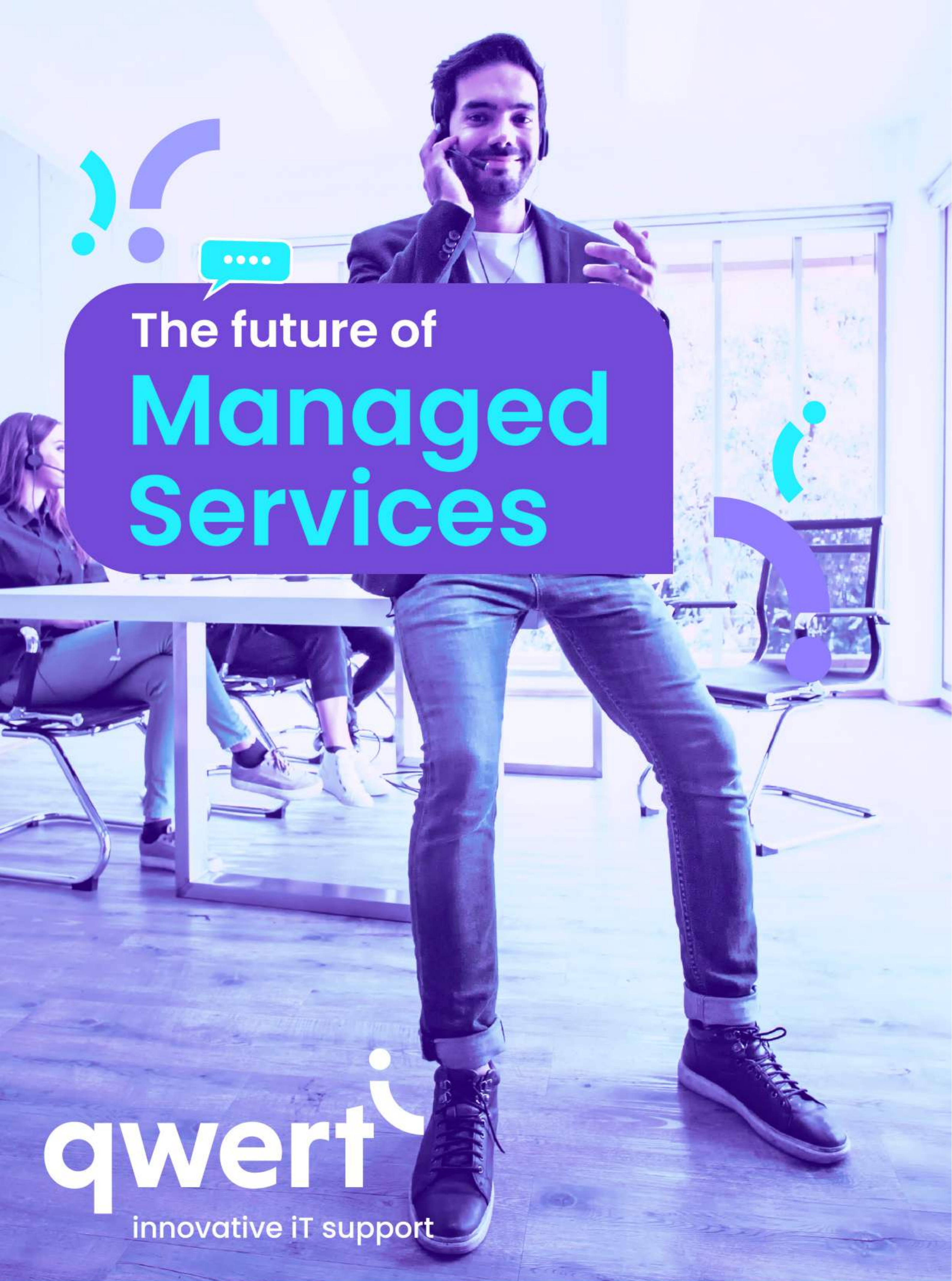


The future of Managed Services

qwerti

innovative iT support

Contents

The future of Managed Services

Managed service providers (MSPs) have been around for long enough for most people to have a fairly solid understanding of what they do. While not always the best source for information, Wikipedia has a useful definition of managed services which leads succinctly to the point of this document.

“Managed services is the practice of outsourcing the responsibility for maintaining, and anticipating need for, a range of processes and functions, ostensibly for the purpose of improved operations and reduced budgetary expenditures through the reduction of directly-employed staff.”

That’s what MSPs have been known for and how their value has traditionally been measured.

Those days are over.

MSPs that continue to provide the value that a modern business needs are more accurately described as MSPPs, or managed service professional providers. qwerti appreciates this and is built solidly around the understanding that the old-school break-and-fix type support is rapidly becoming obsolete. As part of this understanding, qwerti has and continues to, invest in systems and skills that would service a top-100 blue-chip enterprise, and bring this level of service to all businesses.

In other words, the modern MSPP is an expert in strategy, security, and cloud computing and provides access to new technology, which goes well beyond the classic, and frankly old-fashioned, MSP that outsourced skills to free internal staff to work on other functions. The world has moved on and businesses need a trusted advisor.

Without any doubt, a modern managed services provider must be an IT advisor. It must deliver analysis and many more products across the IT ecosystem so that there is no fragmented and siloed approach to services. It must be proactive in its monitoring, identify faults at the source, have visibility (and ability to act) across the entire IT real estate, and offer a virtual CIO (VCIO). Smaller businesses just cannot afford CIO skills and so instead have generalised IT managers and because of this, their strategy ends up lagging behind the business objectives. A VCIO solves this problem.

In summary, the modern, relevant MSPP must focus on three very important areas:

1 **SECURITY**

The MSPP must have all the tools in place to identify where risks are and recommend how a business can mitigate those risks.

2 **COST SAVING**

The MSPP must be able to help businesses mitigate against potentially exorbitant costs, especially in poorly managed cloud services. It must ask: What are you doing in terms of wastage in your environment and what are you doing to drive that down, particularly those customers moving to Azure, AWS and Google, for example, who have no way of controlling their spend.

3 **VCIO (IT STRATEGY)**

The MSPP must be able to align a customer's IT programmes with where the business is going. It must ask: how do we align technology with the business? It must ensure that after a system - or systems - are put in place that the business stays true to the path of continuous improvement. This strategic guidance or compass is provided by the VCIO team that ensures that informed business decisions are made based on risks and weaknesses assessed, and in line with overarching business objectives.

Being part of VOX for so many years, and now supported by the might of Vivica, the qwerti team has grown and morphed into this specialised MSP, or MSPP.

How Managed Services have evolved

Most people reading this will remember a different world just ten short years ago. In most cases, there was a data centre, on-site servers and users who worked within that enclosed safe zone.

This on-site office meant that there was one firewall. A user would send out a ticket if something went wrong and a technician or engineer would walk up or down a flight of stairs and in one visit would resolve the desktop or server problem and that would be the end of it.

How that world has changed!

Now the process has conglomerated into a world of managed services that is not just desktop support, but also cloud support (along with all the applications available), wrapped tightly in a security blanket. Many users sit at remote locations or at home yet the business requires the same security metrics as if everything were on-premise. In addition to this, the business needs the same level of support that it would have been able to enjoy had everything been on-premise.

This has fundamentally changed the dynamic of managed services from "break-and-fix" to "identify, remediate, consult-and-improve". This is where a managed service provider adds value to the modern business. Today the MSPP must be proficient at support for the server, desktop, data, identity and monitoring across vast spaces while ensuring a consistent security and service level no matter where the user is working.

Probably the biggest shift in the evolution of managed services has been the emergence of security being front and centre. The days of patching a firewall and installing an antivirus are long gone and this approach is simply not good enough in 2023 and beyond.

Another area of significant evolution has been the move to the cloud. This refers not only to a business moving its infrastructure into the cloud but also to all the applications that are springing up almost daily.

The third shift has been the trend of working from home. While some businesses had flexible working arrangements, the vast majority were designed around an office space where users would sit in their work areas within a network, behind a firewall, and the IT team could physically see the entire environment. If a user complained about connectivity then a technician would check the firewall or the WiFi and access points and quickly identify and fix the problem. In many instances today, the same user is working on an unsupported home network and the IT team has no visibility of the user's connectivity, which naturally introduces an entirely new set of challenges, most notably security.

The fourth major evolution has been the emergence of strong compliance regulations such as POPI. Information technology must take the lead in processes and compliance due to the very nature of how business has evolved in the fourth industrial revolution. Looking to the future, this evolution is heading towards a space where the MSPP will set up processes and document them for the customer and make sure that its users are trained in these processes and adhere to them.

Previously, this compliance would be handled by a specialist compliance company that would take a business through an ISO certification. As we head into the future, MSPs are going to have to take that on internally.

All of the above has meant that the MSPP has had to evolve its competence and expertise. Complexity, a natural byproduct of innovation and the evolution of computing, has skyrocketed. Besides being complex, there are far more products than before. Previously, an MSP would look at the desktop and server, the cloud provider would manage the cloud and a security advisory would look at the firewall. Today, an MSPP must handle all of that. Essentially, we are talking about one provider, or advisory, as opposed to disparate providers working in silos. This is crucial to enable speed and agility.

This means that effective MSPPs today must manage cloud storage, backup, hardware procurement, change management, continuity, security, systems, monitoring, help desk and improvements. It must be an expert advisory with a holistic knowledge of the IT ecosystem so that it can provide better insights and service than a provider that only has a grasp on one leg of the ecosystem.

Naturally, because of the way managed services have evolved, the entire engagement model is shifting, too. Previously, service level agreements focused on mean time to respond and repair, and uptime as a percentage. This transactional approach is shifting into an advisory space, where the modern MSPP is engaging with the customer, analysing the business and designing the IT infrastructure to meet business requirements and best practice.

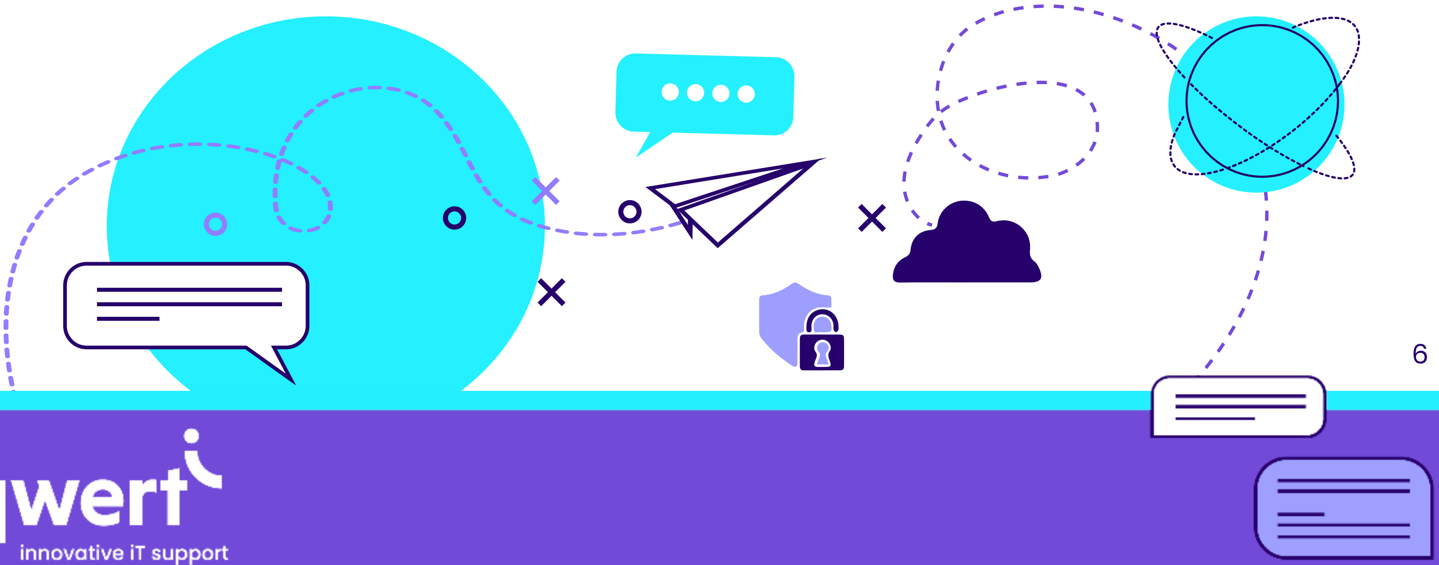
The modern evolved MSPP doesn't go into an environment and propose a product. It must embed itself and understand the business and how it operates, and then focus on the requirements. In doing so, it can be said that it plugs in a service to meet those requirements as opposed to plugging in a product.

Naturally, this has changed the way an MSPP must source and train skills. Gone are the days when it was fine to have technicians focused on their siloed areas who didn't understand how the onion wraps and affects the bigger picture. In those days technicians were professionals in one area.

Today, the MSPP technician needs to be a multi-tool: he or she must understand the firewall and how it talks to the server, understand the server and how it talks to the user, and then understand how the user experiences the environment.

A typical IT manager in years gone by would have a fairly decent understanding of the different parts of an ecosystem and would therefore be patient when technicians were troubleshooting. Nowadays, when desktop users directly log a ticket, they generally don't have the same understanding of the complexity and layers and therefore have radically different expectations of technicians. Essentially, this leaves the MSPP with two teams. One that can manage user expectations at the coalface and deal with their frustrations as they work to solve issues, and another team with highly skilled engineers who are kept in the metaphorical dark dungeon to work on complex problems and deep solutions.

It is abundantly clear that managed services have evolved rapidly in the past few years and will continue to evolve apace. There are a few challenges that businesses face making MSPPs all the more vital to their successful functioning. We'll unpack some of these challenges in the next few sections.



Remote Working and Managed Services

The shift to hybrid and remote working has large implications for end users because CIOs and VCIOs need to develop strategies to accommodate the new disparate workforce, including all their outsourced agreements and end-user computing services.

Remote working arrangements impact technology for users in a variety of ways. The most obvious and urgent problem is that many employees need to upgrade to new devices just so that they can continue working. For example, a company may standardise an I5 processor with 8GB Ram and solid-state drives to enable users to work seamlessly across cloud platforms and collaboration tools. Businesses have found that employees still using older or lower-spec devices are having difficulties with cloud-based collaboration tools which negatively affects the flow and productivity of entire teams. Businesses are at a crossroads - either they must provision new devices or update existing assets.

Besides the actual ability to do their work, companies cannot control what users load onto their devices, meaning they must invest in remote monitoring and management tools and antivirus software to protect the company's data. Beyond this, they need to consider tools to proactively monitor network activity as they can't just dispatch a technician quickly to someone's home - they must be supported remotely. A VPN is non-negotiable so that people can connect to systems securely and not unnecessarily expose businesses to even more vulnerabilities.

When you look at the above, never mind internet backup devices to ensure connectivity during load shedding, and then add on the fact that there needs to be a managed firewall, it becomes clear that costs start piling onto each other and this is too much for many businesses.

Smaller companies may feel that they can get away with free versions of collaboration tools, but as they scale they are going to need to upgrade to the paid-for versions of those tools so that they can secure all the content generated in the business. This, naturally, works on a subscription model, much like every other cloud-based application. Once a business opens the cloud taps, if it is not well-controlled it can lead to a cost crisis.

How remote working affects MSPs

It would stand to reason when considering all of the above, that hybrid and remote working directly impacts MSPs and their ability to service businesses. Remember, not too long ago, an MSP would always have technicians on site, be able to see everyone and every endpoint, and go straight to the problem and fix it on the spot.

Today, there's an influx of tickets arriving at the MSP's virtual service desk. This becomes significantly more complicated when the MSP cannot see the cause of a connectivity issue and needs to dispatch physical support. Businesses bear the brunt of this because call-out fees are significantly more per hour than the usual virtual support as they must go to the location and physically diagnose a problem and fix it. Besides this, there is a time lag which is damaging to productivity and morale.

The modern, agile MSPP will have pre-empted this and invested in enterprise-grade tools, like qwerti has, to be able to offer a comprehensive and proactive service to customers. For example, qwerti has prioritised intelligent tools to be able to provide more value in the form of remote monitoring of networks, connectivity and user devices. This is the opposite of being reactive and has been made possible through the launch of Vivica, which has enabled us to take our desktop monitoring to a new level.

We've already discussed the fact that remote working leads to an influx of tickets, but the responsibility lies with the MSPP to ensure that it has conducted thorough due diligence on its customers so that it can support them properly.

A modern, relevant, MSPP must have remote monitoring tools that are adaptable and able to check the connectivity of all users. This enables a monitoring desk that can attentively deal with real-time problems.

The RMM tools show real-time CPU, memory and RAM usage, which means we can proactively inform users when their devices are being over-utilised and need to be updated. The ability to provide this level of proactive service remotely naturally saves on human resource costs such as the need for a permanent IT manager or technician. Customers save up to 30% on costs by outsourcing their IT needs to qwerti.

Our Simple Network Management Protocol feeds information straight into our network monitoring tool and depending on thresholds we set up for each customer, the tool creates alerts on the monitoring desk. This triggers a trend analysis to see if fibre is down in the area, for example. If necessary, a network engineer is immediately dispatched, bypassing the need for a desktop engineer first. Essentially, it is about using tools to give us deep insights to perform proactive remediation and improve response times. Beyond this, the VCIO service gives customers enterprise-level guidance and strategy all aimed at ensuring that their IT is aligned with best practice and business objectives.

qwerti has also taken privacy exceptionally seriously, and so all activity that takes place on customer computers is recorded - for the customer's safety and our own.

When all is said and done, whether large swathes of the workforce move back to the office or not, the world has changed. Remote and hybrid working has forced rapid digitisation and additional considerations, making the use of MSPPs a compelling competitive advantage for businesses seeking to enjoy maximum efficacy at a well-managed cost.

IT skills shortage and Managed Services

The general IT skills shortage in South Africa is well known. It has been a challenge for companies for many years but has been exacerbated by the pandemic and the rapid shift to the cloud and remote or hybrid working environments.

On the other hand, it is precisely because of the skills shortage that MSPPs are well-positioned to add significant value. Rather than embark on the time-consuming and costly exercise of sourcing and then onboarding full-time IT talent that works according to their agreed shifts, MSPPs can offer a fully outsourced IT skill set available 24 hours a day. Through economies of scale, the strong MSPP will provide access to the best security, compliance, networking and engineering skills at a fraction of the cost.

Let's call a spade a spade. In an environment where there are far fewer highly skilled IT people than there are open positions, potential employees hold the leverage, able to demand ever-increasing salaries. Beyond this, with talent always at risk of being poached, businesses can find themselves in the unfortunate offer and counter-offer scenarios.

Perhaps this is easier to absorb at an enterprise level, but smaller organisations simply cannot afford to be in this position. Consider something like an electrical or plumbing business that has a few staff in an office and a few teams out in the field providing services.

This business, although not large, needs to invest in IT as there are great advances in what's available nowadays such as scheduling appointments, taking pictures and logging directly with insurance companies, and more. In order to be able to do this they need to hire an "IT person", that acts as an IT manager and technician. Then, they will need to spend money on someone proficient in firewall and networking, as well as bring in a security expert and quite possibly another to set up their Microsoft environment.

A small to medium company can easily spend in the region of R700,000 to set up a small server, purchase a firewall and switch, and have one or two access points. On top of this investment is the need for an ongoing IT resource cost of at least R25,000 to R30,000 per month, excluding benefits.

Compare this to an MSPP such as qwerti coming into the picture. qwerti can assure the customer that it will place a skilled person on-site, who has the backing of the entire qwerti team of experts, who can set up and manage the firewall, which qwerti will lease to the customer over a fixed period. In effect, this is an enterprise-level support function offered to a small business and it is made possible by the fact that qwerti is able to deploy slices of all the enterprise-grade technology and human capital investments it has made onto environments of smaller businesses.

Insourcing versus outsourcing

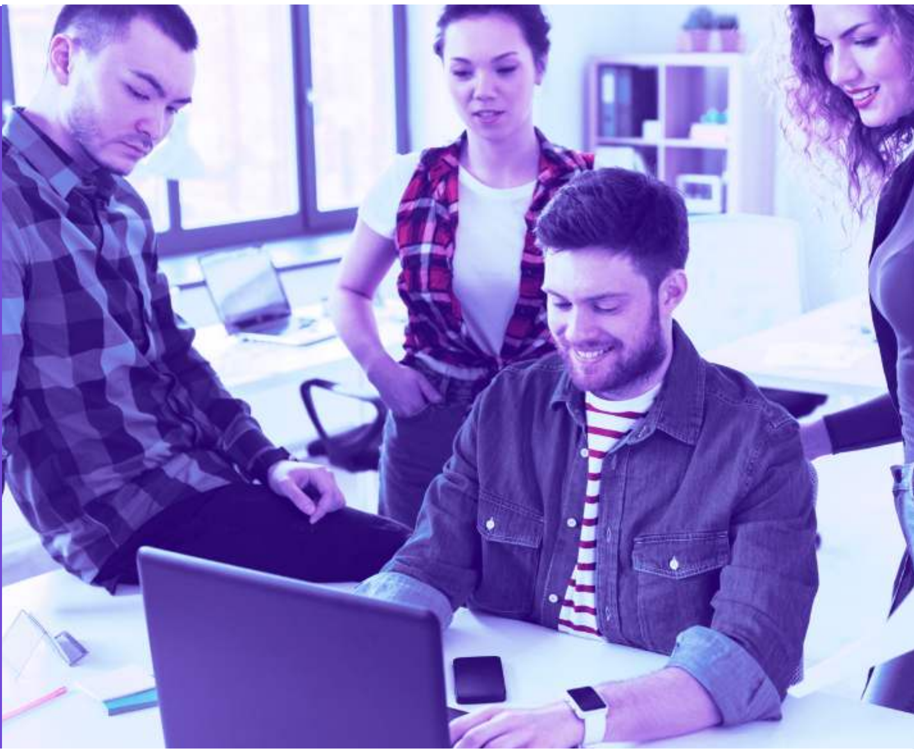
Over the years, the IT industry shifted to outsourcing work to massive international centres such as India in an effort to keep costs down and not have to worry about skills shortages. However, time differences and language barriers proved to be disruptive, as were things such as support calls to do work on laptops at 2 am, among much more.

And so, the IT industry looked towards insourcing, as it had done in the past. However the industry has changed and the skills shortage has become far more pressing, while cybersecurity and compliance have become more important than ever before. It is here that an MSPP steps up - for example, qwerti is a turnkey provider for IT and can do almost anything, within reason, that a customer requires, from the usual remote support to hardware procurement and more.

The power of a modular approach

A business such as qwerti provides turnkey offerings - it has divided up its huge human technology investments into modular services depending on customer needs. Either a customer can choose a full service, across the entire IT ecosystem, or it can decide that it merely wishes to outsource its firewall management. An agile business like qwerti is designed to support this.

With the advent of POPIA and the ever-increasing cyber security threat, an MSPP must be able to bring the level of services previously reserved for enterprise-level organisations to all businesses in South Africa.



If qwerti embeds skills into a business, it takes care of them, removing all the HR burden from the customer. This includes their ongoing training, succession and more. qwerti develops the talent pool and so whether needing support from the central support technicians or the broader team, it is always available.

Larger companies have more complex needs which are exacerbated by their inability to source relevant talent. qwerti answers this by being experts in enterprise-grade Microsoft-approved assessments.

Here we scan the entire environment and uncover all loopholes, red flags and deviations from best practice. Based on this thorough analysis, we make comprehensive recommendations. Once engaged with the customer, their own IT departments benefit from the inevitable skills transfer and learning from our highly experienced team of experts.

In conclusion, in mitigating the skills shortage, an MSPP must go a few steps further for businesses. This includes the capacity to offer enterprise-grade offerings at an affordable cost to all businesses.

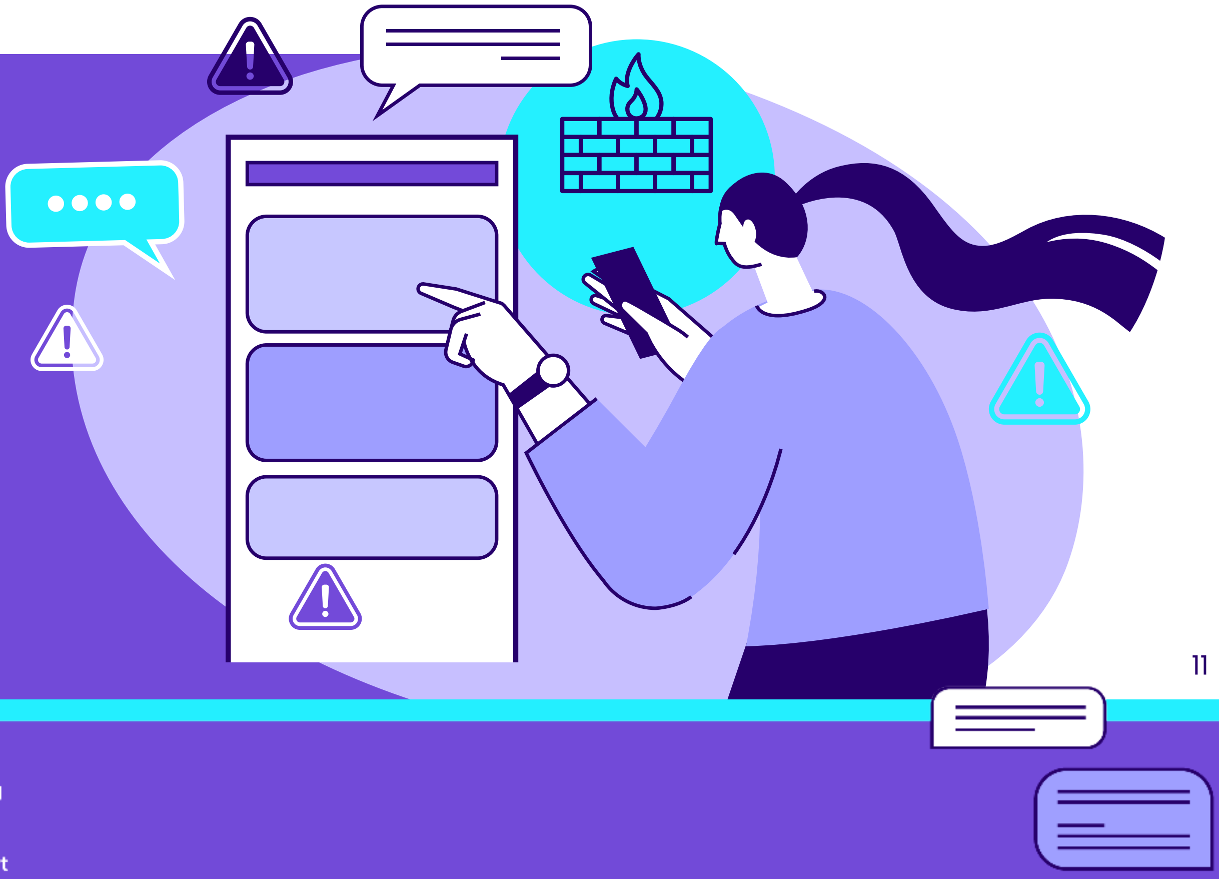
The security risk of an unmanaged firewall

A firewall is either a physical or virtual device that controls access to a company's network and ultimately its data. We live in an age where the value of data has never been higher and efforts to protect it have never been more urgent.

A good analogy to understand the concept of a firewall is to consider the security perimeter of your house. You have a gate and doors that require specific keys to unlock. You, as the homeowner, will make a copy of these keys for family members - or friends - that you trust, and to who you would like to give access to your property. You most certainly don't want the keys getting into the wrong hands. An unmanaged firewall is the IT equivalent of standing on the street corner and handing out keys to your home to anyone who passes.

We live in an information age and data is being produced and exchanged at unprecedented levels, meaning that organisations have a greater responsibility than ever before to ensure that their firewalls and other network devices are maintained and monitored by security professionals. There's simply too much responsibility on the shoulders of businesses to consider otherwise.

Three of the most common mistakes made by organisations are outdated firewall rules that create space for cyberattacks and unauthorised access, non-compliant regulations in terms of cybersecurity and improper firewall rule changes that lead to breaking business applications.



Just how big is the problem?

A 2019 Forrester survey concluded that

69%

of respondents claimed to have an unmanaged firewall in their environment

A 2021 report from Cisco stated that

86%

of organisations had at least one user connect to a phishing site

The same report highlighted that

50%

of organisations encountered ransom-ware-related activity

It is abundantly clear that an unmanaged firewall is a security risk, meaning we need to look at the factors driving decisions around managing or not managing firewalls.

Skills

An entire section of this white paper is dedicated to the IT skills shortage and how businesses navigate these challenges. The skills shortage definitely works in favour of MSPPs, especially where they are experts in managing firewalls.

The choice between insourcing and outsourcing, at its simplest level, comes down to whether a business has the skills to perform a task or not. Larger enterprises may well choose to hire the skills they need. Even then, they need to be aware of when those skills will be useful. Will it be from 9 am to 5 pm, or will they be on hand 24 hours a day? If they need this, an MSPP is likely the route to go. Smaller companies, certainly in the SME space, may not have the luxury of being able to bid for insourced skills that are becoming increasingly expensive. And so, managed services are the route to take for these businesses. When engaging an MSPP such as qwerti they get specialised skills that manage firewalls every day and in a host of different environments.

Efficiency

The last point above refers to a team of highly skilled and experienced experts. There are massive advantages to moving the management of a firewall to a service provider that specialises in, and works on, firewalls every day. These advantages are felt in the areas of ongoing and real-time monitoring, patches and specialised reporting. Being a business services provider, an MSPP such as qwerti is able to translate the reports and findings into language that non-IT people can understand, and then advise on the appropriate steps. Here, the business executives can focus on their core business while transferring the risks associated with firewalls to their service provider.

Cost versus control

If keeping costs down is important then a managed service will typically work out more cost-effective than recruiting, training and utilising internal resources. However, there are instances - especially in enterprise-level organisations in some industries - where high levels of hands-on control are more important than cost. In these instances managing the firewall internally may be the preferred option. Where businesses are cost-sensitive, the outsourced model is the route to go.
Make sure the firewall is managed
Let's be clear, today's next-generation firewalls provide good levels of protection, but in our rapidly evolving world with ever-innovative cyber criminals, or even disgruntled former staff, investing in these best-of-breed firewalls and then leaving them creates unnecessary and avoidable risk.
There is no longer a debate about whether the firewall needs to be managed or unmanaged. Rather, it comes down to whether a business can afford to insource firewall management or whether it chooses to outsource the management to a specialised service provider.