ConversationalGeek®

Conversational Managed Security Services for MSPs

By Nick Cavalancia (Microsoft MVP and CEO of Conversational Geek)

2nd Edition

In this book, you will learn:

- The opportunities that exist for MSPs to offer security services
- How to move your MSP business towards offering managed security services
- The different types of services you can offer under the managed security umbrella

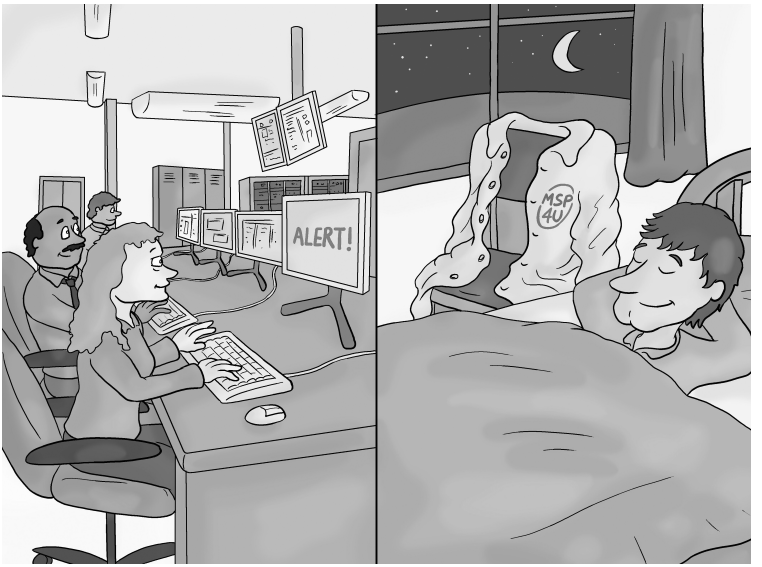
Sponsored by
Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business.

For more details visit
www.barracudamsp.com

Conversational Managed Security Services for MSPs

By Nick Cavalancia



ConversationalGeek®

Conversational Managed Security Services for MSPs

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Nick Cavalancia
Project/Copy Editor:	Ian Whiteling
Content Reviewer(s):	Doris Au
	Morgan Pratt

Note from the Author

While I enjoy knowing that most of the content I write is helpful to IT pros like you, I'm very excited about this particular eBook for two reasons:

First, the current state of cyberattacks is evolving in a way we haven't seen before; there are more players, more attack vectors, more examples of cybercrime not just running like a business, but running like an efficient business. So, having an opportunity to encourage you to offer cybersecurity services that will have an impact feels timely and necessary.

Second, having been an MSP owner myself, I know the struggle of trying to offer new services, augment existing ones, and looking for ways to both increase revenues while actually helping the customer. So, being able to discuss a way for you to augment the technology, people, and processes that make up your cybersecurity services in a way that also takes your offering to a higher level of delivery, efficiency, and efficacy is super exciting from a business standpoint.

I hope this eBook gets you as excited about the prospect of offering cybersecurity services that will truly assist in keeping your customers safe while doing so in a way that also improves your cybersecurity services!

Nick Cavalancia
Microsoft MVP and
CEO of Conversational Geek

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend, and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Greetings. Within these boxes I can share just about anything on the subject at hand.

Read ’em!

The Evolving Need for Cybersecurity Services

"Why do you think WE need cybersecurity services?"

Let's face it – without you, *SMBs are screwed*. These small businesses are trying to operate at a time when we're experiencing never-before seen growth in every aspect of cyber threats. Take the number of phishing attacks alone – in the last year, the world has seen a 150% growth[1]. Add in the growth in the number of Cybercrime as a Service (CCaaS) services available and the use of tools that leverage Generative AI tools, all resulting in increased attack sophistication while

[1] Anti-Phishing Working Group, *Phishing Activity Trends Report* (2023)

lowering the barrier to market for threat actors to implement attacks far more frequently and with greater success.

And the SMB is a target that's growing in interest with threat actors, as SMBs are nearly 350% (that's three and a half times!!) more likely to experience an email-based social engineering attack than their enterprise counterparts[2]. That stat speaks volumes; while the world's largest companies get all the headlines, the availability of every facet of CCaaS has created a "market" that allows literally anyone to jump into the cyberattack game. And, if you were such a person wanting to test out your skills as a cybercriminal, what size organization would *you* go for? Certainly not some massive enterprise with money and resources to squash you like the bug you are. No… you'd go after the little guy – which is exactly what we're seeing; the SMB is growing as a target.

Couple this with the growing number of attack surfaces (generally accepted to be *phishing/social engineering*, *remote access*, *vulnerabilities*, and *supply chain vendors*) as well as the increased number and sophistication of each kind of attack, and it becomes evident that the SMB is in serious trouble if they're not ready for *when* a cyberattack occurs.

Despite all of this, *the SMB most-definitely isn't prepared*.

Over half (58%) of small business don't currently have cybersecurity measures in place[3], and 59% of them believe they are "too small" to be a target of a cyberattack. Something tells me they're (unfortunately) in for a surprise, as many lack the needed preventative measures in place:

---

[2] Barracuda, Spear Phishing Top Threats and Trends Report (2023)

[3] Digital.com, Small Business Survey (Q3, 2022)

- 21% of SMBs have no offline immutable backups[4]
- 34% of SMBs don't utilize phishing testing of employees to thwart phishing attacks[4]
- 30% of SMBs have no written incident response plan[4]
- Of those that do, 35% of them tested the plan over six months ago[4]
- And 75% of SMBs would only survive three to seven days after a ransomware attack[4]

Add all this up and it quickly becomes evident that the cybersecurity measures necessary to properly protect the SMB across all attack surfaces, and an ever-changing set of tactics, campaigns, scams, and techniques, when matched with a lack of in-house cybersecurity expertise are a massive burden.

The Initial Opportunity: Cybersecurity Services

To mitigate these cyber risks, SMBs turn to security centric MSPs like you to not only ensure their IT infrastructures are available and running well, but also to establish layered protection from all cyberthreats.

Generally, this revolves around solutions that assist in securing your customer's environment, including:

- RMM to monitor and secure endpoints, servers, networks and more
- Email security

---

[4] CyberCatch, Small and Medium-Sized Businesses Ransomware Survey (2022)

- Endpoint Detection and Response
- Web/DNS protection
- Security Awareness Training
- Firewall management
- Secure access for cloud applications
- Backup and recovery

The above is by no means an exhaustive list. In fact, I'm more trying to make the point (as denoted by the section title), this is just the *initial* opportunity you have. So, if you're not already offering cybersecurity services, it's time to begin looking into it – and the list above is a good place to start.

I've written two other Conversational Geek eBooks that dive deeper into some of the ways you need to secure your customers that you may want to read as well – take a look at:

Conversational Email Security for MSPs
(goto.cg/CES4MSPs)
and
Conversational Zero Trust Network Access for MSPs
(goto.cg/CZTNA4MSPs)

If you already have cybersecurity services, or are considering putting this kind of offering in place, there are some macro trends you're going to need to deal with that may require your seemingly static service to continually adjust:

- Digital transformation adoption – What started 10 years ago solely to take advantage of the promises of the cloud, is now driven by pandemic responses and the resultant shift businesses are experiencing. This requires companies to move assets to the cloud or transition to SaaS applications. With 36% of SMBs accelerating their technology investments and adoption of new tech[5], what your cybersecurity services need to protect is in a state of flux for the foreseeable future.

- Supporting a remote or hybrid workforce – The idea of a network perimeter is now defined by the user-driven use of BYOD and access to company networks, resources, and services from anywhere, at any time. With 46% of SMBs having some form of a remote work program in place[5], keeping everything secure when your customer doesn't own and can't necessarily manage every device will be a challenge. At least 75% of organizations are concerned about the security risks with an increasingly remote workforce[6] – you're going to need to be concerned as well.

- Email is a primary attack vector – Beyond it being the number 1 form of communication and collaboration, phishing remains the number 2 initial attack vector for data breaches (just behind stolen credentials, which are primarily stolen via – yep, you guessed it – phishing

---

[5] SMB Group, *Business & Technology Challenges and Priorities* (2023)

[6] So Safe, *Human Risk Review* (2023)

attacks).[7] And with users being so used to getting all sorts of requests from both inside and outside the company, they rarely suspect or second guess the legitimacy of the email sender, putting the organization at risk. This makes email of particular focus as part of your cybersecurity offering, considering the great lengths cybercriminals will go to in order to obfuscate their malicious intent with social engineering and sophisticated linking, attachment, and scripting techniques.

- Users not caring about cybersecurity – On top of all this, the users themselves don't see cybersecurity as something that's a part of their job. If they did, 74% of data breaches wouldn't include the "human element" where users fall for phishing scams, social engineering, have their credentials stolen, or are error-prone, impacting the organization[7]. And while you can educate them with Security Awareness Training, you need to create a security culture within a customer's organization – something you're likely not going to be able to do easily. Which means the user's expectation that you're going to protect them is probably going to be your reality.

Cybersecurity is a great opportunity for MSPs. However, offering robust protection that covers relevant threats in today's security landscape (such as ransomware, sophisticated email attacks, zero-day attacks, newly discovered software vulnerabilities, and more) is challenging.

---

[7] Verizon, *Data Breach Investigations Report* (2023)

In fact, most MSPs offer one or more of the aforementioned cybersecurity point solutions to protect and monitor different attack surfaces but don't have the people, process, or technology to quickly sift through the 'noise' of these point solutions, to detect threats and respond to them before their customer's businesses incur damage. Therefore, while most MSPs have added preventive security services to their offerings, many lack proactive security services such as detection and response, in their offering.

What's needed is a far more cohesive and comprehensive approach that involves augmenting your current offering to one that achieves greater visibility, faster response to threats, and better protection.

Moving to Managed Security Services

Let's take the discussion about offering cybersecurity services to your customers to a higher level, one that is above implementing a group of security solutions used to form a layered security strategy for your customers. Don't get me wrong – there's literally *zero* wrong with creating and putting to market such an offering.

Instead, I want you to consider offering a cybersecurity service that has its' people, processes, and technology all working 24x7, making certain that every one of your customers is not only in a constant state of protective security, but also that should an attack occur, they are quickly placed in the hands of a cybersecurity professional who can respond to the problem immediately.

But achieving this higher echelon of cybersecurity offering is not without its' challenges, as most MSPs are still trying to wrap their heads around a solid layered security strategy – let alone offering a far more comprehensive approach to managing the state of a customer's security.

Any good cybersecurity service offering should focus on providing a secure environment by *preventing*, *protecting*, *detecting*, *investigating*, *responding to*, and *remediating* threats. And, while implementing security solutions will put much of this in place, there are some challenges that even you as an MSP will face and need to overcome – beyond even those macro trends previously mentioned. These include:

- Comprehensive visibility – It's one thing to get an alert from, say, the endpoint detection solution you have installed at a customer site. But to effectively detect and respond to threats, it's necessary to have a far more comprehensive ability to monitor customer networks, log sources, endpoints, servers, and more.

- Experience and Expertise – building out a robust cybersecurity offering may be new to some of you. And even if it's not, it's likely that you don't have more than one or two techs that have any grasp of what's going on in the world of cyberattacks. Cybersecurity demands having dedicated experts in-house to understand both the scope of an attack and the actions needed to eliminate the threat and bring the customer environment back to a known-secure state.

- Someone's Got to Be Awake – Threat actors don't conveniently attack during "business hours only", which means you need to have someone monitoring for, and available to respond to, issues 24x7.

- Budget – Like every MSP, you're always looking for cost-effective ways to expand your services. And while software solutions can typically be priced in a way that doesn't impact your company's wallet, building out

some form of a security operations center (SOC) to monitor your customers, along with some security analyst staff, could break the bank.

- Differing Customer Needs – Despite your best efforts, your customers operate using different tech stacks, making it difficult-to-impossible to setup a single cybersecurity service offering that can make all your customers happy.

What are your options?

There are three ways MSPs have traditionally attempted to address these challenges:

1) Partner with local MSSPs – this one has made sense because you gain immediate expertise and staff that are available 24x7. But in many cases customers have simply bypassed the MSP entirely to eliminate the cost of keeping the MSP as the middleman.
2) Building their own security operations center (SOC) – this would include all the required technologies, skilled staff, 24/7 coverage, and don't forget building out playbooks, standard processes, business practices and more. Analysts alone are around $75,000 each. And then there's the cost of a SIEM solution, training, security tools, and a location to host all this. The general rule is it costs $1M annually to run a SOC, so, while it's an *expensive* option, it's still an option.
3) Partner with trusted vendors – there are security vendors that help to augment your cybersecurity offering to deliver MSSP-like security services in a way that presents itself as an extended part of your offering.

Regardless of the option you choose, it's necessary is to shift your thinking from simply executing a software-centric cybersecurity offering to one that is truly *managed*, augmenting staffing and services to help prevent, detect, and respond to cyberthreats around the clock.

But one of the three is a clear winner.

Partnering to Achieve Managed Security Services

In short, I'm talking about partnering with a vendor that offers you a SOC, complete with 24x7 monitoring of customer environments by experienced security analysts that work *with you* to augment not just your staffing, but your services and internal expertise, as well as your company's ability to detect and respond to threats.

You might be wondering if shifting to a managed cybersecurity service makes you a *Managed Security Services Provider* (MSSP). I'm going to say, for most of you (assuming you fit the bill of just offering some cybersecurity-related software solutions), it won't. MSSPs generally include the management of security infrastructure, identity, vulnerability management, intrusion prevention, and more in their stable of services – this *in addition* to the detection and response to threats in their customer's environment.

When thinking about augmenting your cybersecurity services with managed security services, there are a few questions about the arrangement that are important to answer and, in

some cases, can differentiate one MSSP you may be thinking about partnering with from another.

What services are we talking about?

With Managed Security Services, you're gaining an already running, fully staffed SOC that leverages a multi-tenant detection and response platform to monitor your customer's environment for known threats, abnormal activity, and indicators of compromise. Should a threat be detected, a response plan is initiated to isolate and remediate the threat.

So, this is Managed Detection and Response (MDR) then?

Maybe. It depends on your definition. There are a lot of tech-marketing buzzwords being thrown around by vendors trying to differentiate themselves these days as the overarching category of MDR crystalizes. So let me offer up a few definitions that may help (and I should note that even the definitions I give below won't align perfectly with every vendor out there as, again, each vendor is trying to stand out).

- Endpoint Detection and Response (EDR) – EDR is focused on securing endpoints (think workstations, laptops, servers, tablets, smartphones, and even IoT devices). It's usually using some form of artificial intelligence or machine learning to detect anomalous behavior on the endpoint. There's also usually some centralized ability to monitor all the endpoints, alerting to focus efforts on detected threats, and an ability to respond via either built-in actions (e.g., disable the network card on the endpoint) or custom scripts.

- Extended Detection and Response (XDR) – The simplest explanation to differentiate EDR with XDR is

that XDR monitors more parts of your customer's environment (think endpoints, servers, firewalls, routers, email, cloud-based and on-premises assets, and more). The benefits of XDR over just EDR are that the SOC using XDR has far greater visibility across the customer environment, threats can be identified in more ways than just showing themselves on an endpoint, and responses can be far more exact and impactful across the entirety of the network.

- Managed Detection and Response (MDR) – This one gets a little tricky, as some vendors use MDR to mean *managed EDR*, while others mean *managed XDR*. So, it's important to dig a bit deeper with your service partner of choice to understand whether their detection and response is limited to the endpoint or not. But in either case, the *managed* part indicates round-the-clock monitoring, incident investigation, and response by seasoned cybersecurity professionals – the difference is what underlying solution is used; the visibility provided by the solution really will dictate the effectiveness of the managed security service's ability to detect, investigate, and respond to threats.

There's also Threat Detection and Response (TDR), Network Detection and Response (NDR), and some refer to Managed XDR as *MXDR*.

Again, not every tech vendor out there offering some kind of "*DR" offering is going to completely agree. So, the two key points I want you to focus on are:

1) *You want to see that "X"* (that is, you want as much visibility across as many kinds of devices on your customer's environment as possible).

2) Unless you already have a team of in-house cybersecurity experts (and really just need to formalize your offering to be closer to MDR), *you want to see "managed"* so you can bring this level of offering to market quickly and cost-effectively.

Who's doing the work?

One of the confusing points when engaging a Managed XDR vendor is where the work is divided up. Does engaging mean the partner does all the work and just pretends to be an extension of your company, doing all the detection and remediation work for you? Or does it mean they just tell you "*Oh, hey – there's a problem with Customer X. Go fix it.*"? Or is it somewhere in-between?

The answer, in general, all depends on what you want. Most Managed XDR vendors recognize that – just like your customers have differing needs – your needs are not the same as the next MSP wanting to partner up. And so, they design managed security services to meet your staffing, budget, and execution needs.

In the end, it means the Managed XDR vendor you partner with will work to act as an extension of *your business*, filling in the service gaps and allowing your team to be involved as much or as little as necessary in the detection and response activity. If the gap is staffing, they provide you someone to respond to a detected threat. If the gap is expertise, they should provide you

with guidance (I'd love to see ready-made runbooks, personally) so that your team can do the work, leaning on and yet gaining the experience and expertise from the SOC analyst.

Should my customer need to change anything?

As with any service – even your own when you first started – there's always the question of "do we support that?" And it's just as true when considering a Managed XDR vendor; do they, in fact, support all the platforms, applications, operating systems, endpoint types, devices, firewalls, etc. that *your customers already have in place?*

The right answer to whether your customer needs to change anything about their environment is a resounding, *No*.

You're expected to offer flexible solutions that meet your customers' needs (as opposed to you asking them to change what has already implemented to fit your services). In the same way a Managed XDR vendor asking your customers to use specific applications or services is simply not a realistic request.

Your Managed XDR vendor should be able to support your customers' environments as they stand (with the reasonable one-off outlier that, no doubt, will pop up every so often).

What's in it for me?

By partnering with a trusted Managed XDR vendor, you can provide cybersecurity services that accomplish a few cybersecurity goals while remaining flexible enough to cater to the tech stack needs of a wide range of customers:

1) A secure defense – with you continuing to offer a layered approach to help secure your customer's attack surfaces, you help to stop threats before they can do harm.

2) A faster time to market – You can't build a SOC fast enough or inexpensively enough to match the cost savings of simply partnering with a vendor that has built out an "as-a-Service" model that accomplishes the same thing more quickly and cost-effectively.

3) A stronger cybersecurity team – You not only gain a new set of detection and response services, but your team immediately "grows" by extending to the security analysts assigned to you and your customers, increasing your company's experience and expertise.

4) A constant watch for threats – the log and activity data from those same solutions that create a layered defense are ingested into a Managed XDR solution that provides security analysts with the needed organization-wide visibility necessary to detect threats as soon as they occur.

5) A faster (and more accurate) response – Your extended SOC team will be able to correctly identify the threat more quickly, enabling an exact response that remediates the threat and gets the customer operational again.

6) More recurring revenue – I'd be remiss if I didn't address the "not exactly the focus, but still important" elephant in the room. Your cybersecurity services suddenly have tiers of service, whereby you charge a monthly recurring fee for the "managed" option, in addition to the base "protective" service fee. This way, you can keep all your customers happy, regardless of the level of cybersecurity service they see value in.

Assuming you want to augment the basic cybersecurity services you offer today, going the route of partnering with a Managed XDR vendor provides your business and your customers with the greatest benefit, helping you each achieve your goals.

The Big Takeaways

I started this eBook with the title "The Evolving Need for Cybersecurity Services" because of the evolution of cyberthreats that's taking place in front of our eyes. In the same way, cybersecurity services themselves need to evolve – from the somewhat "set it and forget it" approach of installing all the buzzword-worthy software-based security solutions to your customer's environments, to the more mature – and far more effective – approach of *managed security*.

And as you evolve your thinking to take on a more managed approach, you also need to equally expand the focus from just endpoints to every part of the customer environment as being a potential data source (and security sensor of sorts) for an XDR solution used in conjunction with a managed security offering.

Your next step in the journey is looking for the right Managed XDR vendor – one that answers all those questions I posed, and checks all the boxes with regard to how they integrate with your team, business processes, etc.

If you're at this point, I've finished my job of trying to convince you that threats today demand better protection, which means customers are going to be demanding it as well. So, by evolving your cybersecurity services to become a managed offering, you'll be able to better protect your customers against cyberthreats. And, should an attack successfully infiltrate your customers, you rest in knowing that your offering comes complete with the people, processes, and tech in place to quickly and effectively respond to eradicate the threat.

Sponsor Chapter:

Offering Managed Cybersecurity-as-a-Service with Barracuda XDR

Whether your MSP business is simply looking to add another tier of cybersecurity services, or if you're seeking to differentiate yourself from your competition, the addition of 24x7 security monitoring and response will create a materially different experience for your customer.

But as previously explained, getting to a point where your business can offer the equivalent of a security operations center (SOC) – complete with its' monitoring and response stack of solutions, seasoned team of cybersecurity experts, and 24x7 staffing – is usually out of reach for most MSPs.

According to Ponemon's *Economics of Security Operations Centers* report, the average cost just to do the integrating of disparate security data, build out rules, and automate processes into an existing XDR solution is over *$2.7 million*!

But that idea of your customer resting in the knowledge that a security analyst is keeping watch over their environment, ready to respond to threats at a moment's notice is a material departure from your traditional implementation of security solutions to protect a customer environment. So, being able to provide this kind of offering would not only increase revenue, but also result in a happier and more secure customer.

This is why Barracuda MSP, the MSP-dedicated arm of Barracuda Networks, sets itself apart by going beyond its suite of MSP-centric security and data protection solution to offer Barracuda XDR – a service offering designed to work with your cybersecurity business to bring a world-class managed cybersecurity offering to even the smallest of businesses.

By offering managed cybersecurity through XDR, Barracuda MSP provides MSPs with an all-encompassing tailored solution that effectively works to monitor, identify, and respond to threats.

Comprehensive Managed Cybersecurity

There's a lot that needs to go into offering managed cybersecurity to your customers – something Barracuda MSP has put together to create a robust, flexible, and responsive service that plugs into your business as easily as taking on a new software solution. Let's break it down a bit:

- Expert Cybersecurity Team - divided up into four dedicated divisions (red, green, blue, and purple teams), Barracuda MSP's team are seasoned cybersecurity pros with years of experience and expertise.

- Comprehensive Monitoring – With an ability to ingest data from over 40 commonly used security and business technologies including all major EDR solutions, email security solutions, authentication, firewalls, network infrastructure, and other log sources (both on-premises and in the cloud), Barracuda provides your Managed Cybersecurity team with complete visibility into your customer's existing stack to understand what's happening within their environment.

- Intelligent Analysis and Detection – Modern cyberattacks require modern detection. Barracuda uses an AI-powered analytics engine to quickly and accurately detect suspicious, anomalous, or flat-out malicious activity while minimizing false positives.

- Responsive Processes – When a potential threat is detected, the SOC team investigates, identifying the threat and responding based on detailed runbooks for every alarm generated by XDR to mitigate the threat and remediate the situation. Should you or the customer wish to assist in the response, the SOC team works side-by-side providing guidance and expertise.

- Centralized Visibility – MSPs get a multi-tenant dashboard that gives them a single-pane-of-glass view

into the incident events detected by XDR and alarms triaged by the SOC teams, of your customer's environments.

- Fast, Flexible Implementation – It would take you months or quarters to setup every aspect of a SOC. And even then, it likely wouldn't be flexible enough to easily monitor each of your customer's unique environments. With Barracuda's Managed XDR offering, you can easily support just about every environment and have a customer being actively monitored within a matter of weeks.

Getting Your Cybersecurity to *Managed*

Managed cybersecurity needs to be your goal. It's a service that benefits your business and the customer. You quickly gain additional recurring revenue streams while providing a superior cybersecurity service – all without needing to lift a finger. Your customer gains better coverage against threats, more rapid response should an attack occur, a more secure environment overall, and more time focused on being productive.

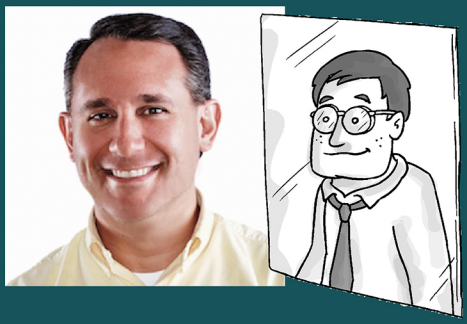
It's a no-brainer.

Barracuda XDR gives even the smallest MSP an ability to provide elevated around-the-clock extended threat detection and response services, allowing you – and your customer – to focus on your business.


MSP
Barracuda
Your journey, secured.
MSP
Barracuda
XDR™
Managed security services made simple
Extended Detection & Response with 24x7x365 SOC-as-a-Service
Schedule a 1:1 demo today
barracudamsp.com/xdr-demo/

Quickly become conversational about managed security services for SMBs

With the global cyber threat developing on an almost daily basis, cybersecurity services also need to evolve to keep pace. This ebook looks at how to take your managed security offering from a “set it and forget it” approach of installing all the buzzword-worthy software-based security solutions to your customer’s environments, to a more mature – and far more effective – approach of managed security. Expanding your view to protecting your customers whole environment at the same time.



About Nick Cavalancia

Nick Cavalancia is a technical evangelist, Microsoft MVP, and CEO of Conversational Geek. He has over 25 years of enterprise IT experience, 10 years of executive-level marketing experience, is an accomplished consultant, speaker, trainer, writer, and columnist, and has achieved industry certifications including MCSE, MCT, Master CNE and Master CNI.

ConversationalGeek®

For more content on topics geeks love visit

conversationalgeek.com