ZTEdge™
DEFEND WHAT MATTERS

Born in the Cloud: A Zero Trust Edge Architecture

Contents

Everyone's on a Digital Transformation Journey

Accelerated by the pandemic, remote work from anywhere has become the norm. Workers and companies have adjusted to new ways of accessing and working with the resources they need.

To maximize effectiveness of virtual operations, organizations are adopting a cloud- and mobility-first model to move online rapidly and completely. As a result of the rush to business digitization, forecasts project that by 2025 there will be 175 zettabytes of data in the global data-sphere. To put that in perspective, the Zettabyte Era was ushered in only in 2016, when global IP traffic first exceeded one zettabyte of data.

The explosion of data that is stored and processed primarily in cloud environments has **resulted in a larger-than-ever, rapidly expanding cyber-attack surface.**

The forces enabling digitization can be found at the intersection of easy-to-use, consumer-like business experiences; enterprise grade online Quality of Service (QoS) from anywhere; "there's an app for that" productivity tools enabling low-friction mobile user efficiency and data exchange; and low-cost commoditized infrastructure for compute and data networks. All one needs is an Internet connection and a device with a browser to enter the all-you-can-eat data buffet — at no charge.

The explosion of data that is stored and processed primarily in cloud environments has resulted in a larger-than-ever, rapidly expanding cyber-attack surface. The perimeter has been redefined: data, and the devices, apps and networks where it flows and resides, are the new perimeter.

Threats to this porous new perimeter are very real as evidenced by the daily drumbeat of headlines about data breaches, and the damage is costly. Cyber thieves, whatever their motivation, seem impervious to traditional cybersecurity controls. Data protection legislation and directives are a step in the right direction, but not enough.

Enter Cloud Cybersecurity, Secure Access Service Edge (SASE) and Zero Trust Architecture

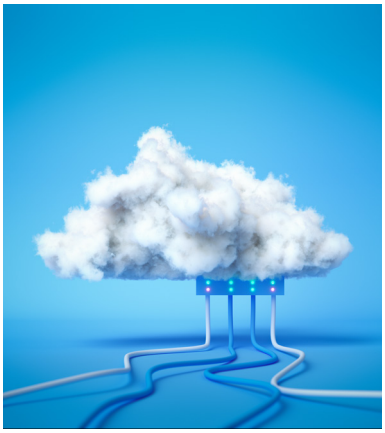
Despite the industry buzz around them, cloud cybersecurity, SASE and Zero Trust architecture are not merely buzzwords. These innovative cybersecurity technological and operational frameworks and standards are transformative. Entire industries and organizations of all sizes across the globe are eager — or more accurately, anxious — to introduce these models to improve their cyber defense posture. Gartner expects that "by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018."

The momentum behind Zero Trust — the concept of rejecting implicit trust in favor of a least-privilege model to block security threats — is huge. In order to bring clarity and provide guidance beyond the plentiful marketing hype around the term, NIST recently released Special Publication 800–207 as a neutral Zero Trust Architecture (ZTA) primer. To cite NIST SP 800–207, "ZT is not a single architecture but a set of guiding principles for workflow, system design and operations." SP 800–207 offers high-level, practical design advice while emphasizing that ZTA is not a single solution but rather, a long journey.

To enable a convenient operating environment that supports user productivity, a cloud-centric model of cybersecurity delivery is a must-have.

> *"By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018."*
>
> Gartner

Cloud Cybersecurity Pioneers



Cybersecurity companies began introducing cloud security 10+ years ago, with the vision of delivering an always-on security service to roaming end users, to help protect their organizations' important data. These innovative early providers disrupted the castle-and-moat appliance-based security architecture and paved the way for an entirely different security consumption model.

The state of technology at that point, a decade ago, presented headwinds that made their attempts at disruption hugely challenging:

- Cloud cybersecurity and edge computing were nascent and unproven
- Broadband networks availability was limited
- Public cloud technologies & tools had only started to emerge
- 4G LTE wireless was just completing trials in 2009
- Wi-Fi was adopted by 25% adoption of all homes only in 2012

Therefore, to enable their innovative security vision, early cloud security trailblazers raised millions of dollars in institutional capital to fund private cloud backbones and infrastructure, and create dozens of proprietary, interconnected premise-based data centers around the world. A decade ago, these pioneering vendors not only innovated the form factor of cybersecurity as a service (SaaS), but were also their own proprietary Internet Service Providers (ISPs).

The trials and tribulations associated with cloud cybersecurity design during this era were similar to those experienced by the Nissan Leaf electrical vehicle designers in 2010. Great idea, but fraught with early design and technology teething pains: irregular battery capacity issues, erratic driving ranges due to variation in outdoor temperatures, brakes improperly designed for the dynamics of electrical vehicles and premature tire wear.

Now, fast forward to 2021. Those cloud cybersecurity services from ten years ago still work, but they are teetering on the brink of obsolescence due to legacy architecture and design. To keep up with sophisticated, advanced new cyberattacks and refresh frail foundations, the providers layer on disparate technologies and features. With new technologies bolted on to aging architectures, around-the-clock human service monitoring is necessary to manually catch — or at least, try to catch — anything that slips through the cracks.

While delivery of security services via the cloud to enforce protection policies at the "edge" (where devices, applications, networks, etc. interact with data) makes all the sense in the world, the architectures and designs of these aging cloud networks need to be newly aligned with the realities of today's modern distributed workplace.

Cloud cybersecurity services from ten years ago still work, but they are teetering on the brink of obsolescence due to legacy architecture and design.

In today's environment, amid a myriad of advanced threats, organizations require:

- Flexibility for virtual and remote work
- Always-available connectivity from all types of devices
- Full mobility
- Cloud access
- Consumer experience-like simplicity
- Enterprise-grade high-performance
- Secure access to sensitive data everywhere
- Low cost operation

ZTEdge™
DEFEND WHAT MATTERS

ZTEdge is a decentralized, state-of-the-art cloud cybersecurity platform that provides dedicated, purpose-built inline Zero Trust controls and leverages modern technologies, architectures, automation, compact codebases and robust public cloud services.

What is ZTEdge™ Architecture?

ZTEdge™ was designed to disrupt the aging disruptors by delivering a decentralized, state-of-the-art cloud cybersecurity platform that provides dedicated, purpose-built inline Zero Trust controls and leverages modern technologies, architectures, automation, compact codebases and robust public cloud services.

The break-through innovation of ZTEdge is that it is Infrastructure as a Service (IaaS) agnostic, supporting Oracle Cloud Infrastructure (OCI), Microsoft Azure, Google Cloud Platform (GCP), Amazon Web Services (AWS), Alibaba Cloud, Rackspace, and other clouds.

Its design has been architected from the ground up as a service layer on top of any foundational IaaS. This enables ZTEdge to be cloud independent regarding underlying infrastructure, yet be able to orchestrate federation of multi-cloud, points of presence (PoPs) around the globe.

Why ZTEdge is Safer by Default

Robust competition among IaaS providers to provide PoPs in virtually every location helps drive down backend cloud hosting costs for ZTEdge and improve unit economics.

ZTEdge's cloud-agnostic design enables new PoPs to be spun up (or down) in various locations, and added to ZTEdge within 72-hours, based on customer requirements. This model, akin to just-in-time service, reduces hosting expenses and creates a PoP-dense ZTEdge cloud. The result? Low end-user connectivity latency and a seamless, overall-positive end-user experience.

PoP density is a SASE critical success factor, which is why the cloud-agnostic nature of the ZTEdge design is key. If a SASE solution is, for example, tightly coupled architecturally with AWS, its PoPs are restricted to global AWS data center locations which, while broad, are still limited. But layer in all other IaaS providers via our multi-cloud approach, and ZTEdge can provide geographically precise and very robust access for superior end-user performance and reduced hosting costs.

ZTEdge™
DEFEND WHAT MATTERS

Regardless of where a user is located, or whether their device is managed or BYOD, their IP address stays the same and enables passwordless authentication to applications and resources.

ZTEdge uses Amazon Route 53, an IaaS-agnostic, proximity-based routing framework to intelligently route users and connect PoPs, regardless of whether the PoPs are on AWS, OCI, GCP or any other IaaS. This routing is seamless to the ZTEdge cybersecurity service and provides an excellent end-customer experience.

The elastic, scalable and IaaS-agnostic architecture of ZTEdge enables the service to detect regional outages and fail-over to an operational service provider. For example, if an outage like the one AWS experienced in its US East-1 region in November 2020 occurs, the ZTEdge redundancy mechanism could automatically spin up an OCI PoP in Northern Virginia, which was online, for uninterrupted service to our ZTEdge customers.

The architecture of ZTEdge enables assignment of a dedicated, local source IP address for each user — a valuable feature that other legacy cloud cybersecurity architectures are unable to match. These source IP addresses can be used to restrict or allow policy-driven end-user access to business applications that are either inside the network perimeter or in the public cloud. Importantly they "travel" with the end-user: regardless of where he or she is located, or whether they are using a corporate-managed device or an unmanaged "bring your own" device (BYOD), their IP address stays the same, and enables passwordless authentication to applications and resources."

Thanks to our geographic proximity-based cloud model, ZTEdge enables customers to explicitly set regions where access enforcement and log files are written. This is a critical requirement for compliance with regulatory and data privacy regimes, such as GDPR. As users roam across locations, policies can be defined to comply with local jurisdiction and vertical industry laws and directives.

Finally, ZTEdge delivers enterprise-grade quality of service (QoS) via dedicated high-bandwidth connectivity (vs connecting over the public Internet), through our partnership with Oracle Cloud FastConnect. This service connection obviates the contention of private cloud network providers that the public cloud cannot reliably deliver mission-critical bandwidth service.

ZTEdge Cloud-based Security Whose Time Has Come

The Nissan Leaf 2010 was a great electric vehicle when it was introduced and well ahead of its time. It helped advance the concept of electrical vehicles from cottage industry to mainstream adoption, as demonstrated by the many electric vehicles on the road today and growing global adoption rates.

In order to similarly pivot to enable cloud-provided cybersecurity services to meet future cybersecurity needs, the right tools and architectures must be built into its very foundations. Yet with so much capital sunk into existing platforms, pivoting is hard. The 2021 Leaf is a total, bottom-up redesign from its original model: it leverages new approaches, platforms and technologies that simply weren't available — perhaps not even conceived of — 10 years ago.

Cloud cybersecurity architectures have similarly experienced evolutionary leaps as cloud adoption and technology have gone mainstream. Today, advanced new solutions like ZTEdge are enabling organizations to ***defend what matters*** as never before.

In order for cloud-provided cybersecurity services to meet future needs, the right tools and architectures must be built into its very foundations. Advanced solutions like ZTEdge enable organizations to ***defend what matters*** as never before.

ZTEdge™
DEFEND WHAT MATTERS

The ZTEdge security platform leverages a Zero Trust security approach to protect what matters to midsize enterprises and small businesses: their users, their network, their data, their applications and especially their customers.

Designed with simplicity in mind and operating at the cloud edge, the platform is flexible to support businesses as they grow and transition digital operations to the cloud. Delivered on a distributed, scalable enterprise-class cloud infrastructure, ZTEdge is available as a service provided by certified, market-leading ZTEdge MSSP partners.

For more information about ZTEdge™, please visit us at
https://www.zerotrustedge.com/

Contact us

www.zerotrustedge.com
info@zerotrustedge.com
US: (201)767-2210
Europe: +44 (0)1905 777970
ROW: +972-2-591-1700