eBook

Forcepoint | Powered by ConversationalGeek

How Zero Trust Provides a Breach-Free Approach Using SASE

A Guide to Empowering and Securing Remote Workers

forcepoint.com

Note from the Author

The world turned upside down in 2020, as people fled their offices to work from home in the face of the global pandemic. Organizations scrambled to adapt, with technology departments working overtime implementing infrastructure changes to accommodate the new work dynamic. As the pandemic progressed, what began as a temporary "new normal," became "this is how things will be going forward." People are no longer just working from home, they are working anywhere–at home, in the office, at branch locations, even on the road, and often from multiple locations in the same day. Securing this new "anywhere" worker with traditional approaches is proving problematic. A new way of thinking is needed. In this eBook we will explore the challenges of securing the anywhere worker and provide a solution. A behavior-centric solution that is based on modern, cloud-based systems that apply Zero Trust principles and behavior monitoring to secure workers and data anywhere.

Introduction

Much has changed in the past 20 years in how we view the concept of "workplace." I remember my first job out of college with an IT consulting company. After a day of onboarding activities, I was escorted to my cubicle and told to make myself at home. The IT security protocol was to simply lock/shut down the computer workstation at the end of the workday and go home. A couple of years later, I was promoted and given an office. To support my newly expanded responsibilities, I was issued a laptop computer, so I could take my work home. On the laptop was a Virtual Private Network (VPN) client that would allow me to dial back into the corporate infrastructure to perform my duties when I was on the road or working remotely. An interesting side effect of me having a corporate VPN-equipped laptop was that I was spending less time in the office, showing up in person only for meetings. And it wasn't just me. Everyone was doing it.

Fast forward to the mid-2010s and corporations everywhere were beginning to move to the "office hoteling" model. With office hoteling, employees could reserve office space on-demand. This allowed many corporations to reduce their expensive office leases and also gave rise to "shared workspace" companies like WeWork and Carr Workplaces. In fact, the IT consulting company I was working for at the time eliminated nearly 80% of its office space, including multiple high-rise buildings.

So where am I going with this? Well, the work from home (WFH) trend is not new. Organizations worldwide were OK with employees working remotely, where appropriate, and there were operational savings to be had in supporting the WFH trend. However, the COVID-19 pandemic changed the rules overnight. According to Gartner we are seeing that 82% of companies plan to allow employees to work remotely.[1] Early on in the pandemic, organizations were 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 go back out to the internet?

A new approach to security is needed. One based on cloud-native solutions that use a data-centric approach to gauge who is trusted to access what resource and under what conditions. And this is what the rest of this eBook is all about.

[1] Gartner Survey, June 5, 2020

The New Status Quo: Working from Home

Working from home 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.[3] 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.

[3] Rogers, Owen and Atelsek, J. "Economics of Hybrid and Multi-Cloud." 451 Research, November 2019,

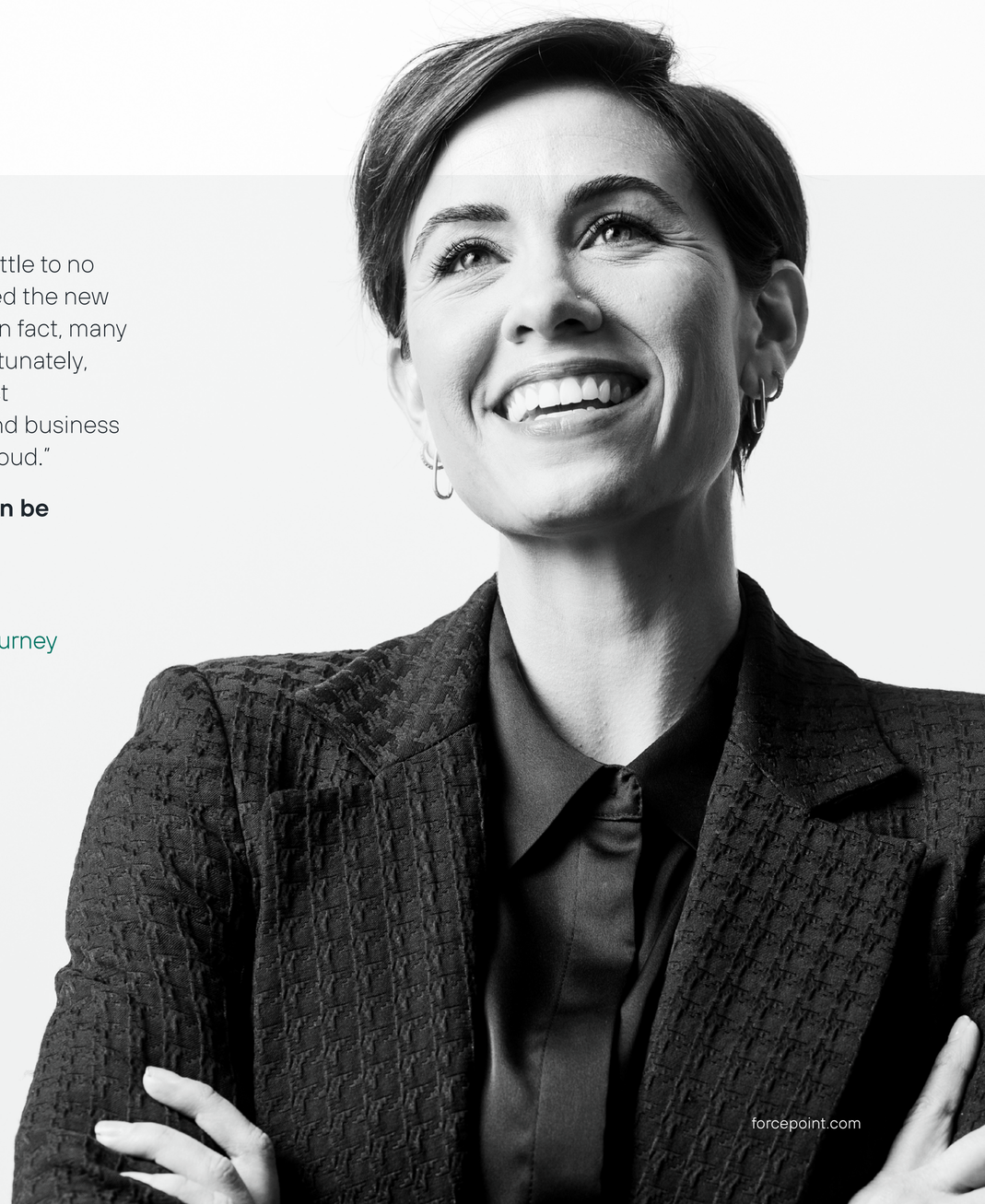
Employees all went remote overnight. Enterprises had to quickly figure out how to secure their remote workers and the sensitive data they needed to do their jobs. This wasn't easy, especially with everything changing so quickly. Having everyone work remote, beyond traditional defenses, increased the attack surface of organizations, making them more vulnerable. We saw an explosion of cyber-attacks on organizations worldwide. Even if we look at something as basic as phishing, the numbers are dramatic: in the first three weeks of March 2020 alone, we saw a 667% increase in phishing attacks from February 2020.[4] The attacks didn't stop there, culminating at the end of 2020 with the highly publicized FireEye breach by a nation state,[5] followed by an attack on the US Department of Treasury,[6] and then an attack on SolarWinds' supply chain two days later.[7]

So, the threats are real. Now, what should organizations do to counter this? What strategy should enterprises 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 enterprises 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.



[4] Banham, Russ. "Rise of Remote Work: Preventing Cybersecurity Risks." Forbes, 28 May 2020
[5] ThreatPost.com
[6] TheGuardian.com
[7] CRN.com

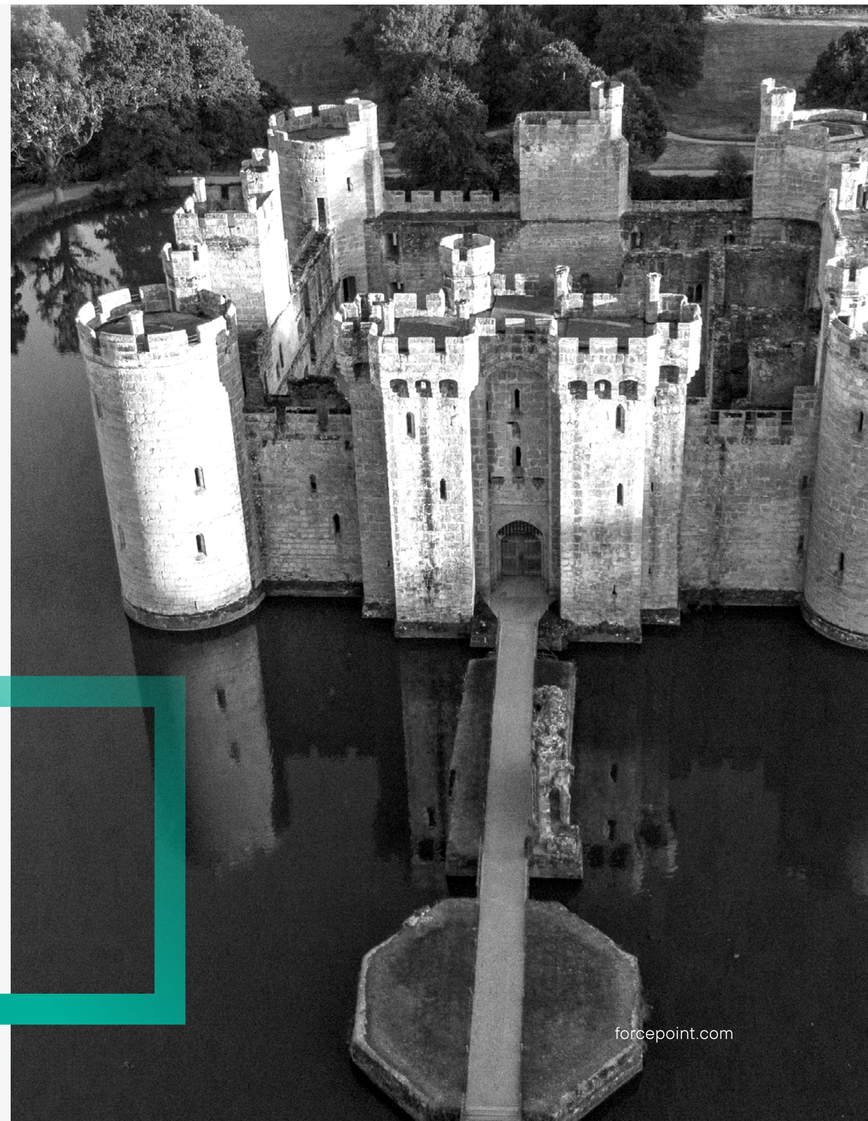
Enterprises who were early in their journey to the cloud

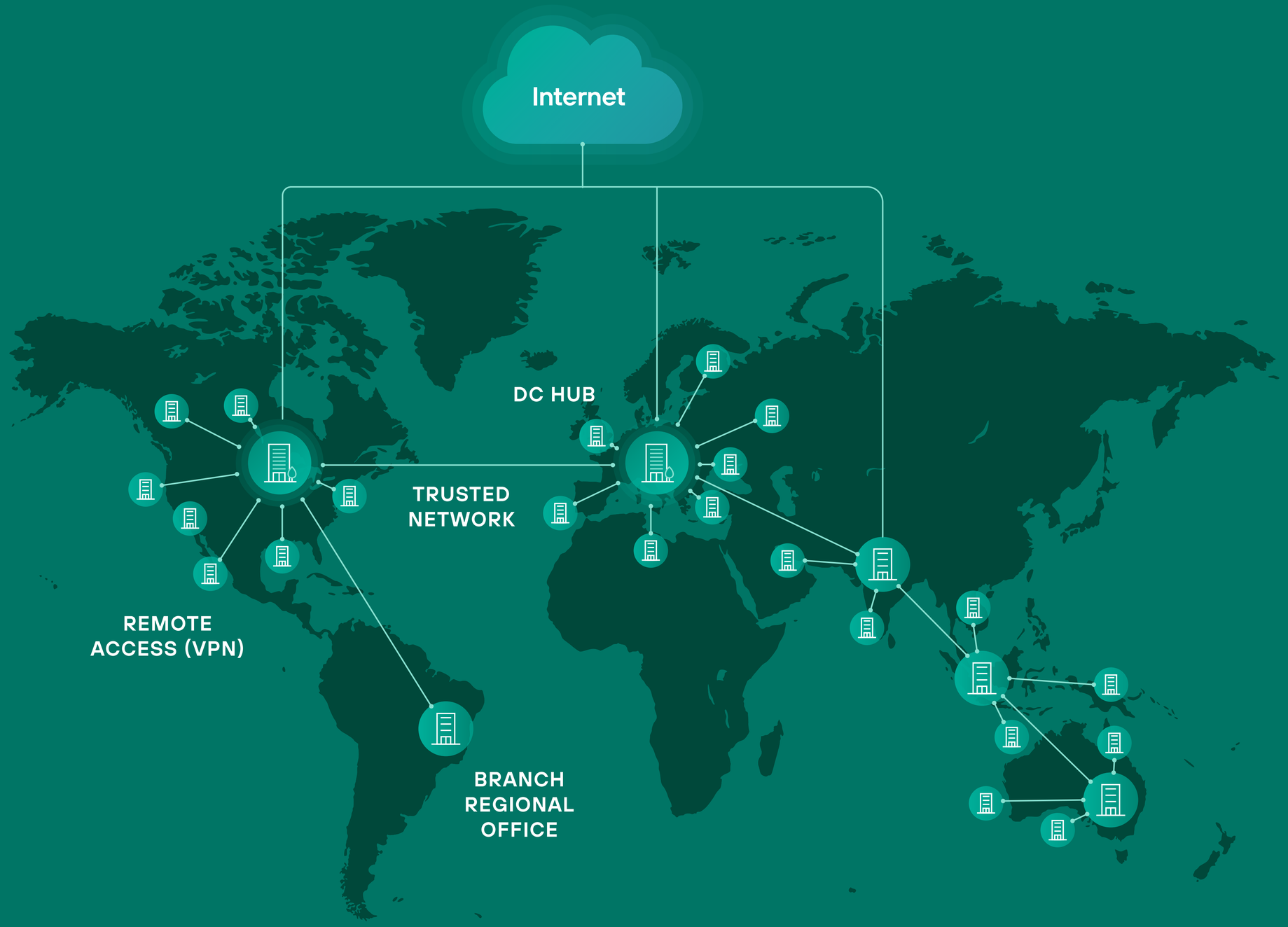
For many years, organizations embraced the traditional castle and moat approach to security.

The crown jewels were inside their brick buildings, which were surrounded by defenses (like firewalls, intrusion prevention, data loss prevention, etc.) to keep attackers and thieves out.

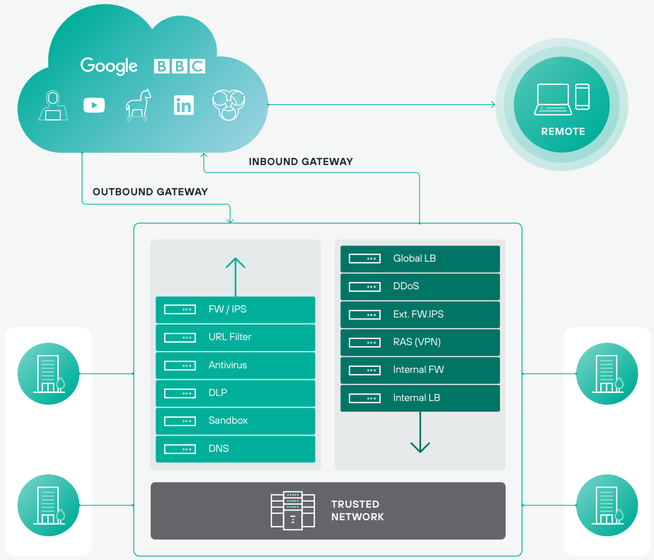
As organizations became more distributed–opening branch locations, having 'road warriors' operate outside the corporate network–they used networking technologies like MPLS leased lines and VPN software to connect the remote sites and remote users back into the network. In essence, these technologies 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 enterprise looks something like the picture to the right.

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 go back out to the internet, like what we see in the graphic on the next page– 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.




Internet
DC HUB
TRUSTED NETWORK
REMOTE ACCESS (VPN)
BRANCH REGIONAL OFFICE

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 organizational security controls). Many organizations were not ready for this and did not have security controls in place for direct-to-internet connectivity. Enterprises were observing their attack surface increase exponentially in real time. Something had to be done, which we will discuss below.



Enterprises who were part-way through their journey to the cloud

Let's now look at organizations that were further along in their cloud journey. These enterprises have fully embraced SaaS productivity apps like Microsoft Office 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.

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 U.S. government agencies to adopt a distributed Zero Trust Network Architecture (ZTNA) approach to security.[9] 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 enterprises 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 have a whole new category of products called SASE, or Secure Access Service Edge. SASE reinvents legacy, on-premises security stacks as a unified or converged security-as-a-service in the cloud. Remote workers connect to SASE directly instead of connecting via the 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.

[8] CISA.gov
[9] CISA.gov

What most enterprises have in common: internal, private applications

Ok, so we 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. And it's not just a usability thing. It's a huge security burden as well.

Why nobody likes VPNs

Let's take a walk down memory lane. In the early days of the internet and corporate IT, VPNs provided a groundbreaking capability. The traveling salespeople and road warriors of old could connect to corporate HQ and check email via on-premises Exchange or Lotus servers, and even interact with business applications running on Oracle or SAP. Yes, using a VPN was a pain in the neck, but so was using computers in general (think MS-DOS command prompt and Windows 95). The internet was not yet the scary place it is now. These were the early days of IT.

Fast forward to today, and the internet has exploded, the application consumption model has changed; we have social media and everyone is hyperconnected–yet we are still using foundationally the same VPN technology. Sure, we went from PPTP to IPSec and IKE to TLS-based technologies like OpenVPN. But that's all under the covers. To the end-user nothing changed. 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. The very ones that enterprises 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.

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 when people start returning to offices at some point in 2021, it will likely be a partial return: maybe a few days a week in the office and the rest still at home. Eventually, they'll start traveling again, working from coffee shops, hotels, and airports. In fact, people 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 cybersecurity risks will keep multiplying.

The Big Need: Protecting Data

Earlier, we 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, it also makes accidents more damaging and malicious acts easier to pull off. IT leaders in enterprises 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.

But 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 we 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. We need a behavior-centric data protection solution.

Continuous activity monitoring

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 SP 800-207 Zero Trust Architecture guidance, National Institute of Science and Technology (NIST) specifically calls for continuous monitoring of user behavior to improve an organization's security posture.[10] 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?

[10] NIST SP 800-207. Zero Trust Architecture

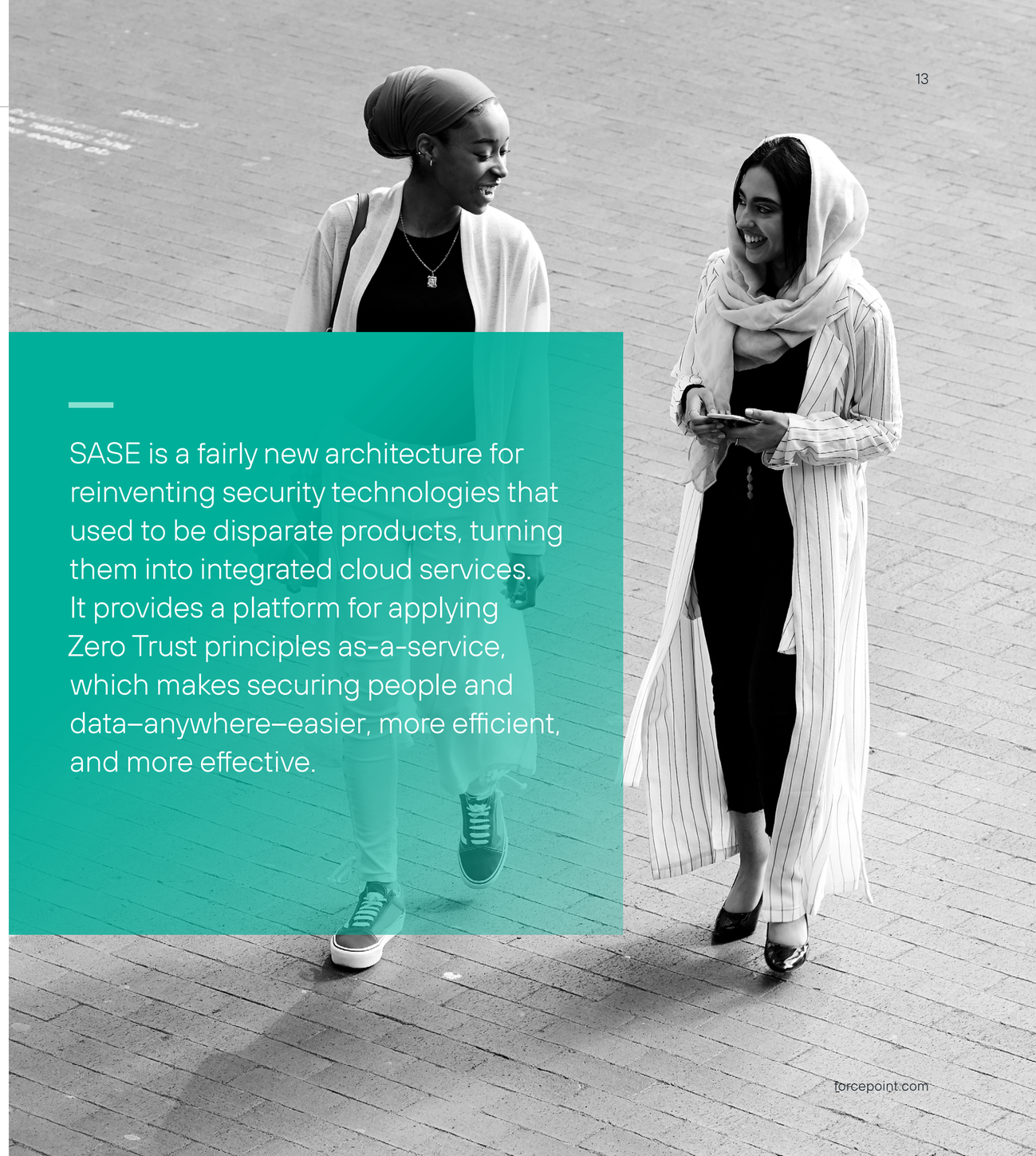
SASE Brings It All Together

The short answer is SASE. SASE is a fairly new architecture for reinventing 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. While most of the vendors in the security industry are all rushing to call their products SASE, Forcepoint is the only vendor to bring it all together in a way that puts data at the center and uses human behaviors to automatically personalize how policies are enforced. They call their approach data-centric SASE.

But first, a little history is in order. In the summer of 2019, Gartner published an architecture for consolidating in the cloud three different security tools that a distributed organization would require to keep its people and data safe no matter where they are.[11] Gartner named this cloud-delivered architecture 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



SASE is a fairly new architecture for reinventing 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.

[11] MacDonald, Neil, Orans, L., Skorupa, J. "The Future of Network Security Is in the Cloud." Gartner, 30 August 2019

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."

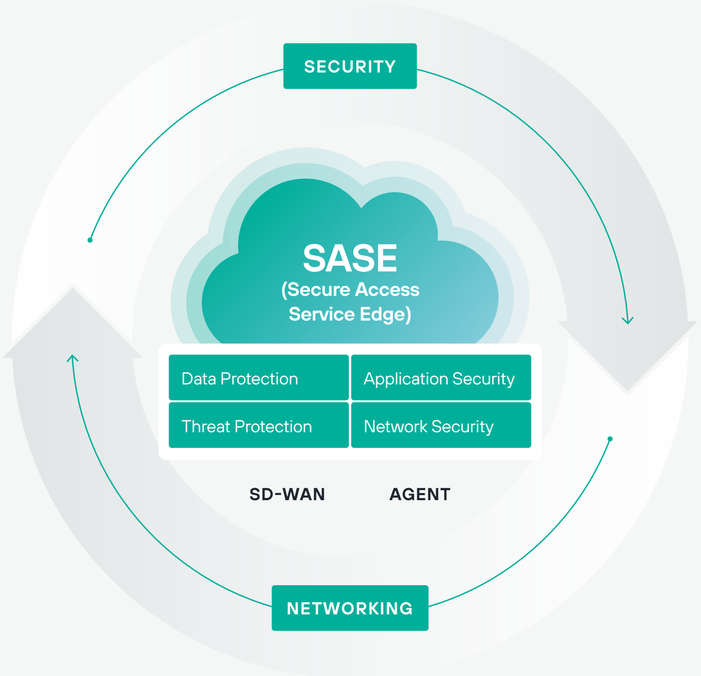
SASE calls for a unified cloud-based security-as-a-service architecture that applies Zero Trust principles across a range of capabilities such as:

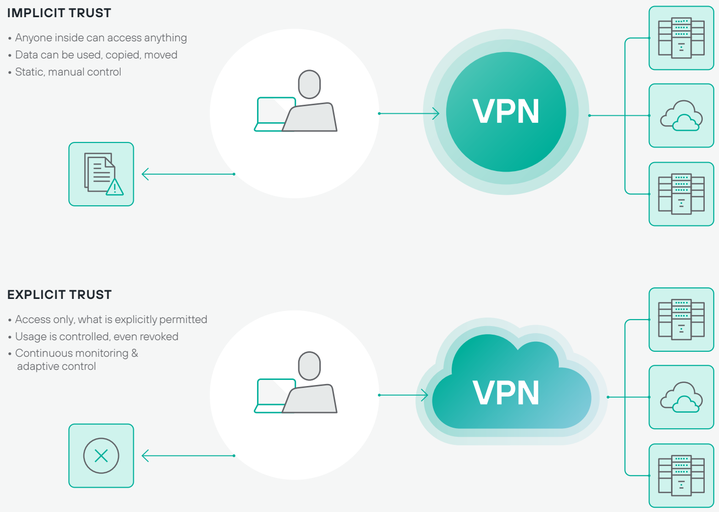
- → Next-Gen Firewall / FWaaS
- → SWG / URL Content Filtering
- → Cloud Access / Action Control
- → DNS protection
- → Bandwidth Control
- → Data Loss Prevention (DLP)
- → Advanced Malware Sandboxing
- → SSL Break and Inspect without any noticeable performance impact to the end user

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.

At the same time, another security paradigm began gaining attention: Zero Trust. Zero Trust is a set of principles for information security originally proposed by John Kindervag at Forrester Research and now standardized by NIST as Special Publication (SP) 800-207. Zero Trust addresses weaknesses of perimeter-focused security techniques by making no assumptions about who is trusted to access resources and who is not. In the context of WFH, a Zero Trust approach to cybersecurity requires employees to have explicit permission at every step of access and using information.

"This is an ideal solution for environments where an organization may not really know who is on the remote device."





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 data-centric behavior monitoring principles in its product lines. This allows your enterprise 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 behavior-based system for dynamically personalizing security enforcement according to each user's own actions.

Forcepoint's SASE platform 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's data-centric SASE platform doesn'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:** Forcepoint's unified agent 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.
- → **Behavior-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:** Forcepoint's dashboards 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.

The Big Takeaways

The world changed profoundly in the face of the COVID pandemic. It will be some time before we will be finally free to go back into the office, and it's likely that many of us will still be working remotely.[2]

The old "castle-moat" approach to security cannot keep up with the new remote work dynamic. 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.

Forcepoint rises up to the challenge by connecting the dots between data-centric SASE and Zero Trust, Forcepoint offers enterprises a unique way to transform their business through cloud-delivered, converged, behavior-centric 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.

[2] PwC's US Remote Work Survey. PwC, 25 June 2020.

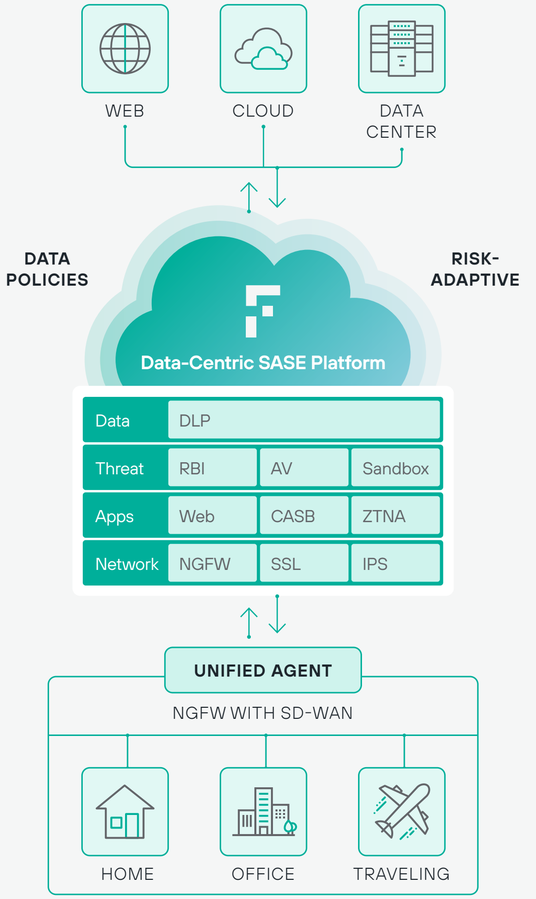
These capabilities include:

- → **Forcepoint Cloud Security Gateway:** Cloud-delivered SASE protection for protecting use of web and cloud applications, complete with true enterprise-class data loss prevention technology in the cloud.
- → **Forcepoint Private Access:** Cloud-delivered Zero Trust Network Access for giving remote workers safe access to private applications without the complexities, bottlenecks, and risks of VPNs.
- → **Forcepoint Next-Generation Firewall:** Advanced NGFW with secure SD-WAN and global scalability.
- → **Forcepoint Data Loss Prevention:** Industry-leading protection for sensitive data and intellectual property everywhere–in the cloud, in networks, and on users' endpoint devices.
- → **Forcepoint Dynamic User Protection:** The industry's first user-activity monitoring solution delivered as a cloud service gives organizations visibility into risky user behavior and mitigates loss at the earliest point of detection.

We invite you to get in touch with us for a live demo to see how all this works in practice.

→ **Request A Demo**

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.



Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-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.

Beyond Remote Workers eBook 06APRR2021