ConversationalGeek®

Conversational Zero Trust Network Access for MSPs

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

In this book, you will learn:

- How to secure network access for your customers' modern workforces
- The core benefits of ZTNA and why VPN isn't enough
- The five guiding principles to building a Zero Trust network

2nd Edition

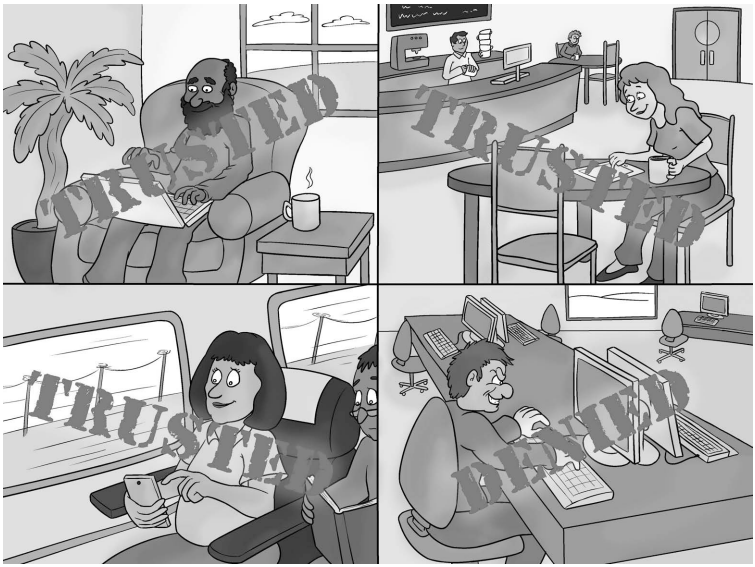
Sponsored by
Barracuda MSP

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 Zero Trust Network Access for MSPs

By Nick Cavalancia



ConversationalGeek®

Conversational Zero Trust Network Access 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:	Pete Roythorne
Content Reviewer(s):	Lindsay Faria
	Doris Au

Note from the Author

Thank you for downloading this eBook.

At the beginning of the pandemic MSPs everywhere found themselves scrambling to get their customers into a position where they could effectively continue their businesses with the bulk of their staff being forced to work from home.

One of the technology mainstays of this transition was the VPN. And while it may have been adequate as a stopgap, 18 months down the line, it's clear that VPN alone really doesn't cut it. It's time for a new and more robust solution.

In *Conversational Zero Trust Network Access for MSPs*, we look at why we shouldn't rely solely on VPNs anymore and how MSPs can help their customers deploy a Zero Trust Architecture to mitigate the security concerns of this "new normal."

The idea is that this eBook will act as a guide to MSP success. In the following pages, you'll learn how you can position and sell ZTNA to your customers effectively. Ultimately, this is about helping you to not only protect your customers' networks and businesses, but also grow your business.

Nick Cavalancia
4-time 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 MSP Need for Zero Trust Network Access

For those in the security industry the concept of Zero Trust is nothing new. But with the dramatic changes that have been forced upon our working practices by the global pandemic, combined with the onslaught of increasingly complex and sophisticated cyber-threats, the need for security architectures built around Zero Trust Network Access (ZTNA) has become more pressing than ever. ZTNA is something that MSPs really need to come to grips with quickly if they are to help protect their customers.

In a business world that no longer has perimeters in the traditional network sense, ZTNA provides a practical solution for striking the right balance between data security and giving end users fast and reliable access to the systems they need to remain productive from anywhere.

This guide will explain the challenges that ZTNA answers, as well as how MSPs can effectively add it to the menu of services they offer their customers (as well as using it to secure their own networks).

Adapting to rapid change

The pandemic caused most organizations to shift the majority – if not all – of their staff to working remotely from home. If you spoke to any MSP in the early days of this transition, the story was pretty much the same – barring a few notable exceptions: Tales of techs working 24/7 to help rebuild their customers' entire systems and infrastructure to be able to handle the new work from home (WFH) environment, leading to wholesale shifts to the cloud, and frantic drives to get staff access to the systems and applications that they needed to do their work. Anecdotally, people talked about doing years' worth of digital transformation in the space of just a few weeks, in the early stages of the pandemic.

With their customers still needing access to on-premises resources, MSPs needed to quickly find ways to get remote employees access to the tools they needed to be able to continue to do their jobs. For most, the obvious answer to this was through VPNs, which allowed staff to create a secure connection into company systems. Nearly two-thirds (63%) of US organizations used a VPN during COVID[1]. While that

[1] Ponemon, *Cybersecurity in the Remote Work Era* (2021)

number has become a more balanced 27%[2], the rampant use of VPNs was a common tale across every vertical, geography, and size of SMB business.

To shift everything at the speed it needed to be shifted, there really wasn't another workable solution. However, as the dust has settled on this new-look landscape, one thing has become abundantly clear: *security for remote access needs an upgrade*. SMBs need to find real, long-term solutions to help them address all their challenges as defined by both their business and their workforce – not just the quick fixes we had to deploy in the early days.

Remote working was already on the rise before the pandemic and this shift has settled post-pandemic to an average of 26% of employees currently work remotely[3], with 66% of employees working remotely, at least part-time[3]. If the stats are anything to go by, it looks pretty certain that working from home will remain a reality for many SMBs across the U.S. and the rest of the world.

While we have created an infrastructure to support working from home, the reality is that the patchwork of solutions that were put in place to keep the lights on and the wheels turning now need to transition to permanent solutions that are designed for one purpose: *to support a hybrid workforce*.

As I mentioned earlier, the initial focus of the work to get businesses up and running was on productivity and continuity. During this time security didn't exactly take a back seat, but the drive to get things moving as quickly as possible perhaps enforced a few shortcuts along the way. Now we need to look

---

[2] Databarracks, *Data Health Check* (2022

[3] Zippia, 25 Trending Remote Work Statistics (2022)

at how we can properly secure the new environment where we are today and where we are going to be in the future.

To do this, there are two major challenges that need to be addressed:

1. The new perimeter – Traditionally, you would be able to look at a customer's network and secure it within set logical and defined boundaries. Yes, you'd have to deal with BYOD, but even that could be managed using guest networks and enforcing policies. Today, the perimeter of the customer network extends all the way to an employee's home and their endpoint device, with a plethora of different security technologies at each of these different points. It's not a place where you can rest easy in the knowledge that a customer has deployed standardized security solutions; this is more like the security technology equivalent of the Wild West. And now the burden falls on you to secure not just the logical perimeter, but also this new "edge."

2. Reduced security posture – Unsurprisingly, cyberattacks are increasing. Disruption of any sort gives cybercriminals the opening they need to get in and wreak havoc. And this has been a massive disruption. As a case in point, the number of phishing attacks in second quarter of 2022 was 4 times that of the same quarter in 2020[4]. The harsh reality is that remote workers are actually hurting their customer's security posture. When they're out of the office, they aren't being constantly reminded to adhere to security guidelines, so many are relaxing their security stance – even if unintentionally.

There is no security baseline for remote employees and since they are unmanaged, you have to assume they are insecure by

---

[4] APWG, *Q2 Phishing Activity Trends Report* (2022)

default – 84% of organizations believe that enabling the remote workforce creates more exposure to cyber risk[5].

3. Increased web-based threats – Attacks on Internet-facing web applications are involved in 70% of all cyber incidents[6], making it the most common attack pattern. Exposed remote desktop applications (commonly summarized under the acronym *RDP* after Microsoft's Remote Desktop Protocol) continue to be the number one initial attack vector in ransomware attacks[7]. And taking advantage of single-factor logon capabilities on VPNs, as well as vulnerabilities found in VPN products has become commonplace in many ransomware gangs.

Additionally, threat actors aren't just targeting the organization as their initial means of gaining access. Websites currently experience an average of 94 attacks every day and are visited by bots approximately 2,600 times a week[8]. As the world continues to embrace virtual hangouts and movie streaming platforms for entertainment, and video conferencing tools to communicate with their co-workers remotely, these high levels of global internet usage show no sign of decreasing.

While the internet has enabled many organizations to ensure their productivity throughout the shifts to remote and—more recently, hybrid—work, our reliance on the internet makes it a lucrative target for attackers, many of whom focused their efforts on exploiting web vulnerabilities.

---

[5] Tenable, *The Future of Cybersecurity In The New World Of Work* (2022)

[6] Verizon, *Data Breach Investigations Report* (2022)

[7] Coveware, *Q2 2022 Quarterly Ransomware Report* (2022)

[8] SiteLock, *SiteLock Website Security Report* (2022)

VPN – a quick fix

The simple answer to managing the security situation amidst the pandemic was to channel all traffic through VPNs. At the time this made perfect sense: VPNs provided a tried and tested technology that offered a secure communications channel to the corporate network, and most companies already had some form of VPN infrastructure in place, so things could be rolled out quickly. Authentication is required to restrict initial access to the VPN tunnel, so there is some control over who is accessing what resources, and with remote users being seen as a node on the corporate network, facilitating connectivity to internal resources was relatively straightforward for MSPs.

As a result, it's hardly surprising that VPNs saw a huge rise in use during the pandemic, with some estimates being as high as a 165% increase[9].

However, the reality is that VPNs have issues and limitations, which mean they aren't truly fit for long-term usage in this new environment. The spike in usage has served to highlight a number of these key problems.

VPNs are notoriously slow, they degrade network performance, using one requires switching between networks, and they are also not mobile friendly, as they consume a lot of battery life. On top of this, a VPN is about privacy, not security; they provide a private channel over which to communicate with the corporate office, but that's about it.

Structurally they are not fit for this purpose. Here are some of the shortcomings we've had to contend with while using VPNs since the pandemic started:

---

9. NordVPN/Dar Reading https://beta.darkreading.com/operations/vpn-usage-surges-as-more-nations-shut-down-offices

- Scale: VPNs were designed to handle only a fraction of the workforce. When rolling them out to an entire remote staff, you need to consider that to access the corporate LAN, every device needs to have the VPN client installed independently. This is time-consuming and inefficient.

- Reliability: You don't have to look far to see reports of user frustration with VPN that focus on almost daily connectivity problems. On top of this, VPN performance usually leaves a lot to be desired, and many enterprise VPN solutions have bad reviews and low NPS scores if you search online. With regular time outs, reauthentication requests, and slow performance, VPNs can end up having a negative effect on productivity, especially when large parts of the workforce is still working from home.

- Device security: A VPN only offers a private tunnel to the network, it does not authenticate the user's identity or the connecting devices' security status. On top of this it does not offer granular control over who can access data and resources.

- Infection spread: The vast majority of at-home users are not trained on security awareness. All it takes is one click on a bad link in a phishing email or on a compromised website and the user's household devices are infected. When that user connects to the VPN to access their company's resources, an attack can easily spread across the whole infrastructure. We know MSPs are being increasingly targeted for their access to other companies, so to take this one step further, the threat could even 'island hop' through the MSP's tool

and infect the rest of their customers. The result of this would be catastrophic for the MSP.

- Lack of real authentication: Some of you may have customers with VPNs (or installed one yourself for them) and recognize that most VPNs require some form of authentication. But that's not always the case. People access SaaS applications from outside the corporate network and there's nothing to make them log into the VPN before accessing them. That can lead to security vulnerabilities. As more businesses adopt the cloud, VPNs would provide connectivity to SaaS infrastructure without requiring additional authentication, which poses an increased security risk.

  In fact, almost one-third (31%) of organizations do not require their remote workers to use authentication methods. And of the 69% that do require authentication, only 35% of them require multi-factor authentication5.

  The Colonial Pipeline ransomware attack[10] last year serves to highlight the danger here. The attack, which took down the largest fuel pipeline in the US, was initiated via the organization's VPN server. The criminal gang behind the attack acquired a list of stolen credentials and were able to work through the list until they found one that gave them access to a VPN without multifactor authentication. This then allowed them to gain unfettered access to the internal network from where they launched their attack.

On top of this, VPNs only facilitate a private connection when accessing resources on the network – what about when those

---

10. www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

very same remote workers need to access a cloud-based resource from a personal device?

All this makes it clear that VPN as a long-term solution isn't going to cut it, and as an MSP your more IT savvy customers are going to be looking to you to help guide them through this terrain. But many more SMBs will just expect things to work, and when it doesn't they're going to call you regardless of whether the BYOD device or contractor device that's being used is technically under your management or not. By providing adequate protection for those devices, which may not be part of your traditional management coverage, you can avoid those painful conversations with clients, and mitigate the risks they face.

So, how do you provide your customers with security, connectivity, and productivity in an environment that consists of insecure personal devices, a need for stronger authentication, and secure connectivity to both on-premises and cloud-based applications and resources, all while much of this very environment isn't even under your control?

Moving from VPN to Zero Trust

One of the cornerstones of establishing the process by which we manage the new work from home environment has to be this: The method that you use to allow remote workers to connect to your customer's network needs to provide access as if the remote worker was internal to the network. That way, users can easily access internal resources as normal.

However, you also need to take things a step further, as you have to enhance the security stance of your customer to the point where even if the remote worker's endpoint device is compromised, the threat actor has no ability to leverage the connection to get access to your customer's network or their resources.

The problem with the current set-up is that VPNs essentially make your customer's network, data, and applications accessible to the remote worker's endpoint upon each connection. If the endpoint device is then infected, all data and applications that can be accessed by that user can also be accessed by a hacker. This increases not just the risks for the customer, but also for the MSP.

Additionally, we shouldn't be viewing VPN by itself as a *solution*; it's not, *it's a tool*. A true solution would incorporate a series of important functionality to better secure the connection. As a basic starting point this should include:

- Remote access – obviously this would be fulfilled by the VPN itself.

- Mobile Device Management – this is an important functionality to have within the WFH scenario because of the number of different devices that staff will be using (from tablets to smartphones), all of which need to be managed in some way. As we mentioned earlier, it's not like a closed office network where you can restrict these devices to using a guest network, so that they are not able to access the core network. When you have everyone working from home you don't have the control over what device people are using to access the VPN. This means that you need to be able to ensure each device meets the required security standard of the company.

- Multi-factor authentication (MFA) – Today MFA is pretty much table stakes for any corporate system. But for the example we're talking about here, this would also need to protect both on-premises and cloud-based resources.

Even packaging your VPN up in this way is starting to feel like another inefficient toolset that is going to put more burden on

the MSP by increasing support costs and ultimately lowering profitability.

Fortunately, there is another way, and the answer here lies in the principle of *Zero Trust* – a security model that is based on the simple concept of "Never Trust. Always Verify."

Zero Trust – A Primer

NIST describes Zero Trust as:

"…an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A Zero Trust Architecture (ZTA) uses Zero Trust principles to plan industrial and enterprise infrastructure and workflows."

What does this mean in practice? The foundation of Zero Trust is the assumption that an organization should not grant anyone access to its resources automatically, nor should it take for granted the identity of anyone inside or outside its own network perimeter.

At no point should you assume any level of trust based on a user's physical or network location (for example, if they are accessing data and resources from a local area network versus the internet) or based on asset ownership (whether the device they are using is enterprise or personally owned). Instead, Zero Trust sets out that you must verify each attempt by a device or individual to obtain access to company resources or data, before that individual session starts.

A Zero Trust network should be built around five fundamental guiding principles:

1. Hostile environment – You should always consider the network environment to be a dangerous place.

2. Everyone is a threat – Threats exist on the network at all times, both internal and external.

3. Don't trust anyone – A person's or device's locality is not sufficient grounds for deciding to trust a network.

4. Authenticate first – Every device, user, and network flow must be authenticated and authorized prior to its session starting.

5. Think broadly – Network policies must be dynamic and relate to as many resources and data sources as possible.

Zero Trust is also about gaining the necessary visibility that you need to fully establish trust for users to work effectively, while at the same time enhancing data security. User trust is critical, but unless it's proven and verified, a user should not access company data in an untrusted environment. Context is an essential element to establish trust in a Zero Trust world.

By thinking of your network in this way and taking a Zero Trust approach you can establish trust in a device or individual and thereby secure network communication and access so that the physical security of the transport layer can be reasonably disregarded.

While Zero Trust has been a focus for enterprise-level businesses in the past, the rapidly changing working landscape means that this focus is now moving down-stream to SMBs. And solutions are coming onto the market aimed specifically at this size of organizations and the MSPs that support them. Today, if you are an MSP and you are not offering ZTNA as part of your services offerings, then you will be at a competitive disadvantage.

You can find out more about a Zero Trust Architecture at
goto.cg/ZTA800-207

And while, you're likely not going to implement a complete Zero Trust environment within each of your customers, there are parts of it that can be taken advantage of now that both better secure your environment and address the issues outlined above regarding your customer's use of a VPN as a remote access solution.

This brings us to *Zero Trust Network Access* (ZTNA).

ZTNA – moving workforces forward securely

As I mentioned above, VPNs, at best, require a one-off authentication before simply allowing a connection to be made to the corporate network. As we've established, the problem with this is that a threat actor could compromise a user's personal device and use the VPN connection to access a corporate network without raising any flags.

In contrast, Zero Trust Network Access (ZTNA) starts with taking a completely opposite approach: no user or device can be trusted to access anything until proven otherwise.

Gartner defines ZTNA as:

"…a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context, and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This

removes application assets from public visibility and significantly reduces the surface area for attack."

However, beyond creating a secure channel, ZTNA adds extra layers of security that align with Zero Trust core principles:

- Support for Many OSs – both traditional endpoint operating systems (e.g, Windows, Mac, Linux), as well as mobile devices (iOS and Android) need to be supported to ensure that ZTNA can work effectively across all devices.

- Identity and devices are scrutinized – NIST talks about one of the tenets of Zero Trust: using the "observable state of client identity, application/service, and the requesting asset"[11] as a factor to consider when processing an access request. For example, determining whether a given device/identity combination has tried to connect to these resources or data before – if they haven't, it may be considered a potential red flag. In some ZTNA solutions, even the security of the device is scrutinized for things such as the presence of an OS firewall, current Antivirus, an up-to-date OS, or disk encryption. The purpose here is to make certain there is nothing out of the ordinary with regard to where/who the request is coming from, and to ensure the device meets the minimum required standards for the network.

- Centralized Authentication – The purpose here is to verify that the actual owner of the account is definitely the one making the authentication request. This is something that is required and even increasingly being enforced. Often, the process relies on using trusted,

[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

cloud-based identity services, as well as multi-factor authentication.

- Policy-based Access – resource requests are scrutinized against previously defined global access control policies to ensure access should be permitted based on both static policy parameters, as well as dynamic parameters (e.g., if that identity/device combination I mentioned didn't pass, then no access is granted).

- Acts as a Proxy for both on-premises and cloud-based resources – VPNs simply provide access to a corporate network. In contrast, ZTNA solutions add the protective Zero Trust layer of security and scrutiny to the connection first, and then proxy access to the needed resource, thereby maintaining control over the access should something about the identity, device, or connection prove to be untrustworthy.

What are the benefits of ZTNA?

Let's look at the benefits of using ZTNA, from both the customer perspective and the perspective of the MSP themselves.

Benefits to the customer

- Secure company devices – Because ZTNA is checking to make sure that company devices are up to date with the latest OS, apps, and security technologies, including web security, you will naturally be enhancing your device security across the business. This in turn will help ensure that the organization is in the best place to defend against other threats like phishing and web-based attacks.

- Network visibility – ZTNA can help get insights into who's accessing what resources using which devices. Organizations can clearly follow activity across their

network, as well as track and observe users and devices accessing on-premises apps. Furthermore, by getting total visibility into access activities, companies can help mitigate risk by being able to use the insights gained from this to define – and redefine – access policies, as well as continuously monitor device security posture.

- Improve your productivity – VPNs are well known for being slow and cumbersome, while ZTNA allows users to get quick and easy access to company resources without that delay, which will clearly improve productivity within an organization.

- Maintaining Secure Access – ZTNA also provides a layer of access benefits that can help maintain security. For example, continuous assessment of user and device identity and posture, the ability to set role and attribute-based controls to grant contextual access to trusted users and devices, and the ability to manage global policies such as disk encryption and device screen lock, as well as automatically block access for compromised devices.

Benefits to the MSP

SMBs are renowned for lacking the resources and dedicated skill sets to effectively implement a lot of security technologies, and this is very much true with zero trust security strategies. Internal IT teams simply do not have the right people or expert cybersecurity skills to manage this process. That's why MSPs need to look at including ZTNA within their offering and then customizing it to their individual client's needs.

Aside from helping customers ensure secure and easy access to their resources for their remote users, ZTNA can also bring other key benefits to the MSP's role, including:

- Secure remote access to the entire environment – This is the most obvious one, but remember, at best all VPNs do is validate the connection and then it's a free-for-all once connected. With ZTNA, you're providing an additional layer of security that actively protects your customer's environment. This is going to make your job as an MSP much easier when it comes to securing the environment.

- Predictable service delivery – One of the challenges with offering security services is that it's largely unpredictable. But because ZTNA is policy based, you are delivering a part of your security services that will consistently enforce preconfigured security, thereby improving the predictability of your security service.

- Discovering all the endpoints, applications, and workloads in your network and infrastructure – Because ZTNA will monitor device access, you can develop a robust inventory of users, devices, and services/apps. While most MSPs will build up an inventory of assets as part of their onboarding process, this only covers the legitimate ones, it's often difficult to know exactly what devices users are really using, particularly if they are working offsite. ZTNA will allow MSPs to see exactly what devices are being used and by whom, which will ultimately help further strengthen the company's security posture.

- Managing compliance – As an offshoot of all the access and device monitoring, ZTNA can also help MSPs drive down compliance costs for their customers, as they have a robust system of record to show to auditors. Additionally, this level of visibility over time can lead to a global policy for access control, which will help you work with your customers to shape an ongoing strategy for data protection and privacy.

Big Takeaways

VPNs were an obvious answer to a big problem at the start of the pandemic when companies were faced with having to rapidly shift to a mostly remote workforce. However, with the dust settling and remote work looking to be an ongoing thing that companies are going to have to adapt to, it is becoming clear we need a new – and long-term – solution to the challenge of securely managing remote access.

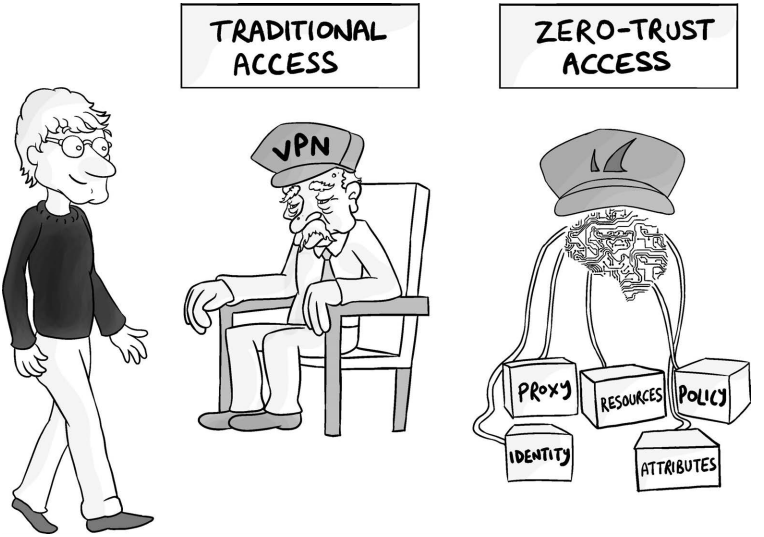
The system of user authentication and authorization used by VPN is at odds with the current direction of business systems and how work is conducted on a daily basis. Zero Trust, where access is granted on the basis of "never trust, always verify," represents the way forward.

Identity-based access or rather trust-based access is a fact and here to stay. As more and more apps move to the cloud it will be unfeasible to authenticate and authorize users based on their location and which network they are connecting from.

ZTNA (zero trust network access) solutions not only ensure that users and devices prove their trustworthiness for the network, but also add additional layers of security that align with Zero Trust core principles, including support for a wide range of OSs, centralized authentication, and policy-based access.

For MSPs, ZTNA is the perfect solution to help guide customers through the next security frontier and build their networks to manage the changing working landscape.

Vendor Chapter: Protecting Customers' Data with Next Generation ZTNA



With working arrangements changing rapidly and the march to cloud-based apps continuing at pace, MSPs desperately need to find a way to ensure their SMB customers can access their data securely and efficiently from wherever they are. As we discussed in the previous part of this book, VPN just doesn't cut it at the level we're currently at.

Access technologies that follow Zero Trust principles, on the other hand, offer a reliable and efficient way to ensure secure access to the resources that companies and their workforces need. Barracuda CloudGen Access for MSPs provides the Zero Trust foundation that users need for efficient access from anywhere and on any device.

Barracuda MSP, the MSP-dedicated business unit of Barracuda Networks, provides industry-leading security and data protection via its purpose-built MSP management platforms. CloudGen Access is one of the core pillars of its Network Security offering.

With Zero Trust being held up as the future of network security, CloudGen Access is designed to help simplify the path to Zero Trust for MSPs and SMBs by giving them the control and visibility they need to provide secure access to critical business apps, without impacting on end-user productivity.

How does Barracuda CloudGen Access do this? To understand this more clearly, we need to look at things through a number of different lenses:

Network Protection

CloudGen Access operates at the network layer. When a device attempts to start a connection to a protected resource, the app intercepts it and opens an mTLS connection with the CloudGen Access Proxy. This sends the device and user attributes to CloudGen Access Console, which checks the attributes and allows or denies the connection to the resource based on admin-configured policies.

mTLS – or mutual transport layer security – is an authentication method that ensures the parties at each end of a network connection are who they claim to be. It does this by verifying that they both have the correct private key.

Unlike with traditional VPN access, you are not connecting directly to the corporate network, but rather directly to an

internal or external resource via the CloudGen Access Proxy. With a traditional VPN you would switch on your VPN, which would route your traffic directly to the corporate network; from where you would connect to the app.

CloudGen Access works very differently:

- First, your app is set up behind the CloudGen Access Proxy. This means that any traffic to your protected app is intercepted by the CloudGen Access app on the endpoint.

- From here, the CloudGen Access app sets up an authenticated tunnel to the CloudGen Access Proxy that serves your protected app. This means that the CloudGen Access app authenticates the proxy and the proxy authenticates the CloudGen Access app. This is in essence the "m" in mTLS – the mutual authentication.

- All traffic then flows encrypted from the CloudGen Access app to the CloudGen Access Proxy, and then, finally, to your protected app.

Resource mapping

When a device enrolls in a tenant via the CloudGen Access app, after the certification process it receives a list of hashed protected resources from the CloudGen Access API. This way, when a user wants to connect to a protected resource, the CloudGen Access app requests a resource access token from the API, which includes the proxy to connect to.

Identities and devices

When you enroll a user on the CloudGen Access console, the app generates an enrollment URL that includes a token that is

valid only for enrollment. This URL can be sent via email or via any provisioning mechanism that the sysadmin decides to use. When a device is enrolled using this enrollment URL, two things happen:

1. CloudGen Access requests the user to authenticate and confirms this using the tenant's configured Identity Provider, such as Azure AD.

2. A certificate is generated that is unique to the device and is stored in the device hardware secure enclave. This way, there is a strong identity connection between the device and the user, which is not present in other systems.

When the CloudGen Access app starts a connection to a protected resource, the certificate is used to authenticate the device. On top of this, the device attributes about the devices security posture are collected by the CloudGen Access App and sent to the API which returns a JWT token after policy validation. The API also uses the same device certificate to sign the JWT token which is shared with the CloudGen Access Proxy for access to be granted.

Remediation engine

When a connection to a resource is denied, the CloudGen Access app receives a list of attributes that are not compliant with the policy/policies configured for the resource, together with a list of steps that the user can perform to fix the issue.

For example, say one of the access policies requires users to enable the firewall on their devices. If the user doesn't have a firewall enabled/turned on they will be denied access to the resource. The user will then receive a response including the reason for the denied access and how to fix the policy violation

– in this case “enable firewall” – with a URL that links to specific content that shows the user how to turn it on.

Access policies

Access policy configuration is a very simple API and UI interface that sets a list of supported policies for a resource in CloudGen Access. Because the app runs at the device level it can easily collect posture and telemetry attribute details in order to offer highly effective policy controls.

Web protection

It’s not enough to just ensure the security of a connection made by a user when they interact with corporate resources. What’s necessary is to also be certain a user is protected from malicious web content through robust content filtering and granular policy enforcement that works regardless of whether the user is on or off the corporate network – all based on real-time threat intelligence

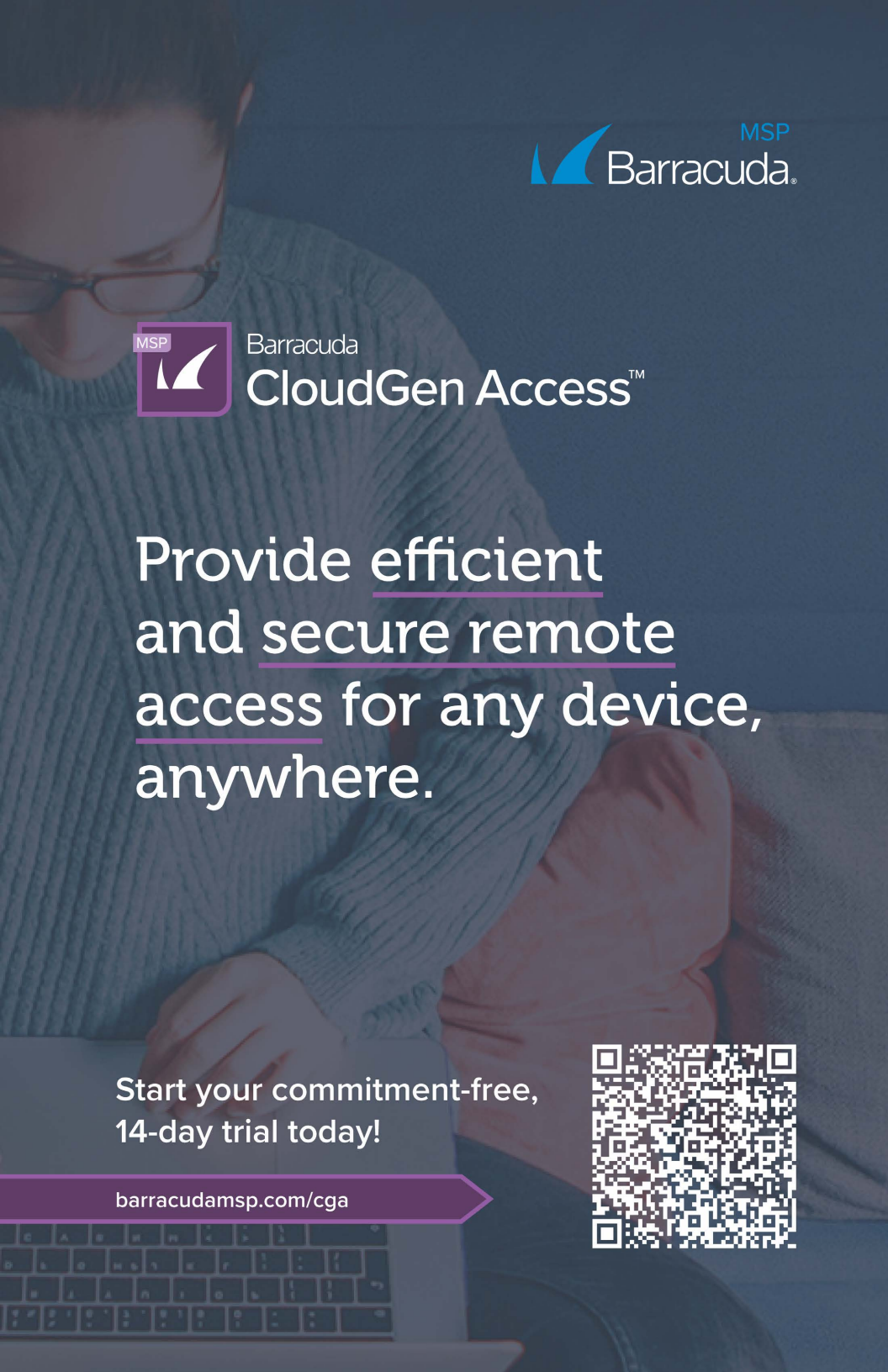
The Big Takeaways

CloudGen Access's approach to Zero Trust distinguishes it from other VPN and Zero Trust solutions in a number of key ways:

- It doesn't expose the enterprise network. It only allows access to the required resource, and it grants explicit access to specific apps based on user identity and group membership, as well as a devices' security status.
- It supports BYOD by validating device security before allowing access to requested infrastructure.
- It ensures retrospective and prospective device security and detects if a device has been exposed to an attack.
- It ensures role and attribute-based access control to ensure access for traveling employees and partners.
- It enables continuous connectivity for roaming devices with a built-in local proxy on the device.
- Unlike the VPN solutions in the market, it protects and blocks threats on your device with its network level interception capabilities and robust content filtering.
- Its built-in remediation engine lets users fix access issues themselves and improves devices security hygiene.

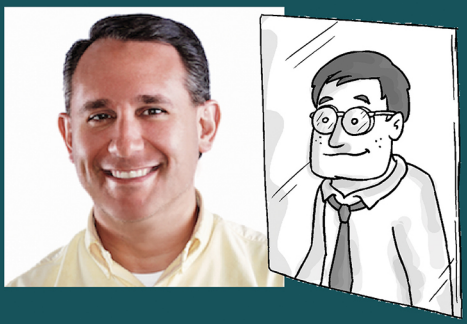
For MSPs looking to move their customers into a Zero Trust architecture CloudGen Access helps empower that shift.

Visit Barracuda MSP's website at barracudamsp.com to learn more about their easy-to-deploy, easy-to-manage solutions, priced to enable MSPs to grow their security offerings.


MSP
Barracuda
MSP
Barracuda
CloudGen Access™
Provide efficient and secure remote access for any device, anywhere.
Start your commitment-free, 14-day trial today!
barracudamsp.com/cga

Quickly become conversational about Zero Trust Network Access (ZTNA) for SMBs

Today's businesses are pushing new boundaries when it comes to how, and from where, they get work done. But how can we ensure that a new flexible, mobile approach to productivity doesn't compromise security practices? Providing network access in this environment has traditionally been done via VPNs, but they are not built with today's security needs in mind. We need a new solution. This guide explains how ZTNA answers this challenge, and how MSPs can effectively add it to their menu of services.



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.