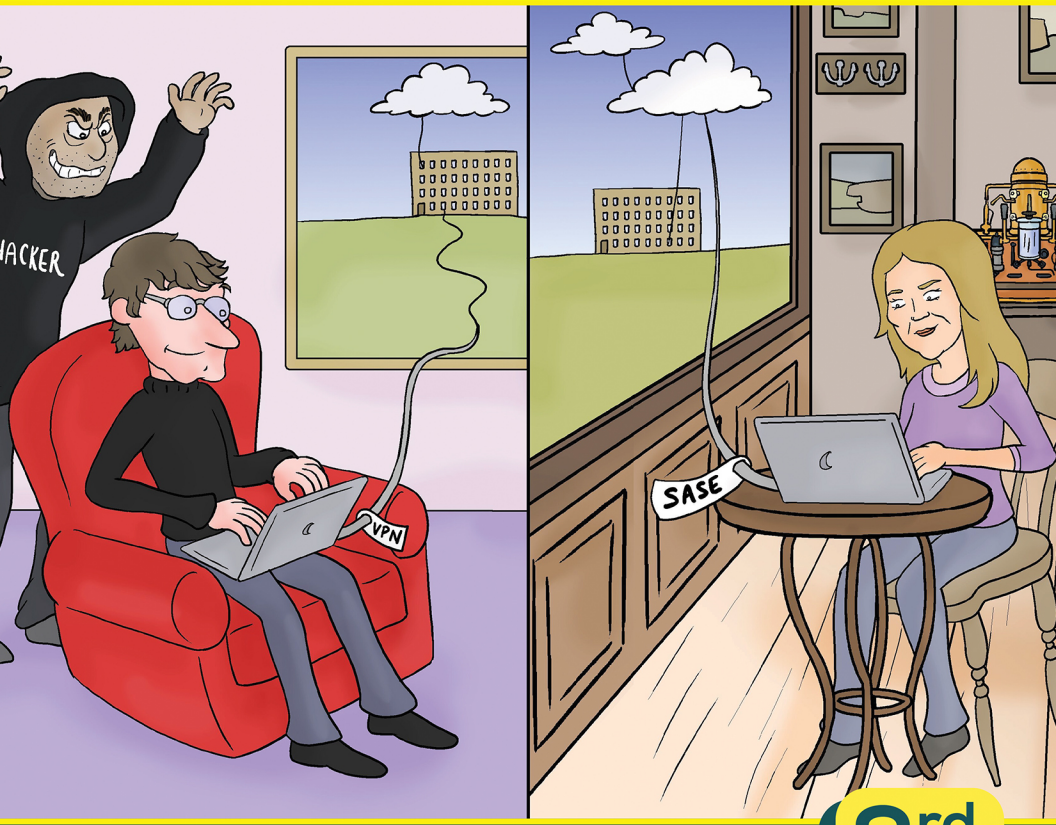
ConversationalGeek®

Conversational SASE and Zero Trust

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



In this book, you will learn:

- Common security problems companies face in the work from home era
- How to find a more secure solution to managing remote workers
- Why there is no one-size-fits-all solution to protecting data

3rd Edition

Sponsored by

Barracuda®

Sponsored by
Barracuda Networks

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. Hundreds of thousands of organizations worldwide trust Barracuda to protect and support them so they can focus on taking their business to the next level.

For more information visit
www.barracuda.com

Conversational SASE and Zero Trust

By Nick Cavalancia

ConversationalGeek®

Conversational SASE and Zero Trust

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):	Morgan Pratt
	Doris Au

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.

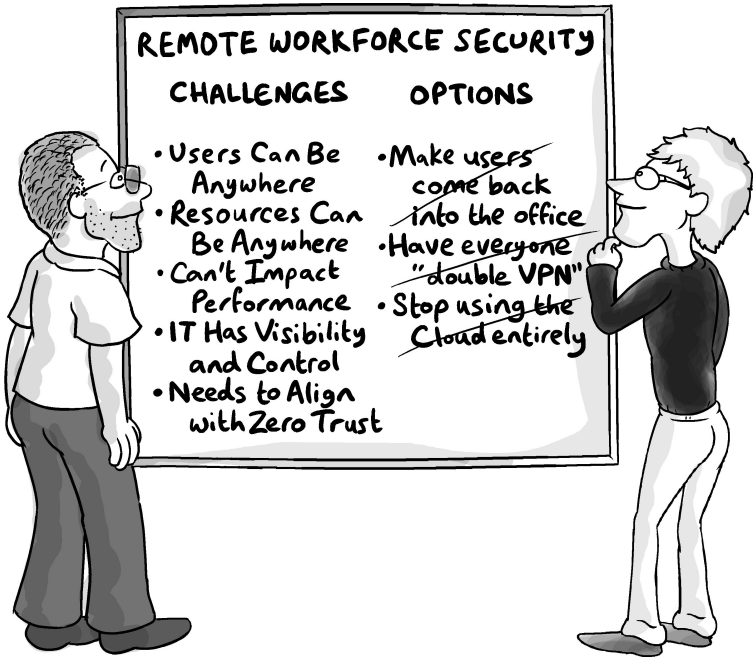
“Geek in the Mirror” Boxes

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!

Empowering and Securing the Hybrid Workforce



Back in 2020, everything changed with regard to an in-office workforce; the shift to a hybrid (and, in some cases, completely remote) workforce mixed with data increasingly being stored within the cloud and no longer inside the corporate network, created a recipe for a potential security disaster. The initial focus in 2020 was solely placed on keeping the business operational with as much as 70% of the workforce working remotely[1].

[1] Owl Labs, State of Remote Work (2020)

This put a strain on organizations early on, with IT teams struggling to accommodate all the new remote workers. Many businesses were literally digging up old VPN concentrator appliances from closets and using them as a stopgap measure. Organizations were doing whatever possible to stay afloat and keep the lights on. The priorities often were (in this order):

1. Application Access
2. Data Security
3. Operational Efficiency

Application access was obviously priority #1. You could not run your business if you didn't have access to the underlying applications. Then you had to figure out how to secure access to these apps and the data retrieved from them. The problem was further exacerbated when some of the now-remote workers didn't have a corporate laptop and were using their personal machines. The last priority, *operational efficiency*, is something that some organizations have only recently figured out as we've experienced evolutionary changes in application usage patterns and business dynamics over the last few years.

The big realization among business and technology leaders was that the old way of operating and securing the business IT infrastructure was not working. Security and network teams started receiving and asking questions like:

- Why should an employee have to learn how to VPN into company headquarters only to access an application hosted in the cloud?

- Why are we using on-premises hardware to secure remote user traffic destined to a cloud service? This is inefficient and a burden on resources.

- Why give employees (assuming it really is them since they're remote and maybe we can't be sure) access to an entire corporate network via VPN, when all they need is access to a single application hosted on the company's internal server?

- More often than not, this internal server is now located in the cloud, so why are the users going through on-premises security stack only to hairpin back out to the internet?

A new approach to security is needed. An approach that ensures more uniform visibility and control across the use of web, cloud, and private apps; and at the same time makes certain there are measures in place protecting sensitive data at every point it could be moved outside the realm of the organization's control.

At the same time, with the increase in cyberattacks from every direction, organizations are realizing the value of – and are moving towards – a Zero Trust security model in an effort to implement sustainable security that still enables the hybrid workforce.

And it's *the intersection* of these two shifts that becomes the challenge; figuring out *how do you provide uniform visibility and control without adding complexity to the network or negatively impacting the performance and experience of the hybrid workforce?*

Increasingly organizations are turning to a Secure Access Service Edge (SASE) architecture to provide a hybrid workforce to security connect to the web and cloud/private apps while safely using the data and resources they need to get their job done. And in conjunction with an organization's Zero Trust initiative, SASE can provide the needed visibility and control to ensure proper access and use of data.

The remainder of this eBook will provide insight into how organizations with a hybrid workforce can best securely connect users to corporate resources (inside and outside the corporate walls) using SASE, and how SASE can help facilitate a stronger state of Zero Trust.

Let's start by looking at the how (and why) organizations connect their remote workforce today and where SASE can simplify and increase user experience, performance, and organizational security.

The New Status Quo: Working from Home

Working remotely is the status quo for many businesses today. But why is it such a challenge for IT and security? Why can't organizations just buy beefier VPN appliances and *voila*, problem solved? To explain, we have to look at the changes sweeping the business technology world.

The past few years have seen an explosive growth in the rapid adoption of cloud services in the form of IaaS, SaaS, and PaaS. We have seen many in-house applications leave the corporate data center to be hosted in the cloud.

Additionally, we're continuing to see explosive growth in the frequency, sophistication, and number of cyber-attacks on organizations worldwide.

- Today, 62% of organizations believe cyberattacks are becoming more sophisticated, 55% say the impact of attacks is becoming more severe, and 53% believe cyberattacks are becoming more targeted[2]

---

[2] Barracuda, *Cybernomics report (2024)*

- 57% of organizations have experienced one or more cyberattacks in the last 12 months[2]

- 48% of organizations have suffered a data breach in the past 12 months and lost, on average, 340,000 individual records[2].

It's evident the threats are real and getting worse. And with the top concern by 83% of organizations revolving around remote devices and employees being breached[3], what should organizations do to counter this? What strategy should organizations adopt to help secure workers, their access, and the data they interact with?

The answers depend on where your organization is in its journey to the cloud. Roughly speaking, organizations can be divided into two categories:

1. Those who are *early* in their cloud journey

2. Those who are *part-way through* or *nearly complete* in their cloud journey

Historically, organizations have placed security as a low priority when considering their move to the cloud; the focus (like the shift to a remote workforce) tends to be on accessibility, reliability, and performance first and foremost. But what's needed is for security – at least, if nothing else, in the context of secure access – to be made an equal priority.

We'll discuss the two scenarios in the sections that follow, and then address what's necessary to provide a more secure method of access.

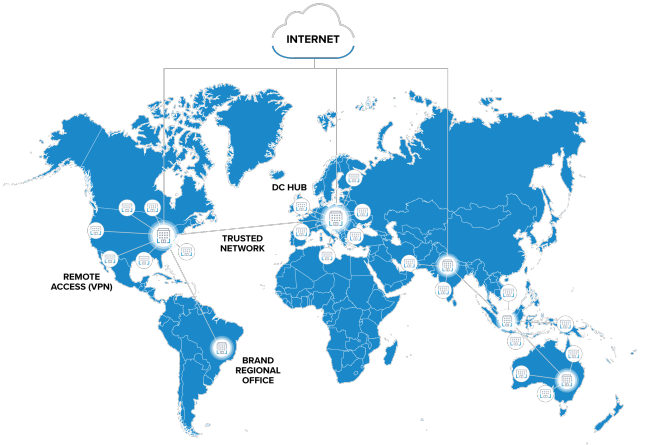
---

[3] VansonBourne, *The State of SMB Cybersecurity in 2024* (2024)

Organizations early in their cloud journey

For many years, organizations embraced the traditional “castle and moat” approach to security – the crown jewels were inside their brick buildings, which were surrounded by layered defenses (like firewalls, intrusion prevention, data loss prevention, etc.) to keep attackers and thieves out.

As organizations became more distributed – opening branch locations, having ‘road warriors’ operate outside the corporate network – they used networking technologies like MPLS leased lines and VPN software to connect the remote sites and remote users back into the network. In essence, these technologies transported remote workers inside the walls of the corporate castle so that they could work as if they were sitting inside the main office. This way, the defenses that protected the office could still protect people when they were not on-site. A typical architecture of a modern, large-scale environment resembles something like the picture below.



The MPLS/VPN approaches worked adequately even as applications and data began to move to the cloud. Of course, employees noticed that there was a performance lag because

the connection had to traverse the entire corporate network security stack and then hairpin back out to the internet, like what we see in the graphic below. This wasn't a big issue when most of the workers were on site. However, with most workers now being remote, performance bottlenecks began hindering productivity and created massive user experience issues.

As a workaround, some users realized that for certain apps hosted in the cloud, they could go directly to the app over the internet, bypassing the VPN (and any of the organization's other security controls).

Many organizations were not ready for this and did not have security controls in place for direct-to-internet connectivity. The result was the observing of their attack surface increase exponentially in real time. Something had to be done… (which I'll discuss further).

Organizations part-way through (or nearly complete in) their cloud journey

Let's now look at organizations that are further along in their cloud journey (which I assume is most of you reading this eBook). Nearly three-quarters (74%) of your IT architecture is hybrid with just under half (44%) of your workloads in the cloud[4]. You've fully embraced SaaS productivity apps like Microsoft 365, Google Workspace, Salesforce, and Adobe Creative Cloud. You may be also hosting virtual machines in the IaaS clouds of AWS, Azure and Google Cloud Platform (GCP). You may even have invested in re-writing a few of your legacy monolithic applications into micro-service architectures running on Kubernetes clusters in the cloud.

These kinds of organizations realize that backhauling user traffic through a VPN, only to let it go out to the internet again, is not going to work in the long run. So, you began allowing

[4] Netwrix, *Hybrid Security Trends Report* (2024)

users to go to the SaaS/IaaS/PaaS services directly over the internet. To keep people safe from internet-borne malware, security began to follow apps and data into the cloud. This paradigm shift from centralized castle and moat approach to decentralized security is still happening right now.

The challenge of the current cyberthreat landscape

Regardless of which journey box your organization fits into, cloud applications, services, and infrastructure have all become targets of cyberattack. As much as 73% of organizations have experienced a cyberattack in the cloud[4] – including account compromise, malware attacks, data leakage, data theft, ransomware and more.

Organizations have recently led with a combination of VPN and multi-factor authentication (MFA) to secure the channel and validate the user. But recent shifts in attacks focusing on VPNs have led to 56% of organizations experiencing one or more VPN-related cyberattacks in the last year[5]. And the evolution of MFA fatigue attacks used to socially engineer owners of credentials to approve compromised access to their own account should have organizations questioning whether the somewhat older thinking of "VPN + MFA" as the answer is even viable in today's state of cybersecurity.

Finding a more secure solution

As businesses and government agencies have become more distributed, we have seen a switch from the old approaches of having security in a central office (HQ), to having it in the cloud. And it's not just organizations on the cutting edge embracing this paradigm shift. In fact, the United States Cybersecurity & Infrastructure Security Agency (CISA) Trusted Internet Connection (TIC) 3.0 guidance is calling for US government

---

[5] Zscaler, VPN Risk Report (2024)

agencies to adopt a distributed Zero Trust Network Architecture (ZTNA) approach to security.

CISA's Trusted Internet Connections initiative has been out since 2007, with its latest iteration – version 3.0 – released earlier this year. TIC aims to help securely "accelerate the adoption of cloud, mobile, and other emerging technologies."

Read more at: goto.cg/CISA-TIC3

In addition to the activity in the public sector, security decision-makers (SDMs) in the private sector say developing a Zero Trust strategy is their number one security priority, with 96% stating that it's critical to their organization's success. On top of this, 61% of organizations claim to have at least started implementing a Zero Trust strategy[6]. If you're not familiar with the concept of Zero Trust, it starts with the premise "never trust; always verify". This means the traditional model of providing a user access to resources and assuming they a) are who they say they are, and b) should be allowed access, is misaligned with modern thinking around cybersecurity.

[6] Entrust, *2024 State of Zero Trust & Encryption Study* (2024)

The National Institute of Standards and Technology's (NIST) SP 800-207 Zero Trust Architecture document provides guidance for architecture and implementation of a Zero Trust network.

Read more about it at:
goto.cg/ZTA800-207

The evolution of tools supporting the new distributed security model began with "secure web gateways" (SWG) that protected employees as they accessed websites and web content. These were not just deployed on-premises, but also in the vendor's data center, whereby employees could connect to the "web gateway service" from the road. Next came the "cloud access security broker" (CASB) services that allowed organizations to implement security controls for data stored in cloud apps.

Over the past two years we have seen SWG and CASB functionality overlap to the point where today we a have a whole new category of products develop, falling under the SASE badge. SASE reinvents legacy, on-premises security stacks as a unified or converged security-as-a-service in the cloud. Remote workers utilizing SASE connect directly to corporate resources instead of first connecting via a VPN to corporate HQ, which solves the performance predicament. But more on that later. Ultimately, having security delivered from the cloud made it possible for organizations to have a uniform view of what was happening, no matter where they were working, and to enforce security policies consistently everywhere.

The common security problem: internal apps

OK, so I mentioned SASE and that is all well and good for securing access to cloud-hosted apps and services. But what about the applications that live on-premises? The reality is that

most mature organizations have private, line-of-business applications running in internal data centers or private clouds. For remote workers, getting to these applications from outside the office still requires extra effort. Usually, this means having remote workers use VPN software on their endpoint devices to connect into the internal network. The thing is… nobody likes using VPN software – for two reasons: first, it creates usability issues and, second, it's a huge security burden as well.

Nobody likes VPNs

VPNs are still, basically, a pain in the neck. Teaching people who have never used them before can be time-consuming: they have to remember which applications need them, how to start the VPN, how to stop it, and how to deal with the differences in performance. This creates confusion and even resentment, both of which get in the way of doing their jobs. Worse yet, VPNs are notorious for slowing down cloud apps, especially highly interactive ones like Microsoft 365 and other office collaboration suites. And these are the very ones that organizations have been switching to. People's frustration gets taken out on helpdesk teams and it motivates users to avoid going through VPN at all costs. Instead, they often look for cloud-based alternatives to internal private applications – magnifying the classic challenge of Shadow IT.

But the rabbit hole goes deeper. When a remote worker connects to corporate a VPN, he or she is typically given the same full range of access on internal networks as if working in an office. They can get to any application, any server, any database, and so on. This also means that anybody who is pretending to be an authorized user, or who has compromised the user's laptop or public Wi-Fi network they're connecting from, can also get to anything. This is not a new problem, but it is exacerbated by people working remotely, especially as the line between work and life begins to blur.

We all have probably had times when we used our business laptop to go to a recreational website, order dinner, or stream content that we might not do from a machine in the office. This kind of activity opens the door for attackers to compromise our devices and use them as a springboard for getting into otherwise-protected corporate networks. Limiting what remote users can access can be done with network security technologies such as firewalls. But setting up intricate rules for controlling which users can get to which parts of the network – called *microsegmentation* – requires expertise and can lead to errors as people move around.

Not just working remotely – working anywhere

Working from home is here to stay. I think this realization is sinking in for most of us. Even as we've seen users start returning to offices this year, it's more of a "partial return": maybe a few days a week in the office and the rest still at home. We're even seeing travel start up again, with users working from coffee shops, hotels, and airports. The assumption moving forward should be that users will be more likely than ever to work in different locations in the same day. This will put even more stress on IT systems that were heroically put in place to handle people working from their homes, and the cyber-security risks will keep multiplying.

The Big Need: Protecting Data

Earlier, I talked about how organizations set priorities when they had to accommodate everyone working from home on short notice. Priority #1 was application access. Priority #2 was data security – a much greater challenge. For starters, remote workers often have a treasure trove of sensitive data on their machines. To exacerbate the problem, in today's era of Bring Your Own Device (BYOD), the endpoint machine may not even be under corporate IT control. Not only does this make WFH a target-rich environment for thieves, but it also makes accidents more damaging and malicious acts easier to pull off. IT leaders around the world are fully aware of this. Which is why organizations are moving quickly to put in place data protection tools to prevent the misuse or loss of data from remote devices. Let's talk about this next.

Protecting data can be hard – and one size doesn't fit all!

The problem with most data protection technologies is that they take a static, black-and-white approach to security: users are either always allowed or always denied. This is even the case when we take the more sophisticated approach to making an access decision, utilizing attributes such as which user, what data, what location, what time, what app, etc. But that's not how the real world works. Most organizations trust people to follow corporate policies and exercise good judgment. They can download and copy sensitive data they need to get their job done. But, if they start making mistakes or abusing their freedom, there are rarely any security mechanisms to stop them. After all, they were already granted access based on the parameters I just mentioned. A new approach is needed. An approach that responds to users' behavior in real-time and places restrictions when their behavior deviates from the norm. In short, we need a risk-based data protection solution.

Protecting data also requires continuous visibility

There is a big push in the cybersecurity industry to develop data protection systems that are able to spot anomalies based on how people interact with data. In fact, in its Zero Trust Architecture guidance, NIST specifically calls for continuous monitoring of user behavior to improve an organization's security posture. Continuous activity monitoring systems use "indicators of behavior" (IoBs) to identify risky situations before they turn into breaches. These systems are most often used in two ways:

1. To continuously validate that people really are who they say they are (and not a thief or malware that has stolen the user's credentials)

2. To automatically personalize security according to the level of risk each individual poses at any given moment

So how do we go about implementing such a system?

SASE Brings It All Together

The short answer is *SASE*. SASE's architecture reinvents security technologies that used to be disparate products, turning them into integrated cloud services. It provides a platform for applying Zero Trust principles as a service, which makes securing people and data – anywhere – easier, more efficient, and more effective.

But first, a little history is in order. In the summer of 2019, Gartner published an architecture for consolidating in the cloud the different security tools that a distributed organization would require to keep its people and data safe no matter where they are[7]. Gartner named this cloud-delivered

---

[7] Gartner, *The Future of Network Security Is in the Cloud* (2019)

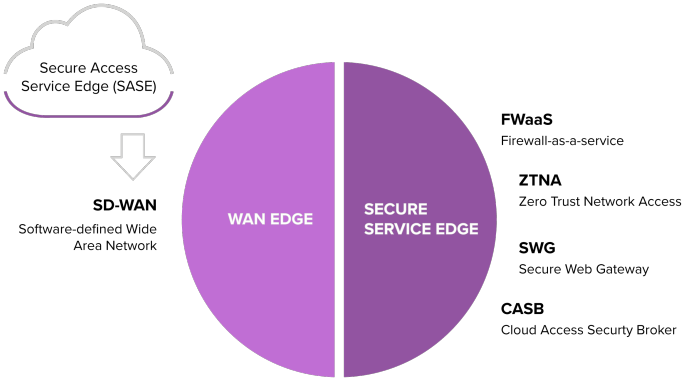
architecture “Secure Access Service Edge” or SASE. In its seminal SASE architecture publication, Gartner highlights two industry-changing trends in corporate IT today:

1. The legacy “data center as the center of the universe” network and network security architecture are obsolete and have become an inhibitor to the needs of digital business

2. The future of network security is in the cloud

As Gartner puts it, SASE is “an emerging offering combining comprehensive Wide Area Network (WAN) capabilities with comprehensive network security functions (such as SWG, CASB, Firewall as a Service [FWaaS] and ZTNA) to support the dynamic secure access needs of digital enterprises.” SASE calls for a unified cloud-based security-as-a-service architecture that applies Zero Trust principles across a range of capabilities. These capabilities include:

- NextGen Firewall / FWaaS
- SWG / URL Content Filtering
- Cloud Access / Action Control
- DNS protection
- Bandwidth Control
- Data Loss Prevention (DLP)
- Advanced Malware Sandboxing
- SSL Break and Inspect without any noticeable performance impact to the end user



SASE doesn't just move old security products into the cloud, it reinvents and integrates them to eliminate gaps and redundancies. It makes securing the use of web content, cloud apps, internal private apps, even network-level applications like SSH over the internet easy – keeping attackers out and sensitive data in.

A lot of security vendors are rushing to call their products SASE. It's critical to look for a SASE approach that brings all the concepts I've mentioned together in a way that puts data at the center and uses human behaviors to automatically personalize how policies are enforced. Think of it as 'data-centric SASE'.

The Big Takeaways

The world changed profoundly in the face of the COVID pandemic. Today's hybrid workforce and the increase in cyberattacks has created security challenges where users need to access on-prem and cloud-based data and applications. The old "castle-moat" approach to security can no longer keep up with the new remote work dynamic, nor the tactics used by threat actors who leverage legitimate credentials to gain access to organization's networks.

To address these challenges, novel solutions have come on the market. Solutions that are based on modern, cloud-based systems utilizing Zero Trust and behavior-centric principles to enable security to be uniformly delivered to people anywhere in the world.

SASE sits at the forefront, providing organizations with a range of capabilities that ensure the security of the organization's data and resources while empowering users to be productive – no matter where they work.

Sponsor Chapter: Barracuda – Empowering Hybrid Workforce Security with Secure Access Service Edge (SASE) Solutions

As businesses adapt to the reality of a hybrid workforce, ensuring secure access to corporate resources—whether on-premises or in the cloud—has become a critical challenge. The rapid shift from centralized office environments to remote workforces has exposed vulnerabilities in traditional security frameworks, which were never designed for today's highly distributed work model.

Organizations need a solution that provides seamless, secure access to resources and applications, regardless of where employees are working. This is where Barracuda Networks steps in. As a trusted provider of security solutions, Barracuda offers a robust portfolio designed to protect businesses in this new era of remote work. Their SecureEdge platform provides the foundation for delivering cloud-first security, protecting hybrid workforces through comprehensive Secure Access Service Edge (SASE) architectures.

Securing Access, the Barracuda Way

Barracuda's network and cloud security solutions are purpose-built to help organizations tackle the complexities of securing hybrid work environments. Below are the key offerings that enable secure, efficient access for remote and on-premises workers alike:

Barracuda SecureEdge

Barracuda SecureEdge is a comprehensive Secure Access Service Edge (SASE) platform that secures access to applications hosted in the cloud or on-premises, enabling organizations to seamlessly protect their remote workforces. Its key components include:

- Unified Cloud-based Security: SecureEdge devices integrate network security functions such as secure web gateways (SWG), firewall, and secure VPN capabilities into a unified, cloud-delivered platform.

- Zero Trust Network Access (ZTNA): SecureEdge Access operates on Zero Trust principles, ensuring that users are authenticated and verified before gaining access to any network resource. This reduces the risk of unauthorized access, even for remote users.

- Optimized Performance for Cloud Apps:
  By eliminating inefficient traffic backhauling, SecureEdge improves the performance of cloud applications, providing users with fast, secure access to their SaaS and IaaS services.

- Comprehensive Visibility and Control: Administrators benefit from centralized control, gaining insight into all users, devices, and applications within the network. SecureEdge ensures consistent security policies are applied across the board.

Addressing the Challenge of Secure Access

Barracuda SecureEdge provide critical benefits to organizations managing the complexities of a hybrid workforce. Here's how these solutions address key challenges:

Elimination of VPN Bottlenecks and Improved User Experience

In traditional setups, remote workers often rely on cumbersome VPNs, leading to poor performance, especially when accessing cloud applications. With Barracuda SecureEdge, organizations can move away from outdated VPN infrastructure. SecureEdge provide secure, direct access to applications without performance degradation, resulting in a significantly improved user experience for remote employees.

By avoiding the need for inefficient traffic backhauling through centralized data centers, SecureEdge allows users to access cloud-based resources faster and more securely. This translates into greater productivity and reduced frustration for employees working remotely.

Enhanced Security with Zero Trust Architecture

SecureEdge is built with Zero Trust framework in mind, ensuring that no user or device is trusted by default, regardless of whether they are inside or outside the corporate network. This model provides robust protection against modern cyber threats, including account compromise, phishing, and malware attacks, which are increasingly targeting remote workers.

The Zero Trust approach ensures that users' identities and devices are continuously verified before they can access any application, mitigating the risk of unauthorized access to sensitive data. By integrating multi-factor authentication (MFA) and end-to-end encryption, these solutions ensure that even if credentials are compromised, unauthorized actors cannot access critical business resources.

Comprehensive Visibility and Centralized Control

For IT teams, managing a hybrid workforce can be daunting, especially when it comes to ensuring security across a diverse range of devices, networks, and locations. Barracuda SecureEdge provide centralized, cloud-based management, enabling IT administrators to maintain full visibility into who is accessing what, from where, and with which device.

With detailed insights and analytics, administrators can monitor user activity and enforce security policies consistently across both cloud and on-premises resources. This centralized approach simplifies management and helps ensure that security policies are both uniform and adaptive to the changing nature of today's hybrid workforce.

Scalability and Future-Proofing for Growing Hybrid Workforces

As businesses continue to embrace hybrid work models, Barracuda SecureEdge is designed to scale seamlessly.

Whether an organization is expanding its workforce or increasing its reliance on cloud services, Barracuda's cloud-first architecture can adapt to changing needs without compromising security or performance.

These solutions are built to integrate with an organization's existing security infrastructure, making them future-proof as businesses evolve and adopt more sophisticated digital technologies. By offering a comprehensive security architecture that grows with the business, Barracuda helps organizations stay agile and secure in an increasingly digital world.

Consistent Security Across Cloud and On-Premises Applications

Many organizations are still navigating a hybrid IT environment, with some applications hosted on-premises while others are fully cloud-based. Barracuda's solutions allow organizations to secure both cloud and internal applications uniformly. SecureEdge offers direct access to cloud-hosted apps, while SecureEdge Access, an agent, ensures secure connections to internal applications without the need for traditional VPNs, which can be both inefficient and insecure.

By providing consistent security regardless of where applications are hosted, Barracuda ensures that hybrid workforces can securely access the resources they need, without compromising on performance or protection.

The Big Takeaways

The shift to a hybrid workforce has created both challenges and opportunities for businesses looking to secure their distributed teams. Barracuda, through its SecureEdge platform, offers a comprehensive, cloud-first approach to securing remote and on-premises resources, utilizing Zero Trust principles and SASE architecture. By eliminating VPN bottlenecks, enhancing security, providing centralized management, and ensuring scalable, consistent protection for all applications, Barracuda empowers organizations to safely embrace the hybrid work model.

Barracuda's cybersecurity solutions are not just about securing access—they're about future-proofing the organization's entire security architecture to meet the demands of today's ever-evolving workforce.

Visit Barracuda's website at barracuda.com to learn more about their easy-to-purchase and deploy cybersecurity solutions.


Barracuda
Barracuda
SecureEdge™
A single platform for all your SASE needs.
FIREWALL | ZERO TRUST | WEB SECURITY | SD-WAN
Learn more today!
barracuda.com/partners/msp/become-a-partner

Quickly become conversational about the role of SASE and Zero Trust in securing remote workers

The forced shift to a hybrid workforce combined with data increasingly being stored within the cloud, has created a recipe for a potential security disaster for organizations. To keep working in the pandemic, many have relied on old technology like VPNs, but with the dust settling this technology is no longer fit for purpose and new solutions are essential. This book looks at why SASE sits at the forefront of how we tackle the challenge of securing remote workers.

About Nick Cavalancia

Nick Cavalancia is a technical evangelist, 4-time Microsoft MVP, and CEO of Conversational Geek. He has over 30 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.