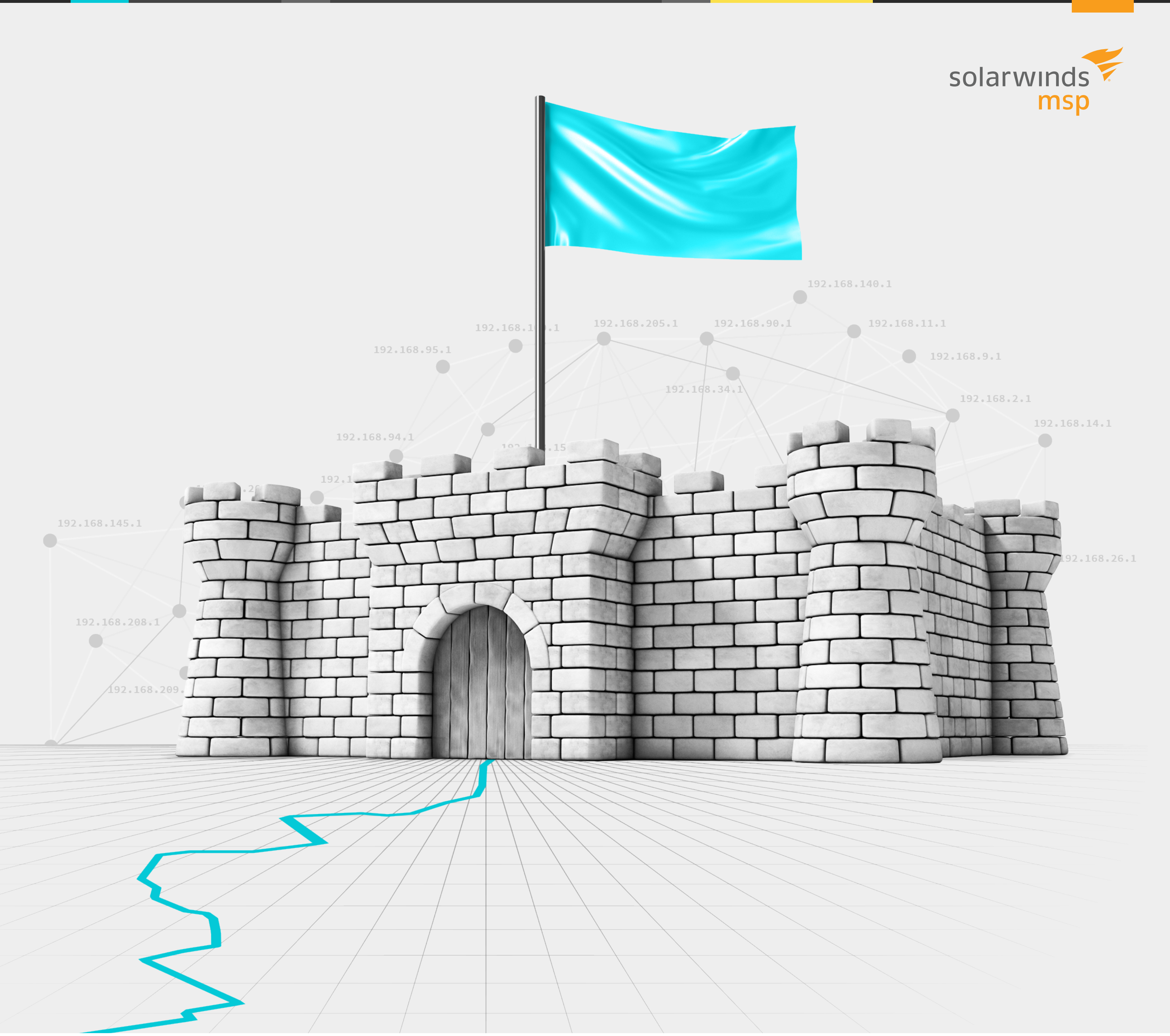


WHITE PAPER

Path to MSSP

EXECUTIVE SUMMARY

One of the hottest debates in IT service management at the moment is whether or not to pursue "Managed Security Service Provider" (MSSP) status. This is largely caused by a lack of clarity over what the name means, whether it is beneficial to use it, or whether customers are even concerned about the distinction between MSPs and MSSPs.

This report defines exactly what an MSSP is and identifies the existing opportunity for those who reach this standard. It also highlights the shortcomings of current service providers and how to overcome them.

This report defines exactly what an MSSP is and identifies the existing opportunity for those who reach this standard. It also highlights the shortcomings of current service providers and how to overcome them.

In summer 2017, SolarWinds MSP examined how more than 400 SMEs and enterprises in the US and UK were addressing their IT security needs and their views of their service providers.

The key result was that 80% of respondents are planning to change the way they manage their IT security in the next 12 months. This might include switching their current service provider and ceasing outsourcing in favor of in-house resources, or vice versa. It is an astonishingly high figure, showing just how turbulent the IT security services market is, and how much opportunity exists as a result.

Five types of opportunity were identified:

i. 60% of respondents are handling security internally—in whole or in part—but more than 4 in 5 (82%) of them are planning to switch to an outsourcing model in the next 12 months. Roughly half are switching because internal resource has proven too expensive, creating a key opportunity for cost-effective service providers. These businesses are the largest category of opportunity (25% of the entire market) and, when combined with their decision to outsource, they are by far the best target for well-equipped service providers.

ii. The next best opportunities, comprising 24% of the market, are those businesses switching from internal to external resource because they need to improve IT security performance. Service providers able to prove deep expertise across the breadth of security services will be able to quickly assert their superiority over internal resource and win the business.

iii. 10% of the market is currently outsourcing their IT security management but has decided to bring it in-house. If service providers can intercept this decision-making and prove that the reason for their disillusionment is not the model but the original incumbent, then they can quickly snap up new customers they would not have otherwise had the opportunity to.

iv. 9% of US and UK businesses are about to switch their current service provider because they are deemed unworthy of the cost. This is in fact a problem of performance and so requires new providers to prove their higher, broader, more innovative capabilities.

v. The final opportunity lies in the 8% of businesses currently outsourcing their IT security but actively seeking a cheaper provider. These are not only the smallest group, but also the least valuable. Winning the business requires undercutting the incumbent and competition, potentially to a degree that makes them unprofitable. While service providers who have automated their processes to reduce their overheads are in a better position than most to offer lower rates, it is still business with little possibility for growth—and is likely to churn in the future.

But how does an IT services provider take advantage of this opportunity?

The key step is to become an MSSP. After all, 70% of the market confirmed they would look more favorably on a service provider that described itself as an MSSP. But other than a name change, what does this entail?

True MSSP status depends on delivering a conclusive portfolio of security services in a reliable, expert, and organized manner. SolarWinds MSP has grouped these into the Four Categories of Security Services, each of which is best delivered in line with the Three Pillars of Security Services Delivery.

70% of the market confirmed they would look more favorably on a service provider that described itself as an MSSP.

By achieving and evidencing these 12 capabilities (each of the Four Categories deployed in accordance with the Three Pillars), customers will have greater confidence in the service provider's ability to manage and protect their network than either their in-house team or their previous provider.

Four Categories of Security Services
Infrastructure
IAM
Data Security
Risk and Vulnerability Management

Three Pillars of Security Services Delivery
Knowlege
Organizational Ability
Technology, Tools, and Resources

Making this leap will undoubtedly put a service provider ahead of the market. The most revealing statistic on service providers' current performance was that businesses had only 66% confidence in their service providers' capabilities in infrastructure security services, which the respondents also ranked as most critical of the Four Categories.

This shows that there is a gulf between what IT security service providers are currently capable of and their customers' requirements—and by extension, also the requirements of becoming an MSSP.

Those that can adapt rapidly to improve their knowledge, skills, and resources in key areas and seize the MSSP mantle will quickly outrun their competition.

WHAT IS A MANAGED SECURITY SERVICES PROVIDER (MSSP)?

To many, "Managed Security Services Provider" is more than a casual description of a particular type of IT services business. In contrast, it should be considered an earned title that suggests defined security capabilities and levels of reliability, above and beyond those levels of service expected of typical providers.

But too many IT service providers have already self-proclaimed themselves MSSPs without considering what it means or whether they fulfil the requirements—if they even know what the requirements are.

Too many IT service providers have already self-proclaimed themselves MSSPs without considering what it means or whether they fulfil the requirements—if they even know what the requirements are.

There are also equally as many service providers who are well and truly beyond the threshold for using the MSSP title, but do not, and so miss out on the benefits of the boosted perception.

Much of this stems from ignorance as to precisely what capabilities and services qualify an IT service provider to operate as an MSSP. There is a general appreciation that it requires certain qualifications, processes, advanced technical capabilities, and resources, but exactly which are needed is often misunderstood.

There is, in fact, a series of very particular services and capabilities that need to be evidenced before an IT service provider can claim to be an MSSP.

The services are organized into the Four Categories of Security Services (each of which can be split into three to five subsectors).

1. Infrastructure

- Endpoint security
- NOC/SOC services
- Network firewalls
- Threat intelligence
- Perimeter-level security

2. Data Security

- Antimalware
- BC/DR
- Digital forensics
- Application whitelisting and data-loss prevention
- Email security

3. Risk and Vulnerability Management

- Vulnerability scanning and patching
- Penetration testing
- Security policy reviews
- Intrusion detection

4. Identity and Access Management

- User access and management rights
- Data governance services
- Authentication and authorization

Delivering each of these services requires three areas of proficiency, or what we have termed here, the Three Pillars of Security Service Delivery:

1. Knowledge

To excel in this area, all technical and consulting teams need to have equally strong knowledge and expertise. Organizing into pockets of knowledge is not only unscalable, but also dangerous if talent leaves the business. Key areas include assessment, management, monitoring, mitigation, identification of issues, and recovery.

2. Organizational Ability

This requires the creation of robust internal processes covering reporting, tracking, and management procedures.This is not only a requirement for effective service delivery and client satisfaction, but can also impact ISO eligibility and ITIL certifications.

3. Technology, Tools, & Resource

Finally, service delivery depends on knowing how to select and best use the tools available. This requires prudent staffing in addition to proper training and certification programs across all tools, software, and resources. Many of these certifications would typically be achieved via your vendors, such as your RMM and SIEM providers.

Combining the Three Pillars with the Four Categories leads to the 12 Core Requirements of Achieving MSSP Status:

The 12 Core Requirements of Achieving MSSP Status

			Four Categories of Security Services			
			Infrastructure	Data Security	Risk and Vulnerability Management	Identity and Access Management
			Endpoint security, NOC/SOC services, network firewalls, threat intelligence, perimeter-level security	Antimalware, BC/DR, digital forensics, application white-listing and data loss prevention, email security	Vulnerability scanning and patching, penetration testing, security policy reviews, intrusion detection	User access and management rights, data governance services, authentication, and authorization
Three Pillars of Security Service Delivery	Knowlege	Strong, broad expertise across all technical and consulting teams	✓	✓	✓	✓
	Organizational Ability	Robust internal processes and service delivery management	✓	✓	✓	✓
	Technology, Tools, and Resource	Comprehensive technical infrastructure and experienced teams	✓	✓	✓	✓

IS FOLLOWING THE "PATH TO MSSP" WORTH THE EFFORT?

So if this is what it takes to be rightfully considered an MSSP, what opportunities exist for those who qualify? Simply put, is it worth the effort of evolving?

To find out, SolarWinds MSP conducted detailed research into the views of more than 400 enterprises and SMEs in the US and UK as to how they were likely to resource their security needs in the next 12 months. In particular, the analysis identified who was best placed to satisfy this need—the typical MSP versus the more accomplished MSSP.

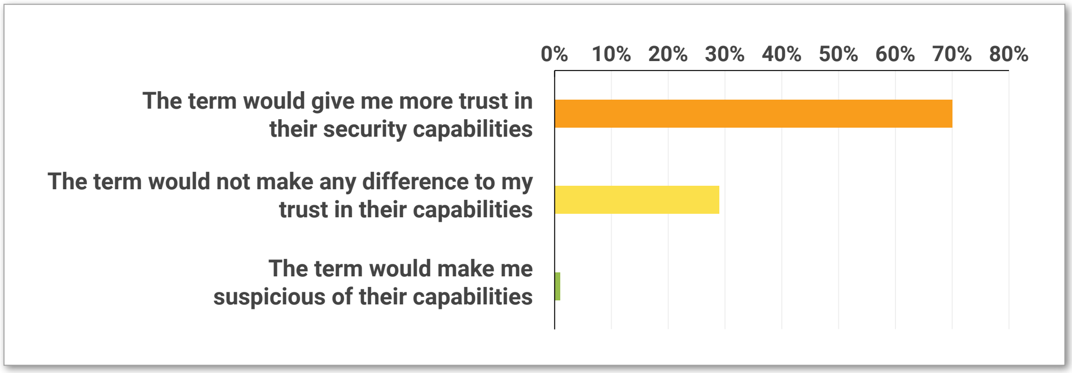
The results painted a picture of an enormously turbulent market, with huge swathes of organizations about to change the way in which they resource their security, and some clear differences between what customers expect and what their service providers are delivering. Of course, where there is change, there is opportunity; but it would seem, only for the rightfully named MSSP.

SolarWinds MSP conducted detailed research into the views of more than 400 enterprises and SMEs in the US and UK as to how they were likely to resource their security needs in the next 12 months.

DOES THE "MSSP" TITLE MATTER?

To many MSP owners, using the title "Managed Security Services Provider" may seem like an empty branding exercise that has no practical benefit. However, this is not the case for client businesses—they put a great deal of stock in what their suppliers call themselves, perhaps more so than would be expected.

Q. How would having the term "managed security services provider" affect your trust of a service provider's capability?



An overwhelming majority (70%) of businesses would look on a potential supplier more favorably if they used the "MSSP" tag, making a clear case for MSPs to focus on ticking off the requirements of each of the Four Categories above.

Despite this, service providers are constantly questioning if this is the space they want to move into. While it is undoubtedly a new sales opportunity and growth market, MSPs are understandably nervous about the degree of additional risk.

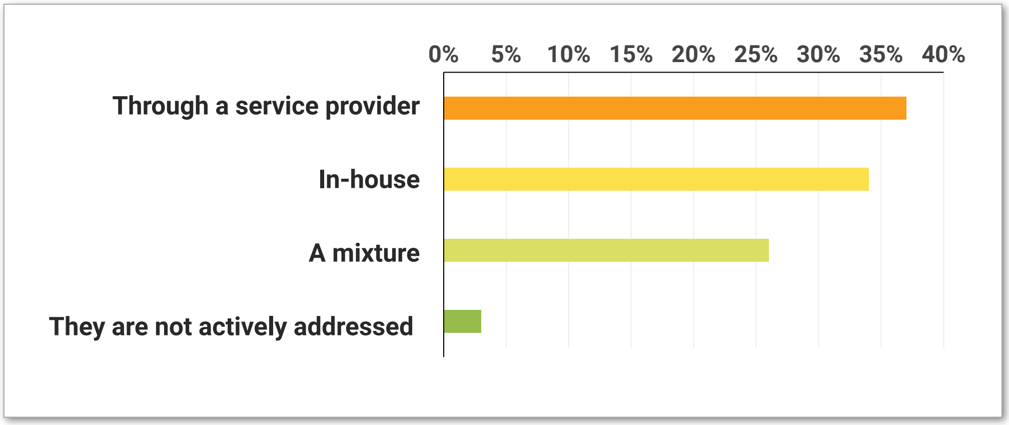
This is why the 12 Core Requirements are so important. If an MSP simply begins using the MSSP title without justification, then they will quickly be found out as they cannot deliver the necessary breadth of services to win clients, nor deliver them sufficiently capably to maintain client satisfaction—nor do so profitably.

But if the MSSP capability is built on the 12 Core Requirements, then the provider can have far more confidence in their ability to control and mitigate much of the risk.

THE MSSP STATUS OPPORTUNITY

Is there actually a market for such a service package, and is it large enough to warrant the investment in re-organizing? Where does the opportunity lie for an MSSP?

Q. How are you currently addressing your security needs?

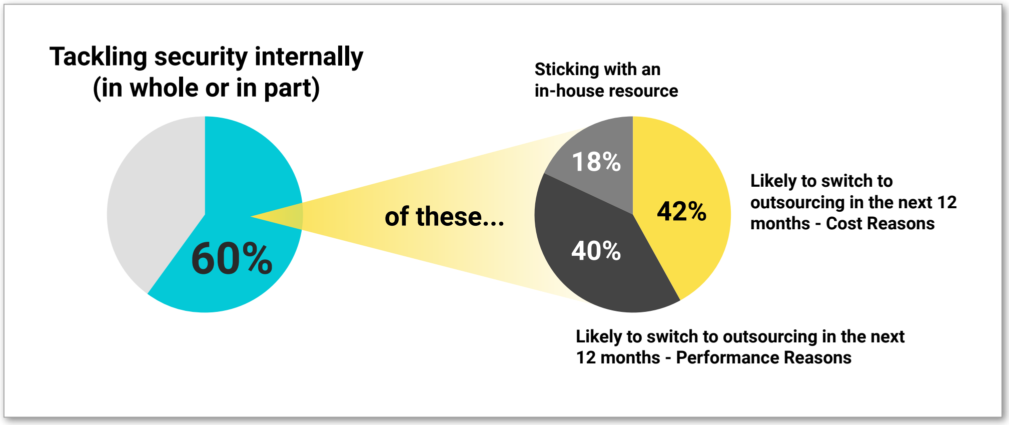


But this is only half the story. This may be how enterprises are currently resourcing their security needs, but 80% are considering a change in the next 12 months. This means there is plenty of opportunity for well-organized and well-resourced MSSPs.

OPPORTUNITY TYPE 1 – THE STRUGGLING INTERNAL TEAMS

For many service providers, it might be a surprise to learn that while 60% of companies are tackling security internally—either wholly or in part—82% of them are planning to switch to outsourcing in the next 12 months: 42% because of cost and 40% because of performance.

These 82% of future outsourcers constitute an enormous 49% of the entire respondent base, making those currently without a provider not only the largest potential opportunity for MSSPs, but also the easiest.



These 82% of future outsourcers constitute an enormous 49% of the entire respondent base, making those currently without a provider not only the largest potential opportunity for MSSPs, but also the easiest.

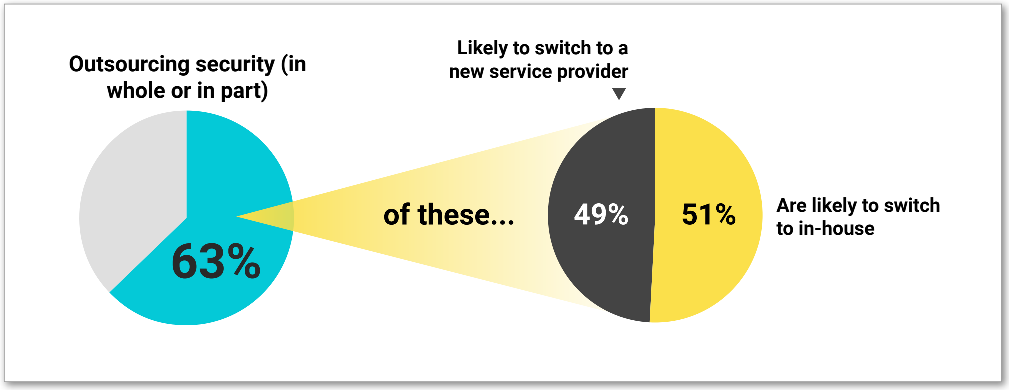
Because these organizations are about to outsource for clear reasons of either cost or performance, the appropriate sales messages are simple.

- **Cost**
  Those who have already automated multiple processes will be the best positioned here
- **Performance**
  Best evidenced by proving high levels of capability across all Four Categories of Security Services and tight adherence to the Three Pillars of Security Service Delivery:
  - Knowledge – shown by being consultative in the sales process, plus highlighting industry qualifications
  - Organizational Ability – shown by highlighting defined processes and structure across all teams
  - Tech, Tools, and Resource – shown with best-of-breed tools and certifications

OPPORTUNITY TYPE 2 – THE DISILLUSIONED OUTSOURCERS

As is always the case, seizing business from other service providers is more complicated.

63% of the market have outsourced at least part of the entire security function, if not all of it. But revealingly, more than half of them (59%), are planning to change in the next 12 months.



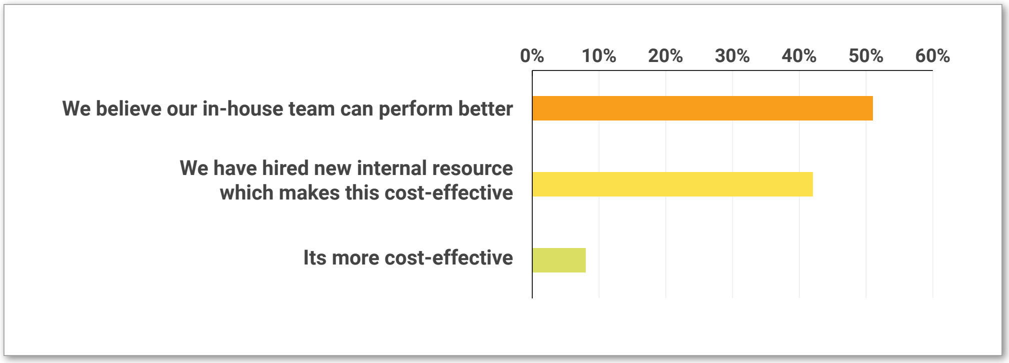
The majority of this group (51%) are convinced of the need to fire their existing provider for a simple reason: they believe they can do a better job, have already reached the end of their patience, and are defecting.

Interestingly, when it comes to their plans for change, there is an almost exact 50/50 split amongst MSP defectors for bringing the security function in-house, and choosing a new provider.

Those considering internal resource

Perhaps surprisingly, those about to bring security management in-house represent a key opportunity for MSSPs. This is because the majority of this group (51%) are convinced of the need to fire their existing provider for a simple reason: they believe they can do a better job, have already reached the end of their patience, and are defecting.

Q. If you are currently outsourcing security management, but are now likely to bring it in-house, why?



The next step for the well-organized MSSP is simple: convince the target business that the problem was not with the outsourcing model, but with the incumbent's skillset and sophistication—and show how your attributes are superior. And the MSSP that can satisfy the 12 Core Requirements is inherently better-suited and able to prove its capabilities.

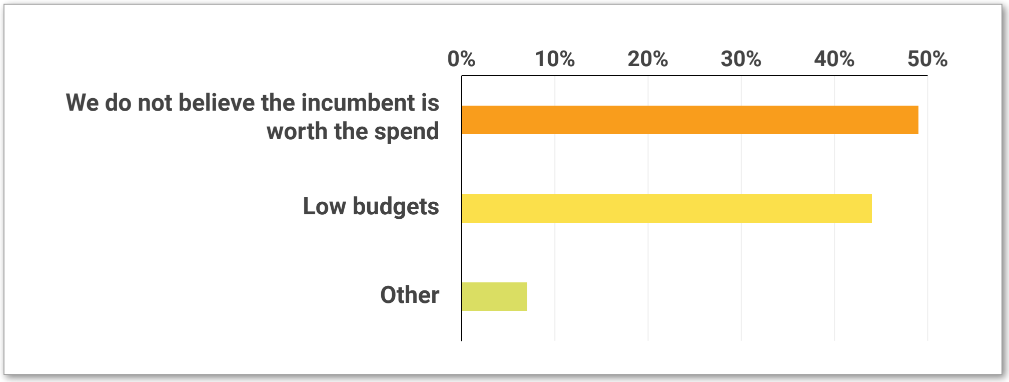
An additional key argument to make to these potential customers is that the stats surrounding Opportunity Type 1 above have already proven that when security is handled in-house, the clear majority end up outsourcing it later when they realize that better performance can be found at lower cost elsewhere.

It is worth the arguably greater effort of targeting this group—these businesses on the verge of taking their security back in-house represent 10% of the entire market.

Those seeking a new service provider

The remainder of those contemplating firing their current provider are of course planning to choose another one (49% of all MSP defectors). And once again, the split in motivation is between cost and performance.

Q. If you are currently outsourcing security management, but are now likely to appoint a new service provider, why?



Exactly half of those seeking a new provider are doing so because they don't think the incumbent is worth the spend. While this objection looks financially-driven, it is actually an issue of performance. They are not receiving the service they expected for the fees they are being charged. Try to win on purely financial terms and you are not addressing the business' core suspicion. Pushing and proving a clear security specialism instead, evidenced with the 12 Core Requirements, will demonstrate a superior and more robust capability than the previous supplier, and ultimately put you in the best possible position to win the business.

The other half of businesses looking for a replacement MSP are doing so for purely financial reasons; they can't afford the incumbent. These businesses are the smallest target group (8% of the entire market) and are the least valuable. The only route to winning them is probably to undercut the previous supplier and any others vying for the account to such a degree that they are barely worth having. Obviously, those MSSPs who have already automated extensively and therefore have lower overheads are in the best possible position, but as all MSP heads know, the client who chooses you because you are the cheapest is the least likely account to grow and the most likely to question your value in the future.

Exactly half of those seeking a new provider are doing so because they don't think the incumbent is worth the spend. While this objection looks financially-driven, it is actually an issue of performance.

How do these opportunity types stack up against each other?

	Category	Description	Core Reasons for Change	% of Entire Market	Quality of Opportunity	How to Target Them
Opportunity Type 1	**The Struggling Internal Teams**	Currently tackling security internally but planning to change in the next 12 months	Cost	25%	Best	Focus on the Organizational Ability Pillar to demonstrate your business' economies and how these trickle down to your rates
			Performance	24%	Best	Use the Four Categories of Security Services to show a wider capability than the internal team, and the Three Pillars to prove your ability to deliver
Opportunity Type 2	**The Disillusioned Outsourcers**	**Group 1:** Those currently outsourcing, but now considering internal resource in the next 12 months	Performance	10%	Good	Show that the reason for their disillusionment is not the model, but the original incumbent; using the 12 Core Requirements to prove the difference between them and you
		Group 2: Those currently outsourcing, but now seeking a new supplier in the next 12 months	Performance	9%	Average	The incumbent has been found lacking so use the 12 Core Requirements, and especially the Three Pillars, to demonstrate your superior service delivery
			Cost	8%	Least Valuable	Use the 12 Core Requirements to secure the business, but it is likely you will have to reduce rates to undercut incumbent
	Category	Description	Core Reasons for Change	% of Entire Market	Quality of Opportunity	How to Target Them

ARE CURRENT SERVICE PROVIDERS ABLE TO TAKE ADVANTAGE OF THESE OPPORTUNITIES?

The five categories of opportunity above all highlight the necessity of the 12 Core Requirements, made up of the Four Categories of Security Services and the Three Pillars of Service Delivery.

MSSPs, who by definition have structured their business in line with these 12 points, are in the best possible place to take advantage of the opportunity.

This begs the question: how many service providers currently qualify? In other words, if you commit to becoming an MSSP, how far ahead of the pack will you be?

In answer to this question, SolarWinds MSP's research also examined businesses' views of their service providers' capabilities, and specifically how many of the 12 Core Requirements were ticked off.

For each of the Four Categories of Security Services, businesses were asked if their service providers:

- Display sufficient knowledge
- Display suitable organizational ability
- Have the necessary technology, tools, and resources to deliver the service

(essentially, whether they conformed to the Three Pillars)

In order to also identify the impact of any shortcomings, the respondents were asked to rank the Four Categories according to their criticality.

The results revealed a startling mismatch and an opportunity for those who have built their business on the 12 Core Requirements, and therefore earned the title of MSSP.

UNDERPERFORMANCE

Infrastructure was ranked as by far the most critical of the Four Categories. The gap by which it leads the other three is the greatest gap amongst any of them. This is perhaps unsurprising given Infrastructure as a category includes some of the most fundamental aspects of IT security—firewalls, endpoint security, and NOC/SOC services, to name a few.

		Confidence in Current Service Provider's...			
		Knowledge in this category Percentage that rated their supplier "experts" or "knowledgeable enough to be of value to me"	**Organizational ability in this category** Percentage that rated their supplier "excellent" or "adequate"	**Technical tools and resource in this category** Percentage that declared "high" or "sufficient" confidence	**Average overall confidence in service provider's capabilities**
Order of criticality	**Infrastructure**	40%	76%	81%	66%
	IAM	49%	89%	93%	77%
	Data Security	43%	86%	87%	72%
	Risk and Vulnerability Management	46%	87%	89%	74%

In contrast, when examining enterprises' confidence in their service providers' degree of accomplishment in each of these categories, Infrastructure was consistently at the bottom, and by a considerable margin. The other three categories, despite being of lesser criticality, were ranked far above Infrastructure, but within only a few percentage points of each other.

In other words, service providers are currently perceived as most proficient in the least critical areas, and least proficient in the most critical.

This could be because the Infrastructure category is the broadest and therefore harder to show mastery of. Or perhaps because it is so fundamental and therefore small errors are more memorable. Or it could simply be an unfair accusation, and actually a matter of how the service providers are being (wrongly) perceived.

Either way, the immediate priority is clear.

Service providers looking to evolve to MSSP status to seize the security services business becoming available in the next 12 months must improve their ability to deliver Infrastructure services. Their poor reputation in this area is undermining their ability to achieve Trusted Advisor status with their clients. Whether this is a case of perception or reality is immaterial: in service industries, perception is reality.

HOW?

Of course, the key to improving service delivery is closer adherence to the Three Pillars. But where to start? Of the three, the one that will most quickly address actual or perceived shortcomings is Knowledge. The data above shows this is the Pillar with by far the lowest scores, probably because it is the Pillar that is so hard to prove excellence in, and the one that can be most subjectively judged.

Knowledge is also the most impactful of the Three Pillars. Strong foundations here will make for prudent decisions on technology, hiring, and organizational structure, improve sales and marketing, and enhance ongoing client service.

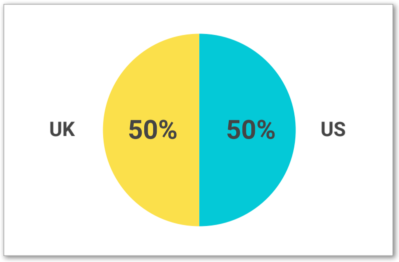
Of course, Knowledge is also always a moving target. But if service providers can stay abreast of new threats and technologies, educate their customers, and ensure their teams hold the latest and most relevant certifications, then the first step to MSSP has been taken.

And once the MSSP title is earned, then all the opportunities detailed above will open up.

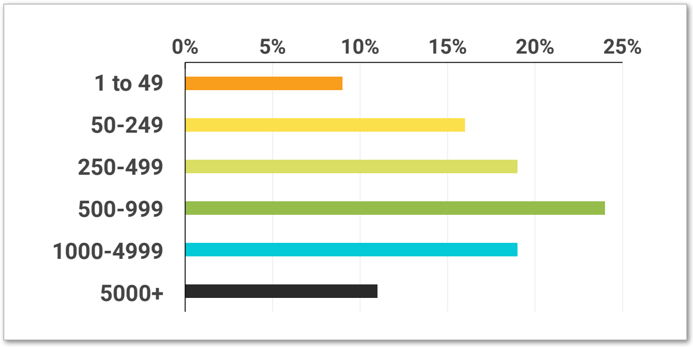
METHODOLOGY FOOTNOTE

In summer 2017, SolarWinds MSP conducted detailed research into the views of more than 400 IT decision-makers. These were equally split across US and UK, and across SMEs and enterprises.

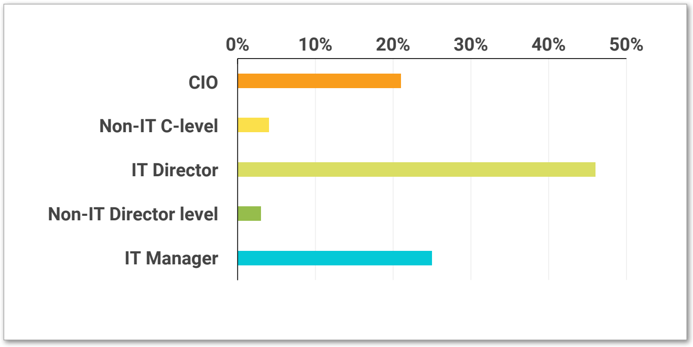
Geographical split



Split of company size, by employee numbers



Split by job title



LAYERED SECURITY COLLECTIVE INTELLIGENCE SMART AUTOMATION

SolarWinds MSP empowers IT service providers with technologies to fuel their success. Solutions that integrate layered security, collective intelligence, and smart automation—both on-premises and in the cloud, backed by actionable data insights, help IT service providers get the job done easier and faster. SolarWinds MSP helps our customers focus on what matters most—meeting their SLAs and delivering services efficiently and effectively.

This document is provided for general guidance and informational purposes only. It is not and shall not constitute legal advice. Information and views expressed in this document may change and/or may not be applicable to you. SolarWinds MSP makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein. If you have any questions in regard to the applicability of any law or regulation discussed herein to you or your organization, we encourage you to work with a legally qualified professional.