TREND MICRO
SECURITY SURVEY 2018

We send out a survey each year to get a feel for what's going on in the wide world of security. This year, we had a sample size of 427 respondents from the IT service industry that gave us some valuable insights into the state of security trends in 2018.

So what's the point of it all for you, you ask?

Well, that's easy – we share the results with you to help you understand which security trends matter for your organization, and how they can affect your business. We'll be highlighting several key stats that can give us a clearer understanding of the future of the security market.

Let's take a look at them now.

Respondent Persona Breakdown

Before we break down the market gaps, it's important to understand who the respondents really are. Take a look at some of the questions we asked:

- **How many employees are in their organization?** - Around 36% of the responses came from organizations with 1-5 employees. On the opposite end of the spectrum, 23% came from organizations with 50+ employees. The difference in the sizes of the organizations helped us understand that the security landscape differs greatly depending on different target markets.

- **How many years have they been in business?** - Out of the 427 respondents, 390 have been in business for 5 years or longer. Only 8 have been in business for one year or less. Generally speaking, that means that most of the survey responses come from experienced IT service providers that know how to survive and thrive.

- **How long have they been offering managed services?** - Of the respondents that offer managed services, the vast majority (60%) have been offering them for 5 or more years. An additional 33% responded that they've been offering them for 3-5 years. That sounds about right – many IT services providers have been selling "bundled" IT services for a long time. Or, to put it another way, managed services won't disappear any time soon.

Security Focus: Endpoints

There's an ever-evolving and rapidly growing category of endpoint devices in the workplace. Based on the data, we recommend that IT service providers offer better comprehensive endpoint protection security services.

The Stats

As endpoint security threats change and evolve, so do the endpoint security solutions. Despite endpoint security being a relatively new facet of security, lots of IT service providers in the marketplace just aren't keeping up with the demand. A whopping 52% of survey respondents said that they've offered their current endpoint security solution for over 5 years.

That's a huge deal. Everyone knows how often technology changes. Imagine using the same software to defend against evolving threats – it's just not effective.
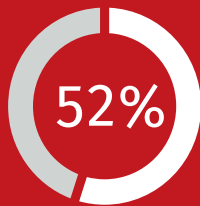
52% of survey respondents said that they've offered their current endpoint security solution for over 5 years.

As it turns out, many vendors are using the endpoint security that comes included with their RMM or PSA. Granted, it's better than having zero security in the first place… but it's just not good enough to keep their customers protected against the modern threats they face.

The Market Opportunity

There's a huge opportunity here. Despite the widespread usage of endpoint security solutions, IT service providers aren't selling them to their customers. Only 152 of our respondents answered the question of whether or not they were selling endpoint security to their customers. Of those 152, only 43% said that they were.

275 survey respondents didn't know how to answer the question. Uh oh.

We're getting a clear picture that IT service providers are either unwilling, unprepared or unable to confidently offer endpoint protection to their clients. However, with the popularity of BYOD policies growing at a steady rate, combined with the rise of IoT devices, IT service providers really can't afford to miss out on the booming endpoint security protection market.

To put it plainly: There's a lot of money to be made within the channel here. And if that weren't enough, substandard endpoint security solutions end up putting customer's data on the line (and the vendor's credibility at risk, too).

Security Focus: Email

Moving on from endpoints, let's look at email security. Emails are a critical part of nearly all businesses – and their security is exceptionally important, considering the rise in data breaches, phishing attacks, ransomware, and more.

Lots of businesses are starting to understand and rely on email security to help them protect their data.

The Stats

90% of advanced threats originate through email. Because of this, security is usually built-in (to some degree) on all major email platforms. However, this basic security is rarely enough to stop any serious threats. That's exactly why many IT service providers are turning to third-party email security solutions to fully protect their clients' networks.

90% of advanced threats originate through email.
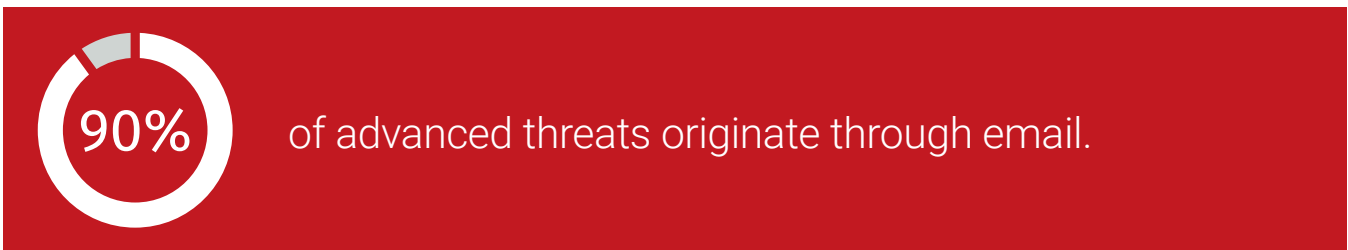
In our survey, we gave IT service providers the option of choosing between six leading endpoint security solutions and one "Other" category. Those 6 included:

- *Trend Micro*
- *Barracuda*
- *Symantec*
- *Proofpoint*
- *Reflexion*
- *GFI*

Surprisingly, 39% of respondents selected "Other." Many still choose to stick with built-in email security coverage, such as the stock Office 365 email security from Microsoft.

That's particularly alarming news when you consider that Business Email Compromise (BEC) attacks are on the rise, representing over $12 billion in projected loss this year.

The Market Opportunity

IT service providers largely recognize the need for email security solutions. Of the surveyed IT service providers who answered the question, "Do you offer email security to your customers?" 64% responded in the affirmative.

That leaves a massive 36% of IT service providers who are not offering email security to their customers. With the demand for more secure IT infrastructures at the startup, SMB, and enterprise levels, this is a gap that really shouldn't be ignored.

Our marketing department keeps a close watch on open and click-through rates of email campaigns revolving around security. Those that mention email security solutions earn, on average, a 2-3% higher open and a 3-4% high click-through rate.

Why? Because nearly all businesses rely on emails. It's a subject that many people understand, and the need for enhanced security is plain to see.
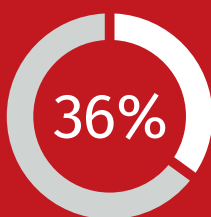
36% of IT service providers are not offering email security to their customers.

Security Focus: Cloud

Much like the lasting popularity of emails, businesses are becoming more mobile and cloud-dependent. As businesses across industries that increasingly embrace the cloud, the need for robust security grows stronger.

The Stats

68% of survey respondents said they resell and manage Microsoft Office 365 or cloud applications for their customers. Conversely, that leaves a wide gap of 32% that simply aren't taking advantage of selling cloud applications.

Curious, considering the widespread adoption across nearly all industries.

Additionally, these cloud applications require effective security to ensure the right levels of data protection at all levels. Despite the demand for cloud services (and security thereof), many IT service providers are leaving customers to fend for themselves.

A surprising 49% choose to trust only the built-in security solutions for cloud applications such as Box, Dropbox, Google Drive, Office 365, and even their email.

The Market Opportunity

Our marketing partner's campaigns tell us that businesses are definitely interested in better cloud security solutions. That's largely thanks to the fact that modern organizations are gaining a better understanding of WHY they need for enhanced security across all their cloud applications.

In other words: As they gain cloud security knowledge, they seek out cloud security solutions.

With that in mind, it shouldn't be a shock to hear that we recommend IT service providers tap into the market by selling cloud services, as well as security services, to ensure the full protection of their customers' data.

32% of IT service providers aren't selling cloud applications.

What We've Learned This Year

In case you skipped to the end, here's a recap.

Customers are increasingly adopting new technologies that offer them previously unattainable benefits, but they're left open to attack. Specifically, there are market gaps in endpoint, email, and cloud protection services that many IT service providers simply aren't capitalizing on.

IT service providers that choose to continue using legacy protection tools will inevitably be left in the dust by those that offer more robust and intelligent security solutions to customers hungry for more flexibility, collaboration and productivity.

No need to worry – that's why Trend Micro is here.

We offer multiple different types of partnerships that can help introduce the right solutions to your business. You can (and should) leverage our managed service provider partnership to fill in any security gaps, so that you can increase your offerings to your clients while maximizing cash flow and getting full vendor support.

TREND MICRO™

Securing Your Connected World

Trend Micro Inc., 225 E John Carpenter Freeway
Suite 1500
Irving, Texas 75062
Phone: (817) 569-8900 Toll-free: (888) 762-8736