CONNECTWISE

EBOOK

Why Your MSP Needs a **Managed SaaS Security** Offering

Table of Contents

INTRODUCTION

The evolving threat landscape and the SaaS blind spot or the SaaS security gap MSPs can't ignore

The global shift to Software-as-a-Service (SaaS) is reshaping how businesses operate. Platforms like Microsoft 365, Google Workspace, and others now serve as the backbone of modern business operations, enabling greater collaboration and efficiency. But with this adoption comes a significant, and often overlooked security challenge.

As a Managed Service Provider (MSP), you are the trusted guardian of your clients' IT infrastructure. You manage their networks, endpoints, and on-premises servers, diligently protecting them from a myriad of threats. But what about the data residing within their SaaS applications? Are you truly offering comprehensive protection if this critical area remains unaddressed or bundled within a broader cybersecurity package?

The time has come for MSPs to recognize and address the unique security risks of SaaS applications head-on. By developing a dedicated, specialized SaaS security service, you can stay ahead of evolving threats while:

Enhancing your value proposition
Differentiate yourself from competitors and become a more strategic partner for your clients.

Unlocking a new revenue stream
Tap into a growing market with a high demand for specialized expertise.

Strengthening your clients' security posture
Reduce your clients' risk of data breaches, compliance violations, and business disruptions.

Maintaining margins and continued growth
With a shifting workload, to remain profitable MSPs who make the shift can maintain and/or grow margins.

CHAPTER 1

The false sense of security in SaaS

MSPs can play a critical role in guiding businesses through the complexities of SaaS security by sparking essential conversations around key cybersecurity challenges.

Core points to identify this false sense of security include:

The Shared Responsibility Model

Clearly explaining the division of security tasks between the SaaS provider and the customer.

Data Sprawl and Shadow IT

How unmanaged or poorly managed SaaS applications can create significant security vulnerabilities.

Insider Threats and Accidental Data Loss

Highlighting the risks originating from within the organization.

Sophisticated Phishing and Account Takeover Attacks

Focusing on threats specifically targeting SaaS environments.

Compliance Requirements

Discussing how regulations like GDPR, HIPAA, and SOC 2 impact SaaS data security.

By explaining the Shared Responsibility Model, you can educate clients on the division of roles and security tasks between the SaaS provider and the customer. This discussion helps clarify the responsibilities of each party in securing data and applications, emphasizing the need for additional security measures beyond what the SaaS provider offers. MSPs can highlight the importance of implementing a **Managed SaaS Security** service to bridge the gap and ensure comprehensive protection for critical assets.

Furthermore, MSPs can engage clients in conversations about the risks associated with Data Sprawl and Shadow IT, showcasing how unmanaged or poorly managed SaaS applications can introduce significant security vulnerabilities. Additionally, discussions around Insider Threats and Accidental Data Loss can shed light on the internal risks that organizations face, underscoring the need for robust security measures and monitoring capabilities.

By highlighting the prevalence of sophisticated Phishing and Account Takeover Attacks targeting SaaS environments, MSPs can demonstrate the evolving threat landscape and the necessity of advanced security solutions to detect and mitigate such threats effectively.

Lastly, addressing Compliance Requirements such as GDPR, HIPAA, and SOC 2 can help organizations understand the regulatory implications of SaaS data security and the importance of aligning security practices with industry standards. Through these strategic conversations, MSPs can build a compelling case for a specific **Managed SaaS Security** service tailored to address the unique security needs of each client.

CHAPTER 2

Why generic cybdersecurity isn't enough for SaaS

In the ever-evolving landscape of cybersecurity, it is essential for Managed Service Providers (MSPs) to recognize the unique challenges posed by securing SaaS environment. While traditional cybersecurity offerings are indispensable, they may fall short in addressing the specific vulnerabilities and complexities inherent in SaaS environments.

One of the primary drawbacks of a general cybersecurity strategy is the lack of SaaS-specific focus. Typically, general cybersecurity services, while effective in safeguarding users, devices, and network perimeters, may not offer the specialized protection required to mitigate SaaS-based threats adequately. Moreover, the dynamic nature of SaaS applications introduces configuration blind spots that demand a nuanced understanding of ever-changing security settings.

Traditional support services may struggle to keep pace with the continual management and configuration required to ensure optimal security posture in SaaS environments. Additionally, the chapter sheds light on the alerting limitations inherent in SaaS solutions, emphasizing the need for proactive monitoring and response mechanisms beyond the scope of conventional support services. Addressing incident response challenges within a SaaS environment calls for a distinct skill set and approach, underscoring the importance of a **Managed SaaS Security** service tailored to navigate the intricacies of responding to security incidents effectively in SaaS applications.

Core limitations of a generic approach to cybersecurity and highlights the necessity of a tailored **Managed SaaS Security** service:

Lack of SaaS-Specific Focus

General cybersecurity services that protect users, devices, and perimeters may not provide adequate protection for SaaS based threats.

Configuration Blind Spots

Ensuring proper configuration of ever-changing SaaS security settings requires specialized understanding.

Alerting Limitations

SaaS solutions often have proper notification processes for security alerts, but this requires continual management and configuration that is outside of traditional support services.

Incident Response Challenges

Responding to security incidents within a SaaS environment requires a different skillset and approach.

CHAPTER 3

Introducing Managed SaaS Security: Your dedicated SaaS application security service

Embarking on the journey of creating a specialized **Managed SaaS Security** service requires a strategic approach to conceptualization and branding. In this chapter, we will walk you through the process of defining and shaping your new service offering, using the example name **Managed SaaS Security** as a starting point. We encourage you to craft a unique and compelling name that aligns with your brand identity and resonates with your target audience.

To effectively position your **Managed SaaS Security** service in the market, it is crucial to define the scope of your offerings and identify key service components that will set you apart from generic cybersecurity solutions. Begin by outlining the specific SaaS platforms you will initially support, such as Microsoft 365 and Google Workspace, to tailor your services to meet the unique security requirements of each platform.

Consider including a range of services within your offering, such as security configuration management, threat monitoring, data loss prevention, user training, and regular assessments, to provide comprehensive protection for your clients' SaaS environments. This process will form the foundation of your **Managed SaaS Security**, ensuring that you deliver value-added security solutions that address the specific needs of organizations relying on SaaS applications.

Specific Steps to define a **Managed SaaS Security** service:

Defining the Scope of "Managed SaaS Security"

What specific SaaS platforms will you support initially (e.g., Microsoft 365, Google Workspace, Salesforce)?

Identifying Key Service Components

- **Security Hardening and Configuration**: Implementing and maintaining optimal security settings within the SaaS platform.
- **Threat Detection and Monitoring**: Utilizing tools and expertise to identify and respond to suspicious activity.
- **Data Loss Prevention (DLP)**: Implementing policies and tools to prevent sensitive data from leaving the secure environment.
- **User Security Awareness Training**: Educating users on threats and best practices.
- **Regular Security Assessments and Reporting**: Providing clients with insights into their SaaS security posture.

Developing a Unique Selling Proposition (USP)

What makes your **Managed SaaS Security service** stand out? Focus on expertise, proactive approach, tailored solutions, and peace of mind.

CHAPTER 4

Pricing Your Managed SaaS Security service for profitability and value

In the realm of Managed Service Providers (MSPs), establishing a compelling case for a specialized **Managed SaaS Security** Service involves delving into various pricing models and strategies. This chapter will serve as a guide to help you navigate the intricacies of pricing your new service offering effectively, ensuring that you strike a balance between profitability and client value.

To build a robust pricing strategy for your **Managed SaaS Security** service, it is essential to first understand the costs associated with delivering comprehensive security solutions tailored to SaaS environments. By calculating the resources, tools, and expert labor required to safeguard clients' SaaS applications effectively, you can determine a pricing structure that aligns with the value proposition of your service.

Embracing a value-based pricing approach that maintains a minimum 65% margin will allow an MSP to price service based on the tangible benefits it offers clients while ensuring profitability and protection for MSP clients.

Additionally, weigh the merits of per-user versus flat-fee pricing models for SaaS security, evaluating the advantages and drawbacks of each to determine the most suitable option for your target market.

Key pricing steps and strategies for your new service:

Per-User vs. Flat-Fee Pricing

Analyze the pros and cons of each model for SaaS security.

Understanding Your Costs

Based on the model selected, calculate the resources, tools, and expert labor (time) required to deliver "**Managed SaaS Security**."

Value-Based Pricing

Price your service based on the value it provides to clients with a minimum of 65% margin.

- **Calculation**: (Tools Cost + Labor Costs) / (1-.65) = Minimum Pricing
- **Example**: (12.00 (tools) + 32.00 (estimated labor) / (1-.65) = $125.71(Minimum Price)

CHAPTER 5

Launching and communicating "Managed SaaS Security" to your clients and prospects

When introducing your **Managed SaaS Security** service to clients and prospects, a well-thought-out launch strategy is essential for garnering interest and driving adoption. Start by prioritizing internal training and enablement to ensure that your team is well-versed in the nuances of discussing and delivering top-notch SaaS security solutions. Equipping your staff with the knowledge and confidence to articulate the value proposition of "**Managed SaaS Security**" will be instrumental in positioning your service as a trusted and reliable choice for clients seeking robust cybersecurity protection.

Crafting a client communication strategy that resonates with both existing clients and potential leads is crucial for effectively promoting your new service offering. Educate your existing clients on the inherent risks associated with their SaaS applications and emphasize the tangible benefits that **Managed SaaS Security** can bring to their organizations.

A successful launch requires a well-defined strategy for both existing clients and potential new customers:

Internal Training and Enablement

Ensure your team is knowledgeable and confident in discussing and delivering the "**Managed SaaS Security**" service.

Client Communication Strategy

- **Tailor Your Messaging**: Focus on the specific pain points and needs of each client.
- **Educate Existing Clients**: Highlight the risks they face within their SaaS applications and the benefits of "**Managed SaaS Security**."
- **Offer Webinars and Workshops**: Educate clients on SaaS security best practices and your new service.

Prospecting and Marketing

- **Update Your Website and Marketing Materials**: Clearly feature **Managed SaaS Security** as a core offering.
- **Develop Targeted Content**: Create blog posts, articles, and social media updates focused on SaaS security challenges and solutions.
- **Run Targeted Marketing Campaigns**: Reach out to businesses that heavily rely on SaaS applications.
- **Highlight "Managed SaaS Security" in Sales Presentations**: Position it as a crucial component of a comprehensive security strategy.

CONCLUSION

Securing the future, one SaaS application at a time

By launching a dedicated SaaS application security service like "**Managed SaaS Security**," your MSP can not only protect your clients from a growing and often underestimated threat but also position yourself as a forward-thinking leader in the cybersecurity landscape. This proactive approach will strengthen client relationships, unlock new revenue opportunities, and ultimately contribute to a more secure digital world for everyone.

Checklist: Launching Your Managed SaaS Application Security Service

This checklist will guide MSP owners through the key steps of pricing, launching, and communicating a new managed SaaS application security service.

PHASE 1

Defining and Pricing Your Service

- ☐ **Identify Target SaaS Platforms**: Determine which SaaS applications you will initially support (e.g., Microsoft 365, Google Workspace).
- ☐ **Define Core Service Components**: Clearly outline the specific security services included (e.g., security configurations, monitoring, and reporting).
- ☐ **Identify Necessary Tools and Technologies:** Research and select SaaS-specific security solutions.
- ☐ **Identify Service Delivery Costs**: Document labor, tools, training, and overhead.
- ☐ **Research Competitor Offerings**: Understand how other MSPs pricing and packaging similar services are.
- ☐ **Choose a Pricing Model**: Select a pricing structure (e.g., per-user, flat-fee, tiered) that aligns with your costs and value.
- ☐ **Set Your Pricing**: Determine the final price points for your service offerings.
  Calculation: (Tools Cost + Labor Costs) / (1-.65) = Minimum Pricing
  Example: (12.00 (tools) + 32.00 (estimated labor) / (1-.65) = $125.71(Minimum Price)
- ☐ **Create a Service Profile**: Detailed documentation of service features, pricing, Service Level Agreements, and client requirements.

PHASE 2

Preparing Your Team and Infrastructure

- ☐ **Train Your Technical Team:** Ensure your team has the necessary skills and knowledge to deliver the new service.
- ☐ **Develop Training Materials:** Create internal training for all employees to understand the service and be able to talk about benefits.
- ☐ **Establish Internal Processes:** Define workflows for onboarding clients, monitoring security, and responding to incidents.

PHASE 3

Communicating and Marketing Your New Service

- ☐ **Brand Your New Service:** Choose a compelling name and potentially create a logo.
- ☐ **Develop Marketing Materials:** Create brochures, datasheets, and website content detailing your SaaS security service.
- ☐ **Update Your Website:** Clearly feature your new service on your website.
- ☐ **Create Targeted Content:** Develop blog posts, articles, and social media updates focused on SaaS security.
- ☐ **Plan Your Client Communication Strategy:** Determine how you will introduce the new service to existing clients.
- ☐ **Prepare Client Presentations:** Develop compelling presentations highlighting the benefits of your SaaS security service.
- ☐ **Host Webinars or Workshops:** Educate clients and prospects on SaaS security risks and your solutions.
- ☐ **Update Sales Training Materials:** Equip your sales team to effectively sell the new service.

PHASE 4

Launching and Ongoing Management

- ☐ **Announce Your New Service:** Officially launch **Managed SaaS Security** to your clients and prospects.
- ☐ **Onboard Initial Clients:** Implement the service for your first customers.
- ☐ **Gather Client Feedback:** Solicit input from early adopters to refine your service.
- ☐ **Monitor Service Delivery:** Ensure your team is delivering the service effectively and according to SLAs.
- ☐ **Track Key Metrics:** Monitor adoption rates, client satisfaction, and profitability.
- ☐ **Continuously Update Your Knowledge:** Stay informed about the latest SaaS security threats and best practices.
- ☐ **Iterate and Improve Your Service:** Based on feedback and evolving threats, refine and expand your **Managed SaaS Security** offering.

ConnectWise Resources

Turn insights into action—explore these resources to boost your Managed SaaS Security game.

Buyers Guides

- MDR Buyers Guide
- SIEM Buyers Guide

Feature Sheets

- SaaS Security
- Cloud Backup

Industry Reports

- MSP Threat Report
- State of SMB Cybersecurity

Featured Webinars

- 2024–2025 Insights and Predictions
- Unlocking Cybersecurity Conversations
- Mastering SMB Cybersecurity Needs and ROI

Get started with ConnectWise to get a head start on **Managed SaaS Security** services

Contact Sales

CONNECTWISE