“MSP Journey” – Growth with Managed Security Services

TABLE OF CONTENTS

Executive Summary

Current Situation and Required Decisions

IT Security—particularly in the form of Managed Security Services—has been shown by every metric and survey to be a central theme for the future for IT service providers, system vendors, and managed service providers.

Yet in practice, that growth is anything but simple for the channel and the provider to harness. Over the course of multiple webinars conducted with 350 total participants from system vendors, the following portrait of the channel came into view:

- 90% believe that customers do not understand security solutions or the benefits they bring.
- Approx. 40% of the participants saw sales communications with customers as a very strong challenge given the mix of complex solutions and low security requirements.
- And almost half of all those surveyed perceived it as difficult to integrate security services into general managed service portfolios.

The “MSP Journey” project seeks to benefit the IT channel by analyzing growth factors.

Methodology and Course of Action

The project's methodology reflects the collected data and facts as well as accompanying interviews with selected successful managed service providers. The data was collected in three surveys conducted on the website www.msp-journey.de as well as two webinars.

The results indicate while all interview partners desire further growth, there is no one-size-fits-all model to reach that objective. There are, however, elements that lend themselves to targeted growth, and which can be reviewed and integrated as clearly recommended action steps into each partner's own corporate development with managed security services.

Findings and Recommendation

The recommendations lend themselves to two dimensions. First, the question: "What can I do within my security strategy to aid my growth." Second: "How can I optimize my implementation?"

- The success criteria for controlled growth are:
- Strong strategic commitment at the executive and all other management levels
- Narrow selection of a target audience with security awareness
- Strong technical competency in the sales force

- The success criteria for good operational implementation are:
- The reduction by the provider to the smallest possible selection with high integration
- Automation of services
- Adherence to process standardizations

Next Steps

The "MSP Journey" project is being extended, and if you still haven't registered yet, then you can register here and not miss another new set of findings:

https://msp-journey.com/

Objectives

Starting Situation

Even if the market oracles talk about constantly growing security budgets, this isn't automatically reflected in growth curves within the channel. There's a perpetual feeling within the channel that the growth should be coming more quickly. Why is that so?

- Customers for security aren't as easy to acquire as the budget predications by market researchers might indicate. This is because they are being asked to spend money on guarding against an invisible threat without necessarily gaining a business advantage from it. We start by talking about costs, and that's not so simple.
- There is a growing number of security solutions, platforms, and tools. In some cases system vendors have 10 different individual security offerings. "What does the customer really need, and how do the solutions fit together?" can be a complex set of questions.
- In some cases, security services overlap with other MSP portfolio offerings such as managed server and managed firewall. As such, the question arises whether the security field is its own section of the portfolio, or whether it should be taken up in my managed services.
- Security solutions are technologically challenging and difficult to master. To what extent can the channel detect anomalies on its own and is in a position to react quickly and appropriately to incidents or risks? Which leads to the question: what services can I best provide myself?
- And then is it really the best idea for it to be sold as "managed"? The customer is being expected to pay significantly more each month without seeing any benefit on the business side? How can the results of managed security services be conveyed in a positive and "management-friendly" way?

We started by challenging our own project presumptions about the situation in the channel by conducting multiple webinars with 350 total participants from system vendors.

The Central Feedback from Those Surveys:

- 90% believe that customers do not understand security solutions and the benefits they bring.
- Approx. 40% of the participants saw sales communications with customers as a very strong challenge given the mix of complex solutions and low security requirements.
- And almost half of all respondents perceived it as difficult to integrate security services into the general managed service portfolio.

What's the biggest hurdle for you to greater managed security service growth?

Results from a snap survey (multiple choices allowed):

Portfolio divided into many small individual services	16%
Complexity of the solutions	33%
Low security needs on part of customers	29%
High costs for customers	41%
Sales approach	37%

Hypothesis: It is very difficult to establish an independent security portfolio parallel to a general managed service offering

Results of snap survey:

I strongly agree	19%
I tend to agree	46%
I tend to disagree	24%
I strongly disagree	11%

Hypothesis: Customers have no understanding of complex technical security solutions and their benefits

Results of snap survey:

I strongly agree	36%
I tend to agree	54%
I tend to disagree	10%
I strongly disagree	0%

Procedure

Methodology

For the MSP Journey project, we focused on two survey formats and personal interviews with experienced and successful system vendors.

On the one hand, we used live surveys on the website as shown here:

SURVEY

What are the greatest sales challenges for managed security services?

- ○ Getting a conversation started about managed security at all
- ○ Qualifying the need
- ○ Displaying the risks of a security incident
- ○ Describing security solutions
- ○ Arguing for the monthly budget%
- ○ Handling potential objections

Results | Vote

A complementary analytical survey was also conducted; the following is a excerpt:

MSP Journey - Analysis of Growth Factors

MSSP - Retrospective

Your development to date with managed security services

Which MANAGED security services did you introduce and in which order?

	Not yet	At the beginning	Recently introduced	Planned
Endpoint Security	○	○	○	○
Server Security	○	○	○	○
Firewall	○	○	○	○
Mobile Security	○	○	○	○
Cloud Security	○	○	○	○
Email Security	○	○	○	○
Multifactor Authentication	○	○	○	○
ZTNA	○	○	○	○
Encryption	○	○	○	○
Backup	○	○	○	○
Vulnerability Management	○	○	○	○
SIEM	○	○	○	○
Detection & Response Services	○	○	○	○
SOC	○	○	○	○
Security Audits	○	○	○	○

More than 1,000 data points were collected between the two survey types.

6 additional extensive interviews with successful companies were also conducted for the purposes of this eB-ook. Our thanks go out to all participants.

The data and information here are gathered into three segments.

1. What are the most important success factors?
2. Is there a tried-and-tested sequence for the introduction of security services?
3. Focus tips on selected topics

Success Criteria

What Best Supports General Growth?

Strategic Commitment

86% see a strong or elevated influence on growth.

What does this involve?

We show a strong degree of subject commitment when it's not unimportant how content is achieved or implemented. We have a strategy and a strong degree of self-commitment to pursue our goal consistently and not deviate from the path. The leadership task for the importance of managed security services can be seen through clear communication internally and consistent decisions externally to the customer.

Which implementation tips apply here?

We talked to others in the company about security services, worked on the portfolio, and made strategic decisions about our target audience. This involvement of employees is important to retaining comprehension and steadfastness for the selected course in decision-making situations.
The commitment can ultimately be seen through our actions, not lip service. Do we live with a "security first" attitude and convey to the customer what we see as the necessary level of protection? Will we try to avoid implementing solutions that deviate from this, even if the customer is not ready to invest sufficiently in security? These situations are the test of our dedication and commitment.

Technical Competency in the Sales Force

83% see a strong or elevated influence.

What does this involve?

The sales force provides real value and benefits to the customer through their consultation. They are there to do more than just break the ice. For smaller system vendors in particular, where the business manager is also responsible for sales, this has a notably positive effect. For larger firms there is a certain risk that the sales team will be unable to communicate the complexity of the issues at hand and will be unable to estimate the concrete customer situation. Customers often notice this, which can also create problems downstream in the interplay with the consultants.

Which implementation tips apply here?

The two recommended steps for a technically competent sales force are constant further training and education and good internal coaching by the sales management team. Trying to easy the load on sales by bringing experienced security consultants on board can be both a blessing and a curse. While it provides important content for the customers, it can also remove the impetus for the sales employees to improve themselves. As such, it's important that, in questionable cases, sales be allowed to conduct the initial consultation on their own.

The Right Target Audience for Security Awareness

66% see a strong or elevated influence.

What does this involve?

The more the customer relies on the availability in the IT systems and customer data, the more crucial that these be secured managed security services. MSSPs who settle on a highly concrete target audience have an easier time placing their services and helping the customer. It's an essential first step to optimizing your own offerings and processes for the customer. If I look to serve doctors or accountants as a focus target audience, then I'll establish solutions that fit those respective target audiences as closely as possible. The target audience does not inherently need to be defined in terms of industry; they can also arise from a homogeneous problem scenario served by a common solution, whatever the customer industry.

Which implementation tips apply here?

There is no obligation to settle upon a specific target audience or industry, even if that is a tried-and-true model for success. For those who do not wish to take this path, there is also the exclusion principle. Instead of concretely defining whom I will work with, it can be simpler to define for whom I do not wish to work. For example, security services may only be suitable above a certain employee head count. Clarifying these issues in advance boosts targeted growth. The statement "our security services are suitable for all customer sizes and scenarios" offers no clarity or control options, and thus should be avoided.

The clear strategic commitment within the company

- **None:** 4%
- **Little:** 8%
- **Moderate:** 21%
- **Strong:** 67%

A technically competent sales force

- **None:** 4%
- **Little:** 13%
- **Moderate:** 39%
- **Strong:** 43%

Customer assessment that secure IT is an absolute must

- **None:** 0%
- **Little:** 33%
- **Moderate:** 33%
- **Strong:** 34%

What Boosts Effective Implementation?

Provider Selection

What does this involve?

Successful managed security service providers reduce their catalog of tools and platforms as much as possible to promote harmony within the components, even if this occasionally means sacrificing some functionality.

Which implementation tips apply here?

Two paths support these success factors. Everyone in the team should share the attitude that a high degree of standardization and automation are more important than individual functionality. Otherwise you end up in too many internal meetings on pure feature discussions. And when checking during vendor selection that initial security services such as endpoint protection and firewall are in place, be sure to also review that the provider offers further services and assess their long-term strategy.

Service Automation

71% see a strong or elevated influence.

What does this involve?

A high degree of competency is required to connect individual security tools with other IT management solutions such as RMM or alerting tools, and to automate processes across all systems. Beyond this, reactions to events can be automatically activated and reviewed.

Which implementation tips apply here?

A high degree of readiness to invest early in automation is required, even if one's own customers are immediately ready to mirror that same investment. Scaling and growth, including in the profits, are ultimately the positive effect from that investment.

Another implementation opportunity is to outsource entire services as managed service providers as well. For example, Managed Detection and Response (MDR) is an offering that many system vendors don't offer themselves within the channel, but rather integrate as a complete service.

Process Standardization

What does this involve?

Care must be taken that the customer receives the same workflows and processes, with few, if any, exceptions permitted.

Which implementation tips apply here?

It is recommended that procedures be considered in advance and harmonized together within the team. Such as the handling of tools and solutions that haven't been mastered in full or even in part. The path to replacing these for the customer, so as to work with one's own standards and processes, may be discussed prior to market launch.

Strong automation and integration.

- **None:** **13%**
- **Little:** **26%**
- **Moderate:** **26%**
- **Strong:** **35%**

Stages of Development as Managed Security Service Provider

Stages of Development as Managed Security Service Provider

One important question in the surveys and interviews centered around which security services were successful for the launch into this business. This eBook hopes to help system vendors who are still in the early stages of the own development.

Based on our findings to date, growth trends can be divided into three phases.

1. 'Starter' with the first three to five well identifiable Managed Security Services
2. 'Grower' with an additional three to five services
3. 'Professional' with additional individual services depending on the corporate orientation

Which Managed Security Services Can be Established from the Start?

Our surveys showed a high degree of overlap between the initial introduced services. The phase we define as 'Starter' lends itself to the following managed security services. The percentage indicates how many of the respondents introduced this service from the start

- Endpoint Security: 77%
- Server Protection: 76%
- Backup: 60%
- Firewall: 55%

Another note for the start phase is that the onboarding of the technical team and the fact that the automation and integration in the existing dashboards for these services should be implemented before offering new services from the many other potential options.

Which Services have a Positive Effect on Earnings Trends?

Companies that are still in the early stages should strongly consider implementing precisely the four starting services from the survey of managed security services, as these were assessed as having the biggest positive influence on revenues.

- Server: 80% high or very high.
- Endpoint: 77% high or very high.
- Firewall: 65% high or very high.
- Backup: 50% high or very high.

In other words, successfully selling these services in the managed variants pays off, and can be pursued on the market until the company has reached a sales and technical level that allows them to shift into the Grower phase.

Where Do Things Go From Here?

The second growth phase—which we designate as 'Grower'—is marked by four security services that the successful vendors built up as a second step:

- XDR
- Mail
- MDR
- MFA

There is strong potential for upselling in the security environment, as these services are related to existing benefits. Even if the starter services are offered as a bundle or a per-user price, the Grower services can then be offered as individual add-ons.

For most small- to mid-sized customers—including those without their own IT department—these four services are easier to conceptualize, and email security and multi-factor authentication in particular are well accepted on the market at this point.

With that said, there are also a variety of other security services that can be placed as the managed variant. As part of this third phase, called 'Professional', the complexity of the services rises, and the customers who benefit from them tend to be larger. These security services can represent outstanding complements for co-managed services operated by internal IT departments.

Examples of this include:

- Cloud Security
- SIEM
- ZTNA

Once this Professional phase has been reached, then it is helpful to analyze customer bottlenecks by talking with the customer directly and soliciting structured feedback, and then initiating needs-guided redevelopment.

Six Focus Tips from the Interviews

"Our concept is also based on the pillars of Basic, Standard, and Premium. The Basic level contains everything that we see as essential, meaning most security services. What's notable is that even the smallest package already includes a SOC solution. For us that means that alarms aren't handled by our technical specialists, but rather the notifications are passed on to the expert team at Sophos."
(Markus Riesenbeck, Riesenbeck-IT)

100% MSP or Bye-Bye – with Markus Riesenbeck

If you look back on your journey up to now, what was the most important strategic decision that you've made? What had the most positive effect on your development?
It's been a long road, of course, but the biggest breakthrough and absolute game changer from my point of view was the point at which we said we would move 100% to managed services. We ultimately conveyed our service concept to all of our existing customers, because we are 100% convinced that it's the ideal and sensible way to secure customers even in this day and age, and to prepare for current challenges. That was, from our point of view, the most important point and brought in the most momentum, because we simply had more opportunities and could concentrate fully on them. And so it had the greatest impact for the team.

You focus on a specific industry, namely physicians. Has working that particular industry meant that you as experts had to incorporate certain things into your security topics?
We work with highly sensitive data. Yet the highest protection class for civilian use as dictated in the European Data Protection Regulations is not always taken so seriously by the health care industry. We have harmonized our concepts based on the health care industry, namely: telematics infrastructure. There are special networks, which in turn need special treatment, such as in separating networks, for example. Or medical technology manufacturers, where we can define who gets access to remote maintenance functions.

Video of the Interview

MSP-Journey – The Podcast

https://msp-journey.de/im-gespraech-mit-markus-riesenbeck/
https://msp-journey.de/msp-journey-der-podcast/

"The key for that shift to selling managed security services was the path into the cloud. Because with that the customer saw that: "I'm always up to date, that's what I want, and I don't have to even make a huge expenditure for services because no classic updates are needed."
(Marc Hurrelmann, Midland IT)

Cloud Services Drive Managed Service Development – with Marc Hurrelmann

In the seven years since you've implemented managed security services: what have been the biggest success factors for you?

While this probably applies to pretty much all projects, it's ultimately getting your own team on board in a positive way. When you're starting on a journey, it's very helpful to have a clear destination. Why am I really doing this, and what can I expect? We ended up putting together a team from various departments, and thus had everyone from accounting, marketing, and sales to engineering involved. We worked like an expanded product management team, and within that circle we fleshed out the service we wanted to offer.

What were the most important managed services for you at the start, the ones where you said: Here's where we're going to get started?

In the security environment, that was at its core the classical endpoint and the area of server protection. One essential factor for us from the beginning was implementing the switch from reactive management to proactive activity. We didn't just want to become active when someone requested something.

The key for that shift over to selling managed security services was the path into the cloud. Because with the cloud service I've already achieved something tremendously important: an "always up to date" platform. That represent enormous added value, and also serves as an incentive for customers, who can always be certain that their solutions are state-of-the-art. And they don't have to spend a lot of money for services, because there are no updates that need to be installed in the classic sense from us as partners. Working from this foundation, we started with the topics of anti-virus and exploit prevention, and then worked step-for-step toward other security services from there.

Video of the Interview

MSP-Journey – The Podcast

https://msp-journey.de/im-gespraech-mit-marc-hurrelmann-midland-it/
https://msp-journey.de/msp-journey-der-podcast/

"Beyond the technical factor, what does the solution offer right now in terms of the actual focus — for example, how good is a data backup solution at the technical level — that matters a lot to us: How can we efficiently manage the solution as a MSP? How can we roll it out efficiently? How can we monitor it out efficiently? None of our services are offered without central monitoring."
(Olaf Pelzer, Comp4U)

We Don't Offer Services without Central Monitoring – Olaf Pelzer

You've said that customers would be overwhelmed if they had to actually manage all of the services. I believe that it's not so simple for system vendors either. What's your view on the matter?
One very important selection criterion is management of the central platform. That's why we didn't select one of the really large RMM vendors, which in turn means that queries and monitoring abilities can be tailored precisely to our needs.

In the end it turned out that, just as an example, the firewall monitoring that we used was actually the one the manufacturer recommended. And through this integration of the technical monitoring, we achieved precisely our goal of being able to identify problems very quickly as they arise. We take care that the solution simply works, including all aspects surrounding that. But we also try to ensure in that same environment that we don't give the customer undue benefit. What I mean by that is: our standard solution establishes secure operations, and we make sure it works. That's not the same as a flat rate with an "all you can eat" mentality. That would be much too expensive.

Video of the Interview

MSP-Journey – The Podcast

https://msp-journey.de/im-gespraech-mit-olaf-pelzer-comp4u/
https://msp-journey.de/msp-journey-der-podcast/

"Above all else, managed services have ensured that we spend significant less time posing the same question to the customer year after year: Can we pitch you on something that you already have? And we wanted to get out of that cycle and deploy our sales talent in places that made more sense."
(Manuel Neubecker, klip-asca)

Managed Security Services Let Us More Effectively Deploy our Sales Team – MSP Journey Interview – with Manuel Neubecker

What in your view are the positive success factors for your current position?
Once it became clear to us that we wanted to pursue this path, we ended up spending significantly less time posing the same question to the customer each and every year: Can we pitch you on something that you already have? Do you want to keep using it or do you want to stay being protected? We wanted to get out of that cycle and deploy our sales talent in places that made more sense. That was the gateway for us to eliminate that ritual, but naturally also to build a bridge toward the point where the customer can expect not just to get a sales pitch on one product or another, but rather a solution that works.

How is it with you and your region in terms of well-known security incidents?
There was a relatively high-profile case in Kaiserslautern that the press picked up on and which the company in question handled relatively openly. Above and beyond the obligation to notification, the company also attended an event that we held a few weeks ago and talked openly about it. Their motto was: we were affected, we've crawled our way out of the crap, and we are now basing things on security. A simpler level of protection was previously in place. If you look at anti-virus or firewall systems, in many cases classic small and mid-sized firms don't have an IT department that can take care of things 24/7 and who can proactively check for attackers. Other solutions are required, other managed services. And that was also the path taken by that customer once they had sorted through the various issues.

Video of the Interview

MSP-Journey – The Podcast

https://msp-journey.de/im-gespraech-mit-manuel-neubecker-klip-asca/
https://msp-journey.de/msp-journey-der-podcast/

"Just as you need good people in your engineering department to bring managed services to life, you need to transport just as much energy and effort in the marketing and sales process. You need the right people for that."
(Max Pfister, niteflite networxx)

You Need Good People in Marketing Just As Much As in Engineering – MSP Journey Interview – with Max Pfister

You're very active in online presentations of security as a topic, to raise your profile and to grow by acquiring new customers. Can you please describe how you approach things within that framework?
When you're at the cusp of 20 employees, word-of-mouth marketing alone isn't nearly sufficient. And that's why I said that we need to engage in active customer acquisition, because we want to keep growing.
We used last year, a Corona year, to slow things down and ask ourselves: How are we even going to go about acquiring customers? How does modern marketing work? I've learned that inbound marketing is the key to success nowadays. And that's naturally driven through channels such as social media, LinkedIn, and Xing. And what we deploy at a concrete level are in fact security checklists, webinars, expert talks, and social media posts that trigger those things. We animate people to initiate contact with us. And from that point we naturally try to identify: How can we, with our portfolio, help them and how can we turn a customer into a fan who then says, "I'd like to work with you long-term."
It's ultimately probably also important to pursue those leads in a structured and clear manner. How have you addressed issues of process?

We were very structured in our managed services. The muddle and disorganized part was in fact our sales processes, and that required some learning. Just as you need good people in your engineering department to bring managed services to life, you need to transport just as much energy and effort in the marketing and sales process. You need the right people for that. One general manager can't possibly do it all. And that's where things kept cracking up.
For us it meant, I now spend 3/4 of my time in marketing. And we have three inside sales employees and a real account manager. We also bought an "expensive" marketing software license and defined a process. And since then things are working well. That's the heart of it all.
Otherwise even the best content is useless. Some one-off measure or Facebook campaign does nothing for you if a really clear process for handling and executing it isn't in place. For us that means that at the moment when somebody downloads a document or registers for a webinar, they get called an hour after that webinar is finished. Experts refer to that as a 'small product.' We always try to pitch the product, and that's the gateway to an expert consultation. The first step is the special offer, an hour talking with our engineers or security architects.

https://msp-journey.de/im-gespraech-mit-max-pfister-niteflite-networxx/
https://msp-journey.de/msp-journey-der-podcast/

"Zero trust is a truly fascinating topic that we'll be dealing with a great deal in the coming years. ZTNA isn't a product at all. It's a philosophy. (Tobias Waltemode, IOK GmbH)

IT Security is Corporate Security and Has Top Priority – with Tobias Waltemode

What have you determined about how security topics can be integrated into your overall managed service portfolio?
We come from the classic "best of breed" approach and made firewall, antivirus, and email security our focal points, addressing them in various stages of maturity depending on the customer situation and desire, and then expanding and operating them for the customers. None of which really fit the times any more, because we could see that we needed to become more agile. In current discussions with customers, we often first talk about security and then the rest of the infrastructure. I think that in five years we'll only ever start by talking about corporate security. Only once we feel that we're on the right path will we then focus on other topics. Security first, and then probably productivity. If we live today from selling and operating servers and storage and network systems for our customers, then from our viewpoint we can't do that going forward without a focus on security. That was a paradigm shift that we first needed to internalize.

How do you understand your holistic security concept?
Customers typically come to us and have some active situation for which they need active assistance. Then we typically begin with a comprehensive audit of the environment. When we visit the customer, we look to see: Where is the server room? Is the door locked? Who has access to the network racks? Can I simply plug my laptop into a network jack or the WLAN and immediately access the core of the company, the data? Those are the banal topics that we start with, after which the audit goes relatively deep into the technologies that we want to offer to our customer as service providers.

Video of the Interview

MSP Journey – The Podcast

https://msp-journey.de/im-gespraech-mit-tobias-waltemode-iok-gmbh/
https://msp-journey.de/msp-journey-der-podcast/

Checklist for

self-assessment of growth factors

Checklist for Self-Assessment of Growth Factors

For those who are wondering where exactly to get started, we've prepared the following self-assessment checklist.

Please assess the factors from this eBook in relation to your company, on a scale from '1 = not at all' to '10 = optimally handled'

Question	Your score from 1 to 10
How high is the strategic commitment from your executive team?	
How high is the strategic commitment from your technical staff?	
How high is the strategic commitment from your sales team?	
How strong is the technical competency in your sales team?	
How clearly have you defined the target audience for managed security?	
We use services from as few different vendors as possible.	
We have a strong degree of automation.	
We have a strong degree of standardization.	
We have been successful with the Starter services.	
We have been successful with the Grower services.	
We have developed a clear service development strategy for new services.	

What concrete steps can you take right now?

What Concrete Steps Can You Take Right Now?

We very much hope that this eBook has provided concrete inspiration on how to improve your managed security services.

If you have questions about this content, or need further assistance, please don't hesitate to contact our MSP experts below.

We wish you all the success on your path to growth with managed security services!

CONTACT

United Kingdom & Ireland: MSPSalesUKI@sophos.com
Benelux, France, Italy & Spain - MSPSalesWER@sophos.com
Nordics & Baltics - MSP.Sales.Northerneurope@sophos.com
Middle East & Africa - MSP.Sales.MEA@sophos.com
Eastern Europe -MSP.Sales.Easterneurope@sophos.com
DACH - MSP.Sales.DACH@Sophos.com

Contributors

Many thanks to our cooperation partners sophos
Sophos is a global leading provider of next-generation cyber-security, protecting more than 500,000 companies and millions of consumers in more than 150 countries against the most modern and refined of cyber-threats.

Using threat intelligence, AI, and machine learning powered by SophosLabs and SophosAI, Sophos offers a broad portfolio of advanced products and services to protect users, networks, and endpoints against ransomware, malware, exploits, phishing, and a variety of other cyberattacks.

About the author:

Olaf Kaiser worked for 15 years with system vendors of 150 to 250 employees, holding management positions in sales and software development. As a business director, he successful grew several firms.
This includes the largest German IT network, iTeam, with 370 locations and 7,000 employees, as well as acmeo, a specialist distributor in the cloud environment with 10 mn. euros in annual revenues. In 2016, Olaf Kaiser joined UBEGA GmbH as managing director and since then has been personally engaged as a consultant for system vendors.

MSP JOURNEY exploring the truth.