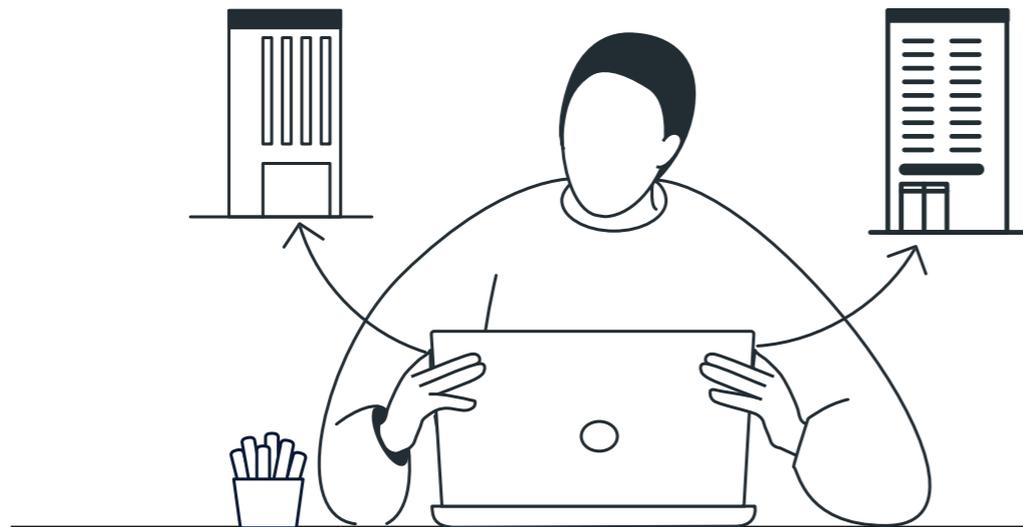


Mobile Access Optimization and Security for the Cloud Era



Secure and Optimized Mobile Access: The Challenges

When providing mobile access to business applications, companies face two basic challenges:



1

Optimizing access for the mobile workforce, which needs to conduct business from anywhere



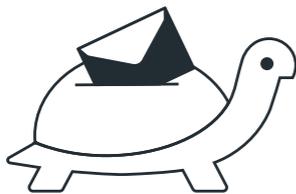
2

Controlling and securing access to business applications in physical or cloud datacenters, or to public cloud applications, such as Office 365.

Use Case #1

Mobile access to physical datacenters

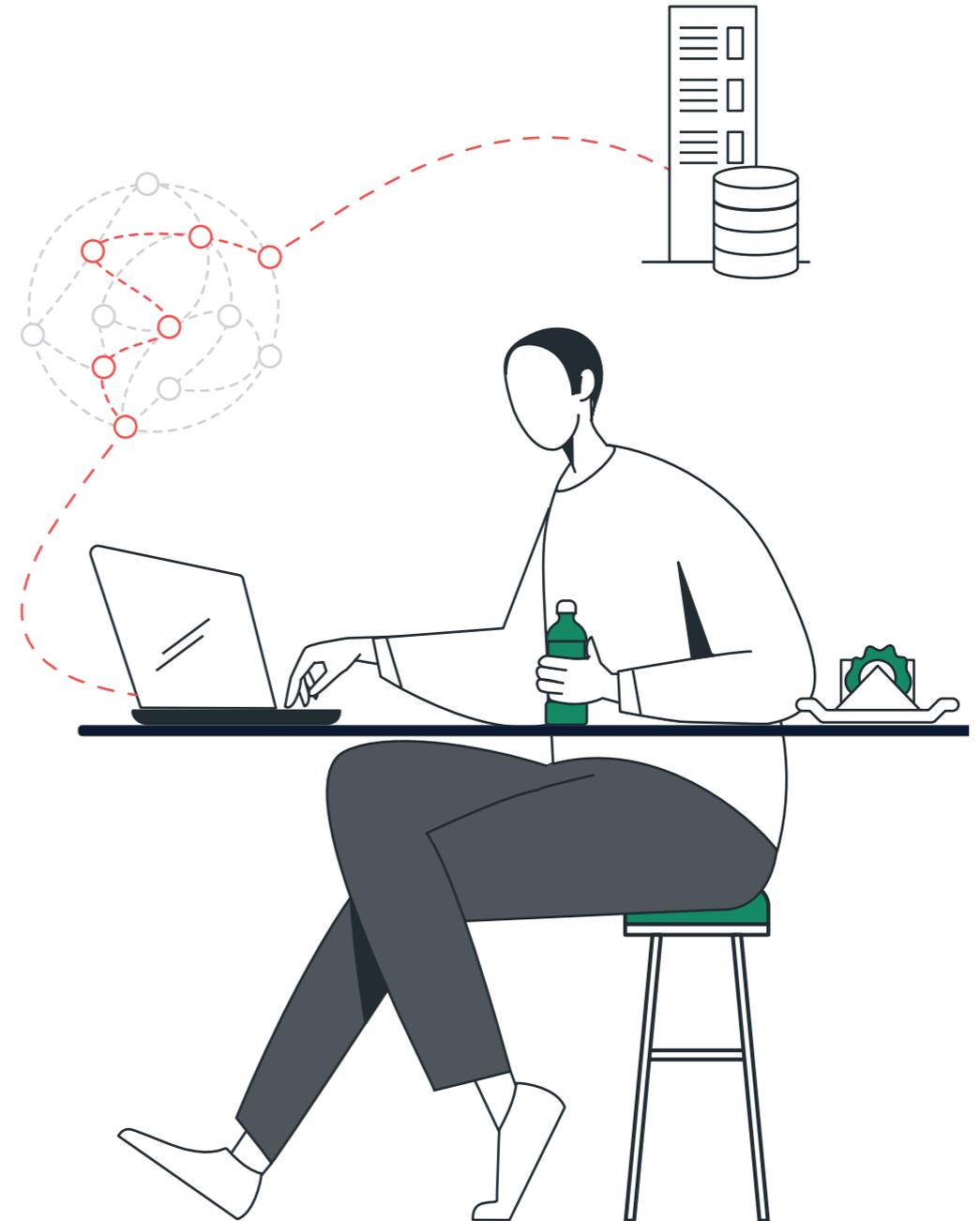
Mobile users need regional or global access to applications hosted in datacenters. Traditionally, they accessed applications by running VPN clients on their mobile devices and connected to VPN concentrators or datacenter firewalls. When mobile users entered the network through remote locations, they would have to traverse the MPLS or Internet VPN to the servers in the datacenter.



Since VPN access is done over the middle mile of the public Internet, users are exposed to erratic Internet routing with its significant **latency and packet loss**. These factors can severely degrade the application experience, frustrating users and hampering their productivity.



Furthermore, once authenticated, mobile VPNs enable users to access the whole network. This means that **hackers may be one password away from getting an unrestricted foothold on the network**.



Use Case #2

Mobile access to cloud datacenters

While similar in concept to physical datacenters, cloud datacenters pose new networking and security challenges for fixed and mobile users.

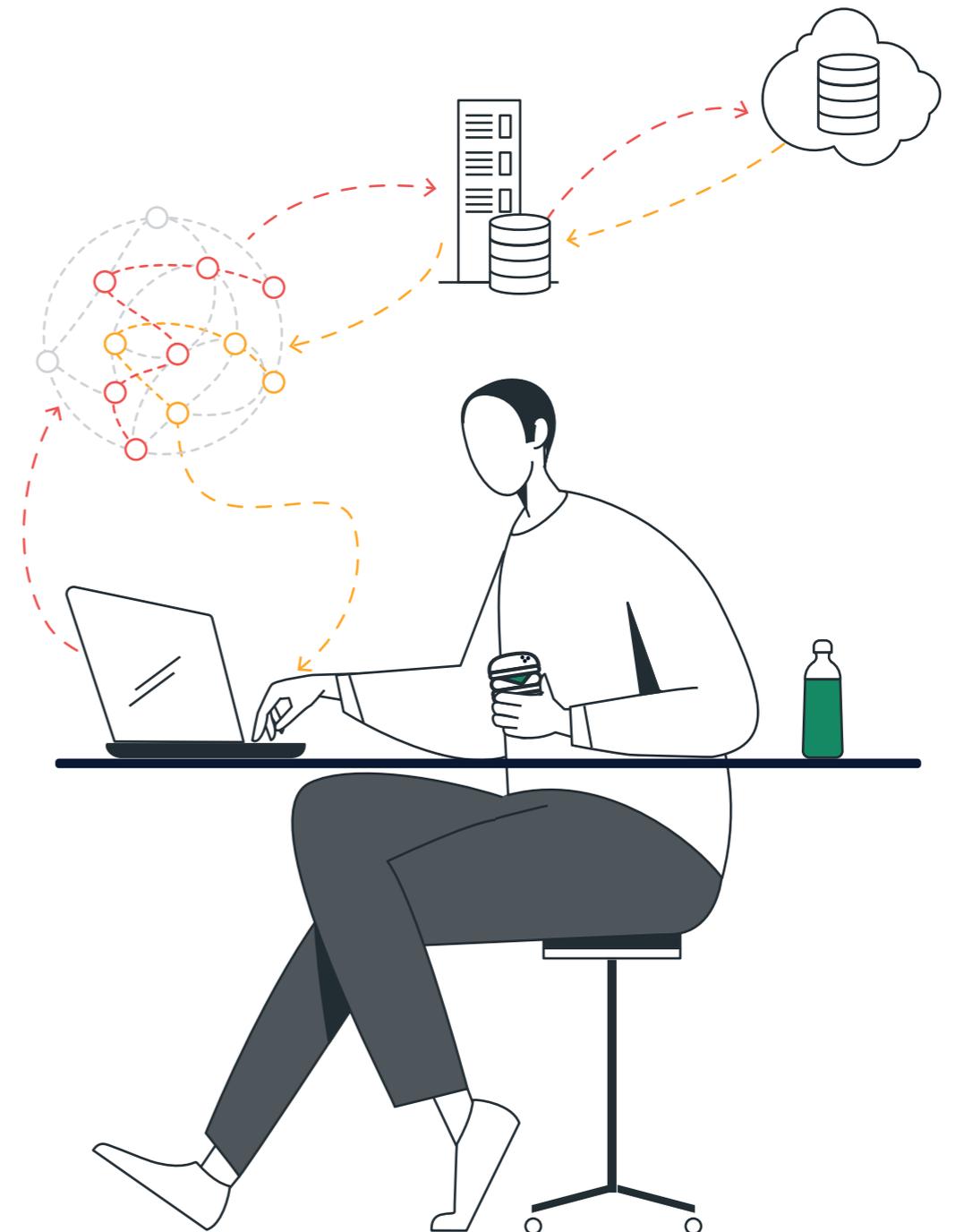
Legacy WAN architectures that backhauled traffic to a physical datacenter, need to incorporate the datacenter's split into physical and cloud datacenter(s), sometimes hundreds of miles apart. None of the obvious solutions are sufficient.

Continuing to forward the traffic from the physical datacenter and then onto the cloud datacenter leaves datacenter-bound and mobile user traffic subject to the erratic routing of the Internet while adding latency due to the "trombone effect."



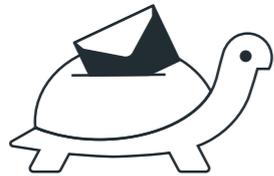
Cloud interconnect services, such as DirectConnect for Amazon Web Services (AWS) and ExpressRoute for Microsoft Azure, provide direct connections from physical datacenter to the cloud. But **mobile users remain subject to Internet performance while site- and user-traffic are subject to tromboning.**

Allowing mobile users direct access to the cloud is equally ineffective. It eliminates tromboning, but leaves users subject to Internet performance. In addition, direct access bypasses the corporate network security stack, requiring the deployment of new cloud-based security solutions.



Use Case #3

Mobile access to cloud applications



Accessing public cloud applications introduces even more nuances. Cloud apps are outside of IT control so WAN optimization capabilities cannot be extended into the application provider's datacenter. Yet users need to access cloud application instances. Take an Office 365

instance located within a specific region. All users, regardless of location, must access that instance and face the same connectivity challenges as they would if accessing the company's data center.



Network security is even harder to implement. Traditional network security relies on a "line of sight" into the traffic to inspect and secure it. But as with direct mobile access to cloud datacenters, direct mobile-to-cloud access bypasses the corporate network security stack.

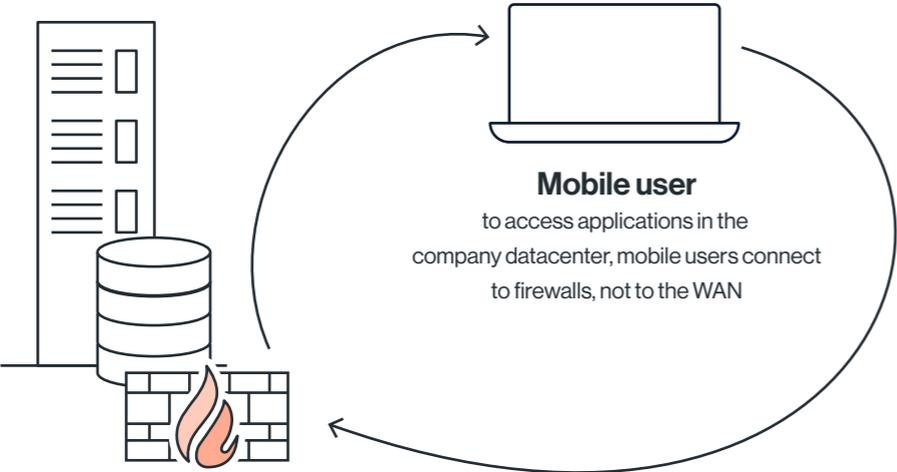
Companies again face a tough choice: either force backhauling of mobile Internet traffic to the datacenter, which adds latency and detracts from the user experience, or increase costs by deploying a cloud-based security point solution — such as a secure web gateway or cloud-access security broker (CASB) — to intercept and inspect all mobile traffic to the cloud.



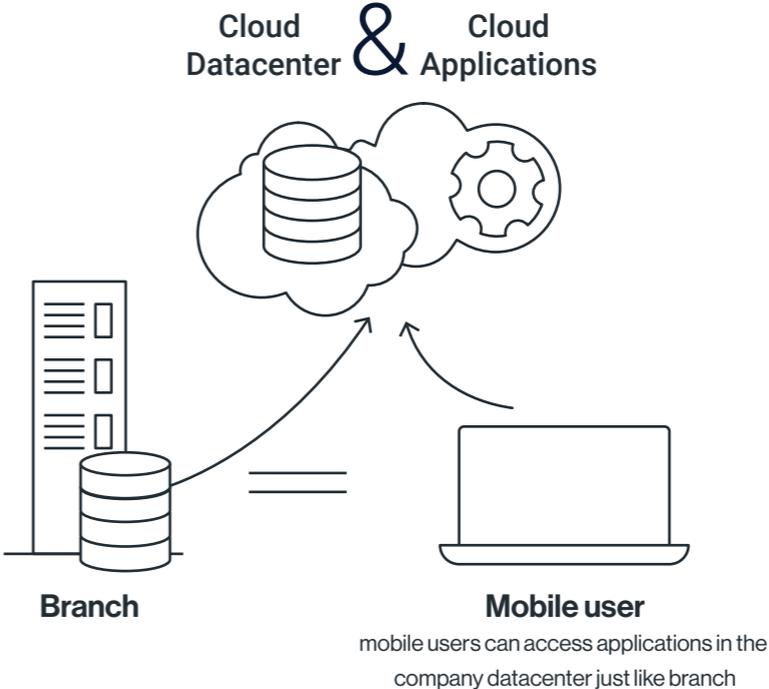
WAN Transformation Takes on Mobile Access Optimization

Historically, mobility was never a “WAN issue.” After all, mobile users connected to firewalls to access applications in the company datacenter, not to the WAN. The WAN connected only physical locations — headquarters, branch offices, manufacturing plants, project sites, and the like. But with mobility the rule, not the exception, separating the two no longer makes sense. Mobility and the cloud are essential to how we work. Any WAN transformation project must account for both of them.

The Old Way



The New Way

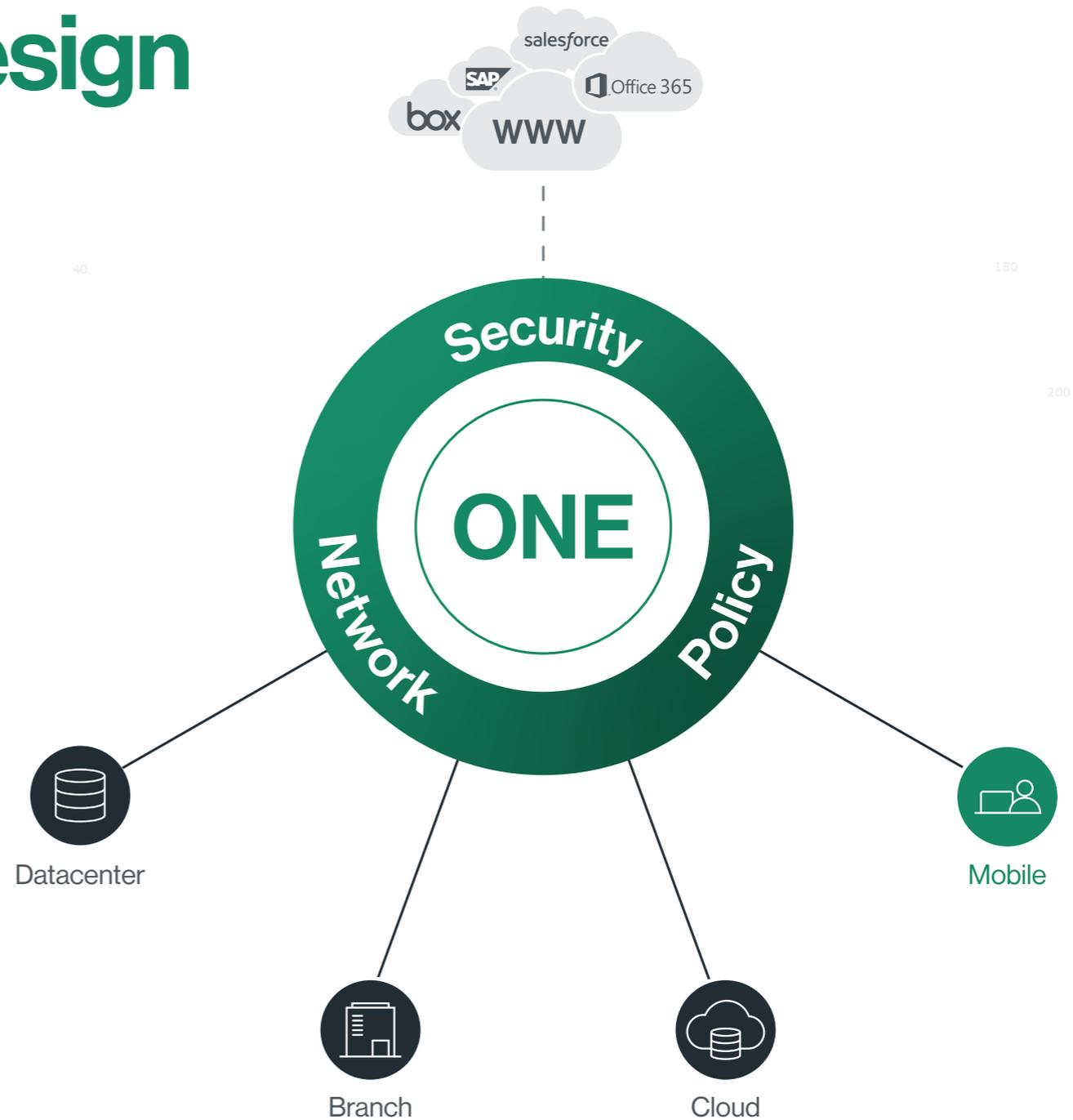


Cloud-native networks optimize mobile access by design

The cloud-native network is a multitenant WAN backbone built from globally dispersed points of presence (PoPs) that are fully meshed, creating a private and optimized global overlay. Edge resources — including physical locations, cloud datacenters, and mobile users — establish secure tunnels to the nearest PoPs using IPsec or DTLS. Cloud applications are accessed by routing traffic to the closest PoP as measured by latency and loss.

The cloud network is a full replacement for traditional mobile VPN access. By running mobile client or with clientless browser access, the mobile device finds and connects to the nearest PoP. The user authenticates using multi-factor authentication. Once connected to the PoP, the user is part of the virtual enterprise WAN and can access any authorized application.

With its global, SLA-backed backbone, the cloud network connects mobile users to both physical and cloud datacenter resources anywhere in the world without the erraticness of the Internet middle mile. And since the IP ranges of both the physical datacenter and the cloud datacenters are visible on the WAN to authorized users, an optimal direct path can be calculated, avoiding tromboning. Gone are the chokepoints and backhauling that undermined mobile user performance.



Mobile Access Comparison

		Direct Access	Legacy VPN	Cloud-native Carrier	
Network	Global Coverage	Does the solution include a globally optimized network? With a global network, the mobile user experience improves by avoiding the delays of the public Internet.	No	No	Yes
	Optimized WAN Access	Does the solution optimize middle-mile traffic to reduce latency and packet loss?	No	No	Yes
	Optimized Cloud Access	Does the solution deliver traffic as close as possible to a cloud datacenter provider (AWS, Azure) and to key cloud applications (Office365, Salesforce,...)?	No	Yes*	Yes
	Seamless Multicloud Support	Does the solution provide access to multiple cloud datacenter services from a single login?	No	Yes*	Yes
	High Availability	Does the solution come standard with highly available access by design?	Yes	No	Yes
Security	Integrated Network-based Protection	Does the solution include a network-based protection for all clients against malware, phishing and advanced threats?	No	Yes*	Yes
	WAN Traffic Inspection	Does the solution secure mobile WAN traffic against the same threats?	No	Yes	Yes
	Multi-factor Authenticaiton	Does the solution improve access security by authenticating users with more than a password?	Yes	Yes	Yes
	Consolidated User Management	Does the solution provide seamless management of mobile and fixed users?	No	No	Yes
	Resource-based Access Restrictions	Does the solution restrict access by IP address, host or application?	No	No	Yes
	Dedicated Client	Does the solution provide a software client for access from a mobile device?	No	Yes	Yes
	Third Party Client	Does the solution provide access from any device capable of establishing an IPsec, SSL, or DTLS tunnel?	Yes	Yes	Yes
	User Provisioning	Does the solution integrate with a company's LDAP server to simplify user account creation?	No	Yes	Yes
	Clientless Access	Does the solution provide secured access from a browser?	No	No	Yes

* Requires backhauling the traffic to the datacenter before capability can be applied. Increases latency and impacts user experience.

Summary

Cato's cloud-native network architecture connects all resources — physical, cloud, and mobile — to a single, virtual enterprise WAN. Result: a deep convergence of multiple capabilities, including WAN optimization, network security, cloud access control, and remote access to the network itself. This remarkably comprehensive design dramatically simplifies enterprise IT and reduces risk and costs.

To learn more visit our website at www.CatoNetworks.com

or contact us for a short and enlightening demo

CONTACT US

