EBOOK

Replace legacy VPNs with modern ZTNA

A secure, work from anywhere solution

CATO NETWORKS | WINDSTREAM ENTERPRISE

Work from anywhere has recently become a hot topic.

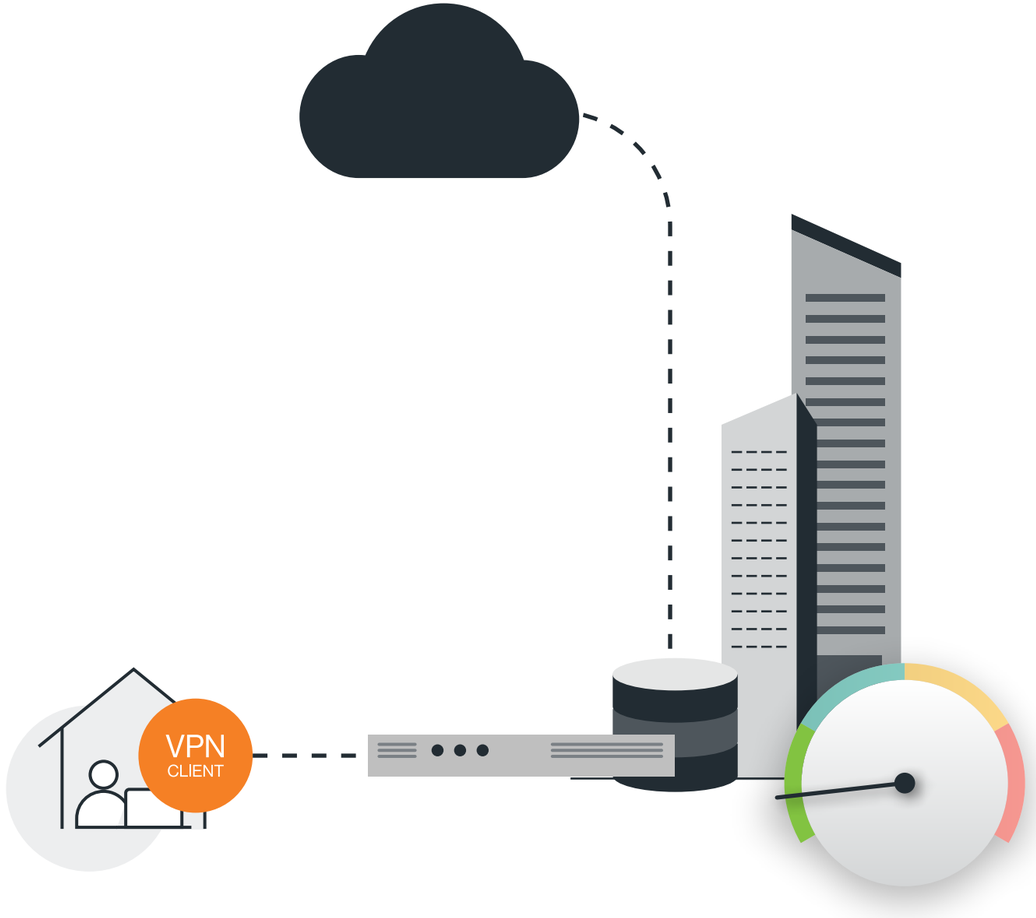
The coronavirus outbreak forced many organizations to move some or all of their employees to work from home. In some cases, work from home was a way to reduce possible exposure, in others it was mandated by health authorities to prevent the spread of the disease across communities.

This unforeseen set of events caught many organizations off guard. Historically, only a subset of the workforce required remote access, including executives, field sales, field service, and other knowledge workers. Now, enterprises need to maintain business continuity by enabling the entire workforce to work remotely.

How VPN works?

The most common enterprise remote access technology is Virtual Private Networking (VPN). How does it work? A VPN client is installed on the users' devices—laptops, smartphones, tablets—to connect over the Internet to a server in the headquarters.

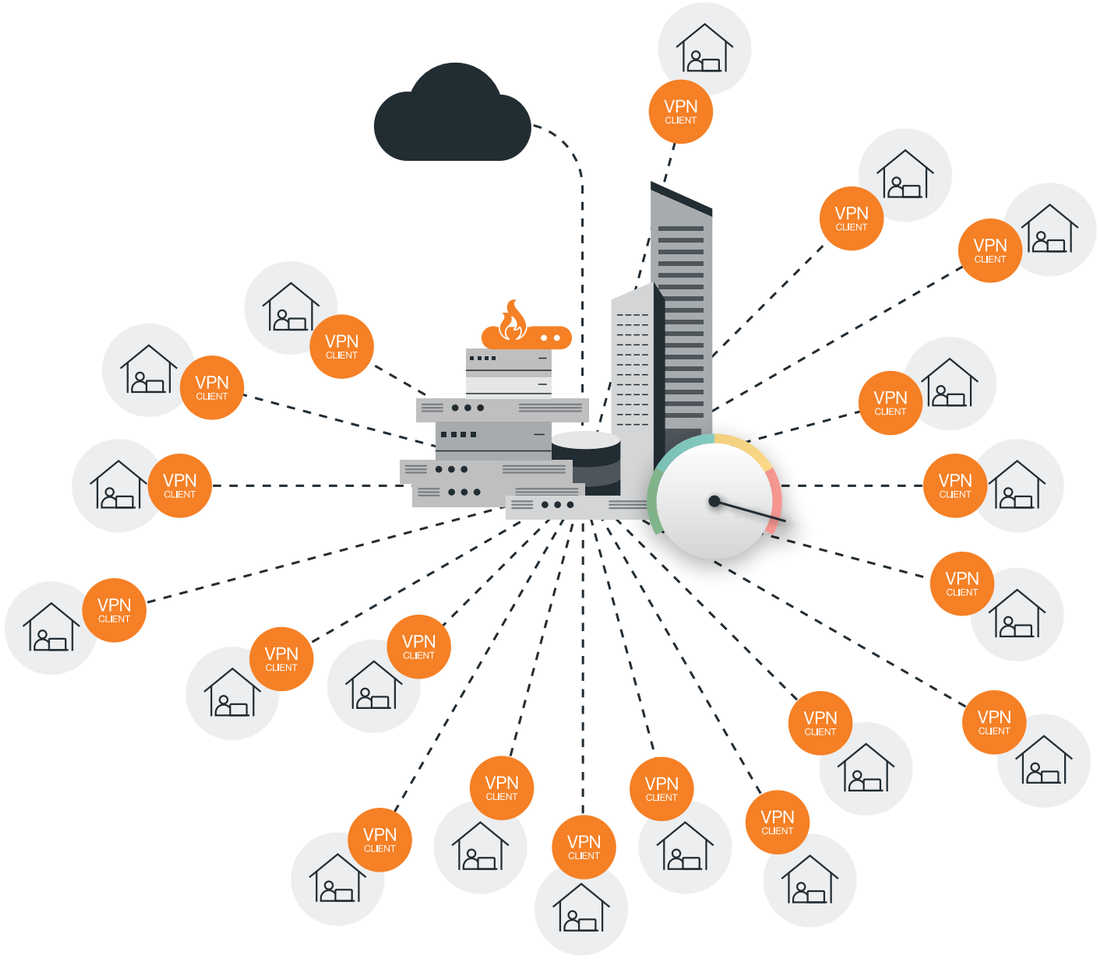
Once connected to the server, users gain access to the corporate network and from there to the applications they need for their work.



VPN was built for the few

To address work-from-anywhere requirement, enterprises extend their VPN technology to all users. However, VPNs were built to enable short duration connectivity for a small subset of the users. For example, a salesperson looking to update the CRM system at the end of the day on the road.

VPNs may not be the right choice to support continuous remote access for all employees.



VPN is incompatible with company-wide work from anywhere requirements

VPN technology has many shortcomings. The most relevant ones for large scale remote access deployments are scalability, availability, and performance.

Scalability

VPN was never meant to scale to continuously connect an entire organization to critical applications. Under a broad work-from-anywhere scenario, VPN servers will come under extreme load that will impact response time and user productivity. To avert this problem, additional VPN servers or VPN concentrators, would have to be deployed in different geographical regions.

Availability

Each component in the VPN architecture has to be configured for high availability. This increases cost and complexity. The project itself is non-trivial and may take a while to deploy, especially in affected regions.

Performance

VPN is using the unpredictable public Internet, which isn't optimized for global access. This is in contrast to the benefits of premium connectivity, such as MPLS or SD-WAN, available in corporate offices.

SASE/SSE: A VPN alternative for continuous work from anywhere by everyone

In mid-2019, Gartner introduced a new cloud-native architectural framework to deliver secure global connectivity to all locations and users. It was named the Secure Access Service Edge (SASE). Two years later, Gartner introduced a new category called the Security Service Edge (SSE) to describe a more limited scope of convergence focused on network security that also included secure connectivity.

> Because SASE/SSE is built as the core network and security infrastructure of the business, and not just as a remote access solution, it offers unprecedented levels of scalability, availability, and performance to all enterprise resources.

Scalability

The SASE/SSE service seamlessly scales to support any number of end users. There is no need to set up regional hubs or VPN concentrators. The SASE/SSE service is built on top of dozens of distributed Points of Presence (PoPs) to deliver a wide range of security and networking services, including remote access, close to all locations and users.

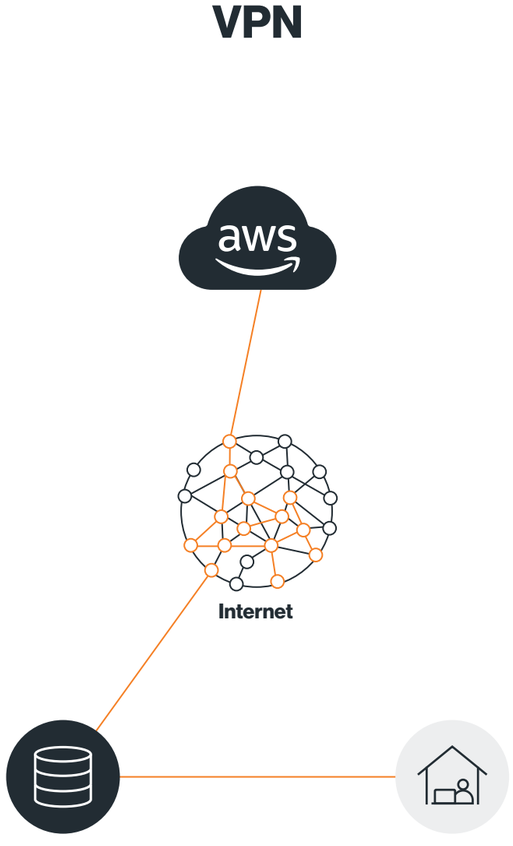
Availability

Availability is inherently designed into the SASE/SSE service. Each resource, a location, a user, or a cloud, establishes a tunnel to the nearest SASE/SSE PoP. Each PoP is built from multiple redundant compute nodes for local resiliency, and multiple regional PoPs dynamically back up one another.

The SASE/SSE tunnel management system automatically seeks an available PoP to deliver continuous service, so the customer doesn't have to worry about high availability design and redundancy planning.

Performance

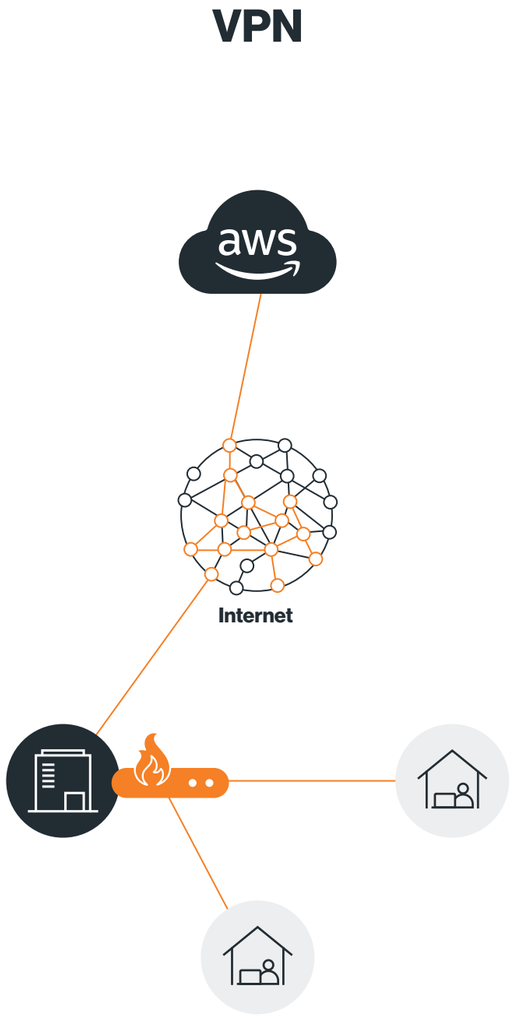
SASE/SSE PoPs are interconnected with a private backbone and closely peer with cloud providers, to ensure optimal routing from each edge to each application. This is in contrast with the use of the public Internet to connect to users to the corporate network.

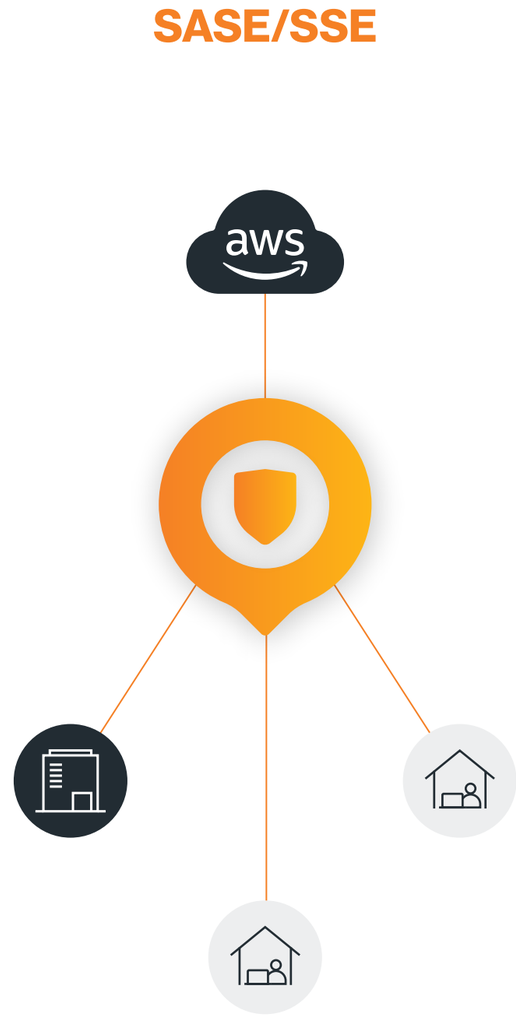


Security

Lastly, since all traffic passes through a full network security stack built into the SASE/SSE service, multi-factor authentication, full access control, and threat prevention are applied.

Because the SASE/SSE service is distributed, SASE/SSE avoids the trombone effect associated with forcing traffic to specific security choke points on the network. All processing is done within the PoP closest to the users while enforcing all corporate network and security policies.





A SASE/SSE service you can deploy today

If you are looking to quickly deploy a work-from-anywhere solution in your business, consider a Windstream Enterprise SASE/SSE solution powered by Cato. Cato was designed from the ground up as a SASE service that is now used by hundreds of organizations to support thousands of locations, and tens of thousands of mobile users.

Cato is built to provide the scalability, availability, performance, and security you need for everyone at every location. Furthermore, Cato's cloud native and software-centric architecture enable you to connect your cloud and on-premises datacenters to Cato in a matter of minutes and offer a self-service client provisioning for your employees on any device.

If you want to learn more about the ways Windstream Enterprise can support your remote access requirements

CONTACT US