust data protection solutions is more than just implementing backup technology. It’s about ensuring operational resilience, reducing risks of downtime, maintaining compliance, and enabling scalable growth. MSPs that shift the conversation from technical tools to business outcomes benefit from a proactive approach that safeguards their customers’ operations and supports sustainable growth in an increasingly competitive landscape.

The MSP Advantage

As an MSP, you are perfectly positioned to offer and sell data protection services to your clients. With technical expertise, and deep knowledge of client infrastructure, you have the ability to manage your clients’ entire solution lifecycle. Combining BCDR with other IT services you already offer, you can provide tightly integrated services that protect customers that simplify their operations.

As an MSP, you are likely viewed as a technology partner, as opposed to *just a vendor*. This trust makes your recommendations around risk mitigation and data protection well-received when positioned properly. Data protection is another important way to ensure your clients are safe, making it simply another extension of what you have already promised to do.

Tips for Selling Data Protection Services

1 Focus on Business Continuity

Disaster Recovery is not tangible until disaster strikes, and this makes it hard to fully grasp the value. Instead of focusing on selling backups, MSPs can shift the focus to protecting business continuity.

Talk to customers about the level of risk they are taking on without, the potential downtime, and the revenue that would be lost in such a crisis.

2 Perform Risk Assessments

Help customers and prospects understand their current risks. Start by identifying the data and systems critical to their operations, and work to move beyond conversations focused on 'just servers'. Aim to understand all the things they can't live without - workstations, different cloud apps, critical files, etc.

Encourage customers to critically assess things like how quickly they could recover if their server is infected with ransomware, or what their plans are for other disasters. Help them quantify the impact - how much revenue would they lose per day? Would they face regulatory fines? Would they lose clients?

3 Highlight Real-World Statistics

- Over half of all businesses that fall victim to a cyber-attack or data breach face public scrutiny and experience declines in brand reputation, customer loyalty, and trust*.
- Approximately 29% of attacked businesses suffer revenue losses, with nearly 40% of them losing over 20% of their total revenue*.
- More than 20% of organizations that endure data loss or a cyber-attack also lose customers, and 40% of those companies see a decrease of more than 20% in their customer base*.

*https://www.acronis.com/en-gb/blog/posts/data-backup-for-business/

4 Price Effectively: Focus on Value

Although you should absolutely run cost analysis when setting prices, don't rely solely on costs to set your BCDR prices - this will sell the service short. Really work with customers and prospects to quantify the damage they would incur should a disaster strike. This makes demonstrating ROI much more effective - the extra $$ per month will be nothing in comparison.

Your MSP should evaluate different pricing approaches (i.e. per device, per GB/TB, flat monthly, or tiered bundles) to determine which fits your business model best, and to potentially provide your customers with options. Be sure to clearly define the scope of your BCDR services for customers to maintain proper expectations.

5 Prepare Objection Handling

Even when value is clearly communicated, customers and prospects may object to the service. Prep your sales team with common objection handlings so they are always prepared to respond to apprehensions like "Our data is already backed up," "We'll worry about this later", or "It's too expensive".

LogMeIn Resolve Data Protection Suite powered by Acronis

LogMeIn Resolve unifies how your MSP manages customer endpoints with advanced capabilities, including data protection. Trust LogMeIn Resolve Data Protection Suite powered by Acronis to keep customers operational even in the event of a disaster

Contact Sales