FirstWave

Whitepaper

Achieve Hockey Stick Revenue Growth with A Scalable Managed Cybersecurity Service

Executive summary

Right across the economy, most interactions with businesses are occurring as digital experiences, and businesses rely on cloud software and services for every aspect of their operations. This has set the foundation of the current end-user era, characterized by affordable and accessible software. Other key trends include the rise of remote working and the growing incidence and impact of cyberattacks.

While the global cybersecurity market is growing at an impressive rate, selling cybersecurity-as-a-service is a more challenging proposition. This is particularly true of the SMB/SME market, where email and the Outlook client in Office 365 are the major threat.

Complexity for these organizations is growing every day, and at the same time, many end-users in this market are time-poor and have many different priorities vying for their attention. There is also a general perception amongst SMBs/SMEs that cybersecurity products are high-friction and offer poor value.

There is a substantial opportunity for service providers to build a thriving cybersecurity-as-a-service offering for SMB/ SME customers. A product-led growth model can help service providers develop a friction-free distribution process to accelerate adoption of new cybersecurity technologies via self-serve distribution platforms. This, in turn, creates the possibility of "hockey stick" revenue growth, with minimal extra expenditure on traditional sales and marketing channels.

Service providers can create a cybersecurity managed service in three steps, which will help to reduce the time and costs to deploy a compelling suite of security services. Those steps are:

- Shifting to an integrated product packaging strategy
- Starting with one simple, compelling offer before scaling rapidly
- Careful selection of a scalable, automated cybersecurity platform

Evolving Digital Journeys And The End-User Era

Right across the economy, there are several major and interrelated trends that are shaping the digital journey for most organizations - enterprise, government and SMB/SME alike.

Most interactions with businesses are occurring as digital experiences, and businesses rely on software for every aspect of their operations. Businesses are in the market for software services that take advantage of the unique opportunities afforded by universal cloud adoption: notably, real-time interconnectivity with data flowing freely where it's needed.

Core cloud infrastructure and applications have set the foundation, and we're shifting to a new era: one which is defined by the end-user.

From the on-premise era of the 1980s and 1990s, to the onset of cloud computing in the early 2000s, the current end-user era is characterized by affordable and accessible software, which has shifted the purchasing decision down to the end-user. The primary decision-making criteria has moved from "how will this product help the organization's bottom line?" to "how will this product help me in my day-to-day work activities?"

On-premise era (1980s-90s)

- Software installed from a box
- Expensive CAPEX purchases
- CIO made purchasing decisions based on IT compatibility

Cloud era (2000s)

- Software moves out of the data center and into the cloud
- Prices plummeted as software became "on demand"
- Non-technical executives made purchasing decisions based on strategic goals

End-user era (2010s-now)

- Infrastructure more elastic and scalable
- Software is free or cheap to try, with options to scale upwards
- End-user drives purchasing decisions based on usability

This shift has been amplified by the last three years of the pandemic. Work now happens wherever and whenever - by both necessity and choice. People with ever-changing working lives need tools that can keep up, and their expectations are higher than ever.

Meanwhile, the incidence and impact of cyberattacks continues to grow. Cybercrime cost U.S. businesses more than $6.9 billion in 2021 - and yet many businesses remain underprepared for the eventuality of an attack - particularly in the SMB/SME market.

- 70%[1] of SMBs/SMEs suffered from at least one cybersecurity incident during the pandemic
- Yet, only 50%[2] have a cybersecurity plan in place

[1]Frost & Sullivan, C-level SME respondents, Oct 2021
[2]UpCity Survey 2022

Why Is It So Hard to Sell Cybersecurity As A Managed Service?

The global cybersecurity market is big business and is growing at an impressive rate. Global market revenue is projected to reach more than US$170B in 2023, and there are around 50,000 cybersecurity firms worldwide, a number that grows daily.

Despite the healthy outlook for the overall market, selling cybersecurity-as-a-service is a more challenging proposition. There are various reasons for this, starting with the fact that many organizations of all sizes still don't understand the scope of the current threat, and how exposed they really are.

This is particularly true of the SMB/SME market, where email is still the major threat - 91% of data breaches are a direct result of phishing. When you consider that the number of paid seats of Office 365 is now climbing rapidly towards 400 million worldwide (source), there is no doubt that Microsoft products still dominate the tech landscape. The numbers suggest that Office 365 and the Outlook mail client simply don't provide the protection many assume it does.

Meanwhile, complexity is emerging for both service providers and their customers from every angle, each of which makes it that much harder to sell and monetize cybersecurity:

- Threats are growing in number and sophistication.
- The work environment is very fluid – with people working from home or remotely, across multiple devices, combined with the continued migration to the cloud.
- There is increased demand to manage many customer-specific solutions and policies for many different threat vectors, from a variety of vendors.
- The current shortage of tech skills across the broader economy is making it harder to keep staff and fill new roles.

To add to the challenges, there are also several factors that are unique to the typical SMB/SME buyer. These end-user buyers are almost always super-generalists, are break-fix oriented, focused on the ground-level reality of their business and are also consumers and individuals. What this means is that it's harder to get their time and attention, and they are far more likely to merge their consumer and work brand affinities and shopping behaviors.

Last but not least, one of the biggest challenges in the SMB/SME market is friction. Because these buyers are far more likely to be time-poor, they are also far more likely to be discouraged by the normal customer onboarding process for cybersecurity products, which typically involves a lot of process, time and other practical issues to go from order to active email security protection for all employees, on all devices, all of the time.

Unfortunately, the overall value of cybersecurity is frequently underestimated - an incredibly dangerous stance given the increasing frequency of cyber attacks.

Cybersecurity Opportunities For Service Providers In The End-User Era

Despite the challenges and complexities of the cybersecurity market, there is a substantial opportunity for service providers to build a thriving cybersecurity-as-a-service offering for SMB/SME customers in the current end-user era.

As the natural evolution of the cloud era, it's unsurprising to see companies such as Atlassian, Dropbox and Slack mentioned frequently as leaders in the end-user era. There is one common factor that differentiates these leaders from the pack: all have embraced a product-led growth model - essentially, one that empowers end users to find, evaluate and adopt products on their own.

The product-led growth model has emerged as a friction-free, product-led distribution process to accelerate adoption of new technology, offering advantages such as:

- **Self-serve distribution platforms:** The product is set up to drive customer adoption, retention and expansion without human touch.
- **Eliminate friction:** There is no need for lengthy onboarding processes involving complex sign-up forms or demos with promises. Users try out the product right away so that time-to-value is near immediate.
- **Creating value instead of extracting value:** The "try before you buy" method allows users to experience the value first-hand without any risk, making them more likely to become engaged, loyal users.
- **Opportunity for "hockey stick" revenue growth:** Once a product gains momentum amongst a community, there is substantial opportunity to reach the inflection point of hockey stick revenue growth, with minimal extra expenditure on traditional sales and marketing channels.

What do we mean by 'hockey stick'?

Normal growth for a SaaS company is 10% to 25% per year[3]

'Hockey Stick" Growth Curve

A large number of customers at lower revenue.

A large number of customers with higher revenue

[3]Harvard Business Review

Five Strategies For Building A Successful End-User Business

01

Focus on the end user: Loyal end-users are more likely to act as front-line champions because their authentic evangelism drives further adoption and sales, both within and outside their organizations. Companies can build communities around end-users and prioritize their experience in product development.

02

Use network effects: End-user advocacy does not mean relying on word-of-mouth or referrals alone. Products should be built to harness network effects stemming from their initial champion's adoption.

03

Employ a transparent pricing model: End users should be able to understand and predict their total spend against budget without needing to conduct additional research or having to discuss with a sales representative.

04

Embed customer success levers: Rather than relying on large customer success teams, look to embed self-serve customer success levers in the product and user journey so that users have the right tools and feel empowered to help themselves when troubleshooting is required.

05

Infuse philosophy throughout organization: Every member of every team across the organization should be an individual evangelist for the product. This helps improve the product and engagement over time.

Where To Start? Building Your Cybersecurity Go-To-Market Offering

Building a cybersecurity managed service in your business may seem like a daunting task. However, it can be achieved with a successful integration and end-user focus, starting with these three steps.

01

Shift your product packaging strategy from add-on to integration

Rethink how you market your product packages - can it be done in a way that encourages end users to think of the higher-margin bundles as being essential, rather than an optional extra or upsell?

The offer of a secure service is likely to have far greater perceived value than a service plus optional security as an add-on.

02

Start with one simple, compelling offer - then scale rapidly

It makes sense to start with one simple cybersecurity product that will secure business customers from where the vast majority of cyber attacks occur - phishing emails. This becomes the launchpad to take them on the cybersecurity journey via your expanded service offering.

Develop an initial targeted use case and solution narrative that is simple and precise, enabling end users to easily grasp what problem the product solves. To achieve product-market fit, users need to be able to adopt a solution with minimal education, dialogue, or support.

From here, packaging should be well-structured so it is crystal clear what users receive in each additional plan. Users can then decide on their own to pick the bundle that works best for their needs.

03

Build your offerings on a scalable delivery platform

A scalable, automated cybersecurity platform will reduce the time and costs to deploy and manage a compelling suite of security services to your customers.

As an entry point, it should offer Advanced Detection and Response (ADR) capabilities for continuous real-time monitoring of email security service and automated threat visibility, detection, alerts with response to attacks and incidents.

Automate Your Cybersecurity With CyberCision™

CyberCision™ is the only automated cybersecurity-as-a-service platform for service providers globally that virtualizes, multi-tenants and integrates these security products at the lowest cost to operate and manage.

It provides end-users that don't own and operate their own cybersecurity infrastructure with the world's leading enterprise grade perimeter security, from the world's leading security technology providers, at an affordable price.

CyberCision™ benefits for service providers:

- Reduced complexity and cost to deploy cybersecurity solutions and 'harden' Office 365
- Increased profitability and competitive advantage - differentiate offers under your brand
- Reduce friction with customers able to manage email security alerts
- High-value, differentiable partner branding for all customers, with complete flexibility to set, modify or remove branding
- Simple, convenient deployment using single, unified management portal/UI

Benefits for your end-users:

- Digital perimeter protection
- Enterprise grade security at an affordable price
- Simple, intuitive view of security status
- Suited for any IT administrator without security expertise
- Instant, 24x7 security visibility across customer organization
- Low time to respond and contain any cyber incidents

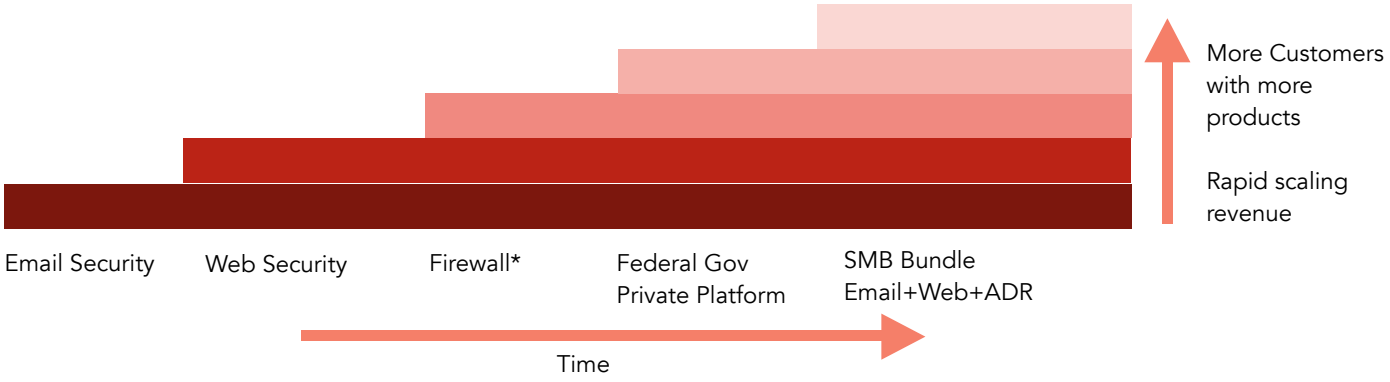
Unlocking Customer Success with CyberCision™

Case Study: Enabling A Major Telco With A Platform To Scale Rapidly

One major telco in the Asia-Pacific region has embraced a simple strategy of placing customers at the center of everything they do and delivering simpler, more flexible cybersecurity products with an exceptional digital service experience.

Cloud email security delivered via CyberCision™ was a quick revenue win, with large uptake of the product across the customer spectrum - from SMBs/SMEs to enterprise. As more cloud cybersecurity solutions were launched, the telco was able to scale solutions rapidly across more threat vectors and into more industry verticals; and build more relevant offer bundles to meet the needs of their large small office/home office and SMB/SME customers.

The telco now has a comprehensive cybersecurity offering, managed and deployed on a single cloud platform.



Case Study: Mid-Sized Service Provider Easily Onboards Hundreds Of Customers At Speed

A mid-sized service provider needed to migrate hundreds of SMB/SME customers from a legacy email security solution, which was not providing an acceptable level of coverage against current and emerging threat vectors. The service provider was facing numerous challenges on this project, with the most significant being that the in-house team were based overseas and were not trained in cybersecurity.

The service provider required a sovereign solution that was easy to deploy and manage, with the ability to scale as the business grows. The CyberCision™ platform minimized the time and resources required to migrate these customers from the legacy solution. Non-IT staff were even able to support the migration.

As a result, each of these customers now have enterprise grade email security that has been bundled into their managed service offering.

Case Study: Cisco Delivers Cybersecurity-As-A-Service with CyberCision™

Global security vendor, Cisco, had difficulty providing an email SaaS solution to their Telco and Service Provider customers who were on-selling security to businesses with under 100 employees.

Cisco contracted an OEM white-labelled version of the CyberCision™ platform to deliver cloud email security for their large global Telcos and Service providers as a true subscription email security service. CyberCision enabled service providers to provision Cisco carrier-grade cloud security services to both enterprise and SMB customers at scale, opening the door to new revenue opportunities with a lower cost-to-serve.

Conclusion

The digital economy continues to evolve: End-users are driving purchasing decisions and they demand software and services that are free, cheap and scalable. Meanwhile, cyberattacks are on the rise and are looming large in the public imagination.

For managed service providers, there is a significant opportunity to be uncovered in selling cybersecurity as a managed service to the SMB/ SME market.

However, challenges also exist - in particular, the general level of understanding of the scope and magnitude of the threat; as well as the perception that cybersecurity products are high-friction and offer poor return-on-investment.

Service providers can overcome the challenges associated with selling managed cybersecurity by embracing a product-led growth model. This can be achieved in conjunction with a scalable, automated cybersecurity platform, which will reduce the time and costs to deploy and manage a compelling suite of security services to customers.

Start Now

With CyberCision™, service providers can build as-a-service cybersecurity packages of carrier-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 CyberCision™ platform incorporates the latest technologies from leading security vendors ready for today's and tomorrow's digital business ecosystem and evolving cybersecurity challenges. Contact us now to see how you can benefit from "hockey stick" style growth enabled by CyberCision™.

Book a Demo

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 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.

firstwave.com | connect@firstwave.com