Securing Remote Work:

Safeguarding Business Continuity with Zscaler

zscaler™

Nothing is more important right now than protecting the health of employees and community members, and that requires enterprises to mitigate the risk of coronavirus (COVID-19) transmission. In the meantime, organizations must ensure business continuity and preserve enterprise productivity, especially when employees are moving to fully remote work. This poses massive challenges for enterprises that must immediately manage an entire staff of remote workers.

> It proves that the investment in cloud-first infrastructure pays back in particular when it can be applied in a VUCA [volatility, uncertainty, complexity, and ambiguity] environment.
>
> Markus Sontheimer, CIO/CDO & Member of the Board of Management, DB Schenker

Some organizations can accommodate remote management and full-staff remote work. But for many enterprises, moving all employees (in some cases hundreds of thousands of users) to remote access can overwhelm not just IT administration, but the network architectures they manage.

Cybercriminals also see the surge in remote work as an opportunity. There are growing numbers of Coronavirus-themed cyberattacks targeting people and companies across the globe. Threat actors are launching malware, ransomware, bots, etc. to take advantage of newly-minted remote employees and extended attack surfaces.

Enterprises must recognize the impacts of moving to remote work:

Bandwidth

Companies that rely on VPN-based internet egress for remote work could be in for a rude awakening. Rapid growth in video-collaboration traffic could saturate existing internet egress connections. Additional VPN connections will overwhelm infrastructure.

Security

Remote work must remain secure. How will moving an entire staff to remote work affect access to needed services and apps? Can the corporate security stack effectively handle the traffic spike?

User Experience

SaaS applications like Office 365 require optimized routing—the more network hops the user must take, the greater the lag in connectivity performance. That problem is heightened when a crush of remote users must first VPN into a central location.

Cost

What new software, IT resources, and infrastructure are needed, and how much will all of it cost?

Timing

Given that remote-work operational models can take months or years to roll out, how quickly can you move to remote work and what is the strategy?

Regulatory Environment

In highly-regulated industries, compliance rules won't necessarily be relaxed in a time of crisis. Newly-remote workers could inadvertently gain access to unauthorized applications and put the company into compliance violation.

VPN Challenges Increase as Remote User Demands Grow

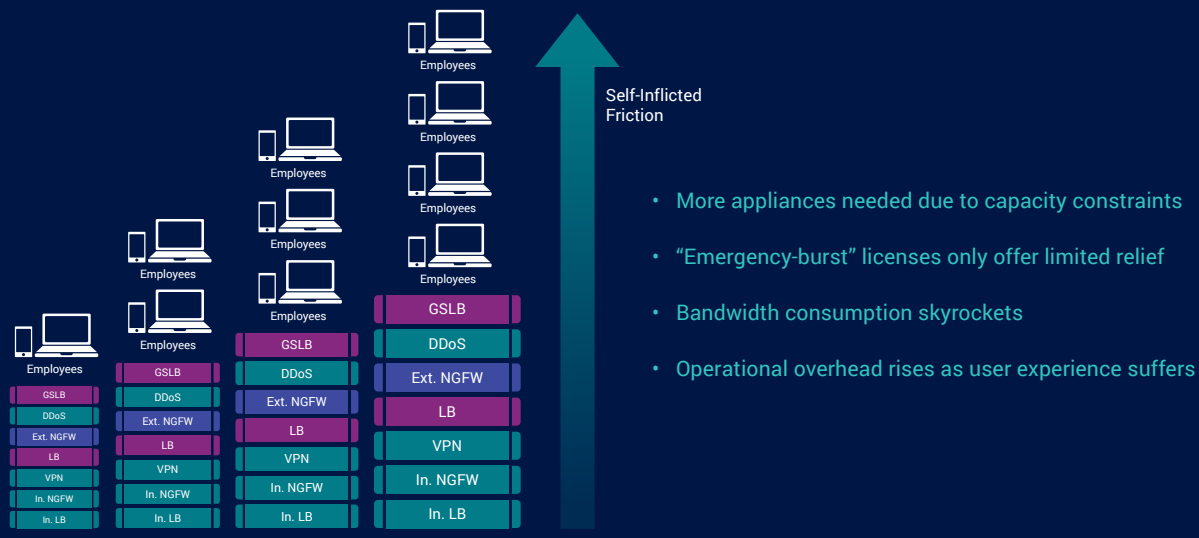

Figure 1. As VPN users and traffic increase, challenges for enterprise networks also increase.

VPN technology requires stacks of gateway appliances and supporting infrastructure (see Figure 1 above), which have bandwidth and licensing capacity constraints. VPN's single-ingress-point model also presents an external attack surface and imposes performance costs of backhauling user traffic to applications in distributed environments.

Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) help mitigate remote workforce challenges using a cloud-delivered service built to secure access to SaaS, the Internet, and private applications.

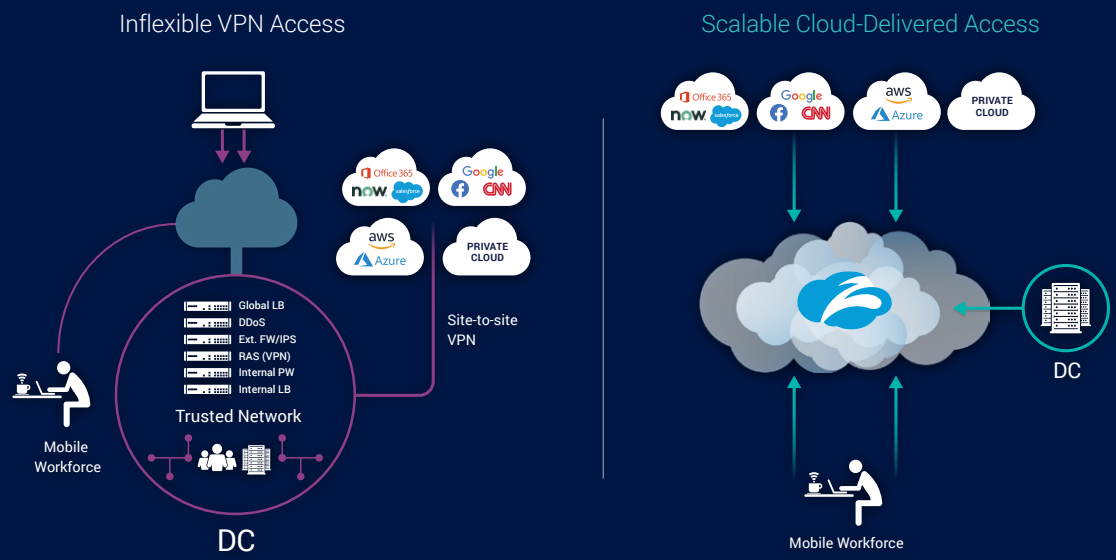

Figure 2. The costly, inflexible, and not-all-that-secure VPN access model (left) is easily overloaded with spikes in remote access. Cloud-delivered remote access like Zscaler (right) scale to accommodate remote work growth.

How Zscaler enables Secure Remote Access

Business Objectives	Strategic Capabilities	Critical Tactics	Using Zscaler
Ensure Network Capacity (e.g. circuits bandwidth, hardware memory or resources, etc)	Enterprises need dynamic scalability that is sustainable for bandwidth, hardware, memory, etc., as well as visibility to assure non-essential traffic is eliminated or minimized.	Schedule user network time by time zone, geographic location. Prioritize user roles so that key people can access the network when needed (C-staff, IT, customer support).	Deploy ZIA and ZPA to go directly to apps and data on the internet and public cloud providers, so that corporate security policy is enforced on all traffic without unwieldy hairpin routing.
Build Flexible Scalability with Minimal Deployment Overhead	Accommodate a greatly expanded remote-work user community as quickly as possible, without crushing operational staff.	Leverage cloud-enabled application access to eliminate bottlenecks in appliances, licensing, or geographic distribution.	Shift remote workers to Zscaler's global cloud platform for reliable, secure application access that can absorb tens or hundreds of thousands of new users in days, not weeks or months.
Secure Employee Access to Applications and Data	Remote employees must have access to applications and data while working remotely.	Develop business specific policies and security rules that apply to remote workers based on identity, job role, access requirements, and geographic locations.	Deploy ZPA and connectors, and use the Zscaler App or browser-based access to connect users to authorized applications based on custom policies. This allows secure access to applications and data while eliminating external-facing inbound connections and reduces the network's attack surface.
Secure Third-Party Access to Applications and Data	Contractors, consultants, vendors, and partners require access to applications and data, without network exposure.	Enable third-party access only to authorized applications; eliminating network connectivity minimizes potential for lateral movement.	Leverage ZPA browser-based access to enable granular control and visibility for third parties — no software installation required.
Preserve Seamless Access to Private Applications in Data Center and Multi-Cloud	Users need access to applications across a variety of back-end environments, without expensive backhaul.	Provide dynamic, secure, direct connectivity to applications in multiple sites simultaneously.	Deploy ZPA connectors across multiple back-end app environments; dynamic path selection ensures transparent, high-performance access for all remote workers regardless of location.
Protect Remote Employees' Devices	Enterprises need to protect remote employee devices while outside of the corporate security boundaries.	Develop access-specific policies to apply to endpoints based on situation.	Deploy Zscaler app to all endpoints either through push, self service portal, or the App Store or Play Store. Use ZIA to apply policy to those Zscaler app deployments to ensure protections in line with risk tolerance levels.
Employ SSL Decryption for All Outbound Traffic	Examine all traffic to Internet and SaaS apps in order to ensure that policies, threat analytics, detection and remediation are applied in order to find threats and prevent infiltration.	Determine if all traffic categories need to be examined, or does your risk profile allow for exclusions (such as PCI DSS and HIPAA compliance).	Enable SSL decryption for ZIA across all locations and endpoints using Zscaler certificates (for quickest deployment).
Determine if Files Are Malicious	Employees will most likely need to exchange a large number of files between both internal and external parties.	Determine from a risk perspective what further file types need to be sandboxed from what locations, and make decisions based on what the business can support.	Use ZIA to enable a clean up "any-any" rule for the most risky file types and implement Quarantine file types.
Ensure Critical Company Data Is Not Exfiltrated	Enterprises will need to continue to ensure that critical data does not leave the business.	Refine data loss prevention (DLP) rules and implement Exact Data Match to more effectively restrict critical data movement.	Use canned and/or custom ZIA DLP rules to look for sensitive data in traffic flow.

With the right planning and actions, companies affected by the COVID-19 outbreak can ensure the safety of their employees while still moving ahead with crucial business objectives. Zscaler's cloud-built, secure access service edge platform was designed specifically to enable direct connectivity via local internet breakouts, ensuring that enterprises (and all those enterprises' remote workers) can move forward in uncertain times.

To help in this unprecedented situation, Zscaler is introducing its **Business Continuity Program** designed to help organizations keep employees safe and maintain enterprise productivity.

Secure Your Remote Workforce Today

About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.