HOW TO TRANSFORM FROM MSP TO MSSP IN 30 DAYS

A PRACTICAL, NO-NONSENSE GUIDE IN HOW TO SPECIALISE IN CYBERSECURITY AND SECURE YOUR FIRM'S FUTURE WITH READY-TO-RESELL SOLUTIONS

AUTHOR

FIONA HODGES | FIFTEEN XV

INTRODUCTION

A NOTE FROM THE AUTHOR

The Australian cybersecurity landscape has changed dramatically in recent years. With the rising sophistication of cyberattacks, businesses of all sizes — particularly small and medium enterprises (SMEs) — are recognising the need for robust cybersecurity solutions.

The good news? For you, this shift presents an unparalleled opportunity: evolving into a Managed Security Service Provider (MSSP).

The great news? The transition is far easier than you'd expect. In this guide, I'm sharing a step-by-step playbook on how to do it in just 30 days.

With decades of experience in the MSP industry and a deep focus on cybersecurity, I've seen firsthand how the landscape has evolved. The demand for advanced security solutions continues to grow, and MSPs are in a strong position to address these challenges. However, becoming an MSSP isn't just about adopting new cybersecurity tools—it requires a thoughtful, strategic approach to service delivery, risk management, and operational readiness.

This playbook is your guide to navigating this transition. It's designed for MSPs, TSPs and all kinds of IT resellers who are ready to specialise in cybersecurity and provide enterprise-grade solutions to their clients — but without the burden of obtaining additional certifications, hiring expensive specialists, or overhauling their existing business model.

At Fifteen, we're the "anti-distributor" – refusing to follow suit of distributors who just take an easy clip on products & leave the rest to you. Instead, we've built a suite of differentiated cyber solutions, which are all 100% ready-to-resell cybersecurity services, enabling MSPs to deliver world-class protection without complexity. This guide will help you understand the market opportunity, plan your service offerings, and successfully position your business as a trusted MSSP.

Whether you're just exploring the idea of expanding your cybersecurity services or are ready to launch more security services, this
playbook provides actionable insights and practical advice to help you succeed. Let's dive in and unlock the potential of becoming an MSSP—together.

> "While everyone else is out there just selling Microsoft's standard security offerings, you're going to stand out from the crowd with a differentiated set of cyber solutions."

Please reach out to me personally at fhodges@fifteenxv.com.au if you have any questions or wish to chat.

Kind regards,

Fiona Hodges
General Manager - Fifteen

Table of CONTENTS

LET'S GET CLEAR:
WHAT IS AN MSSP?

As the cybersecurity threat landscape evolves, Managed Security Service Providers (MSSPs) are increasingly recognised as essential partners for businesses looking to protect their digital assets.

While traditional Managed Service Providers (MSPs) focus on general IT management — such as system maintenance, networking, and end-user support — **MSSPs specialise in delivering advanced cybersecurity services tailored to safeguard clients against modern threats.**

MSSP VS. MSP: WHAT'S THE DIFFERENCE?

At its core, the difference between an MSP and an MSSP lies in their focus:

- **MSPs** provide comprehensive IT support, managing day-to-day technology needs like infrastructure, applications, and end-user services, with security as a consideration.
- **MSSPs** go a step further, delivering advanced cybersecurity. They deliver solutions such as continuous monitoring, threat detection, incident response, and proactive defence strategies to prevent attacks.

With cyber risks on the rise, more businesses are looking for partners who can secure their systems alongside managing them — a gap MSSPs are perfectly positioned to fill.

MSSP SERVICE OFFERINGS

An MSSP provides next-gen cybersecurity services such as:

- **Continuous Threat Exposure Management:** Proactively identify vulnerabilities and misconfigurations before they can be exploited, helping businesses stay ahead of cyber threats.
- **Secure Access Service Edge:** Ensure secure and seamless access to data and applications with cloud-native solutions that integrate security and networking.
- **Secure Networking:** Enable optimised, secure, and scalable network performance for businesses, regardless of size or geographic spread.
- **Complete Email Security:** Protect against phishing, ransomware, and other email-borne threats with robust, multi-layered defence mechanisms.

These services are in stark contrast to the more reactive IT maintenance typically offered by MSPs.

3 REASONS TRANSITIONING TO AN MSSP MAKES SENSE

A trio of colliding forces mean that the time is now to transition to an MSSP. According to Gartner (2024):

1) INCREASED SPEND

Cybersecurity spending is set to increase globally by 15% in 2025, from $183.9 billion to $212 billion. Within this, the segment expecting the most spending growth is security services, followed by security software, and then network security as the third area of growth.

2) IN-HOUSE SKILL SHORTAGE

Secondly, due to the talent crunch, cybersecurity experts aren't so available in house to businesses, meaning they can't manage it themselves and are instead searching for reliable, expert providers who can ensure their defences are as robust as possible.

3) GENERATIVE AI

The rapid rise of Artificial Intelligence usage in every day business practices opens new risk, meaning all businesses will need to take additional steps to secure their environment, from data security to infrastructure protection to governance – further fuelling this growth in years ahead.

TRANSITIONING TO AN MSSP ALLOWS MSPS TO:

- Deliver higher-value services, commanding better margins.
- Meet the increasing demand for specialised security solutions.
- Establish themselves as trusted advisors in an area of critical need.

By positioning your business as an MSSP, you're not just staying relevant — you're leading in a domain that continues to grow year after year.

ADVANTAGES OF MSSPS FOR CLIENTS

From a client's perspective, MSSPs offer distinct advantages over a standard IT outfit:

- **Peace of Mind:** Continuous monitoring ensures threats are identified and mitigated quickly.
- **Expertise Without Complexity:** Clients receive enterprise-grade security solutions without needing in-house specialists.
- **Proactive Protection:** Vulnerabilities are addressed before they become liabilities, reducing downtime and losses.

For MSPs ready to transition, the path to becoming an MSSP is not as daunting as it might appear. In the following sections, we'll explore how you can transform your services and unlock new revenue opportunities.

THE MARKET OPPORTUNITY FOR MSSPS IN AUSTRALIA

ESCALATING CYBER THREATS

Recent reports indicate a substantial increase in cyber incidents across Australia:

- **Data Breaches Rising:** In just one quarter of 2024, approximately 1.8 million Australian user accounts were compromised, marking a 388% increase over the previous quarter.
  Herbert Smith Freehills
- Serious Impact of Ransomware Attacks: In 2024, 73% of ransomware incidents in the healthcare sector led to operational disruptions, including delays in critical treatments and interruptions in hospital services.
  Eftsure
- Business Email Compromise (BEC) and Fraud: These remain among the top self-reported cybercrimes for businesses in Australia.
  Australian Cyber Security Centre

This surge in cyber threats underscores the urgent need for businesses to adopt comprehensive security solutions, thereby creating a fertile ground for MSSPs to offer their expertise.

EXPANDING CYBERSECURITY MARKET

The financial commitment to cybersecurity in Australia is on a significant upward trajectory:

- Market Growth: The Australian cybersecurity market was projected at AUD 9.3 billion (USD 5.8 billion) in 2024, with an annual growth rate exceeding 8%.
  Trade.gov
- Future Projections: The market is expected to grow at a compound annual growth rate (CAGR) of 13% from 2024 to 2030.
  Grand View Research

This expanding market reflects the increasing prioritisation of cybersecurity by Australia businesses, presenting a lucrative opportunity for MSSPs to offer specialised services

REGULATORY LANDSCAPE

The Australian government is intensifying its focus on cybersecurity, introducing new regulations and guidelines:

- **Ransomware Playbook:** In response to significant data breaches, the government has launched a "Ransomware Emergency Response Guide" to guide businesses in managing ransomware attacks, including steps for handling ransom demands and data recovery.
- **Mandatory Reporting:** New legislation requires companies to report ransom payments, with non-compliance attracting fines up to $15,000.

These regulatory measures compel businesses to adopt more stringent cybersecurity practices, increasing the demand for MSSPs who can navigate and implement compliance solutions effectively.

PLANNING YOUR MSSP SERVICE PORTFOLIO

Now that you understand market forces and the size of the opportunity to be had for MSSPs to flourish in Australia, its time to decide what cybersecurity services you'll actually offer.

A strong foundation for any MSSP is built on the right mix of services and solutions tailored to meet market demands. Transitioning MSPs should focus on offering high-impact cybersecurity services that address client needs while maintaining operational independence.

Over the following pages, we break down four key cybersecurity solutions every aspiring MSSP should consider and why diversification of offerings — particularly avoiding over-reliance on a single vendor like Microsoft — can be advantageous.

SECURE ACCESS SERVICE EDGE (SASE)

Now that remote, or at least hybrid, work has become the norm, traditional network boundaries are dissolving. Secure Access Service Edge (SASE) combines wide-area networking (WAN) capabilities with robust cloud-delivered security services to create a unified, scalable solution that addresses modern connectivity and security challenges.

By integrating more than eight layers of protection into one easy-to-manage platform, SASE simplifies cybersecurity. It protects web, cloud, and private applications from anywhere, keeping your clients' businesses secure no matter where employees are or how they access systems.

WHAT IS SASE?

SASE is a framework that unifies networking and security into a single cloud-delivered service, addressing the limitations of traditional network architectures. As organisations increasingly move to distributed workforces, SASE provides a flexible, scalable solution that meets the needs of modern business operations.

Key components of SASE include:

EXTERNAL PROTECTION:

·Cloud Security Posture Management: Ensures compliance and governance for cloud environments.

- **Firewall as a Service:** Delivers centralised, cloud-based firewall capabilities.
- **Secure Web Gateway:** Protects users from web-based threats.
- **Remote Browser Isolation:** Prevents malicious code from affecting endpoints by isolating browsing activity.

INTERNAL PROTECTION:

- **Advanced Threat Protection:** Detects and mitigates advanced cyber threats.
- **Cloud Access Security:** Provides secure access to cloud services and applications.
- **Data Loss Prevention:** Ensures sensitive data is protected from leaks.
- **Zero Trust Network Access:** Implements "never trust, always verify" principles for secure user access.

HOW DOES SASE DIFFER FROM TRADITIONAL NETWORK SECURITY?

SASE moves away from hardware-centric, perimeter-focused security models, offering a dynamic, cloud-native approach that is well-suited for distributed environments. Unlike traditional solutions, SASE consolidates networking and security into a single framework, reducing complexity and improving efficiency.

BENEFITS OF SASE:

- **Scalability:** Adapt to changing business needs and user locations with ease.
- **Cost Efficiency:** Consolidates multiple tools into one platform, reducing operational overhead.
- **Centralised Management:** Unified control over security policies across all users and devices.

WHY SASE IS VITAL FOR MSSPS TO OFFER

For Managed Security Service Providers (MSSPs), SASE offers a transformative approach to delivering secure connectivity to clients:

- **All-in-One Solution:** Combines networking and security in a single framework, simplifying service delivery and reducing operational complexity.
- Flexible Deployment: Tailored to client-specific needs, whether for hybrid workforces, branch offices, or global operations.
- **Increased Revenue Opportunities:** By offering SASE as a managed service, MSSPs can tap into the growing demand for scalable, secure networking solutions, generating recurring revenue streams.
- **Enhanced Client Trust:** With integrated protection and connectivity, SASE ensures clients have a seamless, secure digital experience, reinforcing the MSSP's role as a trusted partner.

By adopting SASE, MSSPs can offer differentiated solutions that cater to evolving client needs while reducing reliance on fragmented, multi-vendor approaches.

CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)

Finding out about a vulnerability days, weeks or even months after it emerged is no longer good enough, or responsible practice. That's why organisations are shifting to adopt not just reactive security strategies but proactive, continuous defence mechanisms.

Continuous Threat Exposure Management (CTEM) is an advanced approach that empowers organisations to assess and fortify their security posture dynamically by identifying vulnerabilities, simulating real-world threats, and optimising defences in near real-time.

WHAT IS CTEM?

CTEM is a comprehensive, proactive security framework designed to address the limitations of static and periodic testing. Unlike traditional penetration testing, which typically involves scheduled assessments to identify specific vulnerabilities at a single point in time, CTEM takes a continuous approach. It creates an ongoing cycle of assessment, analysis, and improvement that ensures your client defences remain relevant and robust in the face of constantly evolving cyber threats.

KEY COMPONENTS OF CTEM INCLUDE:

- **Regular Vulnerability Scans:** These scans provide routine assessments of endpoints, networks, and systems to uncover potential security weaknesses before attackers can exploit them.
- **Simulated Attack Scenarios:** CTEM simulates real-world threats such as phishing, ransomware, or lateral movement within a network to understand how existing defences hold up and where improvements are required.
- **Actionable Reporting:** Detailed reports include insights into vulnerabilities, attack paths, and mitigation strategies, offering clear and practical recommendations for improving cybersecurity measures.

How Does CTEM Differ from Traditional Penetration Testing?

1. FREQUENCY AND SCOPE:

- Traditional penetration testing is typically performed periodically (quarterly or annually) and focuses on a limited set of attack scenarios within a specific timeframe.
- CTEM, by contrast, runs continuously or at regular intervals, offering ongoing monitoring of vulnerabilities and defences.

2. PROACTIVE SIMULATION VS. REACTIVE DISCOVERY:

- Penetration testing aims to uncover vulnerabilities by simulating attacks in a controlled manner.
- CTEM goes a step further by integrating regular vulnerability scans with proactive threat simulations and remediation recommendations, allowing organizations to anticipate and mitigate risks rather than simply react to discovered vulnerabilities.

3. ADAPTABILITY TO CHANGING THREATS:

- As new vulnerabilities and attack techniques emerge, traditional penetration tests may miss novel threats between testing cycles.
- CTEM's continuous nature ensures it stays up to date, identifying both known and emerging risks.

WHY CTEM IS VITAL FOR MSSPS

For Managed Security Service Providers (MSSPs), offering CTEM isn't just about providing advanced security — it's about becoming a strategic partner to clients.

- Enhanced Client Trust: Delivering continuous, transparent assessments positions MSSPs as trusted advisors, prioritizing client security over one-time fixes.
- Customizable Solutions: CTEM solutions can integrate tools from diverse vendors, enabling MSSPs to tailor security strategies to the unique requirements of each client. This flexibility avoids over-reliance on a single vendor ecosystem, fostering innovation and resilience. Operational Efficiency: Automated assessments and simulations help
- streamline operations, allowing MSSPs to manage multiple client environments efficiently while delivering high-value services. Revenue Growth: CTEM represents an ongoing service offering rather than a one-time engagement, creating opportunities for
- recurring revenue.

By adopting CTEM, MSSPs empower their clients to face cybersecurity challenges with confidence, ensuring that defences evolve at the pace of threats and building strong, long-term partnerships in the process.

SECURE NETWORKING SOLUTIONS

As organisations adapt to remote workforces and cloud-centric operations, traditional networking models are becoming less effective in safeguarding data and ensuring seamless connectivity. Secure networking solutions like SD-WAN and Zero Trust Security address these challenges by combining robust security with optimised network performance. These technologies provide organisations with the tools needed to secure their digital environments while enabling flexible and efficient operations.

SOFTWARE-DEFINED WIDE AREA NETWORK (SD-WAN)

SD-WAN is a modern networking solution designed to enhance connectivity across distributed environments, whether for branch offices, remote teams, or hybrid setups. Unlike traditional WANs that rely heavily on fixed, costly MPLS circuits, SD-WAN intelligently routes traffic using multiple connection types to maximise efficiency and reduce costs.

KEY BENEFITS OF SD-WAN INCLUDE:

- Enhanced Performance: Dynamic path selection ensures that critical applications receive the bandwidth and prioritisation they need, minimising latency and downtime.
- Centralised Control: Administrators gain unified visibility and management across the entire network, simplifying operations while improving scalability.
- Integrated Security: SD-WAN incorporates advanced security features such as encryption, firewalls, and traffic segmentation to prevent unauthorised access and protect sensitive data.

By adopting SD-WAN, organisations can deliver secure, high-performance connectivity tailored to the demands of modern digital workflows.

ZERO TRUST SECURITY

Zero Trust Network Access (ZTNA) and Zero Trust Application Access (ZTAA) are integral to a Zero Trust Security framework, which assumes that no user, device, or application should be trusted by default. These solutions ensure that access is tightly controlled, continuously verified, and context-aware, regardless of the location of the user or the device.

Key principles and features of Zero Trust Security include:

- **Context-Aware Access:** Authentication decisions consider factors like user identity, device posture, and location to ensure only authorised users gain access.
- **Least Privilege Principle:** Users and devices are granted access to only the specific resources they need, reducing the potential attack surface.
- **Continuous Monitoring:** ZTNA/ZTAA solutions monitor access requests and user activity in real-time to detect and respond to anomalous behaviours swiftly.
- Application Segmentation: ZTAA enhances protection by granting access at the application level rather than the network level, ensuring stronger isolation and mitigating the risk of lateral movement.

WHY SECURE NETWORKING IS ESSENTIAL FOR MSSPS

For Managed Security Service Providers (MSSPs), incorporating SD-WAN and Zero Trust solutions into their service portfolios delivers significant value to clients:

- **Stronger Cyber Resilience:** These solutions provide comprehensive protection against emerging threats, including ransomware, phishing, and unauthorised access.
- **Optimised Network Performance:** MSSPs can deliver seamless and high-performing connectivity, critical for organisations with diverse and distributed workforces.
- **Customisable Solutions:** SD-WAN and Zero Trust frameworks integrate seamlessly with other services, allowing MSSPs to tailor offerings to fit specific business needs.
- **End-to-End Visibility:** Centralised management enables MSSPs to monitor network traffic, analyse threats, and maintain control over diverse environments with greater efficiency.

By leveraging secure networking solutions, MSSPs position themselves as indispensable partners, delivering both cybersecurity and connectivity to drive organisational agility and trust in today's complex threat landscape.

SECURE WORKSPACE COLLABORATION

Business Email Compromise (BEC) represents one of the most devastating attack vectors, resulting in major financial losses and operational disruptions for businesses of all sizes.

Cybercriminals exploit the trust placed in email communications, often impersonating executives, suppliers, or trusted partners to deceive employees and gain access to funds or sensitive information.

Advanced email security solutions are critical in defending against these sophisticated attacks, offering enhanced visibility, automation, and preventative measures.

KEY ELEMENTS OF A BEC DEFENCE STRATEGY

Effective BEC defence solutions combine advanced technologies and best practices to protect business communications:

- **Real-Time Scanning:** Continuous monitoring of email traffic identifies and blocks phishing attempts, malware-laden messages, and spam, reducing the likelihood of human error.
- **AI-Driven BEC Detection:** Artificial intelligence algorithms analyse behavioural patterns, email metadata, and language cues to flag potential fraud attempts, including domain impersonation or unusual requests.
- **Encryption:** End-to-end encryption safeguards sensitive communications, ensuring that critical data remains protected in transit and at rest.
- **Role-Based Access Controls:** Granular permission settings ensure that only authorised personnel have access to critical systems or high-risk email transactions.

ADDRESSING GAPS IN EMAIL SECURITY

While vendors like Microsoft certainly offer some protection through tools such as Exchange Online and Defender for 365, organisations relying solely on these solutions may encounter limitations, particularly in environments requiring advanced threat analytics or industry-specific compliance measures.

Independent email security solutions often deliver:

- **Customisable Integrations:** Enhanced flexibility to fit unique business workflows and systems.
- **Contextual Insights:** Deeper forensic capabilities to investigate suspicious activities and thwart potential BEC attacks before they escalate.
- **Proactive Safeguards:** Features like automated workflows, data retention policies, and auditing enable tighter control over sensitive information.

WHY EMAIL SECURITY IS VITAL FOR MSSPS

For Managed Security Service Providers (MSSPs), offering robust email security solutions represents a fundamental component of comprehensive cybersecurity services:

- **Client Trust and Assurance:** Protecting email communications solidifies the MSSP's role as a reliable partner in safeguarding critical business processes.
- **Revenue Generation:** Email security solutions provide an avenue for recurring service models, including ongoing threat monitoring and rapid incident response.
- **Adaptable to Compliance Needs:** Industry-specific customisation can allow organisations to meet stringent regulatory requirements, such as ISO 27001.
- **Defence Against Financial Fraud:** Effective BEC solutions mitigate the risk of financial losses from fraudulent transactions, protecting both the client's reputation and bottom line.

By providing comprehensive BEC defence strategies, you will empower your clients to maintain secure and trusted communication channels, transforming email security from a potential weakness into a powerful asset.

THE CASE FOR SOME INDEPENDENCE FROM MICROSOFT

While Microsoft's cybersecurity tools are robust and widely used, many MSPs and MSSPs rely heavily on Microsoft's built-in security, potentially limiting their flexibility to deliver differentiated solutions.

By adopting independent solutions, service providers can offer additional layers of security and advanced customisation that go beyond what Microsoft alone can provide.

1. **Competitive Differentiation:** Many of your MSP and MSSP competitors largely rely only on in-built Microsoft security tools. By offering independent, vendor-agnostic solutions, it allows MSSPs like you to stand out by delivering advanced, tailored security services that exceed the standard protections offered by Microsoft's ecosystem.
2. **Licensing Flexibility:** Vendor lock-in can limit how you scale your business or adjust services.
3. **Resilience:** A disruption in one vendor's cloud infrastructure—such as outages in Azure or Exchange Online—can impact your entire client base.
4. **Tailored Solutions:** Independent solutions enable MSSPs to address niche requirements or unique threats that Microsoft's standard offerings may not cover effectively.
5. **Client Trust:** Some clients prefer to diversify their reliance on vendors, especially when dealing with sensitive data, reducing their exposure to broader vendor-related vulnerabilities.

By incorporating diversified solutions, MSSPs can deliver a stronger, more resilient service portfolio, ensuring that they aren't placing all their eggs in one basket. Building a vendor-agnostic offering strengthens your ability to meet complex client demands and positions you as an agile, independent partner.

MAKING THE MOVE
HOW TO GET STARTED!

If you read all of that and are now thinking, “Okay, sounds great — but HOW? Where do I start?!” you wouldn’t be alone. But its far easier than it seems, with the right partner.

For many MSPs, the leap to becoming an MSSP feels daunting. The allure of adding specialised cybersecurity services is often tempered by perceived barriers: the need for specialised certifications, a lack of in-house expertise, and uncertainty about how to approach sales and marketing for a new offering. These challenges can leave you feeling that the transition is simply out of reach.

But the truth is, it doesn’t have to be complicated. The Fifteen model has specifically been designed to remove roadblocks for MSPs who quickly and easily reap the rewards of cybersecurity as a service.

HERE’S HOW IT WORKS:

- **No Need for ANY Certifications**

Cybersecurity certifications can be expensive, time-intensive, and challenging to maintain. (We know, because we’ve gone through it and now have one of the most certified team’s in the country).

That’s why we’ve eliminated this obstacle entirely. As a Fifteen partner, you gain access to ready-to-resell cybersecurity solutions that are fully certified and managed by us. The heavy lifting—training, vendor certifications, and compliance—has already been done on your behalf.

This means you can start selling cybersecurity services immediately without the need for in-house technical experts or costly upskilling. It’s a simpler, more scalable model, empowering you to deliver enterprise-grade protection with confidence.

- **Marketing-in-a-Box**

Launching your MSSP offering shouldn’t require reinventing the wheel. That’s why we’ve created Marketing-in-a-Box, a comprehensive package of ready-made resources designed to help you take your new services to market quickly and effectively.

THE PACKAGE INCLUDES WHITE LABELLED:

- **Email Campaigns:** Professionally written email sequences to engage prospects and announce your expanded capabilities.
- **Social Media Content:** Posts, graphics, and messaging tailorable to your MSSP brand.
- **Client Presentations:** High-impact slide decks to showcase your new cybersecurity solutions.
- **Assets:** Including whitepapers, fact sheets and even redacted report samples that you can brand and share as your own.

Everything is provided, so you can hit the ground running without having to hire additional marketing resources or spend weeks developing your materials.

- **Sales Enablement and Deal Support**

Marketing is one thing, but once you get in front of a customer, you want to feel comfortable talking about the solution.

Selling cybersecurity can feel like uncharted territory for many — but not when you have Fifteen XV by your side. We're not just a vendor; we're a true partner who actively supports you throughout the sales process.

Here's how we work with you:

- **Presales Engineering:** Our technical specialists are available to assist with everything from product demonstrations to crafting tailored solutions for your clients.
- **Co-Selling and Support:** Our experienced sales and account executives are here to attend meetings, answer tough client questions, and help you close deals. We'll act as an extension of your team, providing confidence and expertise when you need it most.
- **Pricing Strategies:** Unsure how to position or price your MSSP offering? We'll guide you in creating competitive, attractive pricing models that ensure strong margins and client uptake.

With Fifteen XV, you'll never walk into a sales conversation alone. Our team's priority is your success, and we're here to support you at every step of the journey.

- **True Partnership, Not Just a Platform**

Unlike traditional vendor relationships, partnering with Fifteen XV goes beyond delivering solutions. We're here to empower you, working hand-in-hand to help you achieve long-term growth as an MSSP.

From eliminating certification challenges to providing a full suite of marketing and sales resources, we make it easy for you to operationalise your cybersecurity practice. With Fifteen XV, you gain access to more than products—you gain a partner who's invested in your success.

YOUR MSSP KICKSTART CHECKLIST

Making the leap to becoming an MSSP is easier than you think when you follow this simple, step-by-step checklist. Each stage is designed to remove the guesswork, giving you the confidence to launch your cybersecurity services with ease.

1. BOOK AN INTRODUCTORY CALL WITH A FIFTEEN GROWTH SPECIALIST

The first step is to schedule a one-hour session with one of our dedicated growth specialists. During this meeting, we'll:

- Explore your current offerings and your readiness for MSSP services.
- Discuss the cybersecurity needs of your clients and potential upsell opportunities.
- Answer any questions or concerns about the transition process.

By the end of this session, you'll have a clear understanding of how Fifteen's partner model works and the path forward for your business.

2. SELECT YOUR SERVICES

With guidance from our team, you'll select the cybersecurity services that best fit your client base and business goals. Our offerings include:

- **XV CTEM (Continuous Threat Exposure Management):** Help clients proactively uncover and address vulnerabilities.
- **XV SASE (Secure Access Service Edge):** Provide secure remote access solutions tailored for hybrid workplaces.
- **XV SD-WAN (Secure Networking):** Simplify and secure connectivity for modern business networks.
- **XV Email Security:** Offer enterprise-grade email protection with threat detection and filtering.

These services are fully managed and ready to resell, meaning no certifications or technical expertise are required from your team.

3. COMPLETE THE PARTNER WELCOME PROCESS

Becoming a Fifteen partner is straightforward and efficient. Our onboarding process includes:

- Meet your dedicated Partner Success Manager
- A partner agreement that aligns with your business needs.
- Accessing training materials, solution documentation, and your exclusive partner portal.
- Setting up your business within our systems, so you're ready to hit the ground running.

4. SALES ENABLEMENT SESSION

Our sales enablement session is designed to set you up for pricing and selling success. Here's what we'll do:

- Work together to define pricing strategies for your new cybersecurity services.
- Ensure your pricing is competitive while maintaining healthy margins.
- Train your sales team on how to confidently pitch and position MSSP services to your clients.

You'll have the tools, insights, and confidence to close your next cybersecurity deal.

5. MARKETING-IN-A-BOX ACCESS

Launch your MSSP offerings with a fully loaded marketing toolkit. Our team will provide white labelled:

- **Customisable Campaigns:** Ready-to-use email templates and social media posts to announce your new services.
- **Brand Assets:** Professionally designed visuals and messaging for promoting your MSSP offerings.
- **Go-to-Market Strategies:** Practical advice on maximising reach, engagement, and lead generation.

We make it easy to start generating demand and booking client conversations right away.

By the time you complete this checklist, your MSSP business will be ready to roll. With Fifteen as your partner, you'll bypass the usual barriers and accelerate your journey to MSSP success.

ABOUT US

At Fifteen, we pride ourselves on being The Anti-Distributor—your service capability extender. Unlike traditional distributors, we deliver enterprise-grade solutions that empower IT providers to scale, innovate, and meet their clients' evolving demands without compromise.

Our approach is centred around partnership. We simplify complex technologies, enabling our partners to deliver seamless and secure IT services without needing additional certifications or personnel. With deep technical expertise and a passion for excellence, we ensure you can focus on what you do best: growing your business.

Why Choose Us On Your Journey to Becoming an MSSP?

- **Agility Meets Expertise:** From cybersecurity to cloud and networking solutions, we provide managed, ready-to-resell services tailored to your needs.
- **No Certification Hurdles:** Our unique model means we take care of all the certifications and vendor management, so you can resell with ease.
- **End-to-End Support:** Our Australian-based team of engineers and technical specialists are here to assist, from advisory and deployment to ongoing support.
- **Marketing-in-a-box:** We support you from the beginning and help you find leads.
- **Your Success, Our Priority:** We collaborate closely with you to create scalable, branded solutions that make you indispensable to your clients.

Join us in reshaping what it means to be a partner in the IT industry. Together, let's innovate, thrive, and lead.