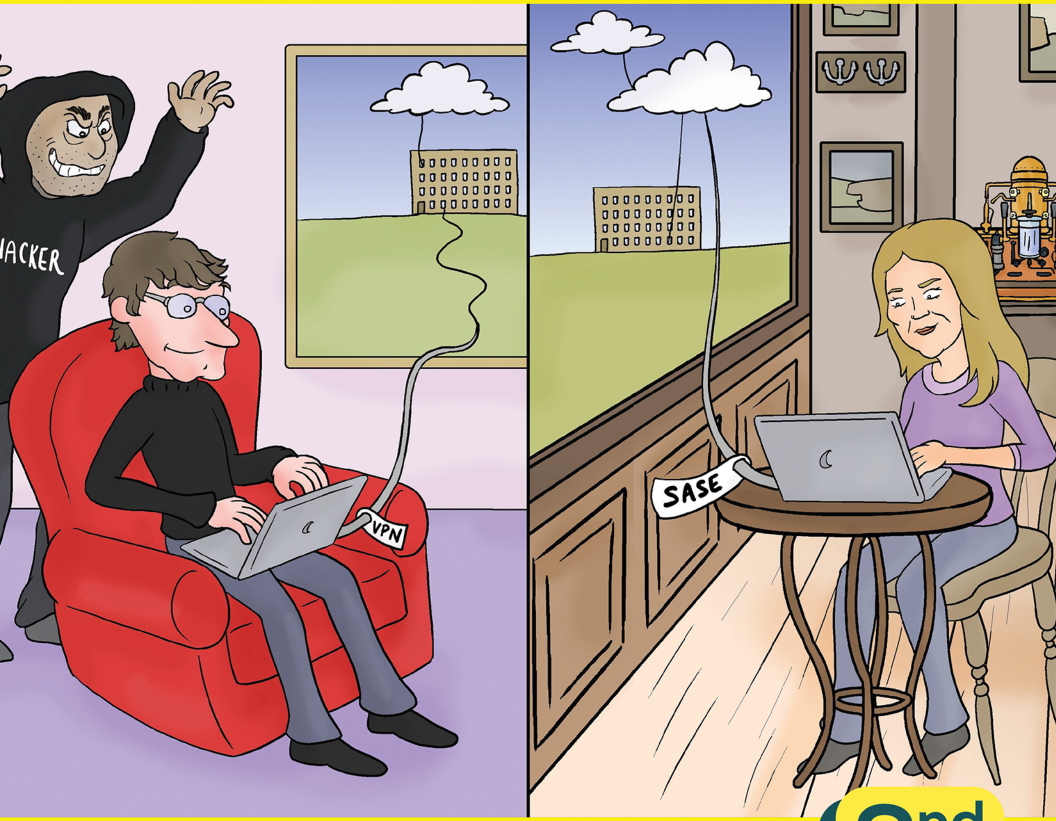
ConversationalGeek®

Conversational
SASE and Zero Trust

By Andrey Zhuk (Cloud Solutions Architect)



2nd Edition

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

Sponsored by
Forcepoint

Sponsored by
Forcepoint

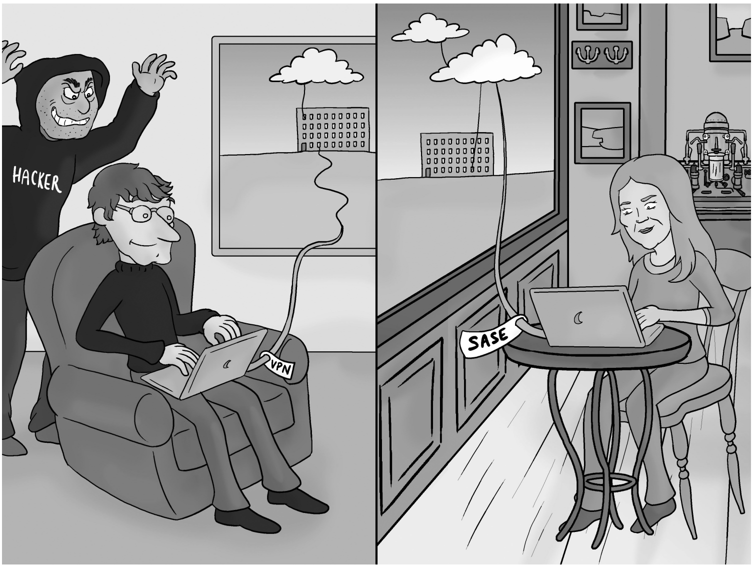
Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

Forcepoint

For more details visit
www.forcepoint.com

Conversational SASE and Zero Trust

By Andrey Zhuk



ConversationalGeek®

Conversational SASE and Zero Trust

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Conversational Geek, the Conversational Geek logo, and J. the Geek are trademarks of Conversational Geek®. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

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:	Andrey Zhuk
Project/Copy Editor:	Pete Roythorne
Content Reviewer(s):	Kim Hahn Jeffrey Birnbaum Ben Webb

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.

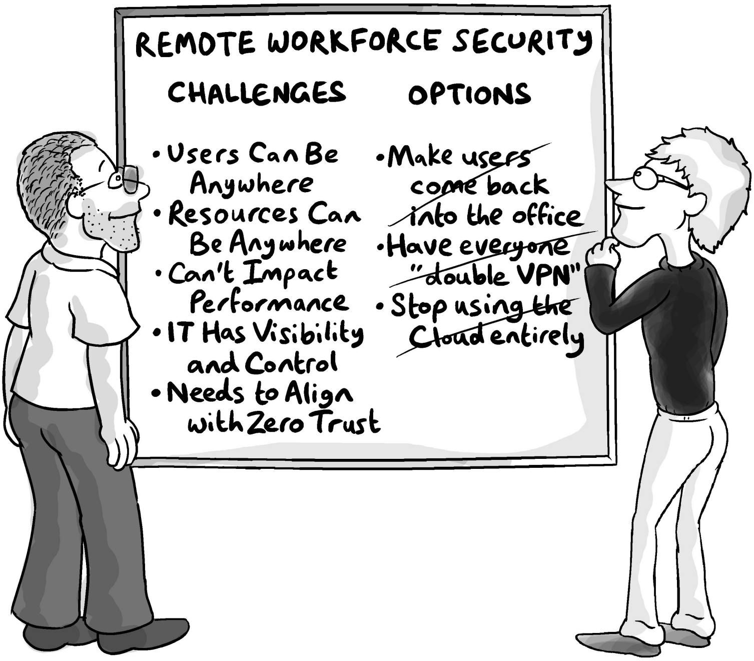
“Geek in the Mirror” Boxes

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


REMOTE WORKFORCE SECURITY
CHALLENGES
OPTIONS
• Users Can Be Anywhere
• Resources Can Be Anywhere
• Can't Impact Performance
• IT Has Visibility and Control
• Needs to Align with Zero Trust
• ~~Make users come back into the office~~
• ~~Have everyone "double VPN"~~
• ~~Stop using the Cloud entirely~~

Recent worldwide events have organization’s ability to secure its’ data and environment changed in 2020. And it didn’t matter if they were a small or very large company, 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 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 in the pandemic, with IT teams struggling to accommodate all the new remote workers. Many of my customers 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 most organizations are still figuring out to this day as we see evolutionary changes in application usage patterns and business dynamics in the era of COVID.

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 – the 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 as part of a 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 from home (WFH) is the new normal of business operations, the new status quo for the foreseeable future. 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.

Even without the COVID-19 pandemic of 2020, the past couple years were interesting times for corporate IT worldwide. We have seen rapid adoption by organizations 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. Most organizations were in the middle of digital transformation projects that involved moving applications, data, and infrastructure from internal data centers and networks up into the cloud. We’ve even seen some organizations do an “almost” 180°, where they went to embrace the cloud, only to realize that cloud is not a panacea and hybrid cloud is the more optimal approach. In short, corporate IT was undergoing many changes as it embarked on the journey to the cloud and the new consumption model for applications.

Then COVID hit.

Employees all went remote overnight. Organizations had to quickly figure out how to secure their remote workers and the sensitive data they needed to do their jobs. This wasn’t easy, especially with everything changing so quickly. Having everyone work remote, beyond traditional defenses, increased the attack surface of organizations, making them more vulnerable.

Fast forward to 2022, and we’re continuing to see explosive growth in the frequency, sophistication, and number of cyber-attacks on organizations worldwide.

- Over half of organizations believe a malware/ ransomware attack is very (31%) to extremely (23%) likely to happen (to them) in the next 12 months.[2]

- Two-Thirds of Organizations Have Experienced Spear Phishing Attacks in 2021[3]

- Organizations have as much as a 70% chance of experiencing a Business Email Compromise attack weekly[4]

It’s evident the threats are real and are getting worse. And a majority of CISOs (78%) say attacks have increased as a result of more employees working from home[5]. So, what should organizations do to counter this? What strategy should

[2] Cybersecturity Insiders, *Ransomware & Malware report (2022)*

[3] GreatHorn, *Business Email Compromise Report* (2021)

[4] Abnormal Security, *Q3 2021 Email Threat Report* (2021)

[5] Carbon Black, *Global Security Insights Report* (2021)

organizations adopt to help secure their workers and their data?

The answers depend on where an organization is in its' journey to the cloud. One may ask: *aren't there any organizations that are completely in the cloud?* Those companies do exist, but they are mostly start-ups and smaller organizations that are agile, with little to no on-premises infrastructure, and who had embraced the new technology paradigm even before the pandemic. In fact, many of these companies don't even have offices. Unfortunately, large enterprises do not fall into this category. Most established larger organizations have technology assets and business processes that existed before there even was a "cloud."

To that end, roughly speaking, organizations can be divided into two categories:

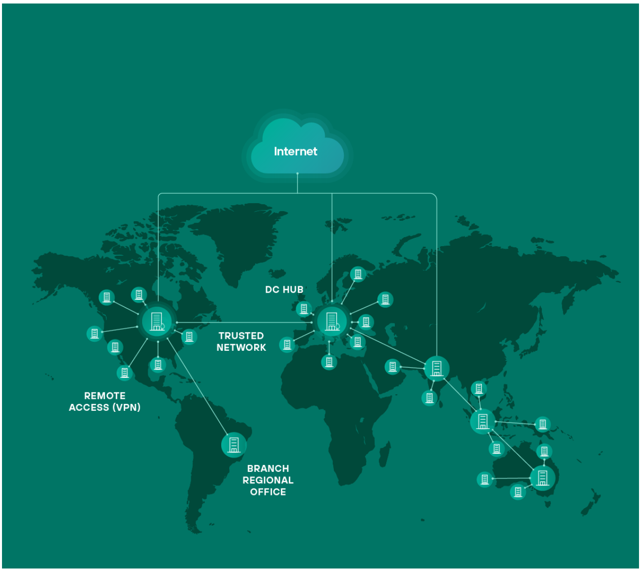
1. Those who were *early* in their cloud journey
2. Those who were *part-way through* their cloud journey

We'll discuss the two scenarios in the sections that follow.

Organizations early in their cloud journey

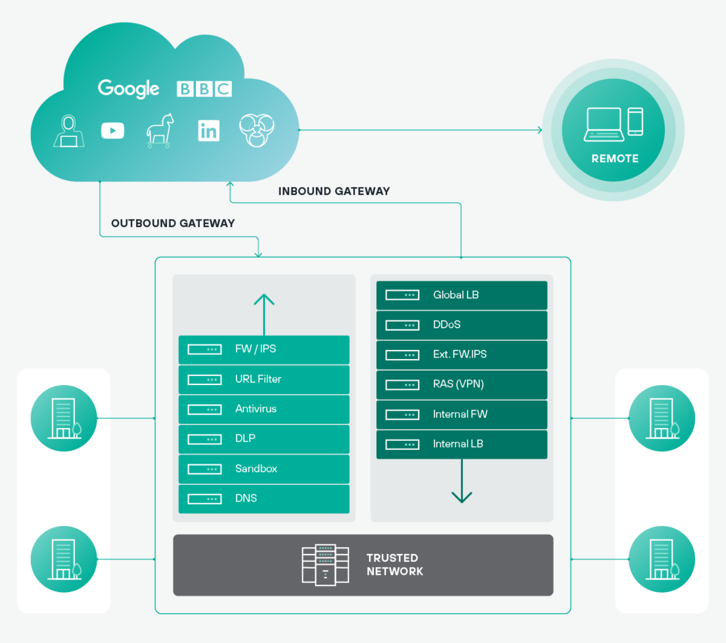
For many years, organizations embraced the traditional "castle and moat" approach to security – the crown jewels were inside their brick buildings, which were surrounded by layered defenses (like firewalls, intrusion prevention, data loss prevention, etc.) to keep attackers and thieves out.

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 their cloud journey

Let's now look at organizations that were further along in their cloud journey. They have fully embraced SaaS productivity apps like Microsoft 365, Google G Suite, Salesforce, Box, and Adobe Creative Cloud. They may be also hosting a few virtual machines in the IaaS clouds of AWS, Azure and Google Cloud Platform (GCP). They may even have invested in re-writing a few of their legacy monolithic applications into micro-service architectures running on Kubernetes clusters in the cloud. These organizations realized that backhauling user traffic through a VPN, only to let it go out to the internet again, was not going to work in the long run. These organizations began allowing 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 happening right now.

Finding a more secure solution

As businesses and government agencies are becoming more distributed, we will see 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 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: **https://www.cisa.gov/trusted-internet-connections**

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, 76% 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.

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

Read more about it at:
https://bit.ly/ZTA800-207

So yes, this shift is real and will not go away even after the COVID pandemic ends.

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

[6] Microsoft Security, *Zero Trust Adoption Report* (April 2021)

SASE badge. SASE reinvents legacy, on-premises security stacks as a unified or converged security-as-a-service in the cloud. Remote workers utilize 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

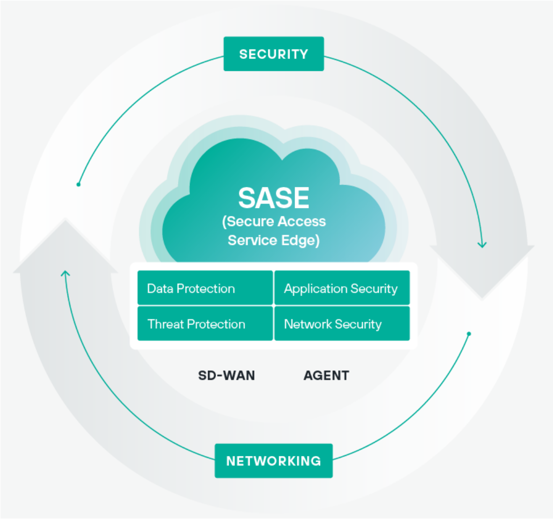
- DNS protection

- 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.

Forcepoint: Practical, Real-World Solutions for Securely Working Anywhere

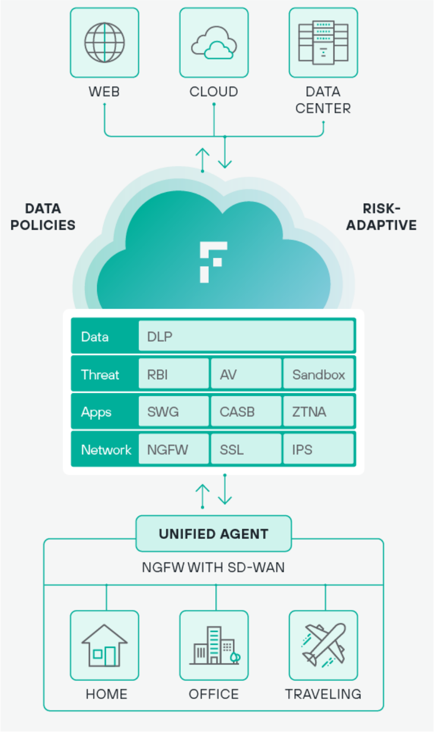
Let's now turn our attention to the practical implementation of SASE and Zero Trust. Forcepoint is the pioneer in combining Zero Trust and risk-based monitoring principles in its product lines. This allows your organization to provide your workers safe access to web, cloud, and private apps from anywhere while keeping advanced threats out and sensitive data in. Forcepoint's unique approach brings together SASE control and protection, cutting-edge data security, and the industry's first risk-based system for dynamically personalizing security enforcement according to each user's own actions.

The Forcepoint approach to SASE is designed to collect contextual information (telemetry) from various parts of the IT chain, including indicators of behavior about what people are doing, context about devices, and the sensitivity of different applications and data. Its automated behavioral intelligence system connects the dots across all of this information to dynamically compute risk scores for every user that enables policy enforcement to be automatically personalized, both by the SASE platform and any third-party systems that integrate with it, such as SIEMs, Identity Providers, and other sensors.

Forcepoint solutions don't just move old security technologies into the cloud; it reinvents them to eliminate the gaps and redundancies that plague point products. Forcepoint brings the following industry-leading security capabilities:

- Discovery and Classification – Discover data everywhere, whether on premises or in the cloud, and classify it by applying tags, including Microsoft Azure Information Protection (AIP), Boldon James and Titus.
- Advanced Data Detection – Leverage advanced detection and forensics like fingerprinting, OCR and machine learning to identify sensitive data.
- Unified Agent – The unified agent from Forcepoint helps to eliminate endpoint software sprawl and the Forcepoint SASE platform makes it possible to enforce the same policies in different places, wherever is most appropriate for any given situation.
- Human-Centric Analysis – Forcepoint Risk-Adaptive Protection enables behavior-centric, continuous, risk-based enforcement, and automated personalization of security controls to be applied where – and when – they're needed most.
- Single Pane of Glass Visibility – Through Forcepoint dashboards, they help you understand what is happening throughout your environment.
- Third Party Integration – Finally, the Forcepoint platform works with other parts of your IT infrastructure, from identity providers and different sources of behavior and device telemetry to SIEM and other tools that your operations depend upon.

Forcepoint rises up to the challenge by connecting the dots between SASE and Zero Trust, and offers organizations a unique way to transform their business through cloud delivered, converged, security platform.



A platform that brings together SASE capabilities under one roof. Customer organizations have the ability to subscribe to only the capabilities they need, while having the option to grow in the future. These key capabilities include several means to securely connect the user to the resources they need without sacrificing performance:

- **Secure Web Gateway** – Cloud-delivered SASE protection for protecting use of the public web, complete with true world-class data loss prevention technology in the cloud.

- **CASB** – Cloud-delivered SASE protection for protecting use of SaaS and IaaS, complete with true world-class data loss prevention technology in the cloud.
- **ZTNA** – Cloud-delivered Zero Trust Network Access for giving remote workers safe access to private applications without the complexities, bottlenecks, and risks of VPNs.

And supplemental capabilities that include work to secure data and access in real-time based on risk:

- **Next Generation Firewall** – Advanced NGFW with secure SD-WAN and global scalability.
- **Data Loss Prevention** – industry-leading protection for sensitive data and intellectual property everywhere – in the cloud, in networks, and on users' endpoint devices.

After all, that's what it's all about: enabling people to work anywhere – and everywhere – while keeping themselves and the data they depend upon safe.

Security Simplified

Consistent security across any app, device or location—all from one security platform.

Forcepoint

forcepoint.com

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 Andrey Zhuk

Andrey Zhuk is a Cloud Security Architect at CTG Federal, where he helps US Government Agencies adopt new cloud services and secure agency assets in the cloud. Andrey is an experienced cloud, cyber and network architect with over 13 years of experience in US Federal Government space.

ConversationalGeek®

For more books on topics geeks love visit

conversationalgeek.com