avast business

WHITE PAPER

Moving to the Cloud: Achieving Digital Transformation with a Zero Trust Approach

Is the Shift to Cloud and Mobility Creating a Cybersecurity Gap?

When it comes to rates of change, cybersecurity has typically been on the conservative side. Establishing cybersecurity systems, testing them, and getting them working properly takes time and resources. Changes introduce risk. And there is an active community of attackers looking for mistakes when changes are made.

But at the same time, the business computing landscape is rapidly evolving and quickly moving to mobile devices and the cloud. Even before COVID 19, the way we work was already changing – mobility, working outside the office, and accessing business applications anywhere, anytime has become the new normal. The pandemic has simply accelerated this change.

FireMon's State of Hybrid Cloud Security Survey tells this story very clearly. The survey found that 60% of businesses are embracing the cloud at a rate that outpaces their ability to secure it. Half of all businesses have deployed two or more clouds. At 44% of the organizations surveyed, the security of the cloud is managed by someone outside the security organization. Such a disjointed approach to managing security is likely to be problematic.

There's no question that the net benefits of the cloud are impressive. The increase in mobility and cloud adoption is good for business, creating new ways of working, increasing collaboration, and expanding choices of applications. But because cybersecurity is often not very agile, legacy solutions that are being retrofitted to cloud usage are getting in the way of a great mobile and cloud experience.

For example, many users are forced to put up with a slow and frustrating experience because they must log into a VPN every time they need to access applications. Too often, connectivity drops, and they must restart their VPN connections. User traffic is often backhauled through a central data center, which slows connection speeds, as their traffic has to go through the data center on its way to the internet and back.

The threat landscape continues to evolve as well, with more attacks popping up every month, from DDoS attacks to malware and ransomware (like NotPetya, WannaCry, and Ryuk). But although the threats have evolved, cybersecurity hasn't. An evolution is now imperative because attackers have figured out the current generation of technology.

Perhaps the biggest change is that the idea of a perimeter separating the safe zone from the danger zone is no longer valid. The defensible network perimeter is still mentioned in reference to the data center, but in reality, that perimeter no longer exists as it once did.

As more privately managed apps move to the cloud and SaaS applications like Office 365 are adopted, companies can no longer control the network as they have in the past. Traditional network security technologies have increasingly become obsolete, as they are meant to secure access to the "on-premise" data center.

So how should we define and secure today's network?

Digital transformation requires a new approach to cybersecurity because, in effect, the attack surface has broadened from the office data center to the far reaches of the internet. The new perimeter is really around the app, users, and their devices. The cloud is here to stay, and we need to do something different to secure it.

Taking Security to the Cloud

The transition from a fixed security architecture designed around a perimeter to one that can address differences in architecture and control points in the cloud requires changes in both theory and practice. In other words, we need a new way of thinking about a solution and new technology to implement it. The new perimeter is really centered around the apps, users, and their devices.

How Cloud-Based and Zero Trust Networking Technologies Integrate for a Complete Solution

The move from hosted and managed appliances to security delivered as a service allows companies to respond faster to changes in the cybersecurity landscape. Hosted security services offer a variety of benefits:

- Security can be managed locally but distributed globally. A simple policy change or changes to the global infrastructure can be made from a single point.
- Less complexity and management, as companies interact remotely with software rather than having to update hardware.

- Improved user experience in accessing private applications with the adoption of zero trust network access technologies (versus backhauling through a corporate data center).
- Increased agility to implement new solutions and change configurations to address new problems.
- Greater visibility, as trusted brokers are the single point of control through which all application access takes place.
- Reduced CapEx and OpEx for security.

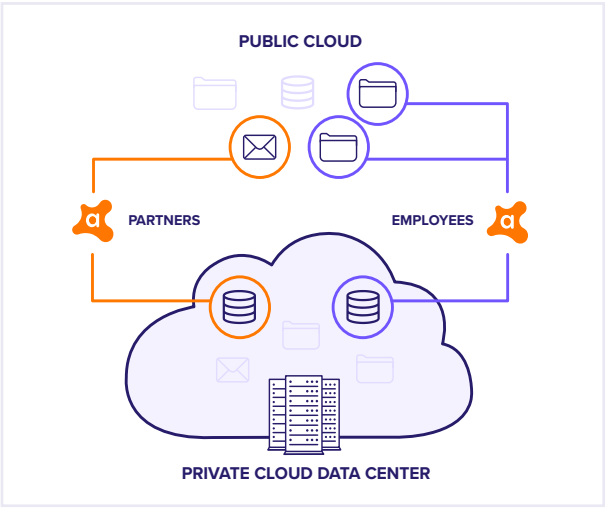
Just as applications moved to the cloud, security must also move to the cloud, for the same reasons.

The evolution of creating network connections

Typically, the process for creating a network inside a company includes asking the network for a connection, and the network provides it. Designers of the network control how that happens and what the connection is like. Cloud-based security addresses the biggest change brought by the cloud: the fact that the network is no longer under the control of the IT organization.

When you have cloud-based solutions, someone else is running the network and security challenges must be addressed in a new way. Cloud-based security solutions decouple application access from network access by using the internet as the connectivity mechanism. The application then provides the connection back to the user. What's more, instead of users connecting inbound to an application, the application provides an inside-out connection back to the cloud broker, explorer where the apps and user connections are stitched together. Applications are never exposed to the internet, making DDoS attacks impossible and removing the need for firewalls, web application firewalls, and other network security appliances and point products.

This structure has the great benefit of delivering microsegmentation without the need for complex network segmentation, and management of ACLs and firewall policies. In effect, the connection made for that user is a microsegment, and is spun up on a per session basis, rather than a static tunnel that is always up and running like with VPN. This microsegmentation greatly limits the lateral spread of malware and over-privileged access by default. The user can do nothing else with the connection but access the application, which greatly limits the lateral spread of malware. This approach uses encrypted end-to-end connections over the internet for speed and scalability, replacing the internal proprietary network as the delivery mechanism and reducing costs.



The rising popularity of ZTNA services

A number of drivers are spurring adoption of ZTNA technologies, but here are some of the most prevalent ones:

VPN Replacement

VPNs are known to be slow, unreliable, and insecure. Let's face it: Users and IT staff hate them for good reason. If the remote users manage to connect, they are connecting from an approved list of IP addresses and are assumed to be trusted. They are granted access to the network through a firewall, which is most often exposed to the internet. On-premise users (and their malware) can then move laterally across the network. Ultimately, this inherent trust leads to risk and over-privileged network access.

By comparison, ZTNA services provide a seamless, faster user experience. ZTNA services are faster because they are brokered in the cloud rather than being tunneled through corporate networks. From a network security standpoint, this approach offers microsegmentation at the application instance level and keeps users off local area network segments, thereby preventing malware from spreading.

Secure Multi-Cloud Access

About half of all companies are running private apps in more than one public cloud service today. With ZTNA services, the trust broker manages all cloud access. ZTNA thus enables migration to the public cloud by standardizing on a single security service that works across all cloud platforms. The user experience is consistent across all environments, which maximizes productivity. With a centralized approach to cloud security, attempts to obviate that framework become easier to see and mitigate. Once ZTNA services are set up, it is easy to pinpoint unauthorized applications, empowering teams to root out shadow IT and apply granular controls.

The Path to Transformation Is Clear

Based on all of this, the path to transformation is clear. We are living in a world of mobile access, cloud hosted applications, and a panoply of devices that have changed when, where, and how we work. Those changes are driving application, network, and security transformations. To accommodate all of these shifts, network security must evolve. It must be able to incorporate dynamic risk evaluation based on a default-deny threat posture. Companies need a way to adopt security that makes sense in the cloud using ZTNA technologies to make secure digital transformation possible.threats, will ensure continuous protection against cyber criminals.

About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.