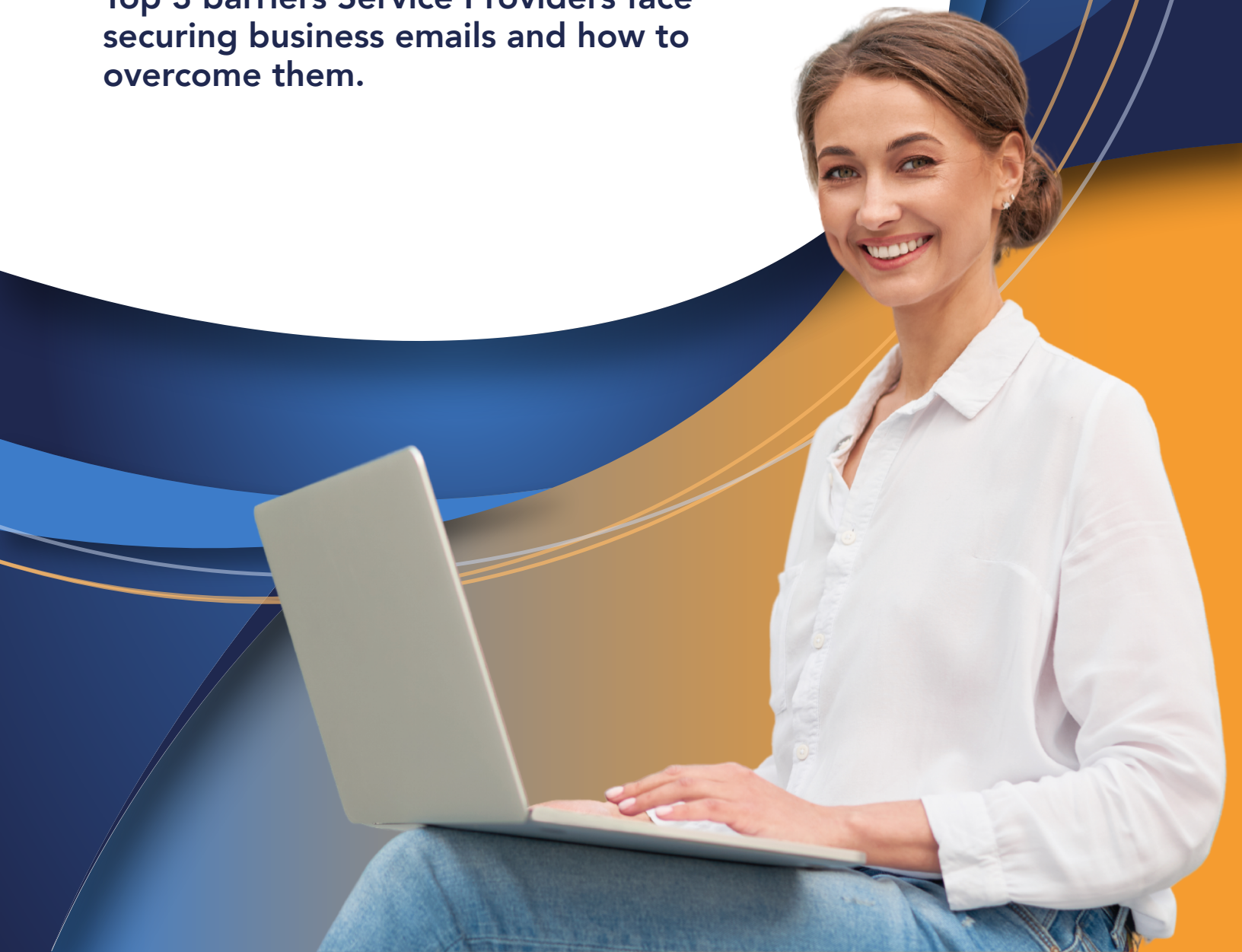
FirstWave

Email Security Protection For Service Providers

Top 3 barriers Service Providers face securing business emails and how to overcome them.



EMAIL SECURITY PROTECTION FOR SERVICE PROVIDERS

While the cybersecurity landscape continues to evolve, one aspect has been consistent in recent times – email remains the primary attack vector for most businesses. Whether through indiscriminate phishing or targeted business email compromise (BEC) attempts, the incidents of threats are increasing and the need for improved email security has never been more important (Source – Cyber Security Ventures).

While general awareness of the importance of cyber security practices has increased, adoption of adequate email security protection is still underwhelming amongst businesses, particularly SMBs (Source – Verizon). Unlike Enterprise businesses, where only 14% report outsourcing the majority of cyber security needs, more than 60% of SMBs rely on a Service Provider to help protect their business (Frost & Sullivan, 2022).

It's important, then, for Service Providers to overcome the barriers to onboarding their customers to world-class email security products and keeping their inboxes safe.

In this ebook we explore 3 of the top barriers Service Providers face when looking to implement email security for their customers, along with a bonus category focused on providing ongoing value for customers.

READY TO LEARN MORE? CLICK TO REQUEST A DEMO FROM A FIRSTWAVE ENGINEER.

1 Market Education

LACK OF UNDERSTANDING OF THE THREAT LANDSCAPE

The adoption of any cyber security service starts with an understanding of the benefits of action, and risk of inaction. Research from Frost & Sullivan estimates that 70% of SMBs suffered at least one cyber security incident during the COVID-19 pandemic (2021).

If a previous incident wasn't enough to show business managers that additional cyber security efforts are essential, new research indicates that SMBs are being increasingly targeted – often by preventable threats like ransomware (47%) and phishing attacks (27%) (Frost & Sullivan, 2022).

As a Service Provider and trusted advisor to your customers, don't wait for them to be spurred into action on the back of a security breach – make sure your team is providing education about the threat landscape regularly to your customers, so they understand the value of adding protection to their IT environment. Some key approaches and topics to discuss may include:

Statistics aren't everything, but they help:

Endless pages of statistics from researchers and analysts aren't going to make the conversation for your customer, but they may help to add more weight and credibility to some key points. This will depend on what's important to your customer, but here are a few stats we can't go passed:

70%

of SMBs reported suffering from a cybersecurity incident during the COVID-19 pandemic (Frost & Sullivan, 2021)

OVER 90%

of cyber security incidents start with phishing emails (Delloitte 2020, Gartner 2021, and many others)

$180 USD

Average cost of cyber security breach in 2021 raised to USD $180 per record (personally identifiable information), with lost business forming the largest cost from a breach. This represented an average cost per breach of USD $4.24m (IMB 2022)

Swiss-cheese model for cyber security:

Just like in the airline industry where the term is often used to describe safety measures, the Swiss-cheese model for cyber security addresses the importance of multiple systems working together to provide extensive and overlapping protection. Threat actors are always finding new and creative ways to try to reach victims, so having layers of redundancy in place is a key attribute to a healthy cyber security posture – that way if they do happen to find a hole in one layer, there is coverage for that spot by the next.

2 Product Education

FAITH IN THE IN-BUILT SECURITY OFFERED THROUGH MICROSOFT DEFENDER

The Swiss-cheese model for cyber security can also be a powerful way to overcome objections that may be raised relating to the inbuilt security elements from Microsoft Defender.

While the in-built email protection capabilities for Office 365 customers are valuable, particularly on the higher-tier E5 license, these don't compare to a fully-fledge email security offering, and aren't in place for most users who simply rely on the basic-tier licenses.

In tests of the efficacy of Microsoft Defender plus CyberCision™ email security, 12% of attack emails were missed by Defender – otherwise making it to the users inbox if it hadn't been for the implementation of CyberCision™ as their true layer of defense, blocking the "Swiss-cheese" holes from the in-built solution.

The most popular and highest risk attack vectors by email include Phishing and Business Email Compromise – areas poorly addressed by Microsoft Defender and the security included with Office 365 licenses. Other risk factors, like Unknown Malware and handling of Embedded URL's, are not supported at all with the standard tiers of license, and are only partially addressed when upgrading to E5 licenses.

Through addressing these crucial areas by default and with greater focus, CyberCision™ email security adds an unrivaled layer to defense. A more detailed comparison of capabilities is available below, or by speaking with our sales team who can help you build your email security go-to-market strategy.

	Office 365- E1 & E3	Office 365- E5	CyberCision Email Security Essentials	CyberCision Email Security Premium
Unwanted Email	Good	Good	Advanced	Advanced
Phishing	Basic	Good	Advanced	Advanced
Business Email Compromise	Basic	Good	Advanced	Advanced
Known Malware	Advanced	Advanced	Advanced	Advanced
Unknown Malware		Good	Advanced	Advanced
Embedded URL's		Good	Advanced	Advanced
Policy Capabilities	Basic	Basic	Advanced	Advanced
Management and Reporting	Basic	Basic	Advanced	Advanced
Mobile App			Real-Time Visibility	Real-Time Visibility
Dark Web Monitoring			Good	Advanced
Post-delivery Email Analysis				Advanced
Retrospective Risk Scoring				Advanced
Automated Remediation				Advanced

3 Product Capability

BARRIERS TO IMPLEMENTATION AND ONBOARDING

At the core of onboarding friction for email security has been the manual work involved in implementation, with cost being the main attribute influenced. For Service Providers implementing an email security solution for a customer often looks like this:

Set Up

Setup of the new solution in preparation of the change - incurring costs for unused license.

Train Staff

Leveraging an appropriately trained staff member to plan and facilitate the change - requiring expertise.

Changeover

Scheduling the changeover, typically out of hours to cause minimum disruption to the client should human-error result in any issues – incurring penalty rates for staff.

Manual Updates

Manually updating DNS settings, mail routing rules, and spam filters – taking time and opening up the possibility for mistakes to impact the client and requiring more time to diagnose and resolve.

The cost involved for the Service Provider either gets pushed onto the customer or absorbed – creating a barrier to sale, or a disincentive to sell as it eats away at the bottom line. With a focus on supporting Service Providers to deploy cyber security solutions to their customers, the CyberCision™ platform addresses these barriers – removing onboarding friction, automating activation, and reducing the cost of implementation and maintenance.

As a centralized platform to manage all customer environments, CyberCision™ overcomes traditional barriers by:

- Automated activation
  - Bypassing long and manual process,
  - Removing burden of expertise from implementation staff,
  - Eliminating human error
- Deploys in minutes, removing after-hours implementation schedules, saving time and money
- Includes APIs to onboard easily at any scale

4 Seeing the Value

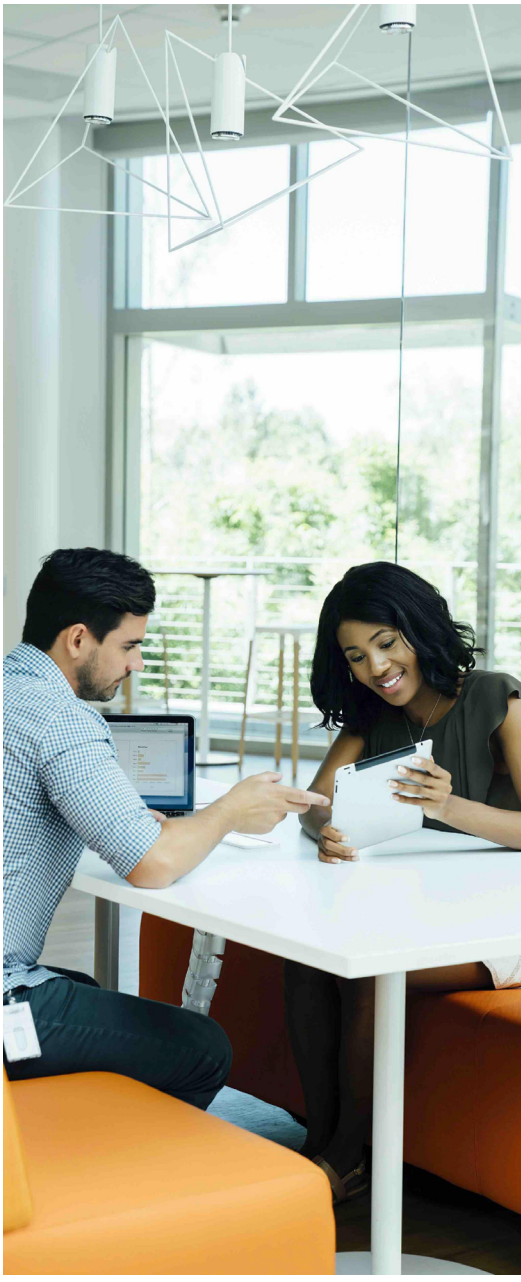
LACK OF VISIBILITY - MOBILE/ APP REPORTS

Once onboarded, email security can become an area of complacency for many businesses; in the early stages of an email security platform being implemented it can be easy to identify and recall the difference between the new state and how it used to be. Over time, however, this becomes more challenging, as does remaining aware of the value of the change once the new state becomes the new norm.

To help customers see the value of their solution, and boost retention for Service Providers, the FirstWave CyberCision™ platform takes visibility seriously. In addition to the dashboard Service Providers can use to manage and build reports on their various customer's environments, the CyberCision™ mobile app also provides a powerful tool that can be put directly into users hands. What's more is this can all be done in your branding – completely white-labelled to suite your business and providing an out-of-the-box solution for your customers.

For Service Providers, the ability to easily implement, manage, and monetize the implementation of email security on top of Office 365 is a game-changer. CyberCision™ M365 Frictionless Email Security enables you to onboard email security customers at scale, at speed, and with minimal effort – opening new channels to market.

Book a demo today to see how you can introduce email security to your customers and help keep them safe.



FirstWave

Ready to level up?

If you need help with taking your cybersecurity protection to the next level, please contact FirstWave and we will be more than happy to help assess your current situation and recommend a solution to help your business.

CONTACT AN EXPERT

FirstWave

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

Get Expert
Solutions

Book a demo

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 Ltd (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.

firstwavecloud.com | +61 2 9409 7000 | connect@firstwavecloud.com