Embracing Delivery of Cybersecurity and Scaling Via Service Providers

How the new machine learning-powered CyberCision platform enables cost-effective service delivery at scale for service providers looking to address the growing demand for managed cybersecurity protection—in particular among SMBs adjusting to the new work-from-home workforce

A Frost & Sullivan White Paper

Powering clients to a future shaped by growth

FROST & SULLIVAN

CONTENTS

Executive Summary

With the increased prevalence of artificial intelligence (AI), machine learning, and sophisticated cyberattacks, businesses are moving towards comprehensive solutions that help them manage, automate, and strengthen their cybersecurity to safeguard the full scope of all physical and digital assets.

Small and mid-sized businesses (SMBs) have been particularly vulnerable to cyberthreats: Data shows that while they have accelerated cloud adoption to compete in today's digital landscape, successful SMBs have also automated their security operations and adopted frictionless solutions to secure their network perimeter.

- Recent Frost & Sullivan research reveals that during the COVID-19 pandemic, more than 84% of SMBs rely on 6 or more Software-as-a-Service (SaaS) applications, and more than 90% use 6 or more private cloud applications.
- Of the SMBs surveyed, 85% state that they have undertaken digital transformation efforts to improve customer and user engagement.
- With a stronger push towards digital transformation and increasing IT complexity, SMBs face higher cyber-risk. Frost & Sullivan's 2021 research reveals that 70% of SMBs suffered from at least one cybersecurity incident during the pandemic, with the biggest threats coming from ransomware, unpatched systems, and web defacements.

As service providers already function as single-stop agents for their customers' cloud, mobile, and IT needs, they are well poised to deliver frontline cybersecurity. This white paper examines the unique opportunities service providers have to provide low-cost, high-value cybersecurity services—in particular to their SMB customers, but in actuality at any scale.

Frost & Sullivan's 2021 research reveals that 70% of SMBs suffered from at least one cybersecurity incident during the pandemic, with the biggest threats coming from ransomware, unpatched systems, and web defacements.

Recapping a Year of Turmoil: SMBs' Unique Challenges

The impact of digital transformation on cybersecurity

The global upheaval of the last 2 years that disrupted societies, governments, businesses, and the technologies that support them, also forced organizations worldwide to shift to remote working practically overnight. Consequently, organizations have adopted new operational infrastructures as data has multiplied exponentially—all opening up a much wider attack surface.

Moreover, cyberattacks have grown smarter, scaling in both sophistication and speed, to penetrate the weak defenses of solutions struggling to protect increasingly digital economies. A recent Frost & Sullivan survey of SMBs[1] generated the following takeaways.

- SMBs are most often targeted by preventable threats. The most common attacks reported by them are ransomware (47%), vulnerabilities from unpatched systems (44%), web defacements (43%), insider threats from employees (31%), and phishing attacks (27%).
- Remote workforces have grown exponentially: 75% of the C-level respondents report that more than 25% of their workforce works from home. Remote workers tend to use their own devices and personal Wi-Fi connections, and without the protective guardrails that come with enterprise networks, they have become a primary target for cybercriminals.
- Digital transformation is accelerating, with almost half (47%) of the SMBs reporting having kicked off digitalization journeys, another 38% either having made significant progress or having completed their transformation roadmaps. This rapid adoption of new technologies coupled with a dramatic increase in active Internet users has opened the door to smarter cyberattackers that are drawn to the significantly widened attack surface.

With digital environments necessitating a shift from device management to threat management, enterprises of all sizes must shift their security focus from solely distributed endpoints to the entirety of their network edge, core, and cloud.

Digital transformation is accelerating, with almost half (47%) of the SMBs reporting having kicked off digitalization journeys, another 38% either having made significant progress or having completed their transformation roadmaps. This rapid adoption of new technologies coupled with a dramatic increase in active Internet users has opened the door to smarter cyberattackers that are drawn to the significantly widened attack surface.

1 Frost & Sullivan, C-level SME respondents, Oct 2021

Critical drivers and challenges for modern SMBs

A 2021 Frost & Sullivan study[2] reveals that a whopping 63% of SMBs consider themselves cloud-first, with a majority of their workloads living in the cloud. Another 31% report having adopted the cloud for select projects, either in testing or production environments.

The 3 leading drivers of digitalization for SMBs today revolve around cloud, mobility, and Internet of Things (IoT):

- **Powering scalability with the cloud:** Unlike the limitations of on-premises hardware, cloud services can rapidly scale up and down as needed, with the added benefit of flexible, pay-as-you-go cost savings. This allows new products and services to more quickly enter the market. By moving workloads to the cloud, enterprises can rely on experienced cloud services providers to shoulder the logistics, allowing business leaders to focus on their operational priorities.
- **Expanded mobility:** Enterprise infrastructure is undergoing significant transformation due to their increasing adoption of mobile devices and cloud computing. The data generated by rich ecosystems of buying, browsing, communicating, and collaborating on mobile devices requires effective storage. As a result, service providers are increasingly shipping storage into cloud applications, allowing businesses to easily understand and access their digital assets as required.
- **Advanced connectivity with IoT:** IoT devices have simplified and streamlined various enterprise processes, such as automating administrative tasks with virtual assistant devices and enhancing warehouse efficiencies with sensors. Additionally, IoT versions of traditional workplace equipment—for instance, smart thermostats—often provide cost savings over time by reducing energy usage, providing real-time monitoring tools, and offering pay-per-use plans.

A 2021 Frost & Sullivan study reveals that a whopping 63% of SMBs consider themselves cloud-first, with a majority of their workloads living in the cloud. Another 31% report having adopted the cloud for select projects, either in testing or production environments.

2 Frost & Sullivan, C-level SME respondents, Oct 2021

While cloud, mobility, and IoT are key drivers of digitalization among today's SMBs, they have also opened the door to critical security challenges that must be addressed:

- **Expanding attack surfaces:** With the rise of cloud applications and networks, enterprise data now lives in multiple ecosystems, many of which are outside the purview of internally protected networks. As a result, applying a single and comprehensive security strategy over the entire network becomes incredibly challenging. Hackers have all the more opportunities: with unaddressed security gaps opening up on an almost daily basis, security teams continually grapple with sophisticated and multi-staged attacks.
- **Global shortages in cybersecurity talent:** Enterprises and service providers are struggling with the shortage of technical skills among their workforce due a lack of adequate, qualified talent to fill the huge and ever-growing cybersecurity job market. Workers transitioning from related sectors are filling the majority of these positions, as opposed to new graduates entering the workforce. Frost & Sullivan research on SMB trends shows that 1 of every 2 SMBs surveyed report having difficulties acquiring properly skilled security talent.

For today's SMBs, digitalization is directly proportional to competitive relevance: enterprises have to continuously innovate to succeed in digital landscapes. To truly thrive in today's digital reality, SMBs require a robust security approach that can sustain the benefits of cloud, mobility, and IoT while managing the challenges that stem from these advancements.

Service Providers' Vital Role in Supporting the SMB Ecosystem

Unlocking the full opportunity of cybersecurity for service providers

Today, service providers are responsible for managing the gateways to all forms of connectivity for their enterprise customers: from the core, to the cloud, to the edge. With the power to detect cyber vulnerabilities as they form, service providers have the opportunity to act as frontline guards in cyber-defense.

Specifically, service providers can create new revenue channels by providing low-cost, high-value cybersecurity services to their existing enterprise customers. For the enterprise, the value of these services is significant:

- **Reduced costs and increased access:** Security vendors have a history of forging partnerships with service providers to deliver security products bundled with core connectivity services. This means enterprises can purchase lower-cost security solutions along with other core communications services through their existing telecommunications providers. Such initiatives massively simplify service provisioning for enterprises: the SMB needs to handle only a single vendor relationship and a single bill. In addition, service providers can provide security solutions to enterprises at scale, significantly reducing the cost of enterprise-grade threat management services.
- **Expertise, simplicity, and scale:** The operational ecosystem of the average service provider is much larger than that of the average enterprise, in terms of both sheer service geography and product breadth. Service providers deliver around-the-clock voice and data services, create and manage custom offers for consumers and small and large enterprises, and operate entire ecosystems of support centers. SMBs are already working with telecommunications service providers, which makes it easier to leverage the latter's existing wealth of resources for robust cybersecurity horsepower that comes backed with world-class expertise and partnerships with best-in-class security vendors.

These benefits are particularly remarkable for SMBs. Unlike larger organizations with robust IT budgets, smaller businesses tend to approach cybersecurity from a work-with-what-you-have mindset, yet many lack the budget or skills necessary to maintain an effective cybersecurity program.

Examining the value model of a managed security strategy

Frost & Sullivan's 2021 research on cybersecurity trends reveals that 60% of SMBs look to outsource cybersecurity to a third party. In particular, 5 factors are driving businesses towards managed security services:

A global cybersecurity skills gap	An increasingly sophisticated threat landscape	Insufficient in-house security tools that cannot meet the detection and response demands of today's advanced cyberthreats	Stringent regulatory and compliance requirements	An urgent need to shift from CapEx to OpEx business models in order to optimize their use of capital (cash)

Simply put, SMBs are in urgent need of comprehensive cyber protection. By leveraging managed security service providers, enterprises are finding themselves in a better position to balance the pressures of day-to-day business while accelerating the execution of critical security projects to maintain holistic perimeter defenses.

Frost & Sullivan's 2021 research on cybersecurity trends reveals that 60% of SMBs look to outsource cybersecurity to a third party.

To achieve comprehensive cybersecurity, SMBs need a solution that can effectively address 5 critical areas:

- **Email:** Every employee that accesses business email from different devices requires protection against initial-stage malware, ransomware, targeted phishing, and impersonation attacks by cybercriminals.

- **Web:** Any employee that uses the web, regardless of source location (from the office, home, or remotely) requires protection against phishing, malicious web content, and malware infections.
- **Endpoint:** This includes the provision of definitive, baseline protection for every SMB employee across all endpoints used for work—whether PC, Mac, Android, or server—against malware, phishing, ransomware, and unwanted applications along with automated zero-day application and threat hunting services.
- **Firewall:** Enterprise customers require protection from ransomware, credentials theft, data theft, and malware when using broadband and internet-connections.
- **Automated detection and response (ADR):** ADR encompasses automated threat visibility, detection, alerting, and response capabilities powered by continuous real-time monitoring. Essential ADR strengths include dark web monitoring services, continuous threat hunting via retrospective analysis of links and attachments, and in-built advanced protection against targeted phishing and impersonation attacks.

Managed service providers can supply the expertise and resources needed to ease the delivery of these 5 critical needs, freeing business leaders to focus on their core processes instead of worrying about building effective security infrastructure from scratch.

The Cybercision Platform: The Power of Cybersecurity-As-A-Service For SMBs

Security through an SMB lens

With the digital world increasingly interconnected to the physical world, consumers are relying on brands that offer seamless cross-channel journeys that bridge the gaps between web applications, mobile devices, and digital channels. Businesses are facing intensifying pressure to tailor services custom fit to match consumers' unique digital identities, allowing curated experiences, recommendations, and marketing offers. Digital transformation, therefore, is a critical lever enterprises can engage to remain both competitive and innovative.

To address the security challenges resulting from digital transformation, enterprises are increasingly relying on managed security services providers to deliver unified, centralized, and automated solutions that offer enhanced visibility, management, and threat remediation, specifically:

- End-to-end security with single-pane visibility over the entire attack landscape, enabling always-visible security and protection
- Consistent orchestration and management of security functions with real-time communication across the network and security infrastructure
- Automated and intelligent incident response and threat remediation, along with continuous compliance and risk assessment

With the digital world increasingly interconnected to the physical world, consumers are relying on brands that offer seamless cross-channel journeys that bridge the gaps between web applications, mobile devices, and digital channels.

By adding cybersecurity to their existing services, SMBs can bolster existing connectivity assets with the critical protections they need, all through a single provider.

As SMBs typically have limited in-house IT and cybersecurity resources, they report high degrees of outsourcing to security service providers. Frost & Sullivan finds that while only 14% of enterprises report outsourcing more than half of their cybersecurity operations, a much higher percentage (60%) of SMBs outsource. This presents a natural fit for partnerships between SMBs and their service providers. By adding cybersecurity to their existing services, SMBs can bolster existing connectivity assets with the critical protections they need, all through a single provider.

Crafting the ideal managed security blueprint for the busy enterprise

For thinly-stretched enterprise IT teams, security, though a priority, often slips through the cracks, making it difficult to intentionally and continuously establish a security-forward organizational stance.

Enter FirstWave. With almost 20 years of experience in delivering cybersecurity solutions, FirstWave presents CyberCision™, an open security management platform (OSMP) purpose-built for service providers to deliver comprehensive security services to SMB (and enterprise) customers. Leading the charge in the new and essential space of OSMP solutions, the value here is two-fold: service providers can easily deliver low-cost, high-revenue security services to their SMB customers, and SMB customers can, in turn, benefit from an enterprise-grade Cybersecurity-as-a-Service solution.

Unique highlights of CyberCision™ include:

- Complete digital perimeter security and protection for all employees and users
- Low-cost pay-as-you-go subscription
- Fast and frictionless deployment requiring only a single order and permission
- Pre-defined security settings and policies that are optimized for SMBs
- Ease of management and use through always-visible security and protection
- As-as-Service model, allowing SMBs to consume as much or as little as they need

In a nutshell, FirstWave's CyberCision™ OSMP provides a comprehensive range of cost-effective enterprise-grade security services to SMBs that prefer not to manage their own cybersecurity teams or security infrastructure.

The Cybercision™ Platform: The Power of Cybersecurity-As-A-Service For Service Providers

Security through the lens of service providers

For service providers, delivering cybersecurity solutions to enterprise customers, while lucrative, can involve significant cost and complexity. FirstWave's OSMP, CyberCision™, is designed to address this problem. CyberCision™ enables service providers to provision enterprise-grade security services to both enterprise and SMB customers at scale, opening the door to new revenue opportunities with a lower cost-to-serve.

With CyberCision™, service providers can build as-a-service cybersecurity packages of enterprise-grade, including a range of management and operational services such as multi-tenanting, billing, and provisioning that enable them to streamline the sales and delivery process at a minimal cost.

The unique advantages of this solution include:

- Providing service providers an accelerated pathway to launch compelling new security services with minimal upfront investment, plus reduced time-to-revenue and cost-to-serve
- Reinforcing, enhancing, and differentiating service providers' core business-to-business (B2B) and enterprise services portfolios (e.g., broadband, mobile, cloud, and managed services like SD-WAN)
- Arming service providers with the tools necessary to create, deliver, and support a range of new cybersecurity offers, bundles, and marketing campaigns
- Delivering a frictionless customer experience through complete digitalization of the customer journey and service life cycle, from purchase and fulfilment to management and support

Providing service providers an accelerated pathway to launch compelling new security services with minimal upfront investment, plus reduced time-to-revenue and cost-to-serve.

These direct benefits to service providers reap further value additions for their SMB customers. Essentially, CyberCision™ serves as a platform that service providers can depend on to scale their managed security services business and operations profitably, drastically reducing the time to market for cybersecurity and serving SMB customers, which was not previously possible.

Crafting the ideal managed security offering for SMB customers

The CyberCision™ solution empowers service providers to build smart, lightweight security bundles using a one-stop approach that pairs complete life cycle management with a centralized view of security status across 5 key zones: email, web, endpoint, firewall, and ADR. While similar capabilities exist in the market, CyberCision™ brings 6 unique differentiators to the table:

- **Single, integrated platform** for a range of multi-vendor, multi-function security services: The platform is security vendor-agnostic; therefore, the service provider is beholden to neither a single vendor for security functions nor service operations (OSS/BSS).
- **Hybrid:** The OSMP solution is deployable on-premises or delivered from the cloud (centralized or distributed).
- **Integrated management, operational functions:** CyberCision™ supports a range of management and operational functions for all security services from a single platform. Service providers can add new security services to their security product portfolio while retaining the benefits and use of the single platform.
- **Simplified, single process:** One process covers the operation of multi-vendor, multi-function security service delivery and billing.
- **Built for scale:** Volume and scale are particularly critical for the SMB segment; therefore, CyberCision™ prioritizes scale-up functions such as multi-tenanting, APIs, and automation to power economies of scale.
- **Open:** The solution can support existing and new third-party vendors and security functions.

To this end, the CyberCision™ OSMP solution can unlock new cybersecurity services revenue in 5 steps; the service provider simply:

1. Subscribes to the CyberCision™ Platform-as-a-Service;
2. Selects which security bundles it wishes to launch along with pricing and Ts&Cs;
3. Publishes the offer bundles and services to its catalogue and/or digital marketplace;
4. Connects its digital marketplace and operational systems to the platform via standard, published APIs; and
5. Markets the services and accepts new revenue-generating orders through its digital marketplace.

The CyberCision™ platform does the rest, effectively eliminating the barriers—cost, complexity, and technology—that have historically prevented service providers from expanding to the security services domain. Now, for their existing and established SMB customer bases, service providers can supercharge their offerings with democratized, enterprise-grade Cybersecurity-as-a-Service support.

About Firstwave Cybercision™

FirstWave CyberCision™ is the world's first open security management platform (OSMP) for service providers and their SMB customers.

WORLD'S FIRST OPEN SECURITY MANAGEMENT PLATFORM (OSMP)

OPEN
Multiple, integrated third-party security vendors & functions

SECURITY
Specialised platform for provisioning at scale

MANAGEMENT
Full lifecycle management capabilities

PLATFORM
One 'place' to deliver & manage security services

FirstWave

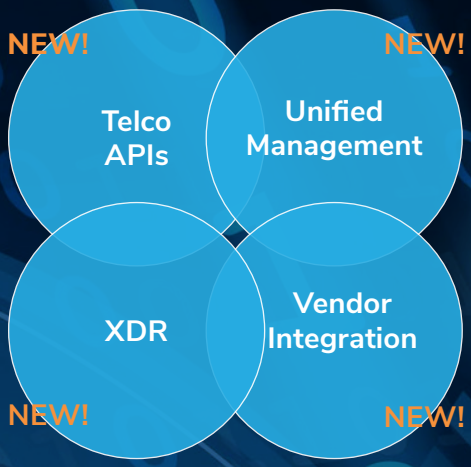
By offering its CyberCision™ OSMP platform to service providers, FirstWave unlocks a game-changing value proposition and accelerated path-to-market for delivering a truly integrated and complete Cybersecurity-as-a-Service solution to businesses of any size, anywhere in the world.

For the service provider as a go-to-market (GTM) partner, the CyberCision™ platform delivers key capabilities with compelling benefits.

CYBERCISION: NEW PLATFORM CAPABILITIES FOR PARTNERS

KEY PARTNER BENEFITS

- New Differentiated Security Bundles
- Improved Channel Selling & Delivery
- Faster Customer Acquisition & Higher ARPU
- Process Simplication & Automation
- Operational Scale & Lower Cost



FirstWave

The CyberCision™ platform incorporates the latest technologies from leading enterprise-grade vendors ready for today's and tomorrow's digital business ecosystem and evolving cybersecurity challenges.

For SMB end users, CyberCision™ enables simple, convenient, and cost-effective ongoing access and use of a truly innovative and comprehensive suite of enterprise-grade cybersecurity services from a single provider with full security visibility, control, and management in the 'palm of the hand'.

NEW PLATFORM FEATURES TO ACCELERATED SP GROWTH

FirstWave has improved on three core platform areas that are a key focus for MSP and Telco partners:

- **Frictionless Email Security** supports speed and scale of adoption. Service providers are now able to easily enable best-in-class email security with our automated provisioning process on Microsoft 365 accounts. This opens new channels to market, removes time consuming manual changes to the process, and empowers service providers to onboard customers rapidly and at scale.
- **The CyberCision Mobile App** increases visibility of the cybersecurity service by providing end users with real-time monitoring of cybersecurity threats along with historical reporting, all available in the palm of their hand under a white-labelled app from their service provider. The visibility provided through the CyberCision Mobile App can help to accelerate adoption of the services, as well as demonstrating ongoing value for long-term customer satisfaction.
- **Advanced Detection & Response Premium** enhances control and introduces an additional level of protection, extending the email protection capabilities with the inclusion of advanced dark web monitoring, post-delivery email analysis, retrospective risk scoring, and automated remediation.

View demo videos of new features

FirstWave

About FirstWave

FirstWave is a publicly-listed, global technology company formed in 2004 in Sydney, Australia.

FirstWave's globally unique CyberCision platform provides best-in-class cybersecurity technologies, enabling FirstWave's Partners, including some of the world's largest telcos and managed service providers (MSPs), to protect their customers from cyber-attacks, while rapidly growing cybersecurity services revenues at scale.

In January 2022, FirstWave acquired Opmantek Limited (Opmantek), a leading provider of enterprise-grade network management, automation and IT audit software, with 150,000 organisations using their software across 178 countries and enterprise clients including Microsoft, Telmex, Claro, NextLink and NASA.

Integrating CyberCision with Opmantek's flagship Network Management Information System (NMIS) and Open-AudIT product enables FirstWave to provide a comprehensive end-to-end solution for network discovery, management and cybersecurity for its Partners globally.

With over 150,000 organisations now using FirstWave technology, we are well positioned to be a leader of transformational change in the IT Operations and Cybersecurity world.

Our passion is to create intelligent software that our service provider partners and customers love.

www.firstwavecloud.com

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion