Malwarebytes™

THE MSP'S GUIDE TO PROFITABLY SELLING SECURITY.

Well- timed sales conversations, tips for upselling and cross- selling services and introduce customers to managed detection and response.

Managed security services had already been growing in popularity with small and medium-sized businesses, but the COVID-19 pandemic really shone a light on their importance.

Business had to embrace new ways of working, often with staff working from home or remote locations. They turned to managed service providers (MSPs) to help make that work. Securing all those users working remotely saw the demand for managed services for security increase drastically. According to IDC that spending is expected to continue increasing with an **annual growth rate of 13%** through 2025.

Businesses are now adapting to what seem to be permanent changes in how work is done, including more remote and hybrid working. This is a massive opportunity for MSPs to not only add new business but also grow their monthly recurring revenue (MRR) from existing customers. Smart MSPs are capitalizing on this today. But the landscape has changed. Where MSP customers may have been rushing to establish and secure remote working arrangements for staff during the pandemic, they are now able to take a more measured approach to their security investment. This allows MSPs to adopt a more consultative approach to their customers, focusing on business benefits that new or enhanced security services can offer. It's also a good time to show the continued value of working with an MSP as part of normal operations. **The MSPs that thrive under these circumstances will share several characteristics:**

- ✓ **Know their customers** extremely well and time their conversations accordingly
- ✓ **Have strong approaches to upselling** higher level security services or cross-selling complementary services and other services that add value
- ✓ **Provide an educational approach** to introduce and sell managed detection and response (MDR)

This paper will look at how to make the most of opportunities presenting themselves to MSPs. This includes best practice for cross-selling complementary services, upselling higher level services, using risk education to sell managed detection and response (MDR), and how to time all these conversations with customers for the best results. This will give you an advantage in the competitive MSP landscape, allowing you to better service your customers and reap the benefits in MRR.

Best practices for cross-selling complementary security services

Cross-selling—selling additional services to existing customers—is a great way to increase MRR. It's easier to have a selling conversation with an existing customer than finding and approaching a new lead and winning brand-new business. However, an MSP should never take existing customers for granted. You must put in the work to effectively cross-sell.

A great way to start the cross-selling conversation is to **introduce a new service to the customer**. Smart MSPs periodically create new services to offer to their existing customers that complement their core offering. This could, for example, be something that customers have been asking about but which is not in the core offering, such as email protection or vulnerability assessment or staff security training.

One thing to keep in mind, however, is that small- and medium-sized business (SMB) customers are often extremely cost conscious. Some may have been under considerable pressure due to the changing business environment. It's often best to take a gentle and creative approach when selling any new service. **Focus on the business benefits** to the customer. These include saving time, saving money, speeding up workflow or reducing downtime. **Offer to discuss the technical details if the customer wants**. Some SMBs want to know the nuts and bolts, others don't. Tailor your approach to touch on what's important to them.

It's also important to remember that the selling conversation continues after you've left the building. Your customer will likely discuss

your offer with other staff. That's why it's vital to **create a strong selling sheet** or other collateral that you can leave with the customer. It ensures your key selling points remain part of the internal conversation. Even if it doesn't clinch the sale today, such an asset may linger in your customer's office and prompt a call when things have changed (new needs, increased budget, or new management, for example). Ideally, your selling sheet will include quotes or references from other customers using the service.

The MSPs that thrive under these circumstances will share several characteristics:

Clearly identify the benefits to the customer

- ✓ Sell the business value, not the technical features of the new service
- ✓ Be sure customers clearly understand how this service improves their security, lowers risk, and benefits their business

Provide a selling sheet or other collateral to share with customers

- ✓ You want to leave the customer with something to study and share with others and guide internal conversations about your product when you're not there.
- ✓ This can prompt a call later when circumstances have changed, and the customer is ready to buy

Provide examples / case studies of how other customers have benefited from the new service

- ✓ Real-world use cases are a powerful selling tool
- ✓ Offer incentives to early customer adopters in exchange for their quote or reference to share with other customers
- ✓ Make sure to include these quotes and references on your assets, including your selling sheets

Incentivize customers with discounts

- ✓ Consider offering incentives on pricing for new services
  - 3 months free
  - 10% reduction on total service package when customer adds on the new service
- ✓ Once the new service is turned on and starts generating new MRR, you will make up for any discounts given up front

Best practices for upselling higher-level security services

Typically, MSPs work with security vendors who offer multiple levels of their products. Higher-level products usually cost more but provide advanced capabilities that MSP customers will benefit from in terms of increased security, lower risk, and other benefits.

MSPs benefit when customers pay for higher-level services through increased margin on the upgraded security tools (more MRR). In addition, **more security features keep customers safer and happier**, meaning less time needs to be spent addressing customer issues. Often the upgraded features can automatically handle things that would prompt a customer call on more basic packages.

However, upselling to those services can be a challenge. An **MSP cannot disparage the customer's existing service**. Instead, sell the new benefits that will come with moving to that higher level.

As with cross-selling, SMB customers are extremely cost conscious. Getting them to **commit to an increased spend requires respect for their current position** and clear communication of the service benefits.

One way to make the benefits of a higher level of service more tempting is to **bundle the service or tool with other items**. This may include additional reports or other functionality. When you can point to these tangible things that come with an upgrade to a new package, this helps the customer more clearly see the benefit of upgrading.

Again, the key to this sale is showing the business benefits. Be sure customers clearly understand how this service improves their security, lowers risk, and benefits their business. **Spend some time to do a side-by-side comparison of their current package** and the upgrade, pointing out the new capabilities and benefits. You're also going to want to leave the customer with a selling sheet that focuses on the benefits of making the upgrade.

4 points for successful MSP upselling

Package the upgraded tools into a new service level

- ✓ If this fits with the MSP's tiered service model, have a 'Platinum Package' that is based on the capabilities and benefits provided by the upgraded tools
- ✓ Don't sell the higher version of the tool, sell the better package

Clearly show how the upgraded service level provides additional, critical benefits to the customer

- ✓ Sell the business value, not the technical features of the upgraded tools
- ✓ Compare side by side with existing tool capabilities and benefits

Provide a selling sheet or collateral to share with customers

- ✓ An asset to leave with the customer so they can review and share with others in the company
- ✓ Let them look or consider later if needed

Provide examples and case studies of how other customers have benefited from the higher-level service

- ✓ A video testimonial from other customers on the positive impact they've realized from the upgraded tools is a powerful asset

Using 'risk education' to sell MDR

Managed detection and response is a useful service for customers which can also help boost an MSP's MRR and improve margins. Perhaps the biggest challenge—but often with the biggest reward—is **educating a customer on the business risks** they face and how MDR can mitigate risk.

It's important for an MSP to **use care during this selling conversation**. You must clearly and accurately communicate the risks facing the customer without being seen as fearmongering. Use news stories to illustrate the risk of ransomware attacks, data theft, distributed denial of service (DDoS) attacks, and other attacks MDR can help defend against. Lead into **how the 24x7 nature of MDR can drastically reduce these threats** and the business risk they pose to the SMB.

Once you've shown what the risks are, **explain how MDR can help**, in plain terms. Discuss the benefits that companies realize when they move to MDR. This includes 24/7 monitoring by expert security analysts, rapid identification and triage of alerts, and a rapid response that protects the customer even outside of MSP support hours. Again, use benefits-focused language to show how MDR benefits the business rather than focusing on technical features.

Once you've completed risk education, then you're ready to have a selling conversation about your MDR solution and **walk the customer through the details**—always tied back to the business benefits—of what you offer, the engagement model, the pricing model and packages available. This is a great time to introduce customer testimonials. Close with a discussion of the next steps to begin moving to MDR.

The 4-step risk-education approach to MDR selling

Package the upgraded tools into a new service level

- ✓ Risk education' is really important – when a customer clearly acknowledges the risk the business faces, they will be more open to new security offerings

Explain what MDR is in very plain terms

- ✓ MDR reduces risk to the business by:
  - 24/7 monitoring by top-tier security analysts
  - Identifying and triaging endpoint alerts
  - Immediately responding to and removing new threats
- ✓ Share industry statistics on the movement to MDR

Highlight the benefits that MDR provides to the business

- ✓ 24/7 monitoring means acting immediately on new threats, not waiting until Monday when the MSP is active
- ✓ Advanced analysts with the scope of knowledge to back up the MSP and SMB's in-house teams and provide defense in depth
- ✓ Threat hunting strengthens defense and reduces risk of breach by pro-actively finding hidden threats that slip by regular endpoint security products

Introduce your MDR solution to your customer

- ✓ Share engagement model (how it works -- customer, MSP, MDR Team)
- ✓ Share pricing and packaging options
- ✓ Share customer testimonials or case studies (if you have them)
- ✓ Provide clear path to evaluate and start
- ✓ Give out a data sheet or other asset for the customer to review and consider

Time the sales conversation with your customers

The secret to sales is timing. If you approach a customer (or potential customer) at the wrong time, making any progress will be difficult. You may even wind up antagonizing them. **The time to sell, cross-sell or upsell to a customer should be chosen with care**. MSPs have better success when they time sales conversations based on the activities and readiness of their customers—SMBs often have tight budgets and need to be in the right state of mind to consider spending more on security.

Perhaps the best way to know when to approach customers for selling conversations is to have non-selling conversations. **Conduct quarterly business reviews or make ad-hoc calls to see how things are going**. Note what your customers are doing, how their needs may be changing, if their understanding of security is maturing, and note what questions they have for you. Unless they ask you, don't try to shoehorn in discussion about new services. When you spot a good case to discuss new services, make a separate appointment.

Another great conversation starter is a security breach (or near breach). A customer that has experienced the pain and cost of a breach will probably be open to hearing about ways to reduce future risk. A high-profile security incident that makes the news can also increase customer interest in improved security even if they weren't affected. A smart MSP will keep a close eye on the news.

Finally, get to know **your customers' budget calendars**. As has been mentioned several times throughout this paper, SMBs often have tight budgets. A selling conversation will not bear fruit if the money simply isn't there. Pay attention when clients talk about budgets and timings and mark it on your calendar.

4 ways MSPs can choose the right time for a conversation

A well-timed conversation is more likely to make a sale

Approach customers who are rapidly evolving their own security knowledge and practice as they are more willing to consider new packages and higher levels of service

- ✓ Take note of each customer through quarterly reviews or ad-hoc check-ins:
  - Are they learning about security?
  - Are they caring more about security over time and realizing the threats they face and risk to their company?

Sell new services after a breach to help reduce future risk

- ✓ Identify customers who have felt the pain of a breach (or near breach), they'll want to reduce future risks
- ✓ Tie your upsell or cross-sell options directly to the cause (or almost cause) of the breach, offering a direct option to protect against future risk from the same attack method

Know your customers' annual budget and purchase periods so you can time your upsell/cross-sell conversation accordingly

Opening conversations is the key to closing the sale

The good news for MSPs is that businesses are more aware than ever about the need for improved security. With more staff working remotely and high-profile breaches making the news, they want to be protected. MSPs that can have good conversations with customers will see increased MRR and better margins as a result.

Increasing revenue from existing customers can seem daunting, but it's really driven by four principles:

1. **Time** your conversations and approach customers when they are open to discussing new options.
2. **Identify** where a cross-sell will benefit an existing client.
3. **Upsell** based on benefits.
4. **Educate** the customer on risks and how your MSP can reduce those risks.

By breaking each of those steps down further, as we have in this paper, it becomes clear **how an** MSP can start sales conversations, ensure those conversations are well-received, and provide customers with improved protection while enhancing MRR.