# SOPHOS
Security made simple.

# Building a Next-Gen Managed Security Practice

## IT Security MSPs: In the beginning...

We all remember the old days of Managed Service Providers (MSP). By acting as an IT security expert for companies who did not have the talent in-house, early MSPs spent significant time on-site with their clients, assessing needs and troubleshooting challenges, providing the kind of IT support many organizations could not afford or create on their own. They also had the unenviable and oft-frustrating task of managing multiple vendors for different product areas, from antivirus, email, encryption, wireless capabilities and more—a time-consuming process that tended to complicate billing and cash-flow issues.

But today's MSPs face challenges that make those older days feel almost simple by comparison.

# The next-gen MSP

The transition to next-gen MSPs comes in no small part to the changing needs of the customer. The role of the MSP has become more ingrained and pivotal to many SMBs, where the MSP can sometimes even rise to the level of a virtual CIO for some clients. The word "virtual" is key when discussing next-gen MSPs. On-site visits and standard set business hours are no longer enough—organizations need and expect their MSP support to be available on-demand, 24-7. And MSPs themselves need the capability to engage with their clients' needs from anywhere. Both client and provider alike want to, and must be, able to be agile and mobile, whether their work takes place from a distinct, brick-and-mortar office or while sitting on their own sofa in their living room.

The MSP must also be able to provide the same level of service, security, mobility and flexibility to all their clients, across the board.

Technological advancements, in terms of hardware, software, and user needs, have altered the workflow and landscape from the previous generation of MSPs. Security has become all the more complex, and the knowledge-base MSPs must have at their disposal has become accordingly more complicated, as businesses turn to the Cloud and web-based resources to manage their products. Clients are no longer tied to one machine, one server, one location, and the corresponding IT security needs of those clients have increased accordingly.

Meanwhile those same business owners, and their employees, have increased their security needs exponentially by not only decoupling from the physical office and taking their work home and on the road, but by also spreading it across multiple devices. MSPs must now have the capability to protect not just desktop computers, but laptops moving from location to location, easily portable tablets, and smartphones capable of handling the workload once limited to a desktop machine.

If the users have made their security requirements more complex by their changing workflow and creating a far more mobile business environment, the bad guys have changed the game even more. It's no longer about stealing a hard drive to smash and grab the data from the disk. Hackers and thieves grow increasingly more sophisticated in their tactics, using subtler techniques like phishing schemes and crimeware to get their hands on important data, or locking users out of their files with ransomware, forcing an organization to pay a fee to regain access to their data.

These more elegant attacks, combined with increased user online presence and, unfortunately, the eternal prevalence of human error, means MSPs must be more on the ball than ever to meet their clients' needs. Not only are your clients' end users targeted by phishing schemes sharp enough to fool even a relatively educated user, those same users have two, three, or perhaps even more devices or tools giving them access to company data and providing potential inlets for attack.

It has been a challenge for MSPs to operate successfully in this new and far more complex environment. The numerous vendors and products MSPs need to provide to cover the full range of services required has never been an easy burden to bear, but in today's fast-paced environment, managing these vendors has become a costly time-sink. MSPs work within a finite budget, and need to determine where their budgets are best spent.

There's also been a shift to a subscription model for MSP services, transitioning away from long-term contracts (which used to be the norm), a change in client needs MSPs have had to adjust to in the next-gen era. This shift impacts the vendor as well, as most vendor services are perpetual licenses rather than monthly, preventing MSPs from managing their billing processes consistently. This change impacts cash flow for an MSP and vendor alike.

MSPs do have options to save on costs, however—buying licenses in bulk or through an aggregator can ease some of the burden.

# How to be a profitable, successful MSP in the next-gen era

So what does an MSP need to do in order to survive successfully in the current market? The trick is differentiating what you provide in order to rise above the competition.

### Be a virtual CIO
Clients are entrusting the security of their greatest assets—their data—to the MSP. A successful MSP will be able to provide both the high-level and user-level guidance the client needs, acting as a resource for the answers, software, hardware, and more.

### Be a service differentiator
Meet the modern client's needs by being constantly available, wherever they are—and wherever you are—through a SaaS-based management console. The right tools will give you the flexibility to match your clients' mobility.

Next-gen MSPs must align their security strategy with vendors. Vendors, meanwhile, need to become more integrated into the MSP vendor ecosystem, developing and providing tools MSPs use to run their business (PSA) and remotely monitor and manage (RMM) for their customers.

### Be a proven security differentiator
Ensure your tools provide top of the line security and protection. Your customers are able to offer secure, uninterrupted service for their users because you've got them covered against outside threats. By finding and working with the right vendors—and by providing them with the education they need to make best use of the tools you provide them—an MSP can be the first and last line of defense against cyber threats.

### Be an efficiency differentiator and pass that efficiency on to your clients

Don't get bogged down. You can minimize the number of vendor partnerships you're engaged in to speed up and streamline your vendor management, and improve your own efficiency by scaling back on the number of unique tools you're using to meet your clients' needs. Finding the right aggregate partner—or better yet, work with a vendor who owns all the technology you'll license through them, which can be a much more efficient option than a "marketplace" or aggregator—can integrate a successful MSP's services, removing much of the manual work MSPs spend updating and managing security services.

**Another method of improving efficiency:** find a better way to manage your licenses. By using a billing and licensing option where you can distribute licenses across multiple clients in a more flexible manner—like an aggregate monthly billing option—you'll speed up the services you offer and be ready to evolve and meet the needs of your clients if those needs grow (or shrink) unexpectedly.

### And lastly, be a financial differentiator

The old paradigm of annual contracts for vendor services is no longer efficient in the rapidly changing world of next-gen MSPs. If you bill your clients monthly, you should be able to pay your own bills monthly. It just makes sense.

**A note on aggregation services:** working vendor to vendor, MSPs often pay for licenses based on devices for each service—so the same user is being charged for their smartphone, laptop, tablet, or more. With the right vendor who understands the MSP model, the MSP can instead pay for the cumulative number of services instead on a user basis, providing far more flexibility and mobility in adapting to your client needs regardless of the number of devices a user owns.

# Introducing Sophos MSP Connect

With Sophos' comprehensive portfolio of services, our MSP security program can give you endpoint, email, web, mobile, wireless, network/firewall, and server capabilities through a single vendor partner—no more chasing down multiple vendors and juggling numerous contracts. And because all of these products fall under the Sophos umbrella, they are fully integrated for enhanced protection, allowing MSPs to offer a stronger, safer level of security.

The Sophos MSP Connect program combines 30 years of industry knowledge with proven security capabilities against opportunistic and targeted security risks.

Not only are the endpoint and network solutions you'll offer to your customers integrated in a single platform, you'll also have one management dashboard, which provides a single pane of glass to see all your security licenses, and all your customer information, in one view. No more bouncing between multiple tools or management resources. A single, complete mechanism to view your clients' status, watch for risks and respond to threats through a single tool.

Sophos is 100% channel. MSPs purchasing partner-owned licenses means they only have to buy those licenses one time, and can distribute those licenses across multiple customers—no more managing numerous transactions to meet client needs.

And with Sophos' MSP Connect, you receive one monthly invoice to better align with how you're billing your own clients.

Sophos is already a leader in next-gen security, and now MSPs can leverage that expertise to provide their users with top of the line security, lower operating costs and improved operational efficiency. Acting as a virtual company leader, providing the very best in service, security, efficiency and cost—this is the next-gen MSP. And with Sophos MSP Connect, it's all within your reach.

Learn more about the Sophos MSP program at www.sophos.com/MSP

**SOPHOS**