Securing Cloud Transformation with a Zero Trust Approach

zscaler™

Rapid Adoption of Cloud and Mobility is Creating a Cybersecurity Gap

When it comes to rates of change, cybersecurity has rightly been on the conservative side. Setting up cybersecurity systems, testing them, and getting them working properly takes time. 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 changing and quickly moving to mobile devices and the cloud. The way we work has changed – mobility, working from home, and accessing business applications anywhere anytime is commonplace.

FireMon's State of Hybrid Cloud Security Survey tells this story clearly. The survey found that 60% of businesses are embracing 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 enterprise 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, older 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're logging 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 to 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 iEncrypt). But although the threats have evolved, cybersecurity hasn't. Such 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 workable. 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. The new perimeter is around the app, users, and their devices.

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 are obsolete, as they are meant to secure access to the data center. This was possible when they controlled the network.

So how do they do network security now? The answer is they can't.

Digital transformation requires a new approach to cybersecurity because, in effect, the attack surface has broadened. The cloud is here to stay, but we need to do something different to secure it.

Companies are recognizing this new reality already. As Tony Fergusson, IT Infrastructure Architect at MAN Energy Solutions, said recently in a Zscaler case study, "The Enterprise IT landscape is changing with the adoption of mobility and cloud services, and enterprises need to change their architecture to meet the growing needs of securing users from anywhere on any device."

How Cloud-Based and Zero Trust Networking Technologies Set the Stage for a Complete Solution

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 we need new technology to implement it.

Security itself must move to the cloud

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.

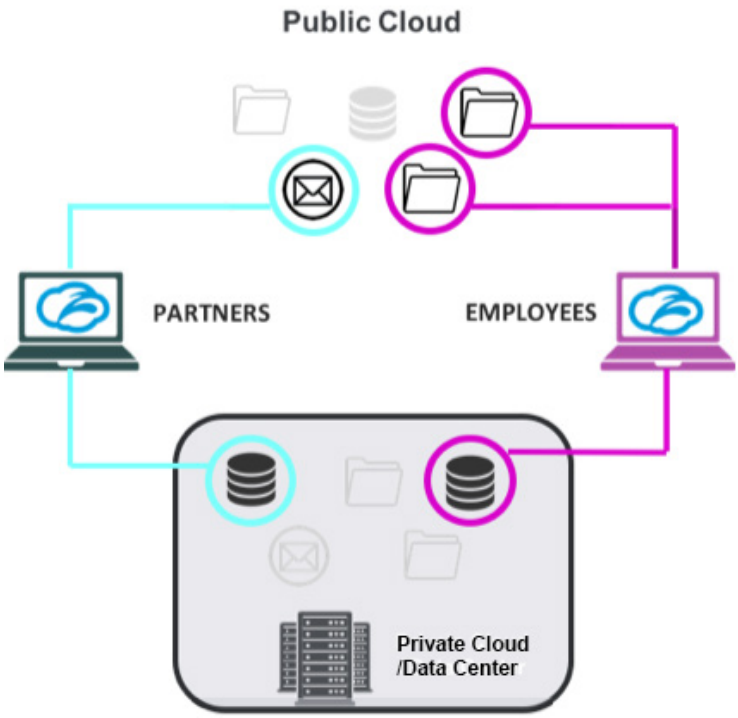
Just as applications moved to the cloud, and for the same reasons, security must move to the cloud as well.

The process of creating network connections must evolve

Right now, the typical process of creating a network inside a company is that you ask 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 enterprise.

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, 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 that it delivers 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 overprivileged 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 zero trust paradigm has been updated to support an agile cloud-based framework

Many of the ideas that underpin a cloud-based zero trust network access (ZTNA) security solution have their roots in the zero trust paradigm, which has been around for more than a decade and provides the basics of what is needed for a cloud-based world.

Initially, zero trust started with default deny and no automatic connections. No connections were made until there was a reason to make them. Zero trust started with a radically different perspective in terms of security assumptions, but the technology does not deliver on those assumptions. Zero trust solutions lacked the ability to be adaptive.

When implementing zero trust style security systems with existing technology like VPNs, DMZs, and firewalls, there were still vulnerabilities and ways to abuse trust. For instance, VPNs tunnel remote users through holes that are created in the firewall to connect users to the corporate network. Once inside the corporate network, even with that tunnel, lateral movement and propagation of threats are possible. Using DMZs exposes the front of applications to the internet, where they are accessible to the good guys, but also to the bad guys. We don't just simply need to add a better lock on the door; instead, the door should never be visible in the first place!

Zero trust didn't have any ways to address this initially. It had to evolve. The Continuous Adaptive Risk and Trust Assessment (CARTA) framework created by Gartner shows how to complete the journey to zero trust.

Completing the Journey to Zero Trust

The CARTA framework, in which ZTNA technologies play an integral role, is deep and complicated. In this section, we present highlights that describe what is needed to complete the journey to a fully functional cloud-ready cybersecurity infrastructure.

The CARTA framework creates the context for zero trust adoption

Gartner realized that zero trust needed to evolve. Gartner promoted this evolution by creating the CARTA framework, which operates on a more sophisticated view of what zero trust is. With CARTA, the world of zero trust isn't a world with no perimeters. Instead, CARTA advocates a large number of very targeted zones of access. Ideally, anytime someone asks for access, they get a dedicated micro-tunnel that's tailored for them. But to make this work, these tunnels must be dynamic, and terminated once the session ends.

CARTA also recommends more intelligence and adaptability such as:

- using the full context to create network connections; and
- knowing as much as possible about the user making the request to connect to an application.

Rather than zero trust, trust is inevitable, but it should be based on as much evidence as possible — who the user is, what and where the device is, the time of day, and so on. Once connections are created, activity must be monitored to see if the connections are being used properly. The CARTA framework thus innovates by continuing security after connections are made.

Trust can no longer be "set and forget." Security teams must then monitor activity on an ongoing basis to assess risk and adapt security as needed. This is what ZTNA technologies specialize in delivering.

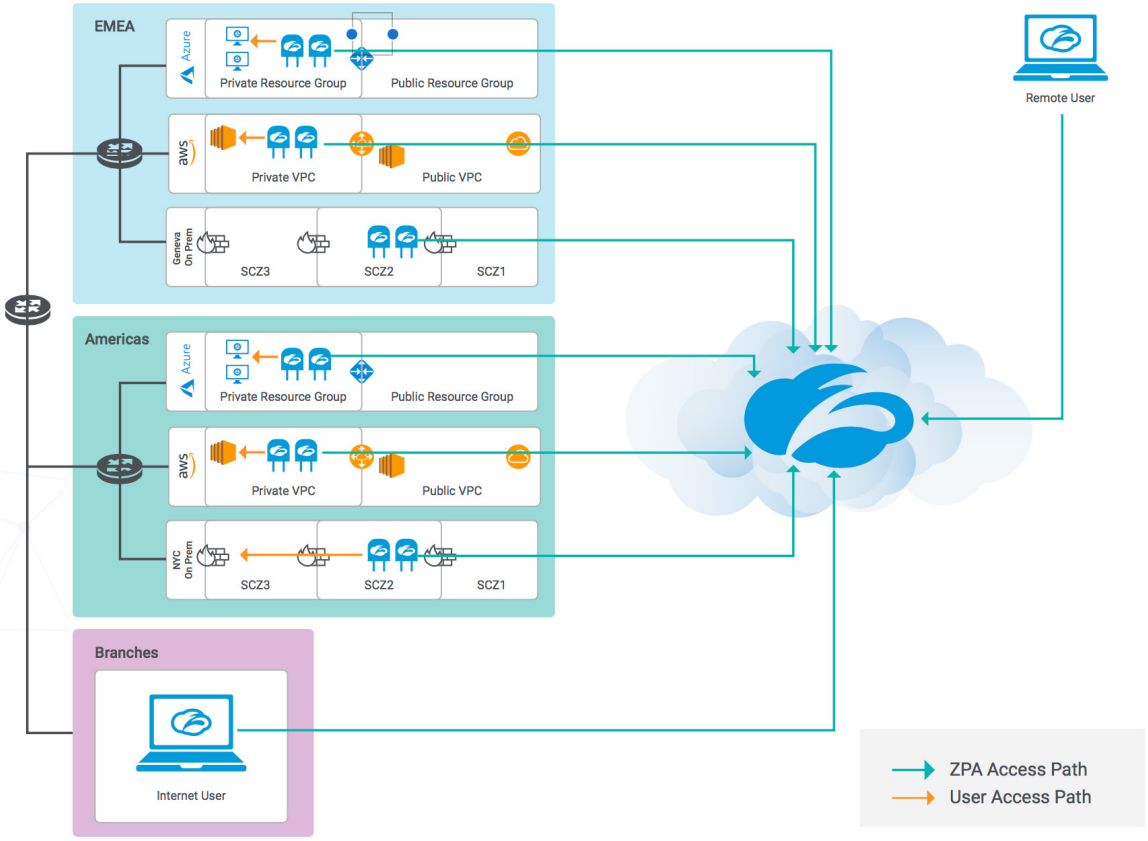
ZTNA technologies make zero trust possible

ZTNA technologies provide the enterprise starting point for CARTA. The N in ZTNA is a bit of a misnomer, as the network plays a smaller role in this type of technology. It is really about application access; with ZTNA, the application is in charge, not the network.

ZTNA technology, which is also known as software-defined perimeters (SDPs), creates an identity- and context-based, logical-access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities.

There is no more tunneling through a firewall. Instead of connecting to the application or asking the network for a connection, the user asks a trust broker to create a connection to the application. The broker verifies the identity, context, and policy adherence of the specified participants before allowing access. The application then connects back to the user, creating, in effect, a specialized network segment for that particular instance of that application. This approach removes the application assets from public visibility and significantly reduces the attack surface. In addition, just as CARTA recommends, after the connection is made, the connection is monitored.

Gartner's recommends using ZTNA technologies "as a service," as they are more secure and easier to consume in that way. Secure access capabilities must evolve to the cloud, where the users are and where applications and services are moving. Many software-defined perimeter solutions are cloud based, including Zscaler's.



The capabilities of ZTNA technologies are as follows:

- Microsegmentation not network segmentation
- Application access without network access
- Mask applications from the internet with inside-out connections
- Ability to discover previously unknown applications to which you have entitlement (a Zscaler Private Access feature)
- Integrations with SAML for identity-based access
- Integrations with technologies like Zscaler Internet Access for added capabilities like traffic inspection for outbound traffic, monitoring for botnet calls, data loss prevention, and visibility into anomalous activities. This ensures an overarching security view across privately and externally managed apps.

With ZTNA, the process of creating a connection is first based on the authentication of the user and device. The conceptual model below shows the idea. First, you authenticate to the trust broker and your identity is verified. You are provided with a list of applications that are available to you. When the

Drivers for adopting ZTNA services

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

VPN Alternative

VPNs are known to be slow but they are often the starting point for implementation of securing access to multi-cloud environments, which eventually lead companies to adopt ZTNA technologies. 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 networks with large segments, preventing malware from spreading.

As Angel Santo, CIO at NTSB, said in a recent Zscaler case study, “When our employees connected remotely to NTSB’s servers and applications through the VPN and TIC, they had to leave one destination and head to another, and then repeat the laborious process, because they can’t easily move between clouds. This added frustration during investigations.”

Secure Multi-Cloud Access

About half of all enterprises 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.

Secure Partner Access

Providing access to third parties is a critical service component of most business models. The attendant risks are high; many security breaches occur via third parties, whether business partners, subcontractors, or franchises. Even if there are corporate guidelines about devices employees can use to access the corporate network, such guidelines are a nonstarter for third-party access. By using ZTNA services, organizations secure access from unmanaged devices without placing them on the network, minimizing risk of over-privileged access, but still allowing partners access and connections to achieve the goals of the business.

Accelerate M&A and Divestitures

Mergers and acquisitions (M&A) typically require converging multiple networks and dealing with overlapping IP addresses because of network address translation (NAT). Massive delays are associated with moving from the current state. As a recent *Wall Street Journal* article noted, "70% of M&A-driven IT integration initiatives that fail do so as a result of missteps in the earliest stages, including weak

The Road to Transformation Is Clear

Based on all of this, the road 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 enterprise application, network, and security transformations. To accommodate all of these mega 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 the Gartner CARTA to define the framework and ZTNA technologies to make secure digital transformation possible.

About Zscaler™

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com