GUIDE

3 Steps to Building Your Managed Security Service

Introduction

Managed security services provide a great way to deliver the protection that today's small and medium businesses (SMBs) require while offering an opportunity to differentiate and grow your business through new revenue and services. Done right, managed security services can be a valuable extension to your existing service portfolio and provide a cost-effective and efficient way to provide security services suitable for SMB budgets.

The key is identifying the type of security your SMB clients need in relation to their attack surface – the possible ways they could be vulnerable to a cyberattack or security risk – and budget. Then it's a matter of putting best practices and technologies in place to protect them. The tools you choose should enable you to continually assess the state of their security, protect endpoints and networks, monitor IT environments, and recover systems in the event of any unexpected issues.

Once you have identified the right combination of security tools, the next step is understanding how to define, bundle, price, and market your security services. This guide looks at strategies and best practices that include:

- Creating service bundles to fit SMB security needs
- Pricing security services
- Developing go-to-market strategies for existing customers and prospects

Contents

Defining and Bundling Your Managed Security Services

We all know too well that SMB security needs and budgets vary widely. By defining the types of services you want to offer and organizing them into different tiers or packages, you can efficiently respond to a range of business types and vertical markets where security needs, security knowledge level, and budgets may differ.

Identifying a core set of layered security services will also help standardize your security offerings and provide your SMB clients with a much easier way to see the service options and security levels available to them. It will also simplify your sales process by providing a foundation for discussing clients' current and future security needs. For example, a basic security package may get them to try your managed security service, but over time, you'll be able to offer them a more complete package and build added value.

Sample Security Bundles

In the second guide in this series, 3 Essential Components of a Managed Security Service for SMBs, we outlined the 12 essential technologies that should be part of any SMBs' security stack for protecting data, devices, and people.

With this in mind, a good foundational set of bundled services should include these services along with the ability to continually assess, measure, and monitor your clients' environment. Then you can adopt an a la carte approach for additional services that can be offered as options to any of the bundles you create. This allows more flexibility to customize services for any challenging situation, whether it's a budget issue or the need to integrate with existing security solutions or services.

The three service bundles below provide a good guideline for offering comprehensive protection. All three bundles include protection for data, devices, and people, but choosing the most appropriate solution for your clients depends on their budget, data sensitivity, and attack surface.

Bundling is not a one size fits all approach, but it's a scalable starting point to help you effectively price and market your security services. For example, MSPs typically offer IT services in reactive, proactive, and managed service bundles. You could add Essential security services to your Reactive service bundle, Premium security services to your Proactive service bundle and so on.

ESSENTIAL

ANTIVIRUS

One of the most important ways to defend devices within your client's business is by installing and monitoring antivirus software on all devices. You should always be able to monitor whether every device has antivirus installed and whether it has been activated.

PATCH MANAGEMENT

Regular patch management ensures software and applications are patched and updated, providing a critical defense against software vulnerabilities that could lead to successful cyberattacks.

EMAIL SECURITY

Email security delivers end-to-end encryption so the content of your clients' emails can only be read by the sender and the receiver. Any outsider who does not have the key to decrypt the message and its attachments will not be able to view the information in it.

SECURE REMOTE WORKING

To ensure remote employees have a secure connection to company data and applications, it is important to provide them with a VPN connection to their company network that encrypts all traffic.

BACKUP & DISASTER RECOVERY

Even the most sophisticated security measures are not enough in some cases. So it is important to have a solid backup and disaster recovery solution in place that can restore operations quickly and easily, at the push of a button.

PREMIUM

Includes the features of the **Essential Package and:**

WEB GATEWAY

Secure web gateways filter unwanted and malicious web traffic to protect PCs from a cyberattacks. It usually incorporates URL filtering, SSL inspection, sandboxing of unknown files, and policy application.

AUTHENTICATION

This starts with defining password policies for each of your clients. It also helps to install a password manager that generates random, strong passwords for each login environment and allows for Single Sign On. Multi-factor authentication is another good option.

TOTAL

Includes both the **Essential** and **Premium Packages and:**

ENFORCEABLE PROCESSES AND POLICIES

This requires sitting down with your client to define their business processes and security policies. The next step is to create enforceable practices that every employee must follow.

DATA LOSS PREVENTION

A data loss prevention solution prevents end users from sharing sensitive data outside the company network by helping you regulate what data end users can transfer outside the network.

SERVER HARDENING

Web servers usually sit at the edge of the network making them more vulnerable to attacks. Proper hardening ensures default configurations are changed and that certain services are disabled.

SECURITY AWARENESS AND TRAINING

It's crucial to educate your clients on how to defend themselves, for example, by creating strong passwords and recognizing phishing emails. Knowledge is key when it comes to cybersecurity, so it is important to provide regular training.

Key Pricing Strategies for Managed Security Services

Just as bundling your security services reduces complexity for your customers, your pricing strategy should also be clear and understandable. Pricing should be dictated by your business needs, existing costs, quality of your services, and ultimately the value you deliver. While there are several pricing models used in the MSP market today – per device, per user, flat rate, or a value-add approach – it really comes down to determining the model that works best for your business and the clients you serve. Ultimately, the right pricing for your business will drive better margins on the services you deliver, create strong recurring revenue streams, and build valuable client relationships that position you for ongoing success.

It's important to recognize that there is no golden model or standard for pricing in the industry. A good best practice to follow is to ensure your pricing reflects the true value of your services without the influence of competitor rates.

A key step in determining your value is to evaluate your existing cost structure and identify your break-even costs for providing services. Then add the costs associated with the security services in your bundles, which should include the key categories below, in addition to your desired margin. It may be helpful to capture all of these costs in a grid.

SOLUTION COSTS

Determine the monthly or annual costs for the security tools, solutions, and equipment you use to deliver services. This should include the cost of security solutions that are needed to deliver your tiered bundles and the costs associated with each.

BUSINESS COSTS

Account for all administrative and office costs, including facility leases and rents, utilities, accounting software, insurance, and office supplies. Include costs for providing health insurance and other compensation for your staff, if wages were not fully captured in your labor costs.

LABOR COSTS

Categorize all ongoing tasks performed by your team of technicians, contractors, and administrative staff. Assign time required for each task and an hourly rate. Include a section for security services and list the general tasks associated with your service bundles. This will offer a good picture of the labor involved to run each aspect of your current business as well as the security services you plan to provide.

INITIAL COSTS

Include a breakdown of the tasks required for an initial setup, such as anything involved in configuring and deploying services like antivirus and backup, as well as special considerations required for the client's IT environment. For new customers or prospects, you may want to include a line item for a security assessment or audit – this can be helpful in quickly gauging their security status, security needs, and overall risks in the IT environment before determining the best services bundle and pricing.

Assigning Markups to Your Pricing

Once you have a good picture of the costs to run your business and deliver security services, you should also evaluate the markup you will assign to your service bundles. A good rule of thumb here is to consider the types of SMBs you currently serve – number of users, locations, data, type of business, and any ongoing support costs.

Risks should also be considered. Potential risks typically include highly sensitive data, critical uptime, or network monitoring requirements. It's also important to assess the number of high-touch clients you serve as this may require additional time regardless of how much you automate your service delivery.

Best Practices for Marketing Security Services

According to Datto's State of the MSP Report[1], sales and marketing are the top challenges facing MSPs today. The research found that an estimated 53% of MSPs struggle with effectively marketing and selling their services. It's easy to see why. Busy MSPs often don't have the time, resources, or skill set to implement a go-to-market plan and manage an ongoing marketing effort.

Fortunately, you don't need to be a marketing expert. Marketing and selling your security services really starts with understanding your customer's business and communicating information that provides value. You should be the first source your SMB customers turn to when it comes to questions or needs about security services, threats, and risks, or breaking news about security that may impact their operations. Effective and popular methods of customer communications include:

- Monthly newsletters
- Emails
- Social media
- Webinars
- Websites

But before you start developing marketing campaigns, you need to understand your customers' key pain points, their security maturity, and purchasing style. Are they more interested in price, service, or quality? Is security important to them or is it a "grudge" purchase (hint: many feel it's a grudge purchase, but it's actually a strategic differentiator). Learning what makes them tick will help you develop messages that resonate and provide information that actually helps them understand or solve a problem they are struggling with.

Here are a few best practices to follow when marketing to your client base:

BE PROACTIVE AND CURRENT

The changing threat landscape provides a marketing opportunity to educate clients on emerging threats. From emailing tips on how to avoid phishing scams or new strains of ransomware to patching updates, you have the opportunity to deliver expert advice. One of our partners created a Ransomware Diffusion Program that provides key services and education to their clients to help them prevent ransomware attacks.

BE CONSISTENT

Plan ahead and dedicate an internal resource that can act as a regular point of contact for customer communications. This will help you avoid long lapses between communications when you're dealing with emergency issues or other demands.

BE STRATEGIC

Understand the type of communication that works best for your clients and also your resources. Emails and newsletters can be a great way to deliver updates. Your website is also a good source for the latest information. If you have identified a common pain point for a specific vertical you serve, consider hosting a webinar.

Summary

Adding managed security services to your existing portfolio can provide significant advantages, but it's important to follow best practices to make the transition successful for you and your client base.

Identifying the security services that your SMB clients require, based on the potential vulnerabilities in their IT environment and the security risks their type of business may be exposed to, is critical to ensuring data, devices, and employees can be effectively secured. The next step is understanding how best to build, price, market, and sell managed security services.

Defining your security service offering, creating service bundles, determining the right pricing, and developing go-to-market strategies are all essential elements to delivering managed security services. With these tips in mind and a good sense of what may work best for your clients' security needs and your business model, managed security services can drive new value, recurring revenue, and build strong client partnerships.

[1] Datto 2018 State of the MSP Report

About Avast Business

Avast Business provides integrated, enterprise-grade endpoint and network security solutions for SMBs and IT service providers Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. The result is superior protection that businesses can count on. For more information about our managed services and cybersecurity solutions, visit www.avast.com/business.