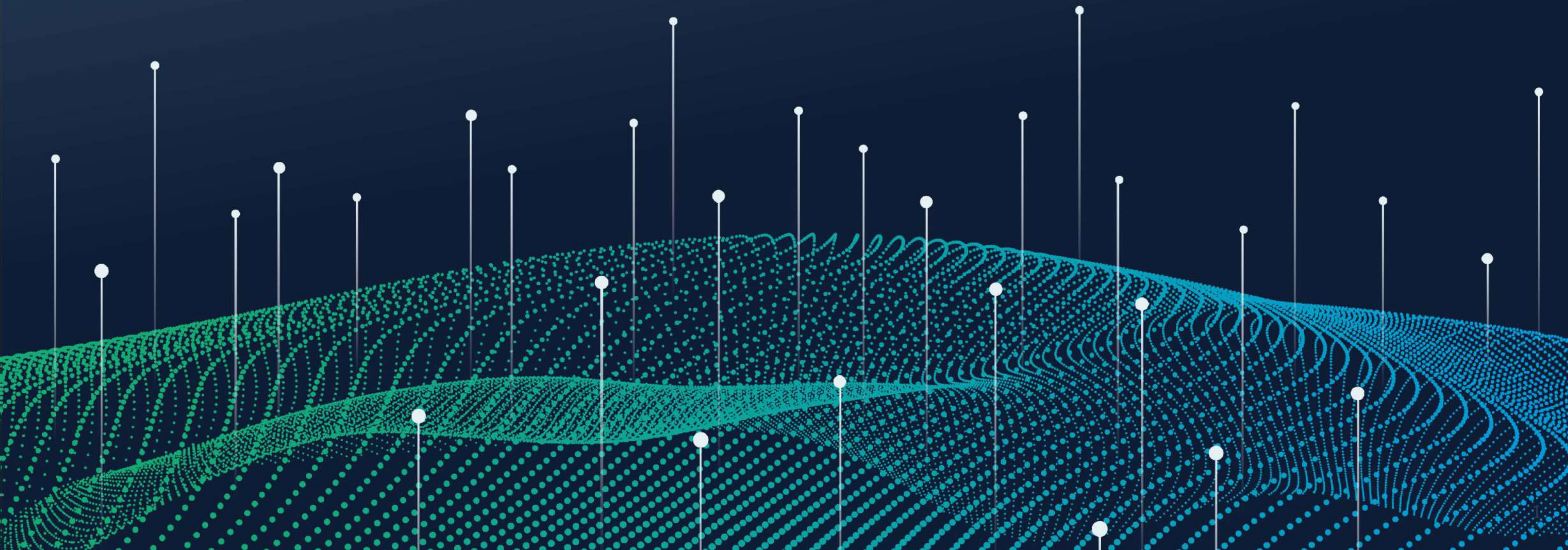
Securing Remote Work

Safeguarding Business Continuity with Zscaler™



Contents

Foreword

These are unpredictable and unsettling times. Like all of you, I am watching events unfold in the global response to COVID-19, and I am doing what is best for my family, the Zscaler family, and Zscaler customers and partners. Zscaler's mission is to provide secure, fast, and reliable access to applications, no matter where they are hosted, and no matter where users connect. Zscaler is playing a pivotal role for enterprises as they respond to the crisis: We have an obligation to help customers keep employees safe and productive as they work remotely.

We've all been talking about remote work for years, but now most organizations find themselves immediately forced into it. How exactly do you follow social-distancing mandates in a global, interconnected organization without losing productivity or exposing the business to unnecessary risk? This is a central question today for the entire C-suite.

The stark truth is that employees will do whatever is easiest to get the information they need to get their jobs done, even bypassing slow VPNs to connect directly to resources. This greatly increases risk. It's hard to blame the employees: They simply want to turn on their computer or mobile device and go to work. Most of them will just go directly to the internet to access cloud applications like Salesforce, AWS, and others for their day-to-day work.

Like so many of you, the Zscaler staff is working remotely now too. We all use the Zscaler cloud platform to enable our teams to deliver the same level of productivity regardless of where they work, what device they're using, or what business applications they need.

In recent months, as COVID-19 has spread, enterprises have reached out to us to help them achieve this same level of productivity by providing access to all internal and external applications as quickly as possible.

Many enterprises have put business-continuity plans in place, but few plans (or planners) could have anticipated COVID-19's far-reaching impact, in particular, the urgent shift to a 100-percent remote workforce. When asking asking employees to work remotely, organizations have to take many things into consideration to keep employees secure and productive: Will all employees be able to access all applications remotely? Can the IT team provide support remotely? What's the impact on your organization's security posture? What will user performance look like?

When remote-work enablement is done right, employee teams are able to:

- Access all authorized applications, whether they are SaaS apps like Salesforce, collaboration tools like Microsoft 365 (formerly Office 365), or internal apps.
- Securely surf the internet.
- Deliver IT support from any location on any device.
- Lessen bandwidth use to cut costs and improve employees' overall user experience.
- Do all of this while improving overall security by minimizing the attack surface.

To ensure organizations can swiftly respond to this situation (and future crises), Zscaler has developed a program focused on enabling employees to work from anywhere,[1] and to help enterprises accelerate their digital transformation initiatives. The program helps organizations achieve the above objectives, enabling fast, secure, and reliable employee access to the applications and services they need to get their work done. The Zscaler work-from-anywhere solution includes free professional services support for the rapid transition to remote access.

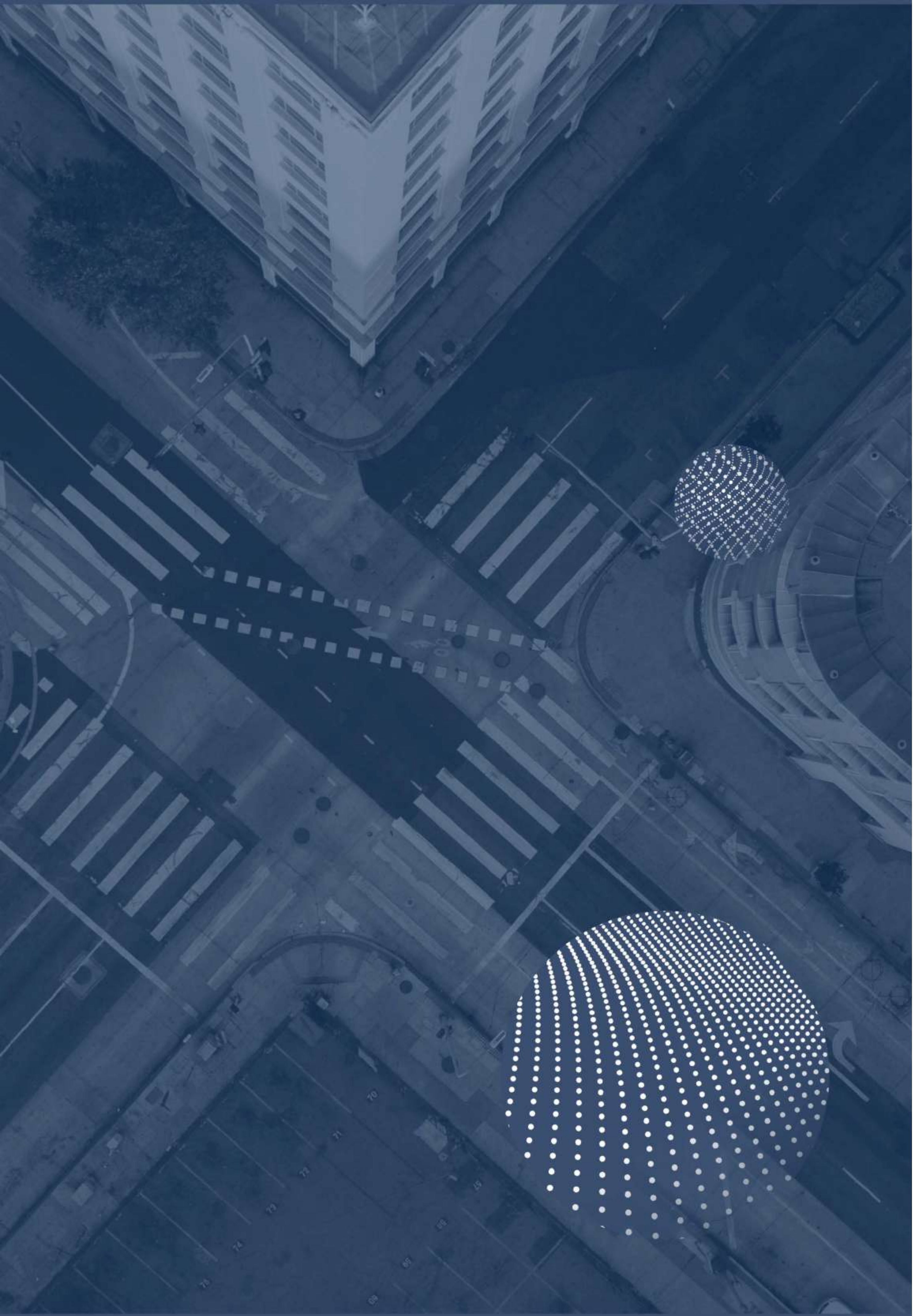
Zscaler is committed to helping our customers, employees, and partners remain safe by enabling them to work from anywhere. Please accept my best wishes for your good health and that of your families.

Jay Chaudhry
Chairman and Chief Executive Officer, Zscaler
May, 2020

[1] https://www.zscaler.com/solutions/work-from-home

CHAPTER 1

COVID-19 has changed the way the world does business



A global pandemic is declared

On March 11th, 2020, the World Health Organization declared the novel coronavirus (COVID-19) to be a global pandemic.[2] With cases reported across 114 countries at that time, the virus posed a serious threat to public health safety across the globe. Governments across the world moved swiftly to take action — closing their borders, issuing nationwide quarantines and lockdowns, and enforcing public health measures for social distancing to slow the transmission of the virus.

Federal, provincial, and municipal governments worldwide issued stay-at-home orders to their citizens. Thousands of businesses, services, and government agencies found themselves forced to mobilize rapidly to ensure essential services such as healthcare, food, and public utilities remained available to the public. To keep their economies running, they also faced the daunting task of enabling millions of workers around the globe to continue to perform their day-to-day work remotely.[3]

[2] "WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020": https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[3] "California orders its nearly 40 million residents to stay home to prevent the spread of coronavirus": https://www.cnn.com/2020/03/19/us/california-coronavirus-stay-home-order/index.html

The IT challenges of enabling work from anywhere

Remote work requires significant adjustments for both organizations and for employees. Our mutual reliance on the internet, the cloud, and on services that allow us to work and learn from home has never been greater. After the COVID-19 outbreak, utilization of tools to enable remote work increased dramatically.[4]

To ensure business continuity and preserve enterprise productivity, organizations have had to transition to a 100-percent remote workforce (or nearly 100-percent remote workforce) in short order. And their IT teams are grappling with just how to do that.

This sudden shift to remote work places new pressures on IT leaders. New priorities have emerged: CIOs and CISOs are currently heads-down trying to enable and secure the suddenly-remote reality. But that urgent initiative has brought them face to face with the limitations of their legacy architectures and processes. To facilitate the shift to remote work, they must assess the shortfalls of their current network infrastructure, implement new security measures, and audit their application ecosystem.

The timeline is understandably aggressive: A company that can't work remotely can't work, period. IT's mandate to get employees up and running first and then address security afterward has forced security teams to bring deadlines forward and play catch up. This means that CISOs must find and patch holes as quickly as they can, perform risk-assessments on the fly, and collaborate with IT and network operations teams to operate systems never intended to support a 100-percent remote workforce.

Many IT organizations have been challenged to support this urgent remote-work pivot. The reason can be found in how IT operated pre-COVID-19.

We have suddenly become reliant on services that allow us to work and learn from anywhere

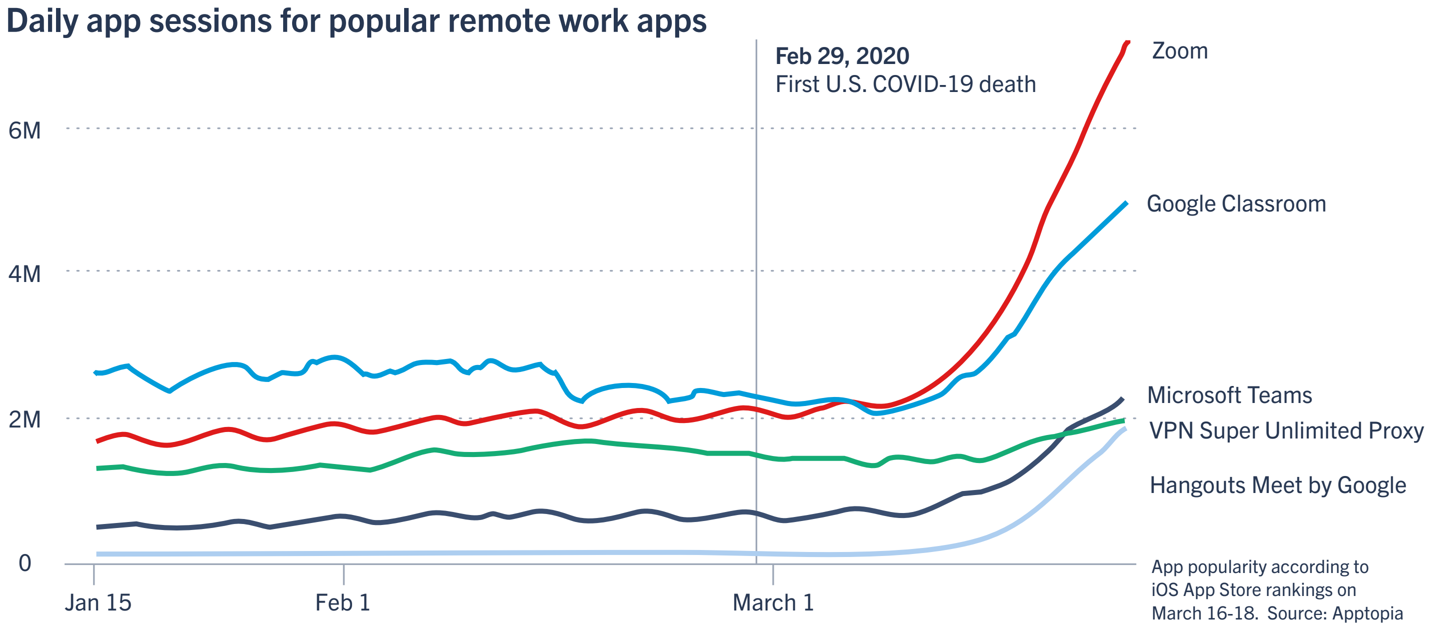


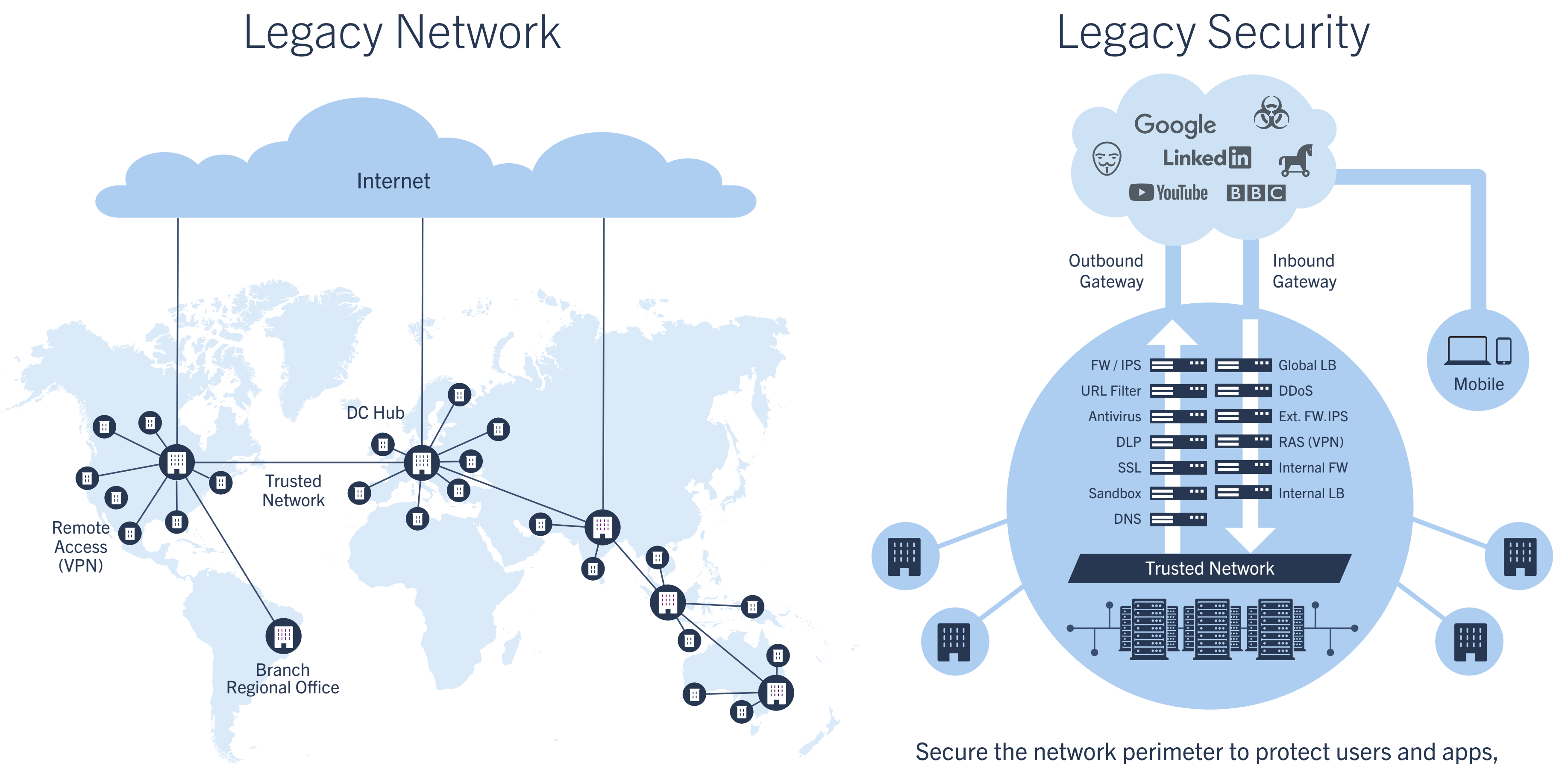
Figure 1-1. Reliance on SaaS and web apps has increased exponentially with remote work; Source: New York Times

[4] *The New York Times* — "The Virus Changed the Way We Internet": https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html

Before COVID-19, most employees at most organizations worked in a corporate or branch office. Their organizations provided them with all the tools and services needed to accomplish their job in the office and on-premise. Notably, those tools and services included the capability to connect to public and private resources. If those employees had to travel or work from outside the office, their go-to connection method was to use virtual private networks (VPNs)[5] that routed their traffic back to the company network so that they could pass through the controls there, and then access the services they needed.

Before COVID-19, working from home (or anywhere outside the office) was an ad-hoc privilege reserved for a small percentage of employees. With millions of formerly-office-bound users now having to work remotely, legacy networking and security paradigms have had to scale to provide the controls required for a now 100-percent cloud- and mobile-first world. Except most can't. And most haven't.

> “*We would have failed using our legacy VPN solution. It was designed to handle a peak load of 2,000 concurrent users and was never designed for the amount of traffic that comes with a global pandemic. Given the current global supply-chain constraints, sourcing the needed hardware for our old legacy solution would be impossible for our current remote worker demand. I don't even want to imagine where we'd be under those circumstances.*”
>
> Alex Philips, Chief Information Officer,
> National Oilwell Varco


Legacy Network

Legacy Security

Secure the network perimeter to protect users and apps, with a linear stack of appliances to protect the gateway.

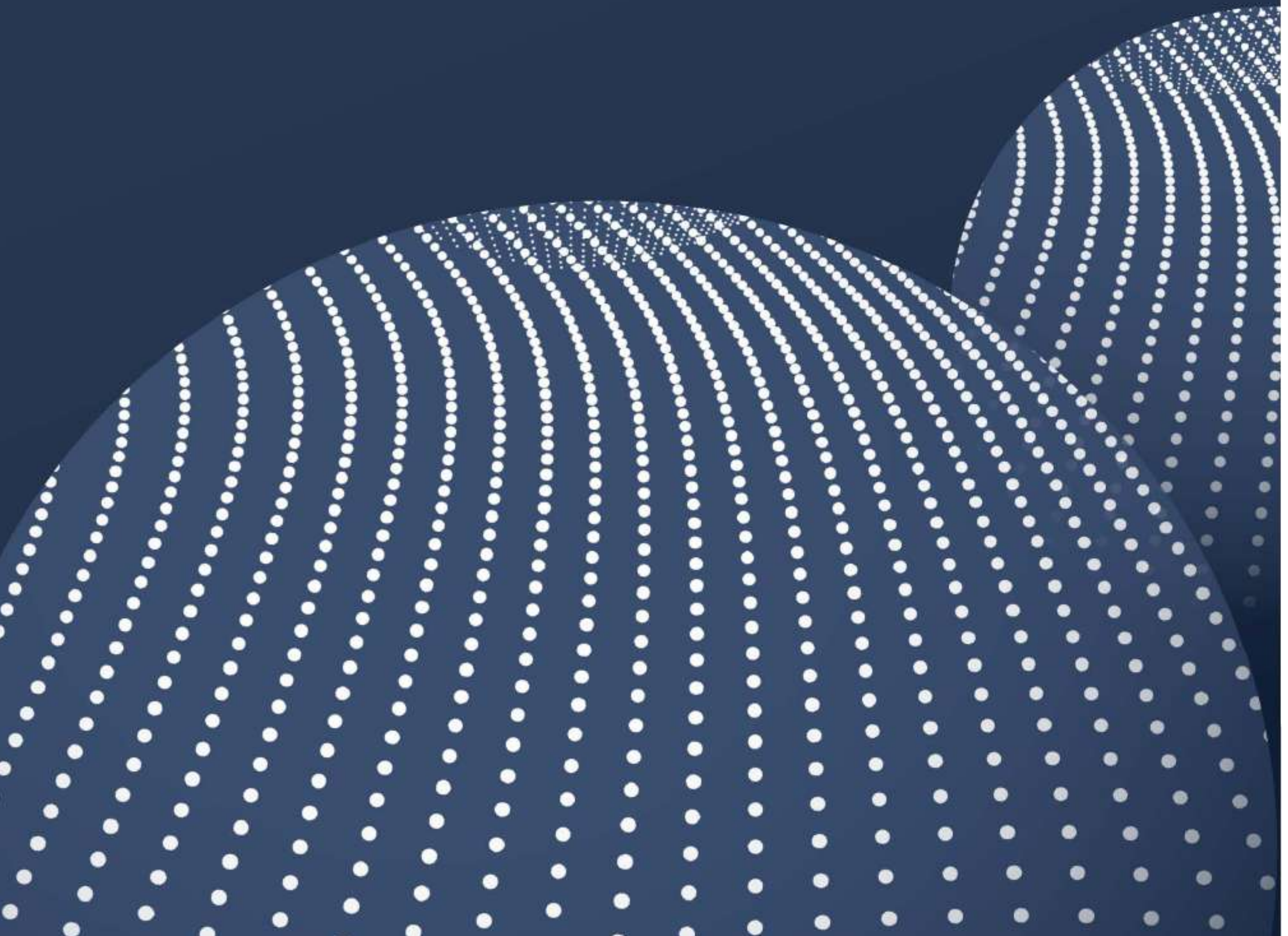
Figure 1-2. Legacy network and security topologies

[5] https://www.zscaler.com/solutions/vpn-retirement

Key Takeaways

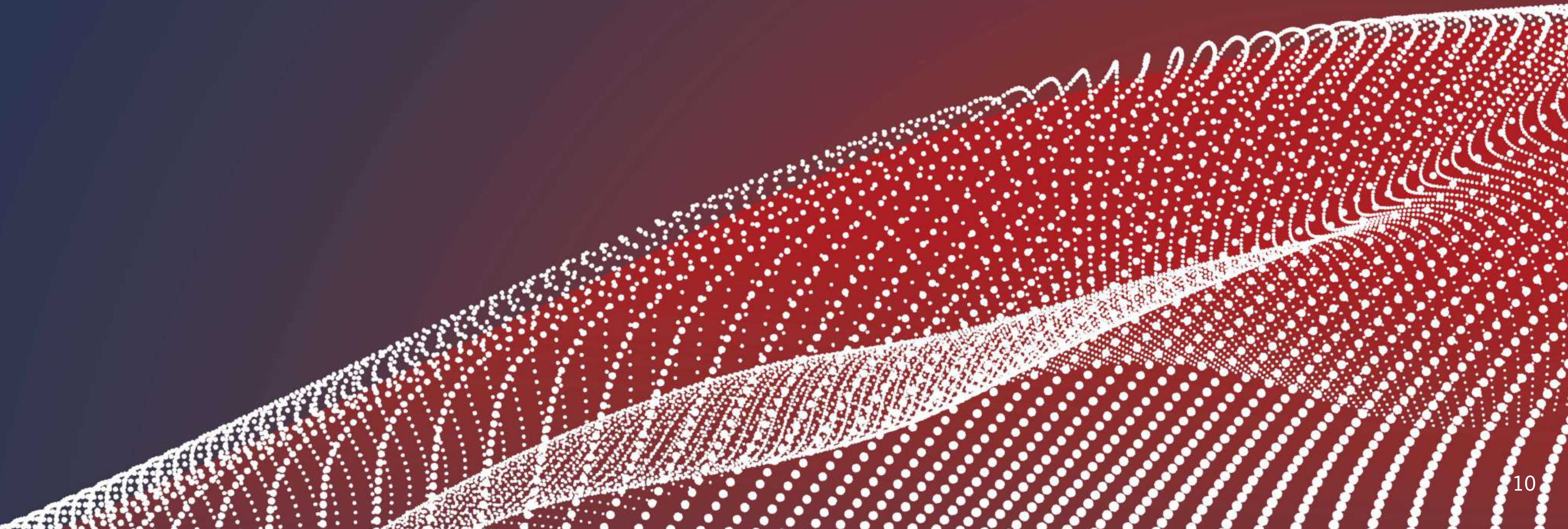
- Remote work requires significant adjustments for both organizations and for employees.

- Legacy IT topologies were not designed for the amount of remote traffic that comes with the transition to a 100-percent remote workforce.



CHAPTER 2

Enterprise challenges with supporting work from anywhere



Enabling remote access with legacy infrastructure will strain any IT organization

With employees working remotely amid the global COVID-19 outbreak, the need for enterprise-grade remote-access solutions has become paramount to a company's viability. To deliver on the mandate to provide those enterprise-grade remote WFA solutions, IT teams must prioritize security, scalability, and availability.

Organizations worldwide have struggled with the imperative to provide remote solutions at scale on short notice. IT teams tasked with ensuring business continuity and maintaining remote employee productivity should focus on three objectives:

1. **Make all employees as productive working remotely as they are working in the office.**
2. **Provide employees with seamless access to all applications required to perform their day-to-day work.**
3. **Ensure all work-related mobile devices have secure, direct connectivity to the internet, rather than via an indirect private network.**

Easier said than done: With the urgent pivot to a remote workforce, many organizations have encountered mission-critical challenges associated with enabling remote access. The harsh reality is that their legacy network and security infrastructures are just not built for a cloud- and mobile-first world.

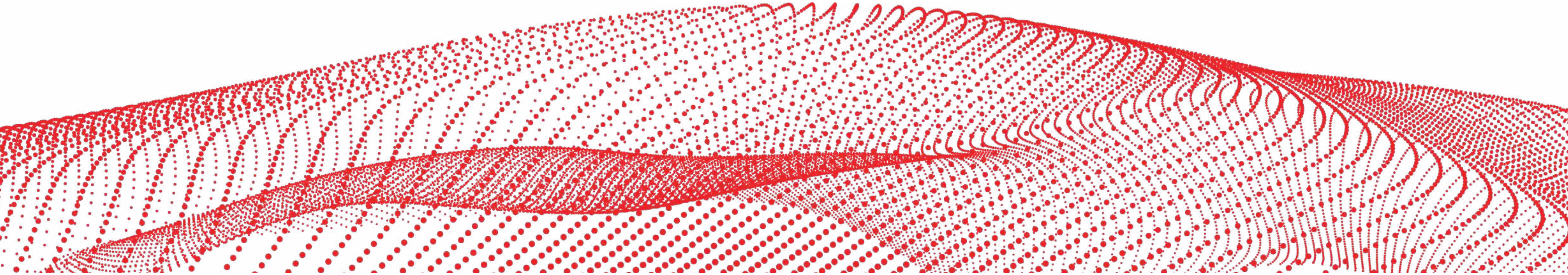
Organizations have relied on VPN for remote employee access

To enable remote-employee connectivity to corporate resources, organizations have typically relied on VPNs. VPNs route traffic indirectly: They grant the user access to the corporate network first, and only then (after distant security-processing) can the user get to the requested application.

This approach may have been fine when the organization supported only a small percentage of remote workers or road warriors: little traffic, little contention, little latency. However, when the number of concurrent remote users grows, traffic bottlenecks, and the existing legacy VPN solutions become untenable. VPNs route traffic destined for SaaS applications like Microsoft 365 (M365) first to the data center for security control, and only then to the application. Add to that circuitous routing a large amount of internet traffic and users must endure added bandwidth-contention for resources and a significantly-degraded user experience.

Worse, VPN-based solutions can increase risk, particularly when their use is expanded to more people. VPNs extend threat surface: Every remote employee represents an unmanaged “branch office” which IT must now secure. There are more points of vulnerability, and a single compromised VPN connection exposes the entire corporate network.

> *If we allowed them to come back on the network via VPN, we were opening our corporate network to whatever evil lay on the other side of the VPN.*
>
> Larry Biagini, former Vice President and Chief Technology Officer, General Electric Company;[6] Zscaler Chief Technology Evangelist



[6] *Secure Cloud Transformation: The CIO’s Journey,* by Richard Stiennon, ©2018, IT Harvest Press: Chapter 8; Page 209: https://securecloudtransformation.zscaler.com/ebook/chapter-8

Challenges with legacy remote-work solutions

Organizations, whether commercial or public sector, must recognize the operational impacts of moving to remote work, and carefully assess the efficacy of their current solutions. Legacy solutions were never designed to support a 100-percent remote workforce. The challenges associated with employing them for that purpose are significant, and their extended use can materially impact the business:

Bandwidth constraints: Organizations that rely on VPN-based internet egress for remote work could be in for a rude awakening. How will moving an entire staff to remote work affect access to needed internet services and apps? (The growth in video-collaboration traffic alone will saturate existing internet egress connections.) These additional VPN connections will overwhelm the existing infrastructure.

Increased risk exposure: Remote work must remain secure. While VPN is needed to access internal applications in the data center, it's not required to access the internet or SaaS applications. Users seeking a fast remote-connection experience will directly access these applications without the proper security controls in place. (The pain is real: Compare video-over-VPN performance to say, Netflix.) Cybercriminals are well aware of this and have been busy launching new ransomware, sophisticated social-engineering campaigns, and targeted attacks.[7] Can the corporate security stack effectively thwart these attacks? (Not when users bypass it.)

Poor user experience: SaaS applications like Microsoft 365 and Zoom play a critical role in facilitating collaboration and driving productivity across a remote and distributed workforce. But these and other SaaS applications are latency-sensitive, and prefer short, fast, and optimized routing. The more network hops the user must take, the greater the

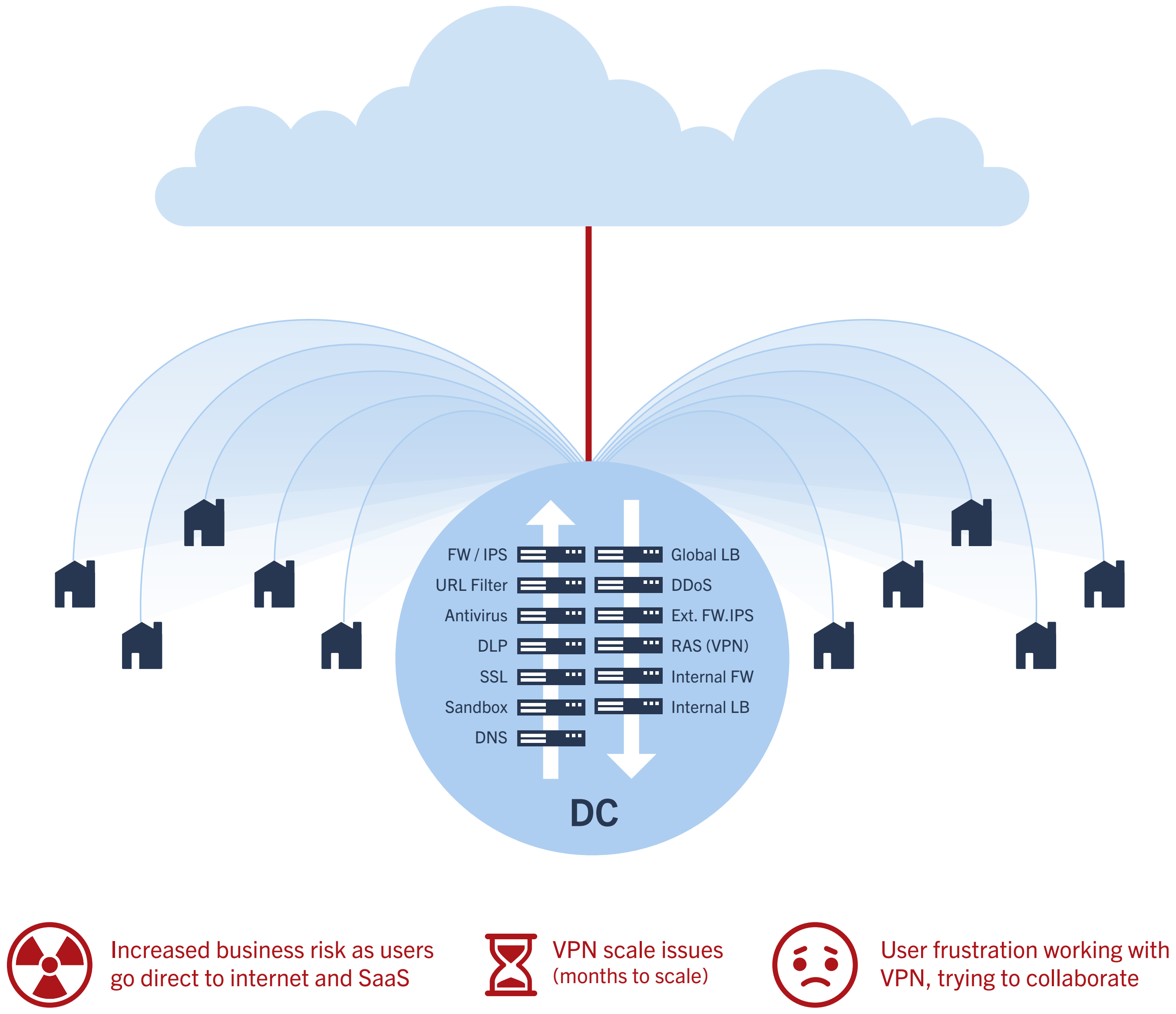

FW / IPS
URL Filter
Antivirus
DLP
SSL
Sandbox
DNS
Global LB
DDoS
Ext. FW.IPS
RAS (VPN)
Internal FW
Internal LB
DC
Increased business risk as users go direct to internet and SaaS
VPN scale issues (months to scale)
User frustration working with VPN, trying to collaborate

Figure 2-1: Using legacy infrastructure when working remotely has many challenges

[7] https://www.zscaler.com/threatlabz/global-internet-threats-insights

lag in connectivity performance. When a surge of remote user traffic needs to be backhauled through a VPN connection to a centralized internet gateway, latency increases, inhibiting users' ability to collaborate.[8]

Inability to scale quickly: Procuring, configuring, racking, stacking, and managing additional VPN and gateway appliances to accommodate a growing remote workforce isn't a trivial exercise in the best of times. Add disruptions to the hardware supply chain, and scaling can take weeks, even months. Such delays affect employee productivity, which, in turn, impacts business performance. Spinning up virtual machines (VMs) of single-tenant appliances as a workaround isn't a viable alternative: It increases complexity and worse, risk, as every firewall exposed to the internet becomes a new attack surface, offering an inviting entry point for cyber attacks.[9]

Regulatory compliance: In highly-regulated industries, compliance rules won't necessarily be relaxed in a time of crisis. Without proper controls in place, newly-remote workers could inadvertently gain access to unauthorized applications, and put the company into compliance violation.

Rising costs: Legacy security architectures require all remote-user traffic to be backhauled to the data center before it can go to the internet. And routing and processing that traffic requires stacks of gateway appliances and supporting network infrastructure. (See Figure 2-2.) This invariably increases the overall costs. Morever, cost containment becomes a massive challenge when traffic continues to surge and scale.

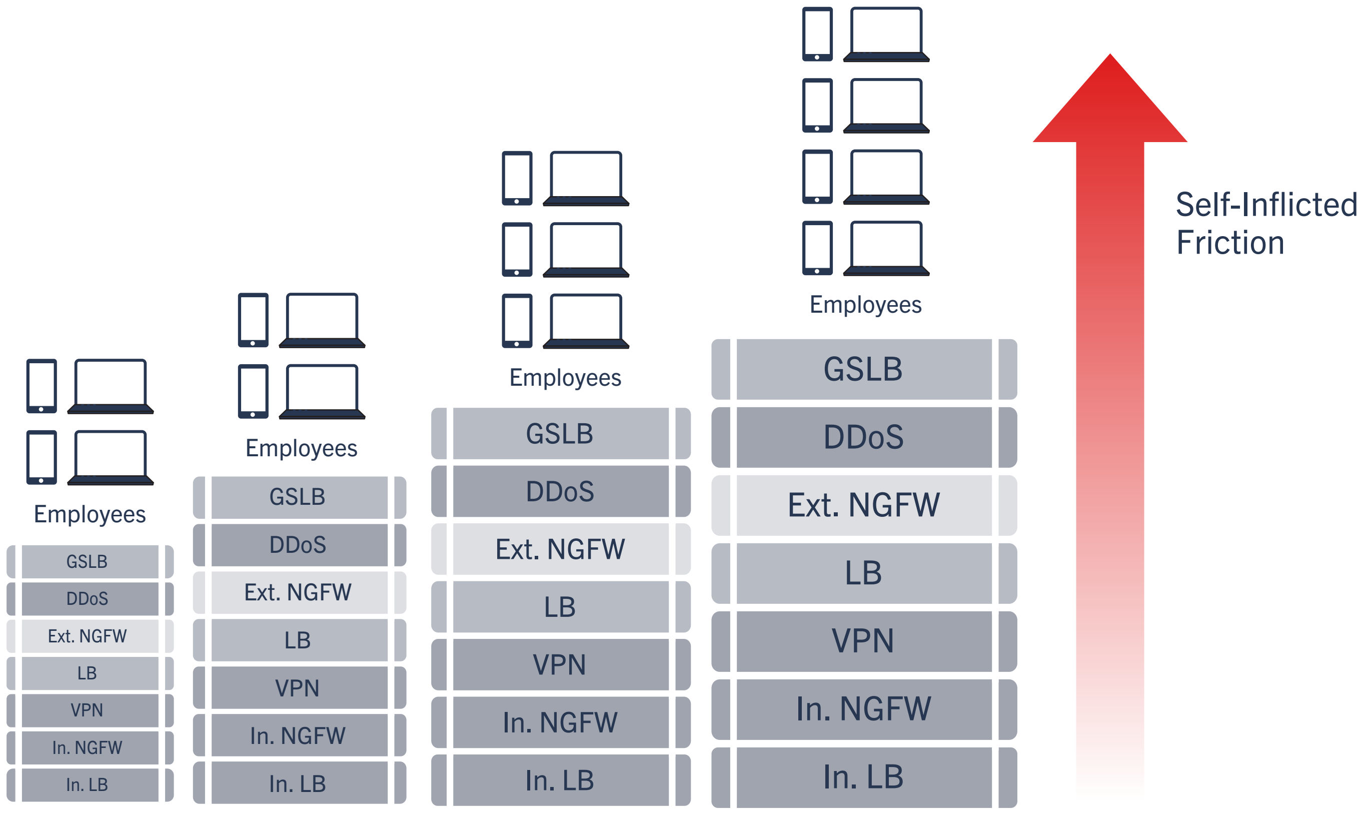


Figure 2-2. As user traffic to the data center increases, associated network insfrastrucure and secure applicance costs increase exponentially.

[8] "Cisco rations VPNs for staff as strain of 100,000+ home workers hits its network": https://www.theregister.co.uk/2020/04/02/cisco_rations_staff_vpn/

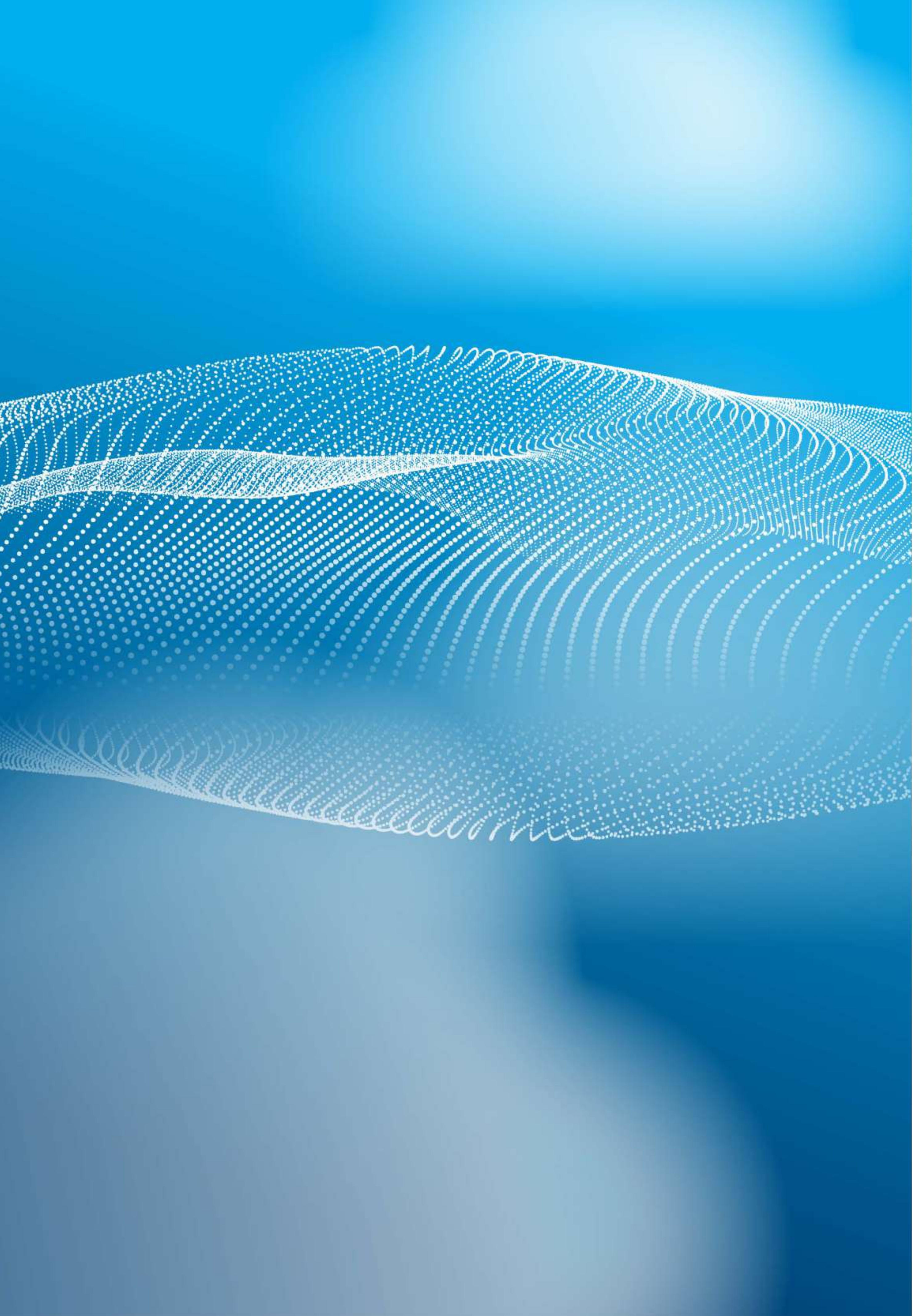
[9] "Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems": https://www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to-hit-remote-work.html

Key Takeaways

- Workforce mobility makes every user a potential source of security vulnerability.
- Policy enforcement is critical when users connect to corporate resources, irrespective of their location.
- While a traditional VPN may provide some of the needed access controls to enable a small percentage of remote users, it cannot scale easily, affordably, securely, or quickly enough to support a pivot to a fully-remote workforce.

CHAPTER 3

In search of (urgent) agility: Cloud architectures for working from anywhere



Many organizations today are still not ready to transition to a fully-remote workforce because most of their infrastructure was built for a pre-cloud, pre-mobile world that was never meant to support broad remote access.

When remote working was merely the exception, a small percentage of traveling employees could VPN back to the data center. If they wanted to access resources or applications in the cloud or the internet, their traffic would be backhauled to the data center before reaching the cloud. This is analogous to flying from New York to London via Miami. The greater the distance the data travels, the slower the user experience and the greater the attack-surface extension, invariably increasing the cyber risk and threat to the business.

Two common cloud architectures have emerged to support remote access. (And one does it far better than the other.)

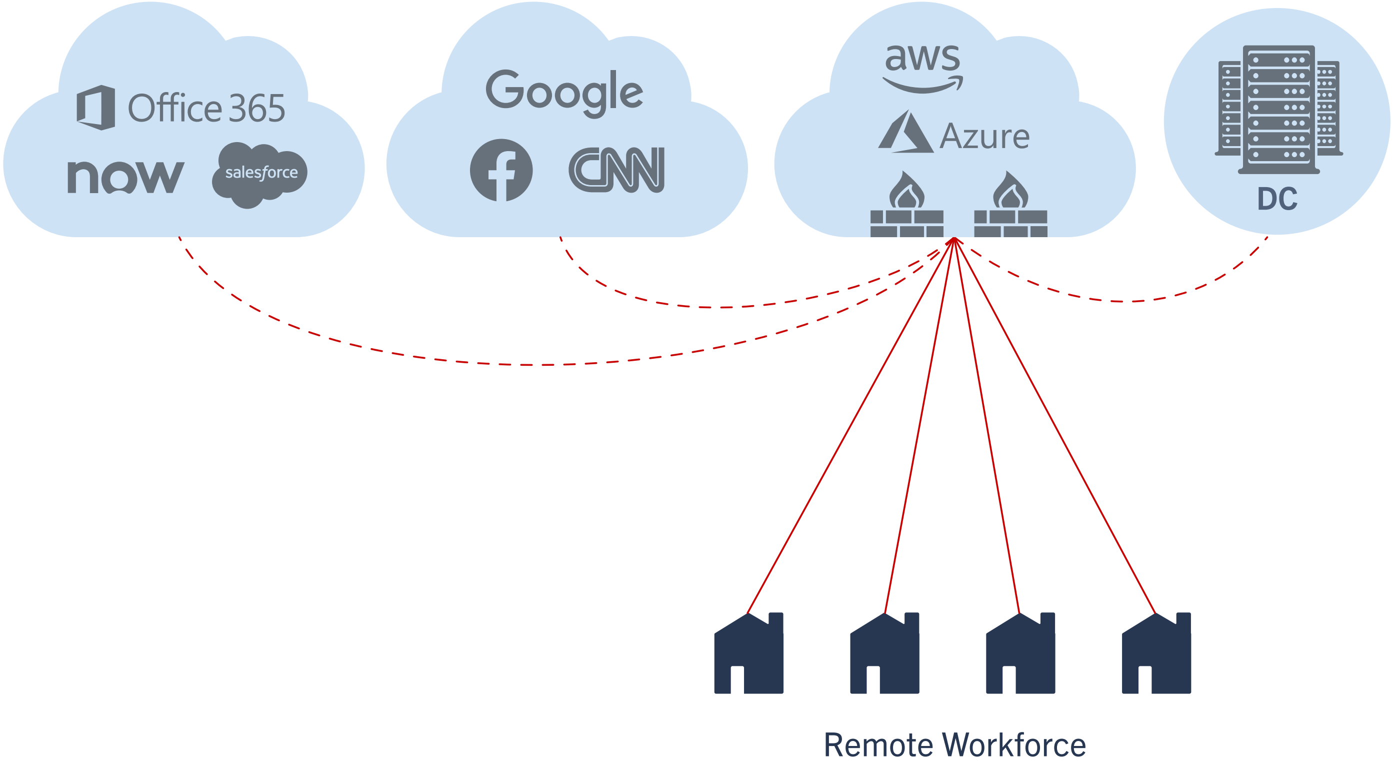
Legacy firewall/VPN deployed as virtual machines in the cloud

Legacy VPN and firewall vendors commonly recommend enterprises spin up virtual machines in the public cloud, a cloud model illustrated in Figure 3-1. This is an indirect, "destination-based" model: In this architecture, user traffic travels to a VPN deployed in the public cloud first before being allowed to head to its intended destination — either in the data center or in the cloud.

This approach replicates legacy hub-and-spoke/castle-and-moat architecture shortcomings: For one, traffic moves indirectly, slowing performance. (Backhauling in the cloud is still backhauling.) In effect, it extends the enterprise perimeter that must be secured out to the cloud, adding to attackable-surface exposure.

The "Legacy firewall/VPN" model virtualizes a hardware stack in the cloud, preserving all the bottlenecks that come with it. This model places the onus of hardware management on the service vendor, but the enterprise still pays for each "instance," an expense that can limit scalability.

Cloud-based remote access demands an architecture that secures traffic without compromise to performance or threat posture. Moving a legacy security stack to the cloud doesn't make it any faster, more scalable, or more secure. Instead, it further extends an already-inadequate security perimeter, placing remote users and the business at risk. Describing it as a cloud-based security alternative is disingenuous, comparable to stacking DVD players in a single data center and calling it Netflix.



Retrofit legacy firewalls/VPNs as virtual machines in the public cloud

Akin to stacking DVDs to build a streaming service

- Poor work / collaboration experience
- Limited security
- Large attack surface (external and internal)

Figure 3-1. Retrofit legacy firewalls/VPNs as virtual machines in the public cloud

SASE + ZTNA: The cloud-native architecture for enabling working from anywhere

There is an alternative approach to enable and secure remote access: a secure access service edge (SASE) architecture employing zero trust network access (ZTNA) security principles.

SASE

The secure access service edge (SASE)[10] architecture is an agile, cloud-native, service-rich model. Defined by Gartner Research in 2019, SASE prioritizes security services delivered at the cloud edge:

- Service points of presence (POPs) are highly-distributed, placing cloud services at cloud-edge internet access points, near to wherever a user might be located.
- Policy-governed services applied close to the user eliminate unnecessary backhaul, improving performance.
- Cloud multitenancy fosters dynamic scaling to meet demand (including spikes that might occur during a crisis).
- A proxy-based architecture inspects all incoming and outgoing data traffic, in particular, encrypted traffic at scale.
- Attack surface is minimized, protecting against targeted attacks.

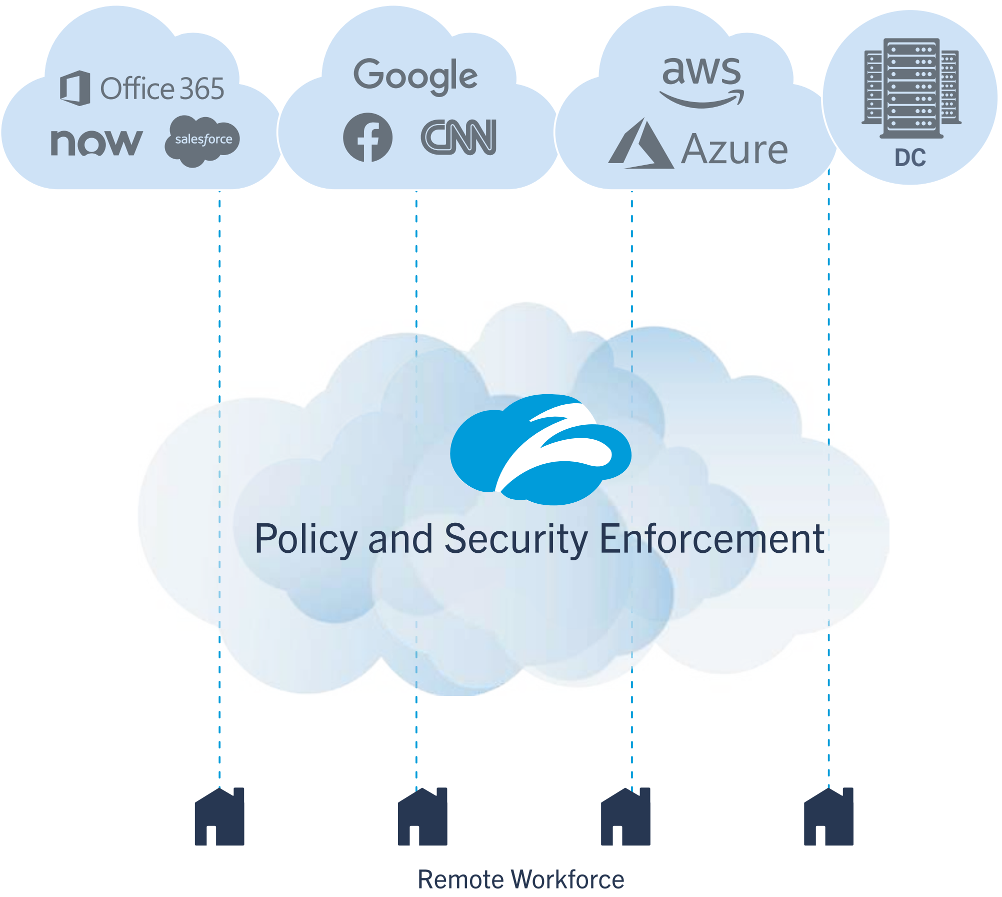
SASE encompasses network security functions including secure web gateway (SWG), cloud access service broker (CASB), firewall-as-a-service (FWaaS), and ZTNA.

[10] https://www.zscaler.com/products/secure-access-service-edge

ZTNA

Zero trust network access[11] ("ZTNA," in Gartner Research acronym form) is the security approach implemented in a SASE architecture. (See Figure 3-2.) ZTNA transforms security, moving beyond the legacy "castle-and-moat" secure-the-perimeter approach to a model that secures direct connections to outside-the-perimeter resources. (Because how can you secure a perimeter that includes the open internet?)

Core to ZTNA is "Zero Trust,"[12] a security ideology that eliminates excessive implicit trust from an enterprise by establishing an initial security posture of default-deny. ZTNA is an adaptive trust model, where trust is never implicit, and access is granted on a "need-to-know," least-privileged basis defined by granular policies. Trust is minimized and dynamic, shifting with changes in context based on user, device, location, and app.



Cloud-native Zero Trust Network Access (ZTNA)

Built to support a 100% mobile workforce

- Fast collaboration experience
- Full security and data-protection stack
- Zero attack surface

Figure 3-2. Cloud-native Zero Trust Network Access

[11] https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-access

[12] https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust

Zscaler Cloud Security Platform

Born in the cloud, the Zscaler Cloud Security Platform is a true SASE service. It connects users directly to resources — whether in a data center or in the cloud — via local internet breakouts. Security is delivered inline, close to the user, optimizing performance by ensuring user traffic travels the shortest path to any application, from any device, irrespective of user location. The Zscaler SASE architecture minimizes data travel, and in the process dramatically reduces corporate attack surface.

Zscaler's globally-distributed platform optimizes connectivity: Users are always only a short hop to their applications. Through peering with hundreds of partners in major internet exchanges around the world, the Zscaler Cloud Security Platform ensures optimal performance and reliability for users, especially when it comes to remote access.

The Zscaler Cloud Security Platform is a zero-trust exchange. The platform employs ZTNA security and includes a zero-trust layer that prevents outside connection from an open, unverified network.

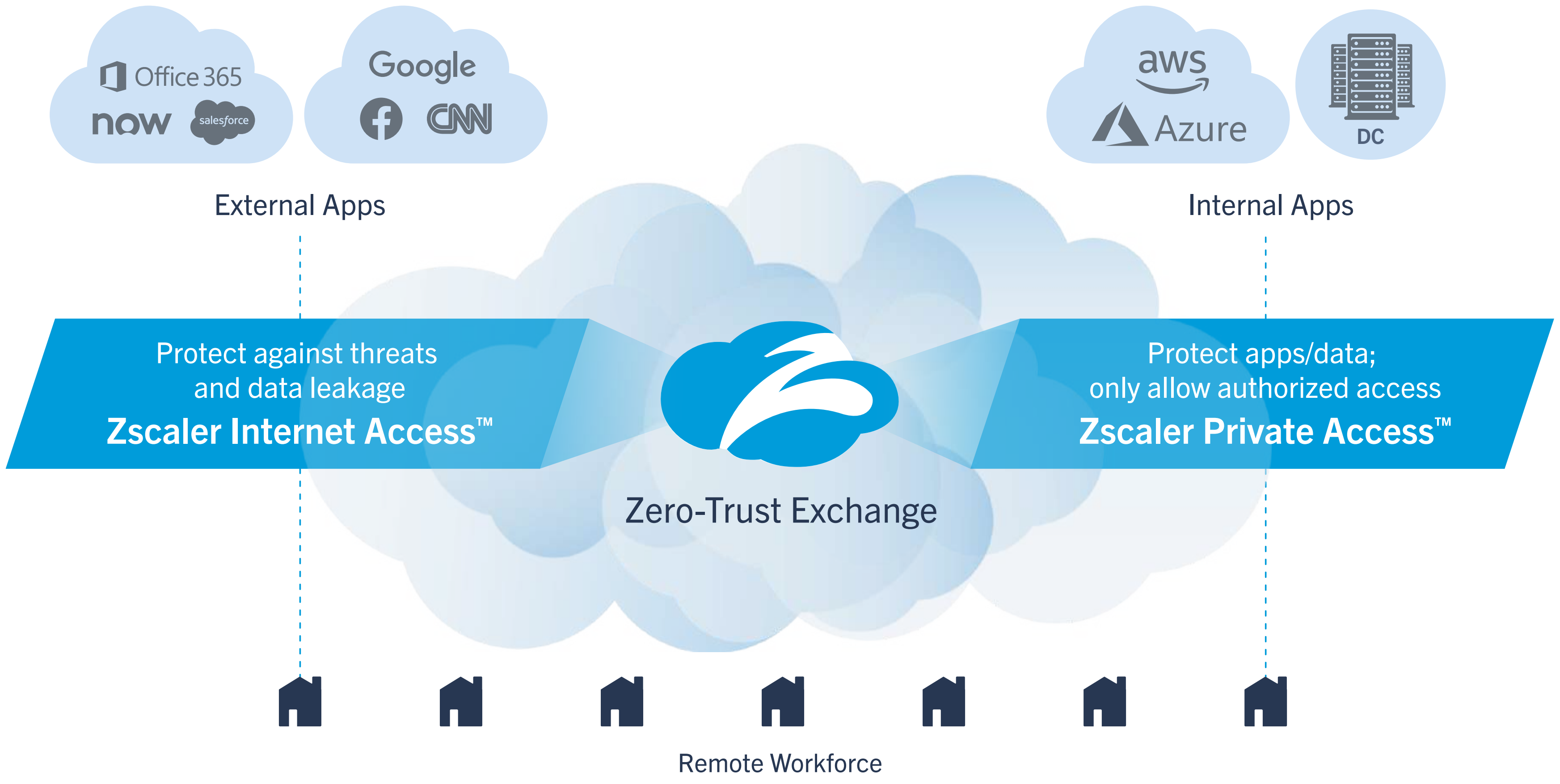
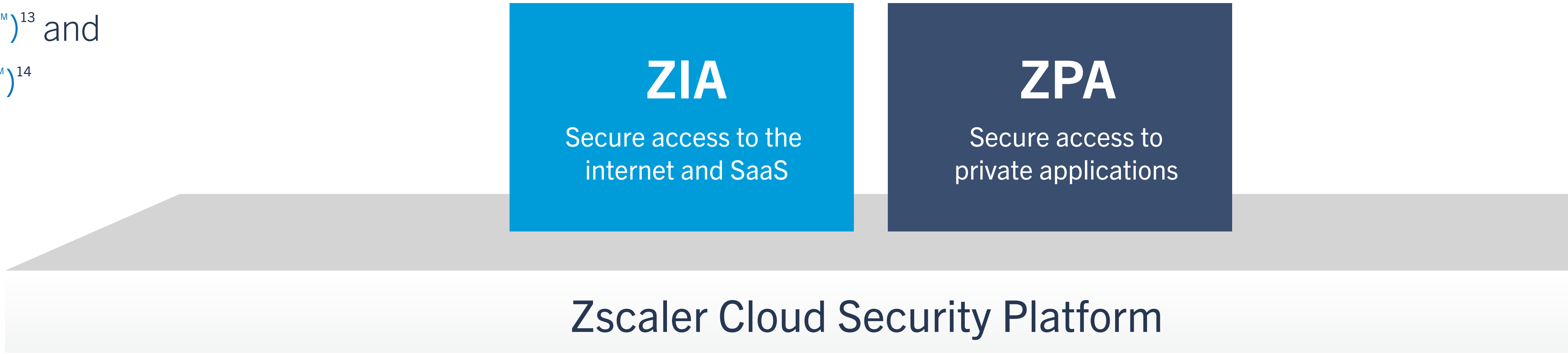


Figure 3-3. The Zscaler Cloud Security Platform acts as an exchange service with zero trust.

There are two key product lines in the Zscaler platform:

Zscaler Internet Access™ (ZIA™)[13] and
Zscaler Private Access™ (ZPA™)[14]


ZIA

Secure access to the internet and SaaS

ZPA

Secure access to private applications

Zscaler Cloud Security Platform

[13] https://www.zscaler.com/products/zscaler-internet-access

[14] https://www.zscaler.com/products/zscaler-private-access

Zscaler Internet Access (ZIA)

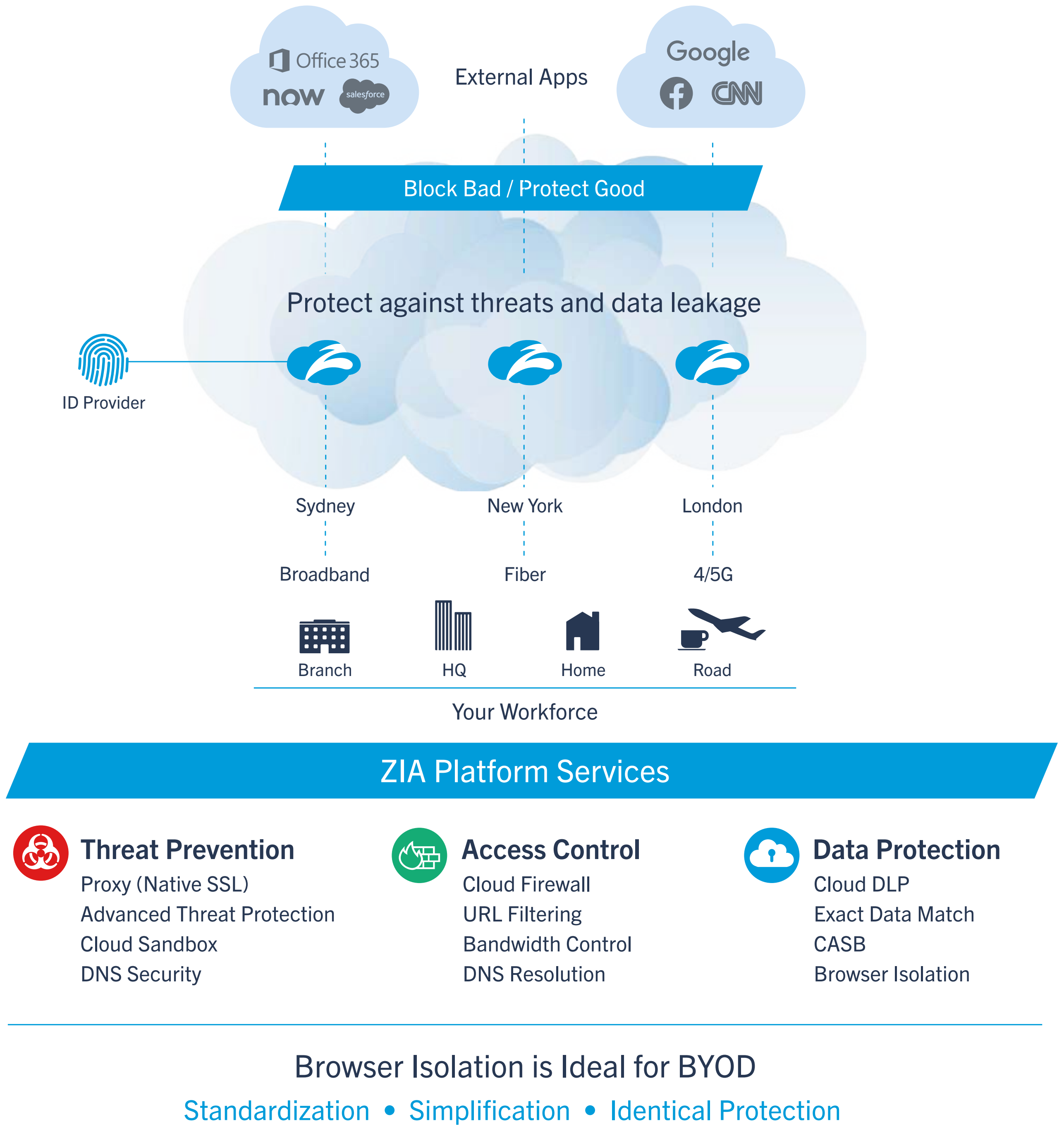
ZIA is deployed as a cloud service and secures traffic between a user's client device and the open internet (or public cloud), regardless of from where a user connects.

When securing cloud traffic, proximity matters: The Zscaler Cloud Security Platform is widely (*very* widely) distributed, with services provided close to each and every user. Traffic travels a minimum distance, optimizing user experience. To get to the internet, a ZIA user connects (automatically) first to the nearest of 150+ Zscaler data centers around the world. Policy is then enforced, and the user is then directed to the nearest destination enabling the shortest path of connection.

For user authentication, ZIA uses an identity provider solution — Okta, Microsoft Azure AD, or similar — to authorize a user to connect securely to a destination. Access is governed by enterprise-defined policies that follow the user, no matter the user's location. For example, a ZIA user in Milan, Italy would connect to public-cloud applications through Zscaler's Milan data center. When in New York, that same user would connect through Zscaler's local New York data center, with the same access policies applied (and security delivered immediately, and nearby).

Threat prevention is core to ZIA. ZIA is based on a full-proxy architecture with inline SSL interception capabilities. More than 90 percent of internet traffic is now encrypted.[15] Organizations not inspecting SSL traffic are blind to most threats. ZIA runs a full security stack — starting with inline antivirus, to advanced threat protection, to full cloud sandbox services — that can detect and stop zero-day threats regardless of from where they emanate, or where targeted users reside.

ZIA employs a full next-generation firewall along with URL-filtering and sophisticated DNS. Enterprises use ZIA bandwidth controls to prioritize traffic, favoring business-critical



Threat Prevention
Proxy (Native SSL)
Advanced Threat Protection
Cloud Sandbox
DNS Security

Access Control
Cloud Firewall
URL Filtering
Bandwidth Control
DNS Resolution

Data Protection
Cloud DLP
Exact Data Match
CASB
Browser Isolation

Browser Isolation is Ideal for BYOD
Standardization • Simplification • Identical Protection

Figure 3-4. Zscaler Internet Access — fast, secure access to internet/SaaS

[15] https://transparencyreport.google.com/https/overview?hl=en&time_os_region=chrome-usage:1;series:time;groupby:os&lu=load_os_region&load_os_region=chrome-usage:1;series:page-load;groupby:os

applications over applications that may reduce user productivity, such as YouTube or Spotify. ZIA also has a full suite of data-protection services, including cloud application controls, data loss prevention (DLP) with exact-data-match capabilities, and cloud access service broker (CASB) controls that can allow enterprise users to utilize sanctioned applications safely. Zscaler browser isolation capability renders content in a cloud browser, and streams content in pixel form to end users. For enterprises seeking to expand remote access, this feature can be beneficial for securing BYOD access.

ZIA simplifies administration, and elastically scales as workloads increase. ZIA enables enterprises to standardize security policies in a consistent manner across an entire workforce, whether employees are sitting in the corporate office or working remotely.

Zscaler Private Access (ZPA)

Zscaler Private Access (ZPA) enables users to connect to internal applications or resources, an activity that — in legacy environments — requires being on the corporate network or connected to the corporate network via VPN. Like ZIA, ZPA is based on fundamental ZTNA principles. Applications — whether hosted in a data center or in a virtual private cloud (VPC) in AWS or Azure — will never listen to an inbound connection. ZPA obscures internal resources from the threat of outside access: With it, an enterprise runs what is essentially a dark network. (Threat actors cannot attack what they cannot see.) ZPA acts as “matchmaker” — Applications connect to Zscaler, and users connect to Zscaler.

The Zscaler Cloud Security Platform (in concert with an identity-provider solution) authenticates a user, and ZPA then brokers a connection between user and “allowable” destination. Corporate-defined policies govern what is “allowable” for each user.

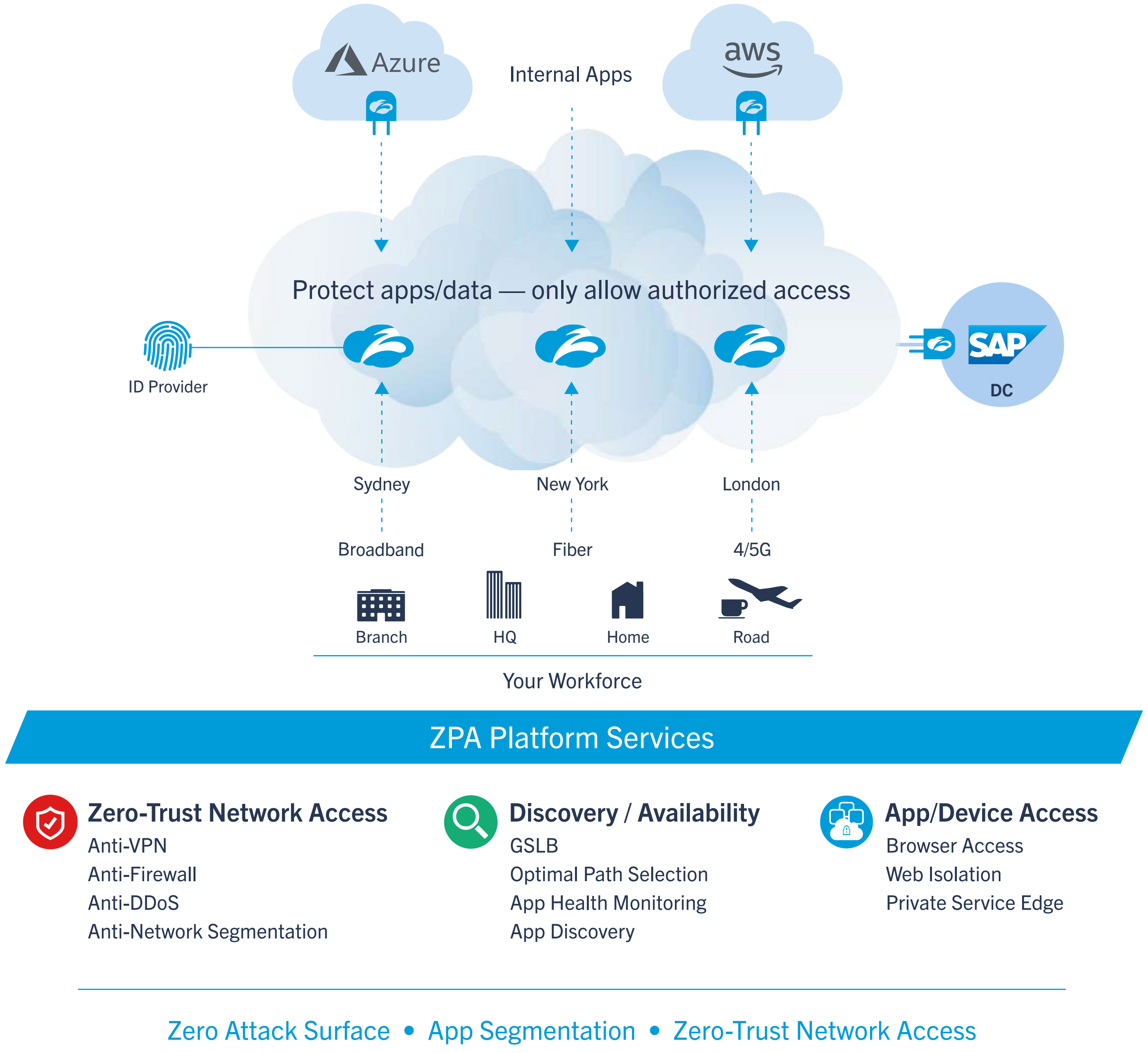


Figure 3-5. Zscaler Private Access — fast, secure access to internal applications

ZPA fundamentally changes enterprise user access to internal applications, and obviates the need for legacy technologies. For example, ZPA's secured direct connectivity supplants VPN access. There is no longer the need to inspect incoming traffic: No need for an enterprise to deploy complex firewalls because there are no inbound rules to govern. There is no longer a need for an inbound listening port in a data center hosting internal applications.

ZPA prevents DDoS attacks since secure connectivity is shielded behind Zscaler's IPs. Load-balancing and optimal path selection are also easier. The ZPA brokerage service automatically chooses the best path between user and internal application using Zscaler's cloud services distributed across 150+ data centers. And like ZIA, ZPA offers browser isolation capabilities.

ZPA employs the Zscaler Cloud Security Platform's fundamental ZTNA capabilities. ZPA enables users to connect to internal applications directly, wherever they may be and wherever corporate resources may be hosted. ZPA dramatically reduces attack surface, simplifies app segmentation, and eases administration. Most importantly, ZPA offers an affordable, scalable, and performance-enhancing remote-access alternative to legacy VPN models.

Secure, agile, scalable: Business continuity with Zscaler

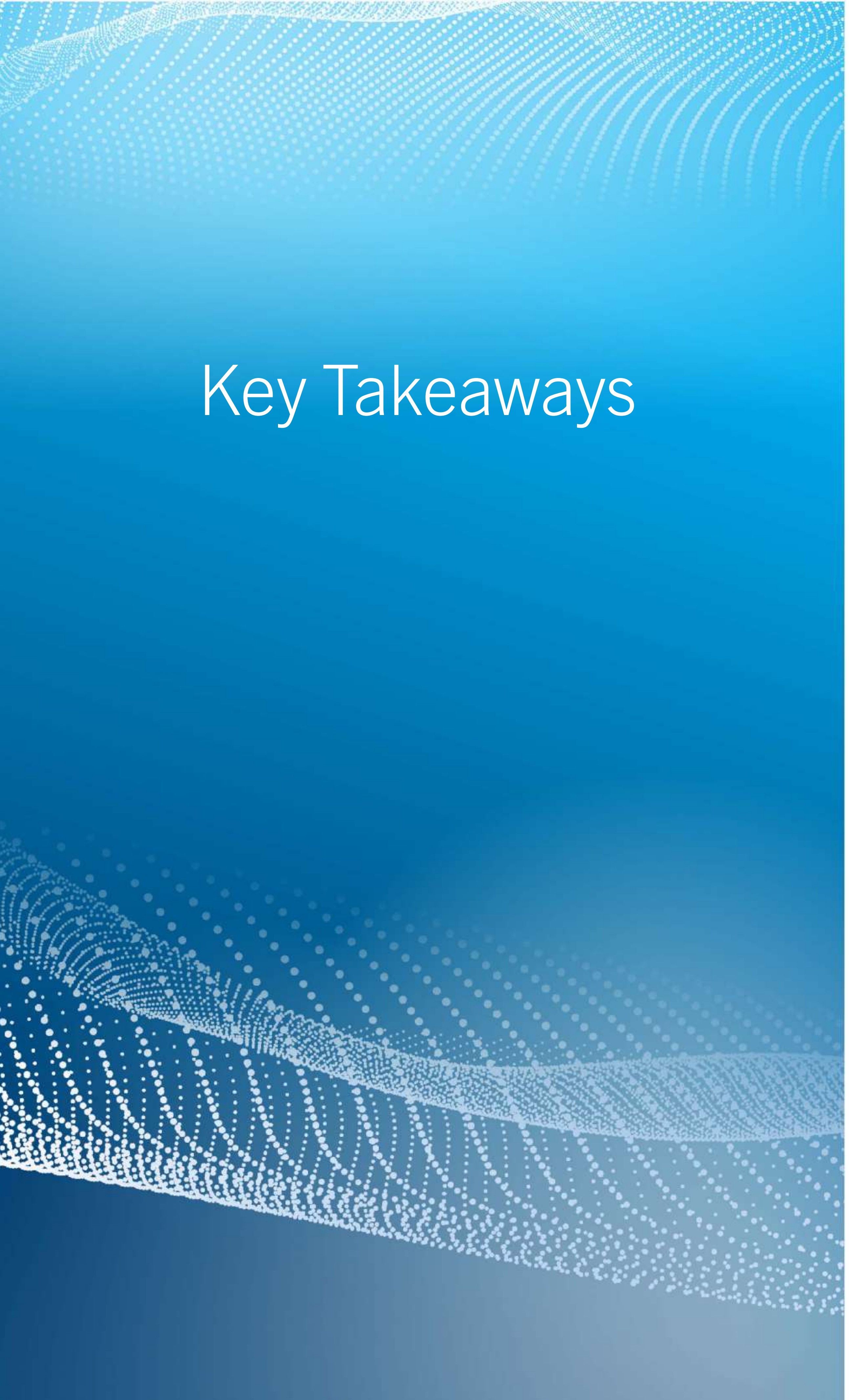
Ensuring business continuity is top of mind for CIOs and CISOs today. In a time of crisis, business continuity is more than an objective: It's a mandate for corporate preservation.

The COVID-19 outbreak has challenged enterprises' ability to pivot to fully-remote access. Perseverance through a crisis takes agility, scalability, flexibility, and an enterprise mindset to look beyond legacy systems. It also takes the right partners: Vendor and partner ecosystems must be able to deliver business continuity and ensure that their own services are not disrupted.

Zscaler was born in the cloud, designed from the beginning to deliver agility in disruptive times. Its core architecture is multitenant and architected to scale, with reserve capacity deployed in all of Zscaler's 150+ data centers worldwide. Zscaler can also expand to other cloud carriers like AWS to deploy additional capacity should the need arise. As part of its ISO 27001, SOC2, and FedRAMP compliance, Zscaler continuously runs business continuity and disaster recovery drills[16] — commissioning new data centers,[17] administering services, and running standard operating procedures, all with 100 percent of employees working remotely.

[16] https://www.zscaler.com/blogs/corporate/zscaler-cloud-operations-conducts-successful-business-continuity-drill

[17] https://www.zscaler.com/blogs/corporate/zscaler-teams-open-new-data-center-canada-without-leaving-home



Key Takeaways

- Many organizations today are still not ready to transition to a fully-remote workforce because their infrastructure was built for a pre-cloud and pre-mobile world, and is ill-equipped to secure broad remote access.

- “Virtualizing” legacy firewalls and VPNs in a public cloud offers little to secure remote access, and delivers a performance-degraded user experience.

- Cloud-native SASE with ZTNA security is the industry-recommended approach to safeguard remote workers and businesses.

CHAPTER 4

How Zscaler delivers productivity and security for a work-from-anywhere workforce

Ensuring business continuity requires empowering employees to be as productive and secure working remotely as they are working in the corporate office. An enterprise-grade, remote-access solution must meet seven fundamental requirements:

1. **Secure access to all applications:** To be able to work from anywhere productively, employees need secure access to the range of applications required for them to do their day-to-day work. These applications could be internet or SaaS applications (often referred to as external apps), or they could be internal applications that (generally) reside in the company's data center or a public cloud.
2. **Cloud identity access management:** Whether employees work in the office or remotely, their access must still be governed. Only authorized employees should be able to access specific applications and resources.
3. **Fast user experience:** To remain productive, it's critical remote employees have a good user experience, one that is equivalent to what they would have working in the office.
4. **Rapid deployment:** Downtime reduces productivity. And reduced productivity impacts the bottom line. In a crisis situation like the COVID-19 outbreak, IT teams must deploy remote-access capability quickly.
5. **Visibility and troubleshooting:** Effective operations management requires comprehensive monitoring and transparency. IT needs to have real-time visibility of users and applications, whether access is remote or on-premise. When things go wrong, IT must be able to figure out the root cause and then troubleshoot.
6. **Cyber threat protection:** When employees work remotely, the internet becomes the new network. With SaaS applications in use, the cloud becomes the organization's new data center. It's a new paradigm, one that requires new security measures.
7. **Data protection:** Remote employees can access data and store files outside of the data center. Without proper controls in place, those activities can leave an IT organization in the dark when it comes to protecting corporate intellectual property.

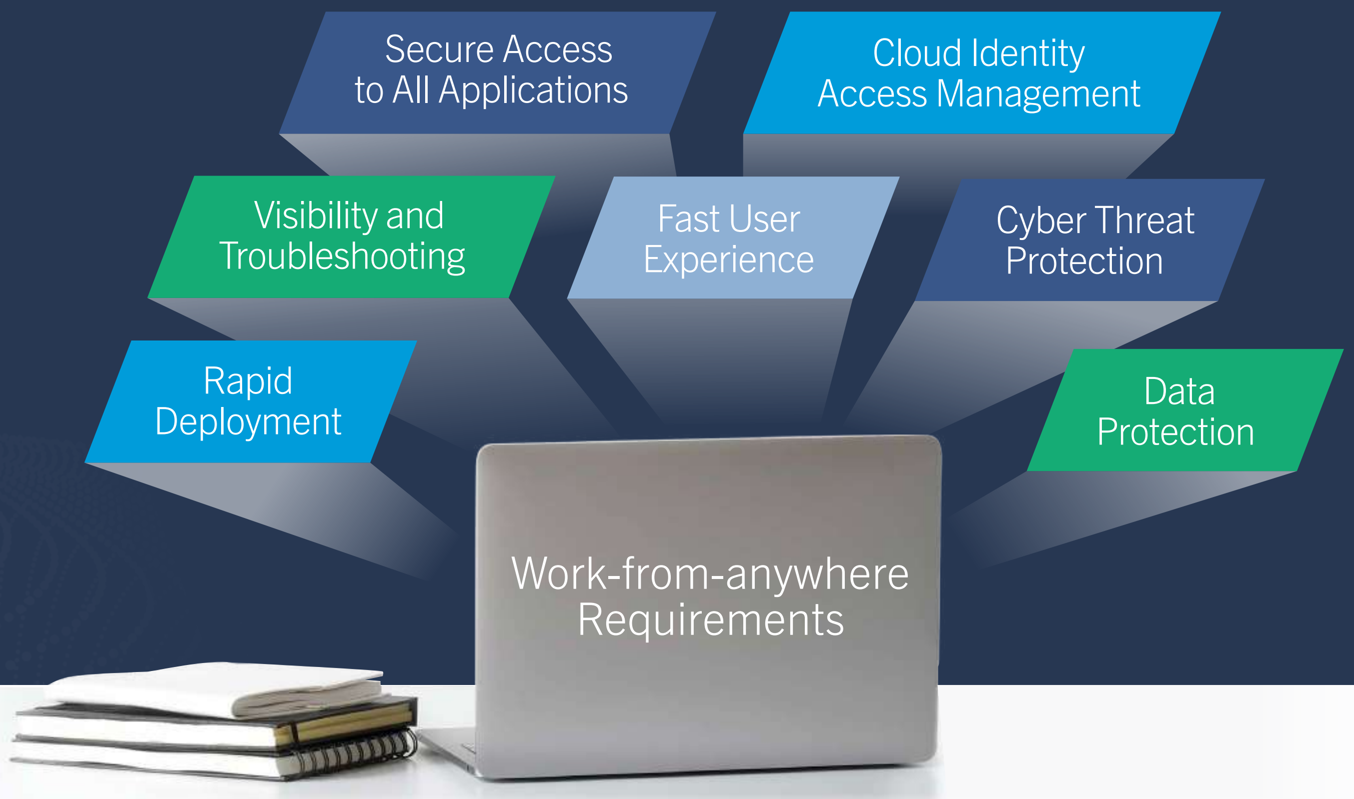

Secure Access to All Applications
Cloud Identity Access Management
Visibility and Troubleshooting
Fast User Experience
Cyber Threat Protection
Rapid Deployment
Data Protection
Work-from-anywhere Requirements

Figure 4-1: Seven key requirements for enabling remote access

1. Secure access to all applications

For a productive work-from-anywhere experience, employees require the same level of security and unencumbered access to applications — whether internal or external — that they enjoy in the office.

	Internal Applications	External Applications
Hosted In	Data center, AWS, Azure	SaaS or Internet
Remote-access Impacts	• Requires VPN to access or to be on a corporate network • Prone to performance issues	• Not managed by the enterprise • Exposed to threat and data loss

Table 4-1: Common applications accessed by an enterprise employee

Performance matters: When users employ a VPN to access internal apps securely, and then encounter sluggish performance or a dropped connection, the temptation to turn the VPN off and bypass it is always there. Accessing the internet and SaaS applications without proper security controls in place introduces new risks. But enterprises can avoid that gamble.

Zscaler provides a seamless experience for remote users, with no need to log in and out. Instead, access is continuous, regardless of changes to network connectivity, and security is enforced instantly in the cloud.

Zscaler secure access for external applications

Zscaler Internet Access (ZIA)[18] secures user connections to external applications. ZIA is a SASE solution, and sits inline, near to every user, regardless of whether that user connects from a remote or an office location.

When a user connects, ZIA employs multiple security techniques to inspect every byte of both ingoing and outgoing traffic to ensure that the user is protected, and no critical data leaks out. ZIA delivers a full security stack as a service from the cloud, eliminating the need to build an outbound gateway, which is typically a stack of boxes that provide destination-delivered proxy, DNS, DLP, sandboxing, and firewall capabilities.

Zscaler secure access for internal applications

Zscaler Private Access (ZPA)[19] secures user connections to internal applications. ZPA, like ZIA, is a SASE solution. It is a part of the Zscaler Cloud Security Platform and functions as an inline proxy, near to every user, regardless of user location or access point.

ZPA enables remote users to access internal applications (whether in the data center or in the cloud) directly, eliminating the need for VPNs. ZPA — like ZIA — employs policy-based controls to govern user access. Applications and data are protected behind the Zscaler Cloud Security Platform, and users are allowed to access only their authorized applications.

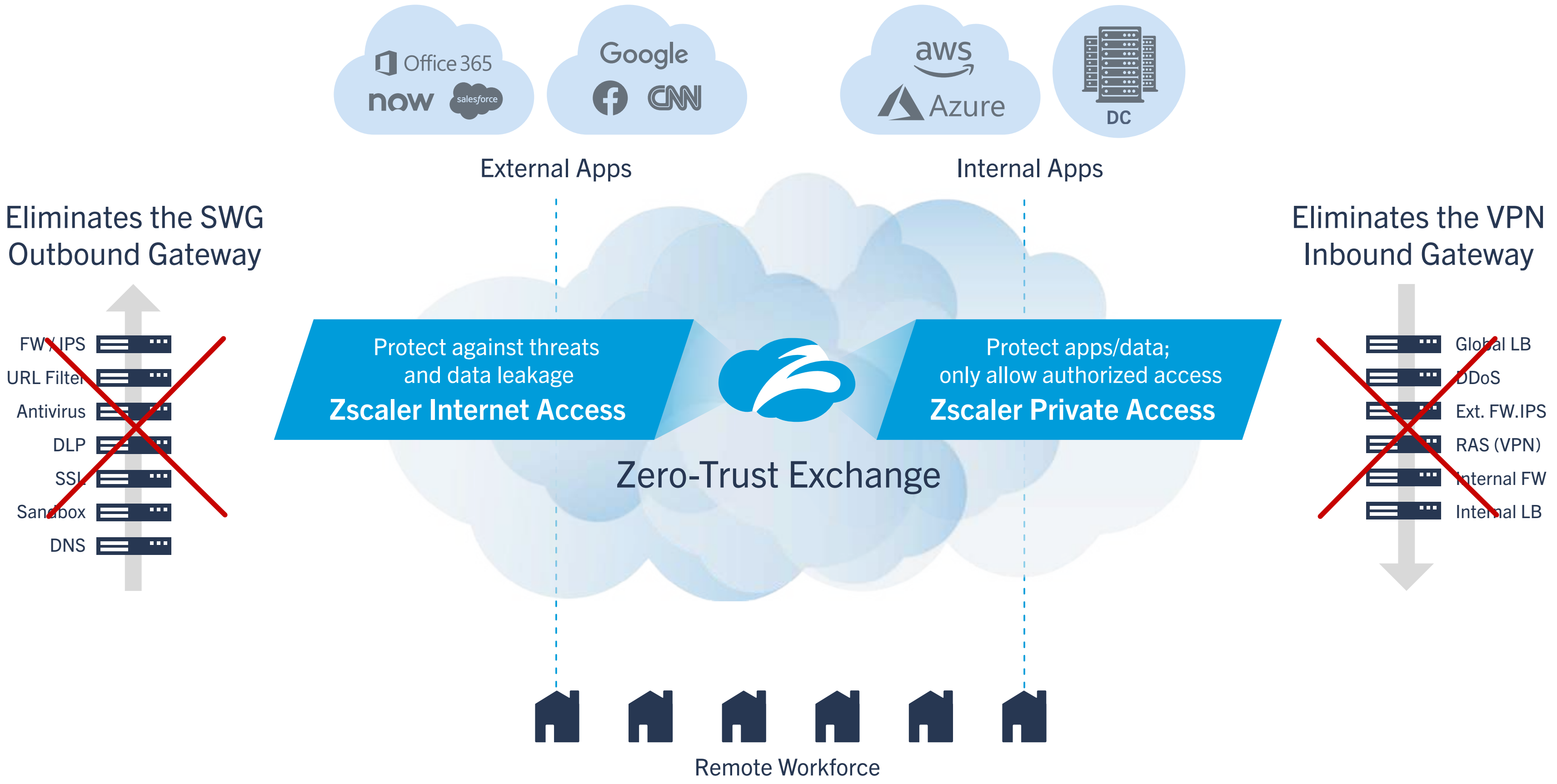


Figure 4-2: Zscaler provides secure access to all applications.

[18] https://www.zscaler.com/products/zscaler-internet-access

[19] https://www.zscaler.com/products/zscaler-private-access

2. Cloud identity access management

Traditionally, organizations have employed on-premise solutions like OpenLDAP and Microsoft Active Directory (AD) as their core identity provider. These solutions are often referred to as user directories, and they typically provide two key pieces of information: user credentials and user group affiliation(s).

As users have shifted to a cloud- and mobile-first way of work, identity-solution directory capabilities have added more cloud- and device-specific attributes. Those attributes can include device type, device location, authorized applications, and so forth. Such attributes enable the enterprise application of more granular and contextual policies. For example, User A may be authorized to access Salesforce.com from a company-authorized laptop, but not from an uncontrolled mobile device. User B may be authorized to access SAP or Workday from a home country, but not from a restricted geography for security reasons.

Employees who work remotely must rely on the cloud for access to resources they need to get work done. As enterprises migrate applications to the cloud, there is a need to enforce greater control over which employees can access those cloud resources. Defining "trust" parameters and establishing identity becomes crucial, and that requires a first line of defense: a single aggregation point for verifying identity for all applications. Security assertion markup language (SAML) has emerged as the standard for federated identity management across multiple systems. By defining a *lingua franca* for standardizing mechanisms for communication of security and identity information between business partners, SAML makes federated identity a reality.

A cloud identity and access management (IAM) solution centralizes identity and authentication services, giving an IT team comprehensive control over a cloud environment and its security, and enabling that team to track which users access which applications, and when.

Authorization is typically done by policy on the gateway. But applied improperly, this approach can result in misconfigurations. The application, as well as the access gateway, must act on the same assertion from the identity provider as "the-single-source-of-truth" resource. This will ensure there are no mismatched firewall rules or orphaned rule lines in the firewall as people, organizations, and roles change over time.

IAMs do more than just verify identity. They can also deliver detailed analysis. Identity solutions providers can detect potentially malicious or harmful activity based on deviations from the norm.

Ideally, the identity system authenticates and provides entitlement and authorization for the use of resources. At a security minimum, a standard IAM solution should provide multi-factor authentication, step-up authentication, and adaptive authentication capabilities. The identity provider must become the single point for all permission management.

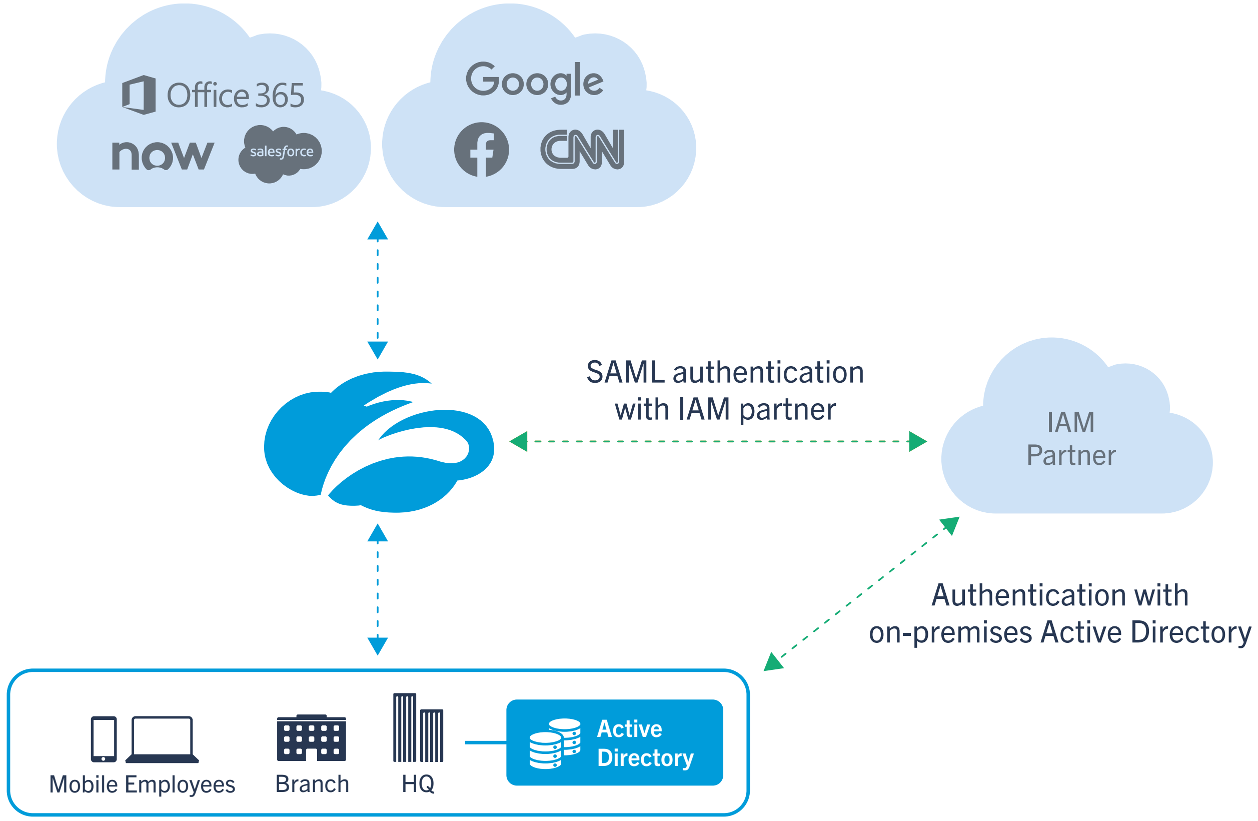

Office 365
now
salesforce
Google
CNN
SAML authentication with IAM partner
IAM Partner
Authentication with on-premises Active Directory
Mobile Employees
Branch
HQ
Active Directory

Figure 4-3: Zscaler and IAM

Zscaler supports SAML. The Zscaler Cloud Security Platform integrates with solutions from leading IAM vendors,[20] including Azure AD, Okta, and Ping. With deep IAM integration, Zscaler authenticates users and enforces contextual access via a SAML-enabled channel, without having to rely on weaker legacy approaches like using ACLs or IP addresses to enforce contextual access policies.

Zscaler also provides an easy, consistent mechanism for managing user-and-group account lifecycles in the Zscaler cloud. The Zscaler Cloud Security Platform employs the system for cross-domain identity management (SCIM) protocol. SCIM communicates user identity data between identity providers (such as companies with multiple individual users) and service providers requiring user identity information (such as enterprise SaaS apps). SCIM makes user data more secure, and simplifies the user experience by automating the user-identity lifecycle-management process.

[20] https://www.zscaler.com/partners/technology/identity-access-management

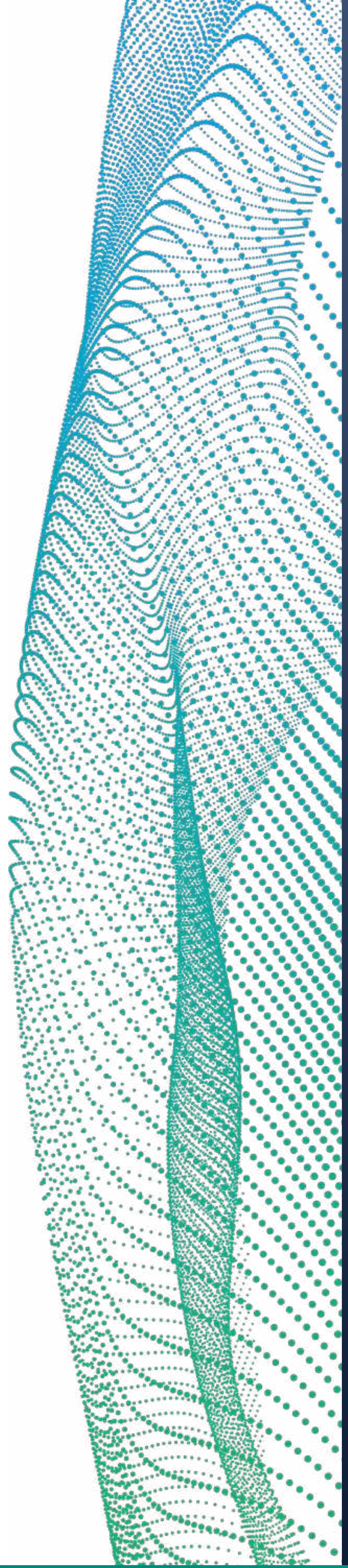
3. Fast user experience

Users should enjoy secure access to applications and services (regardless of where users are located or where apps are hosted) without compromise to user experience. It's that last part that can get tricky. More remote work means more corporate traffic destined for the internet. Remote workers still need to communicate with customers, suppliers, partners, and team members. They just can't do it in-person. During a crisis like the COVID-19 outbreak, increased corporate use of video-conferencing and chat applications such as Microsoft Teams, Zoom, and Slack causes a metaphorical explosion in internet data traffic.

Traffic growth — particularly resulting from that new reliance on collaboration tools — can impact user experience. The issue is magnified in organizations that still rely on traditional hub-and-spoke network topologies, and where traffic is backhauled from remote location to data center before reaching the cloud. Backhauling adds latency that degrades SaaS application performance. This introduces significant (and frustrating) connectivity and performance challenges for remote employees, preventing them from performing day-to-day work effectively.

ZIA ensures fast access to external applications

ZIA sits in the cloud, inline between the user and external applications or the internet. Remote employees get to their destinations fast by connecting to one of Zscaler's 150+ data centers around the world.

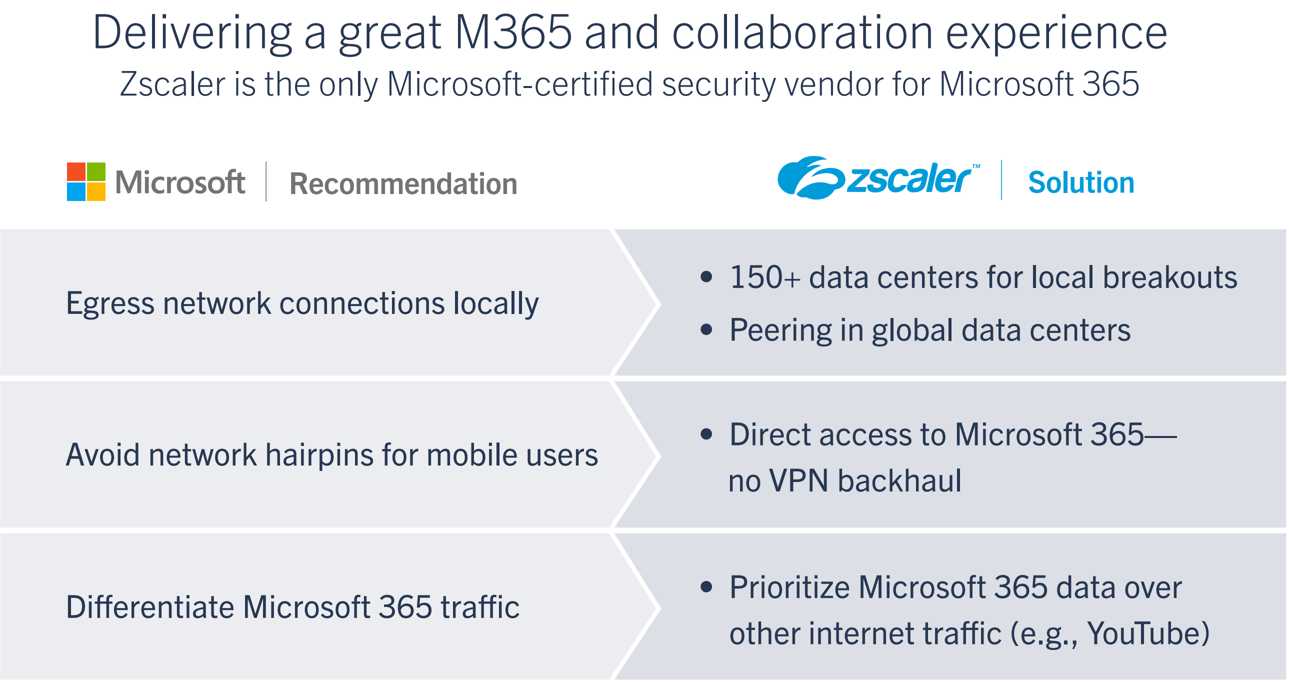


> “*Network gymnastics to route traffic to and from the enterprise data center make no sense when very little of what a user needs remains in the data center. Worse, we impact user productivity, user experience and costs by restricting access to SaaS only if a user is on the enterprise network or has used a VPN, or requiring different agents for SWG, CASB, and VPN, which creates agent bloat and user confusion. In other cases, branch-office traffic is forced through the data center for inspection when users access any cloud-based resource, increasing latency and the cost associated with dedicated MPLS circuits.*[21]
>
> Gartner Research, *The Future of Network Security is in the Cloud*”

[21] “The Future of Network Security is in the Cloud”: Gartner Research — Published: 30 August 2019 ID: G00441737: https://www.zscaler.com/gartner-secure-access-service-edge-sase

Microsoft 365 (M365) is one of the most commonly-used enterprise SaaS applications. Ensuring users have a fast and productive experience with M365 becomes even more important in work-from-anywhere scenarios.

Microsoft's guidelines for Microsoft 365 recommend network traffic egress locally. This performance-optimization requirement aligns perfectly with Zscaler's model of local internet breakouts: Zscaler is the only Microsoft certified security vendor for Microsoft 365.[22] In addition, Zscaler peers with Microsoft across its core data centers around the globe. This allows all security services to be rendered locally, within just a couple of milliseconds' hop away from the front door of the Microsoft 365 services, ensuring a superior user experience without compromising security.



Delivering a great M365 and collaboration experience

Zscaler is the only Microsoft-certified security vendor for Microsoft 365

Microsoft | Recommendation	zscaler | Solution
Egress network connections locally	• 150+ data centers for local breakouts • Peering in global data centers
Avoid network hairpins for mobile users	• Direct access to Microsoft 365—no VPN backhaul
Differentiate Microsoft 365 traffic	• Prioritize Microsoft 365 data over other internet traffic (e.g., YouTube)

Figure 4-4: Delivering a great Microsoft 365 and collaboration experience

ZPA ensures fast access to internal applications

User experience can worsen when remote users need to access their company's internal applications through VPN. In a legacy network environment, when thousands of users begin working remotely, there is a surge of new traffic that must be backhauled through that VPN connection to a centralized internet gateway, inducing latency and inhibiting user ability to collaborate.[23]

With ZPA, remote users are able to access critical internal applications fast without the performance limitations associated with backhauling traffic through VPNs. They are able to connect locally to their apps through the Zscaler Security Cloud Platform, and are protected by comprehensive security and policy enforcement, no matter their location.

[22] Microsoft Networking Partner Program (as of June 2020): https://www.zscaler.com/press/zscaler-and-microsoft-accelerate-digital-transformation-through-office-365

[23] "Cisco rations VPNs for staff as strain of 100,000+ home workers hits its network": https://www.theregister.co.uk/2020/04/02/cisco_rations_staff_vpn/

4. Rapid deployment

COVID-19 forced organizations across the globe to make an immediate shift, and made remote-access capability for the entire workforce a requirement overnight. In most organizations, poor connectivity means poor productivity. For CIOs, this has precipitated the need to look for a secure and scalable solution that can be deployed in days to transition their workforce to this new operating model. The only solution that can help CIOs meet such an aggressive timeline is a cloud-native architecture like Zscaler — one that can be deployed rapidly without the need to order hardware, wait for it to be shipped, and then install it (as is the case for legacy solutions and virtual appliances hosted in the cloud).

> *If you need more equipment, it takes time. You have to buy it, wait for it to ship and arrive, then you have to deploy it, update the hardware, and keep it updated. And that's just the VPN stack. Trying to scale VPNs and other legacy remote access technology, adding tens of thousands of users, can take months and break a corporate network. Adding three to five months is a good guesstimate for such an upgrade.*[24]
>
> Stan Lowe, Global Chief Information Security Officer, Zscaler

Zscaler can be rapidly deployed for remote work access. Here's how:

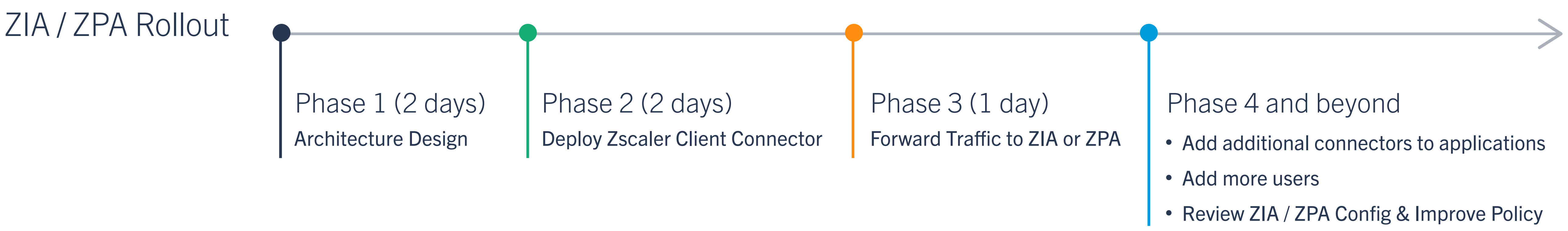
1. **Simplified access:** Sending traffic to Zscaler is simple, and requires no changes to underlying network infrastructure. All that is required is to get data packets from the egress point to Zscaler's nearby front door. There is no need for complicated internal network hardware modifications. A redundant pair of network tunnels are configured from the egress router, and Zscaler becomes the direct, default route to both the internet and to internal resources. In this way, when the majority of the workforce shifts to remote work, business continuity can be preserved instantly.

2. **Centralized policy management:** Zscaler security and policy configurations follow the end user. Policy is dynamically applied to users, applications, and data, and not to a network or a location. The Zscaler platform defines policy at a user and application level: An unauthorized user cannot connect to an individual resource. Administration is easy: Zscaler policies can be set up and configured in a matter of hours. Users will only see apps they are allowed to access, as defined by policy. Policy-based security is centralized, enabling simple connectivity and sophisticated controls, without the user ever having to consider anything.

[24] "VPNs: Not a cybersecurity slam dunk for telecommuters in the age of COVID-19": https://www.scmagazine.com/home/security-news/news-archive/coronavirus/vpns-not-a-cybersecurity-slam-dunk-for-telecommuters-in-the-age-of-covid-19/

3. **Thin client:** Traditional legacy remote-access models burden client devices with so-called “thick” agents: To connect users to internal resources over VPN requires identity- and authorization-processing controls residing on the client device. Maintaining those “fattened” client devices can be cumbersome, both for administrators and end users: Patching is an onerous, reactive process that’s difficult to manage, with IT teams required to keep up with (and then respond to) the latest threats. Worse, constant security updates interrupt user work, and often require user intervention, which can introduce errors that can lead to security risk. SASE mandates a thin client to facilitate endpoint management and accelerate rapid rollouts. The Zscaler Client Connector is a lightweight agent that — like consumer-model analogs — is easy to download, and (instantly) deployable to hundreds of thousands of users. Interoperability is simple: The thin-client Zscaler Client Connector uses SAML and authorizes identity via Zscaler’s integration with one of any number of partner identity provider (IDP) solutions.

4. **Cloud-Scaling:** Zscaler is a 100-percent cloud-native service and not a solution that has been migrated from hardware to a cloud-hosting provider. Being cloud-native makes Zscaler faster and easier to deploy than a hardware alternative: There’s no need to order, install, configure, or manage appliances. (See Figure 4-5.) The Zscaler Cloud Security Platform is a true multitenant architecture, with each enterprise customer uniquely and privately deployed within its own tenant space. As a customer’s traffic scales, capacity is added instantly, no appliances to be sized, ordered, or shipped. This on-demand scalability is especially critical during a pandemic or crisis situation where global supply chains may face significant shortages and delays,[25] impacting equipment delivery to hardware vendors.


ZIA / ZPA Rollout

Phase 1 (2 days)
Architecture Design

Phase 2 (2 days)
Deploy Zscaler Client Connector

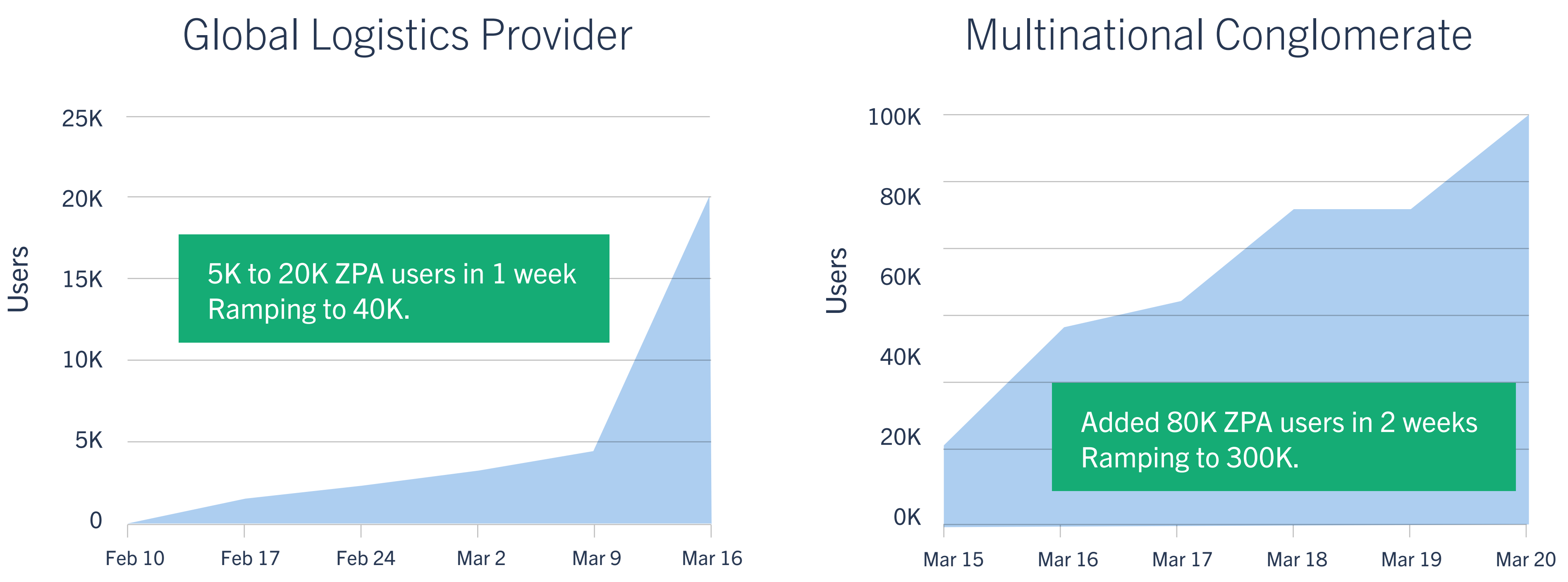
Phase 3 (1 day)
Forward Traffic to ZIA or ZPA

Phase 4 and beyond
- Add additional connectors to applications
- Add more users
- Review ZIA / ZPA Config & Improve Policy

Figure 4-5. Zscaler can be rolled out in just days.

[25] *Wall Street Journal* — “Employers Face Shortages of Tech Gear as Coronavirus Forces Shipment Delays”: https://www.wsj.com/articles/cios-face-shortages-of-tech-gear-as-coronavirus-forces-shipment-delays-11586338202

Figure 4-6 highlights two recent customer success stories of rapid deployment to enable a remote work-from-anywhere experience necessitated by COVID-19. The first example is of a global logistics provider that ramped up from 5,000 users to 20,000 ZPA users in just one week, and they are on track to ramp up all its 40,000 users to work remotely using ZIA and ZPA. This would not have been possible deploying VPN hardware to scale-out application access. Another success story is from a multinational conglomerate that transitioned 80,000 VPN users to ZIA and ZPA in just two weeks, and is now on track to deploy ZPA for all 300,000 of its users to access their internal applications and carry on their business, while providing direct and secure internet access in parallel.



Global Logistics Provider

5K to 20K ZPA users in 1 week
Ramping to 40K.

Multinational Conglomerate

Added 80K ZPA users in 2 weeks
Ramping to 300K.

Figure 4-6. Real-world examples of enabling thousands of remote users with ZPA in days

> *At Powerco, we fast-tracked a project and deployed Zscaler Private Access and Zscaler Internet Access to our staff in a bid to scale our remote access capability and increase security while working from home. There was a staged rollout planned over a four-week period. We did this all in four days and not long after that we had the majority of Powerco staff working from home as part of the level-four lockdown. Talk about a test of the technology!*
>
> Aaron Gayton,
> Chief Information Security Officer,
> Powerco

5. Visibility and troubleshooting

The ability to monitor user performance becomes a different kind of challenge when all employees work remotely, many work on unmanaged devices, and all employ the internet as their new corporate network. IT needs real-time visibility into users and applications: to be able to see exactly what is going on at every point between a user's device and an application's front door in order to quickly pinpoint the source of any performance problems so corrective actions can be taken.

Figure 4-7 below illustrates a typical, large-enterprise, hub-and-spoke network architecture. Most organizations have a wide range of network troubleshooting and end-user-monitoring tools installed across this complex legacy topology.

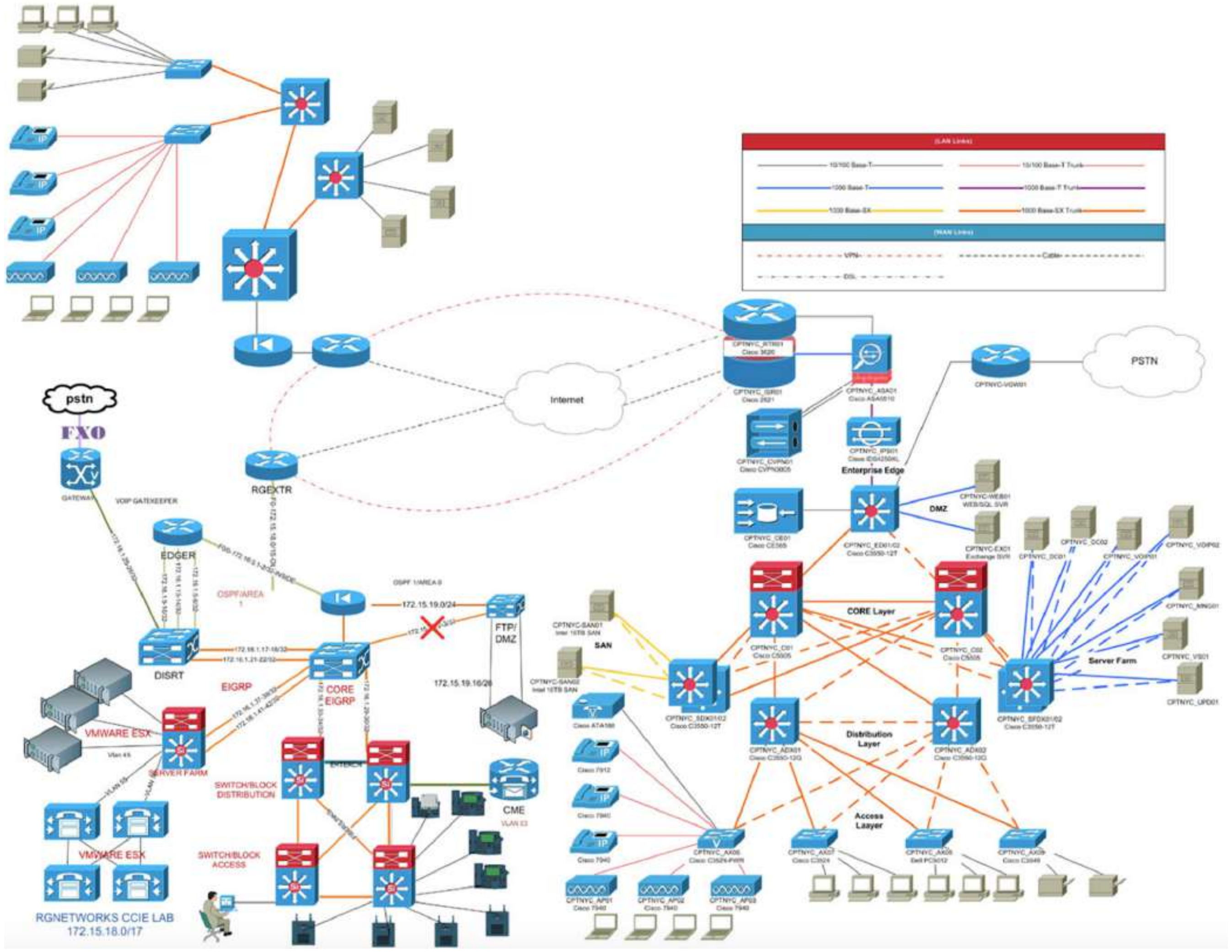
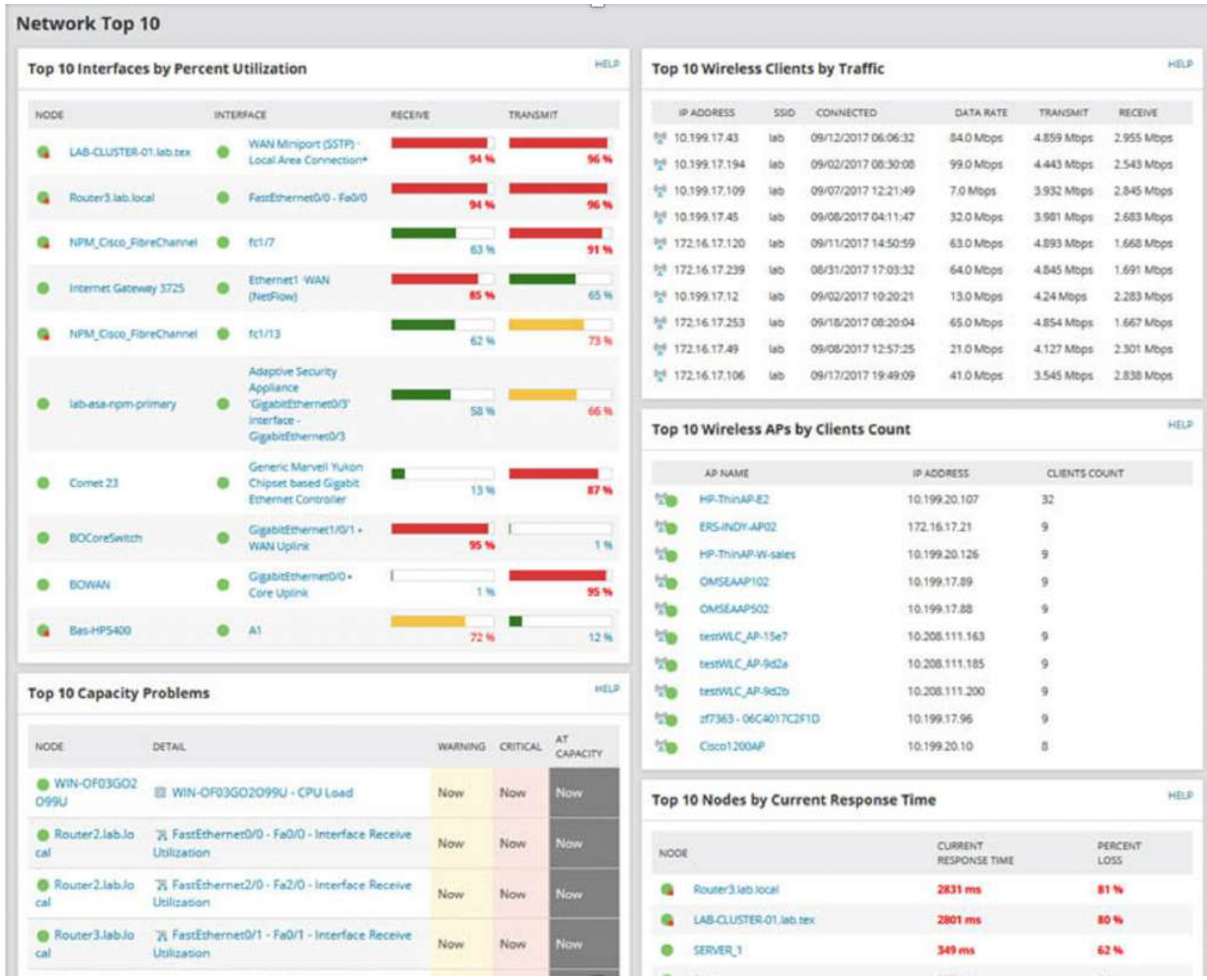


Figure 4-7. A typical enterprise corporate network with complex topology and hub-and-spoke architecture

These tools were designed to troubleshoot users and activities across the private network that connects a branch office to a data center. They provide a significant amount of low-level information to help diagnose issues. (See Figure 4-8.)



Network Top 10

Top 10 Interfaces by Percent Utilization

NODE	INTERFACE	RECEIVE	TRANSMIT
LAB-CLUSTER-01.lab.tex	WAN Miniport (SSTP) · Local Area Connection*	94 %	96 %
Router3.lab.local	FastEthernet0/0 · Fa0/0	94 %	96 %
NPM_Cisco_FibreChannel	fc1/7	63 %	91 %
Internet Gateway 3725	Ethernet1 · WAN (NetFlow)	85 %	65 %
NPM_Cisco_FibreChannel	fc1/13	62 %	73 %
lab-asa-npm-primary	Adaptive Security Appliance 'GigabitEthernet0/3' interface · GigabitEthernet0/3	58 %	66 %
Comet 23	Generic Marvell Yukon Chipset based Gigabit Ethernet Controller	13 %	87 %
BOCoreSwitch	GigabitEthernet1/0/1 · WAN Uplink	95 %	1 %
BOWAN	GigabitEthernet0/0 · Core Uplink	1 %	95 %
Bas-HP5400	A1	72 %	12 %

Top 10 Capacity Problems

NODE	DETAIL	WARNING	CRITICAL	AT CAPACITY
WIN-OF03GO2099U	WIN-OF03GO2099U - CPU Load	Now	Now	Now
Router2.lab.local	FastEthernet0/0 - Fa0/0 - Interface Receive Utilization	Now	Now	Now
Router2.lab.local	FastEthernet2/0 - Fa2/0 - Interface Receive Utilization	Now	Now	Now
Router3.lab.local	FastEthernet0/1 - Fa0/1 - Interface Receive Utilization	Now	Now	Now

Top 10 Wireless Clients by Traffic

IP ADDRESS	SSID	CONNECTED	DATA RATE	TRANSMIT	RECEIVE
10.199.17.43	lab	09/12/2017 06:06:32	84.0 Mbps	4.859 Mbps	2.955 Mbps
10.199.17.194	lab	09/02/2017 08:30:08	99.0 Mbps	4.443 Mbps	2.543 Mbps
10.199.17.109	lab	09/07/2017 12:21:49	7.0 Mbps	3.932 Mbps	2.845 Mbps
10.199.17.45	lab	09/08/2017 04:11:47	32.0 Mbps	3.981 Mbps	2.683 Mbps
172.16.17.120	lab	09/11/2017 14:50:59	63.0 Mbps	4.893 Mbps	1.668 Mbps
172.16.17.239	lab	08/31/2017 17:03:32	64.0 Mbps	4.845 Mbps	1.691 Mbps
10.199.17.12	lab	09/02/2017 10:20:21	13.0 Mbps	4.24 Mbps	2.283 Mbps
172.16.17.253	lab	09/18/2017 08:20:04	65.0 Mbps	4.854 Mbps	1.667 Mbps
172.16.17.49	lab	09/08/2017 12:57:25	21.0 Mbps	4.127 Mbps	2.301 Mbps
172.16.17.106	lab	09/17/2017 19:49:09	41.0 Mbps	3.545 Mbps	2.838 Mbps

Top 10 Wireless APs by Clients Count

AP NAME	IP ADDRESS	CLIENTS COUNT
HP-ThinAP-E2	10.199.20.107	32
ERS-INDY-AP02	172.16.17.21	9
HP-ThinAP-W-sales	10.199.20.126	9
OMSEAAP102	10.199.17.89	9
OMSEAAP502	10.199.17.88	9
testWLC_AP-15e7	10.208.111.163	9
testWLC_AP-9d2a	10.208.111.185	9
testWLC_AP-9d2b	10.208.111.200	9
zf7363 - 06C4017C2F1D	10.199.17.96	9
Cisco1200AP	10.199.20.10	8

Top 10 Nodes by Current Response Time

NODE	CURRENT RESPONSE TIME	PERCENT LOSS
Router3.lab.local	2831 ms	81 %
LAB-CLUSTER-01.lab.tex	2801 ms	80 %
SERVER_1	349 ms	62 %

Figure 4-8. Traditional network monitoring tools only provide low-level network diagnostics.

When employees work in a branch office or headquarters, they connect directly to the private corporate network, making it easy for IT to monitor and control everything they do. But legacy monitoring tools can see only what's happening on the private corporate network. When employees work from home or from a remote location, their traffic traverses the open internet and not the private network, concealing their activity from oversight.

Increased use of SaaS applications further complicates monitoring in a legacy environment. Many SaaS apps employ their own monitoring tools, saddling an organization with yet more tools to monitor (from one, or often many vendors), something that can distract IT teams with "alert fatigue". When it comes to monitoring infrastructure and employee digital experience, the multiple-tool approach is a long way from the management vision of single-pane-of-glass visibility.

Legacy monitoring tools are complex, inflexible, fallible, and not particularly interoperable. They reinforce workflows that are reactive, not proactive: More often than not, legacy-network IT administrators must comb through monitoring data (and history reports) to determine the cause of a problem only after the problem has been reported. These limitations make it difficult (if not impossible) for IT teams to optimize end-user connectivity performance.

Connectivity performance depends on where a user is located, and where cloud services are hosted. (See Figure 4-9.) In a legacy network environment with indirect routing, proximity to service can make a big difference to user experience. For example, a Singapore-based user connecting to a company's Microsoft 365 tenant hosted in the eastern United States would expect to experience an unacceptable TCP-connection latency, perhaps as much as 250 milliseconds. A New York City-based user in the same company would have an entirely different experience connecting to the same (nearby) tenant. Ideally, IT must benchmark unique user experiences: Networks and applications can change frequently in a short period of time, impacting user experience and performance consistency.

Often, performance issues may be related to an end user's device. Applications may appear to respond slower when a user's laptop battery is low, or if Wi-Fi signal strength is weak. And sometimes an app (say, Skype) may connect easily on one device (say, a MacBook) but not another (say, an Android phone).

End-user performance metrics should be gauged in three key areas: endpoint, network path, and application. Legacy point tools such as application-monitoring tools or network path-monitoring solutions can diagnose and even pinpoint the exact location and source of an issue that may arise, but that still leaves IT teams with significant blind spots.

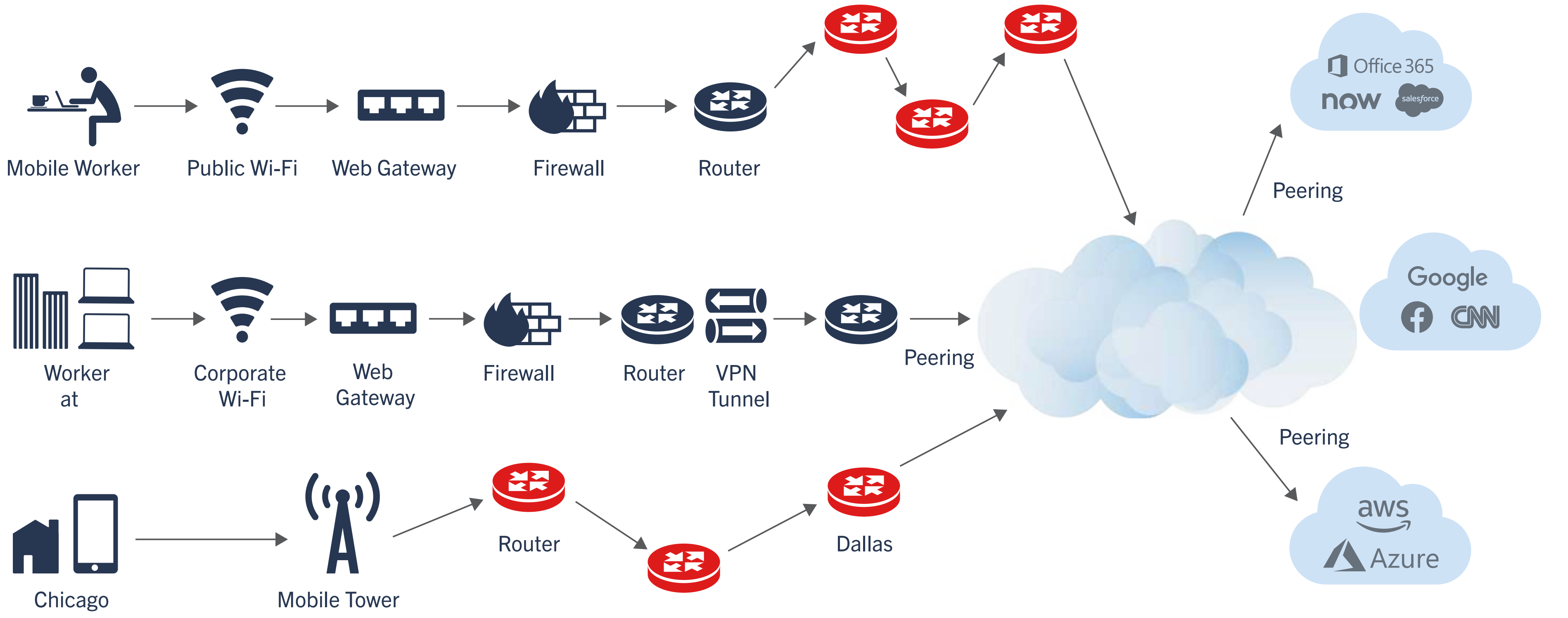


Figure 4-9. User experience challenges in the cloud and mobile world

> *Existing device-centric network monitoring does not scale to provide the needed visibility for cloud and digital-business-era applications.*
>
> Gartner Research,
> *Rethinking Nework Monitoring for the Cloud Era,*
> Gregg Siegried and Simon Richard;
> 06 December 2018

Let's look at the example of key executives from Company ABC working remotely. The CEO's Microsoft 365 performance is slow. The first person that the CEO is going to call is the CIO, or possibly the IT team. How should IT triage that problem? What could be contributing to the slow M365 performance? Is it the device? A DNS-resolution issue? Could it be a local Wi-Fi issue? Something related to the last-mile delivery and/or service provider?

In this scenario, one (or many) of the ten internet hops data travels to get to M365 could be experiencing an issue somewhere and contributing to performance lag. The problem could potentially be the application itself. Without the right tools to diagnose the problem, how can the IT team troubleshoot, then remediate to ensure that the CEO is back on track to having a productive remote work experience? And how can that IT team proactively monitor to prevent similar future escalations?

Zscaler Digital Exchange™ provides real time end-to-end user experience

CIOs must achieve two seemingly-at-odds objectives: Enable secure remote access and preserve user experience. To address these critical requirements, Zscaler offers Zscaler Digital Experience (ZDX™).[26] ZDX aggregates and analyzes performance metrics to measure the end-user experience for every user within an organization on every device — without the need to deploy multiple point products. ZDX delivers on the "single-pane-of-glass" ideal, giving the IT team comprehensive, unified visibility to identify performance issues, whether those issues are due to the end-user device, network path, or application.

ZDX leverages the Zscaler Cloud Security Platform architecture that sits inline between user and application. ZDX — in concert with the lightweight Zscaler Client Connector agent — collects telemetry information dynamically to measure end-to-end performance and user experience. With such detailed monitoring capabilities, ZDX provides rich insight into the digital experience of employees, meaning IT can quickly identify potential problems, and optimize performance.

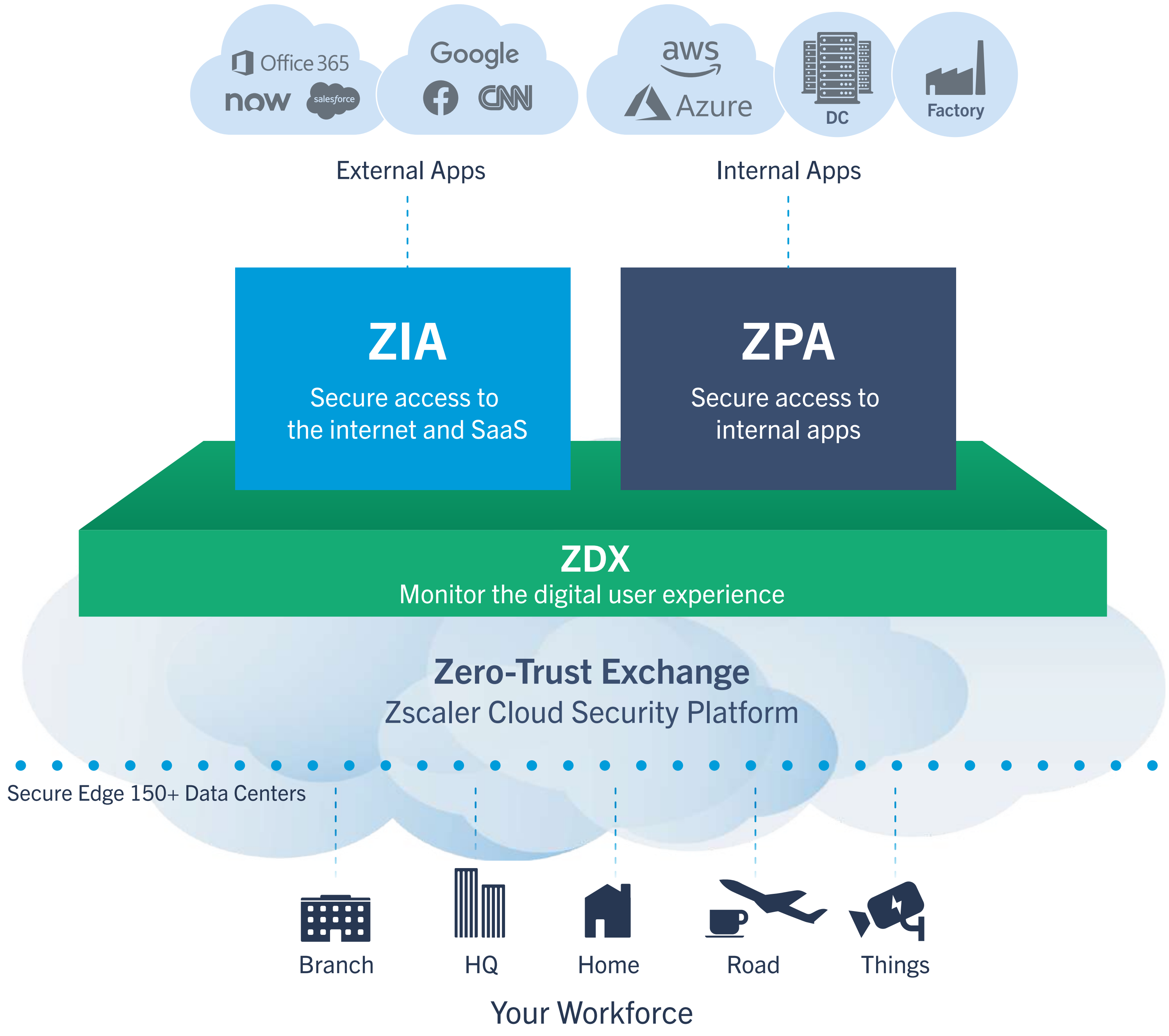
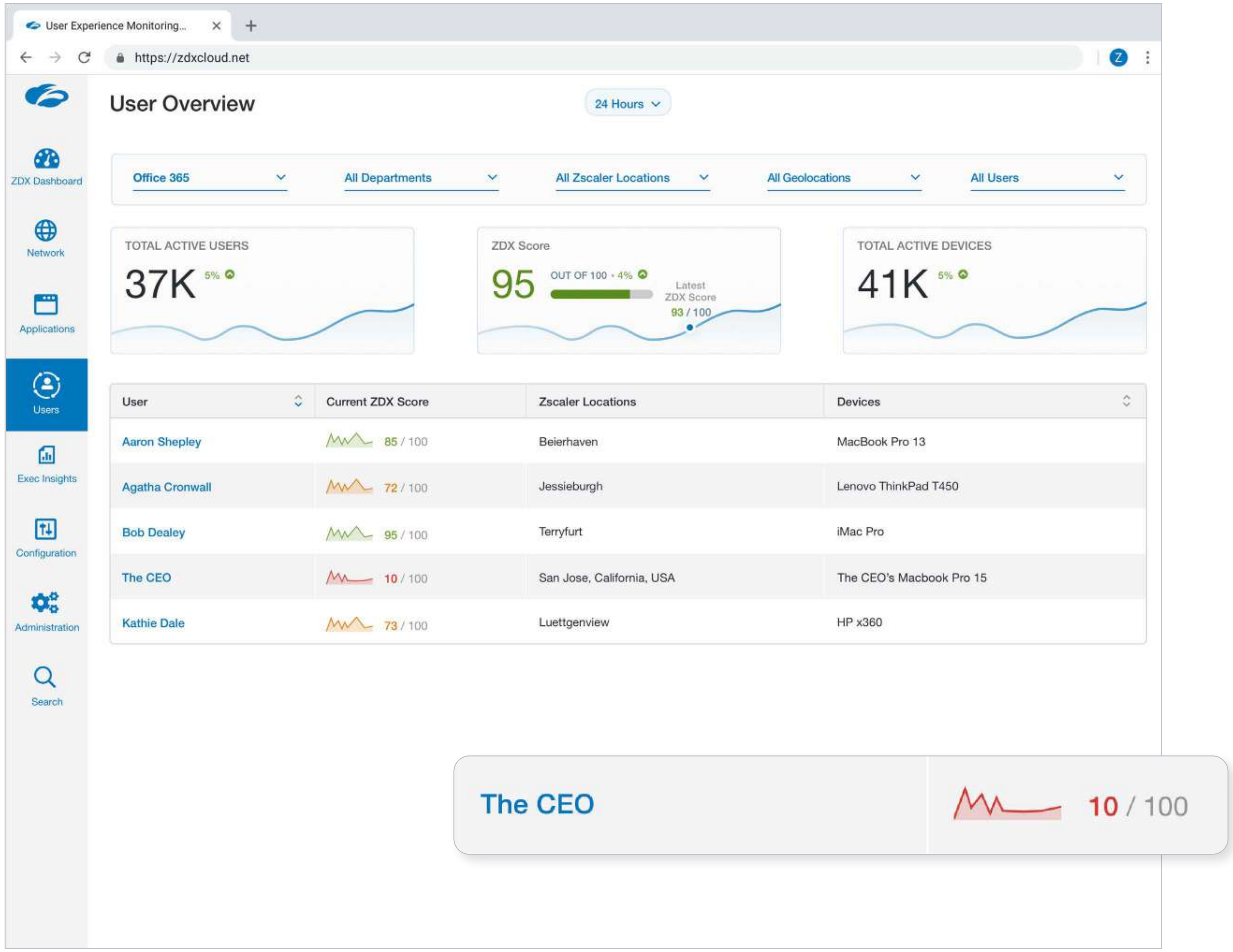

Office 365
now
salesforce
Google
CNN
aws
Azure
DC
Factory
External Apps
Internal Apps
ZIA
Secure access to the internet and SaaS
ZPA
Secure access to internal apps
ZDX
Monitor the digital user experience
Zero-Trust Exchange
Zscaler Cloud Security Platform
Secure Edge 150+ Data Centers
Branch
HQ
Home
Road
Things
Your Workforce

Figure 4-10. ZDX provides a full picture of a user's experience all the way through to the device level.

[26] Video — Zenith Live 2019: https://zscaler.wistia.com/medias/rolnlbftn5

Let's return to the example of Company ABC's CEO who experienced poor Microsoft 365 performance working remotely. ZDX shows that the CEO is accessing Microsoft 365 in San Jose, California, on a MacBook Pro, and has a user experience score of ten out of 100, which is poor. (See Figure 4-11.)



User	Current ZDX Score	Zscaler Locations	Devices
Aaron Shepley	85 / 100	Beierhaven	MacBook Pro 13
Agatha Cronwall	72 / 100	Jessieburgh	Lenovo ThinkPad T450
Bob Dealey	95 / 100	Terryfurt	iMac Pro
The CEO	10 / 100	San Jose, California, USA	The CEO's Macbook Pro 15
Kathie Dale	73 / 100	Luettgenview	HP x360

Figure 4-11. Microsoft 365 performance for Company ABC

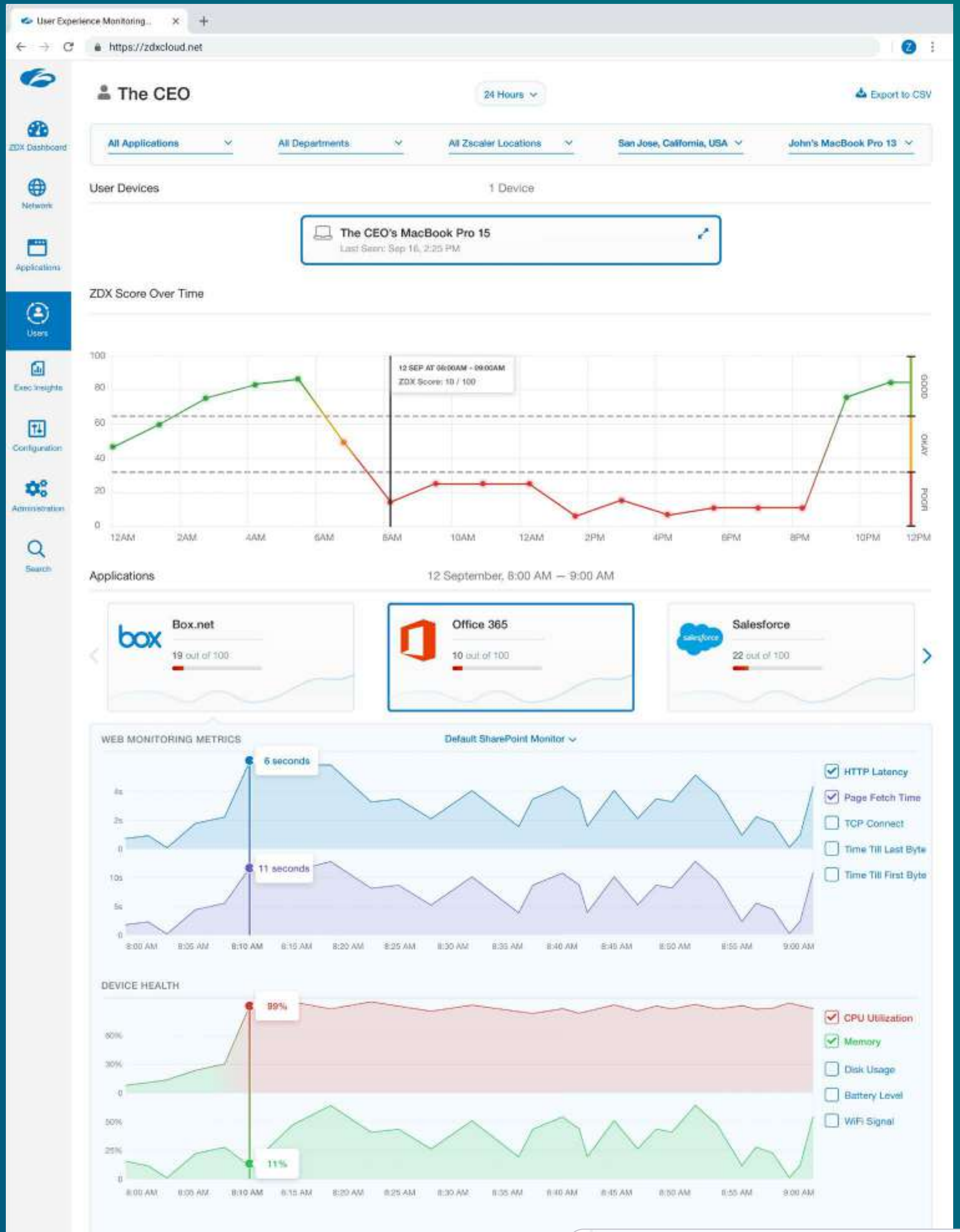


Figure 4-12. A user-level view of application performance for Company ABC

ZDX provides a full picture of the CEO's Microsoft 365 user experience over the past 24 hours, and enables IT administrators to drill down further on several metrics. (See Figure 4-12.)

From this view, IT can determine that the CEO is not only having a bad day with Microsoft 365, but is also suffering a degraded experience with Company ABC's other sanctioned SaaS applications Box and Salesforce.

In this example, clicking on Microsoft 365 brings up some of the default, built-in metrics. SharePoint page load time shows a latency, and page fetch times are slow. Digging deeper highlights the CEO's device health and vital statistics, including CPU utilization, memory, Wi-Fi connection status, battery levels, and more. The CEO's CPU utilization appears to have spiked around 8:10AM, and remained high.

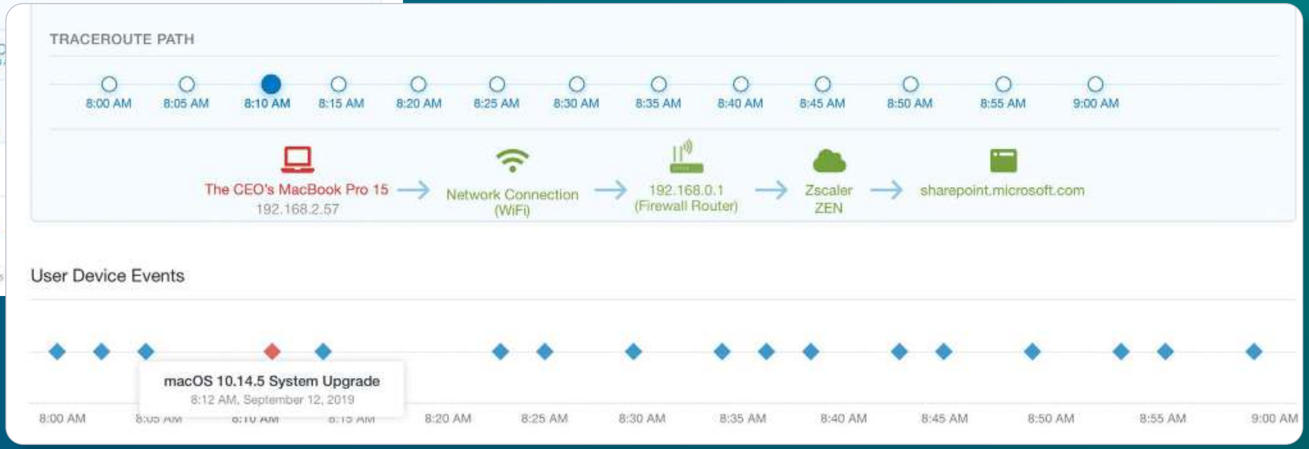


Figure 4-13. ZDX enables granular drilldowns from the user endpoint to the application front door.

What happened here? A subsequent view highlights that the CEO's MacBook got an operating system upgrade at 8:12AM. Since then, spiked CPU utilization has consistently impacted application performance. (See Figure 4-13.) ZDX provides a top-down view of organizational health, and lets IT quickly drill down to the individual user-level to isolate specific cause. With the granular visibility provided by ZDX, IT teams can now isolate user experience issues and leverage the relevant troubleshooting tools to resolve them.

Zscaler customers benefit from the collective experience of millions of end users around the globe, and from the collective expertise of the Zscaler security team. Zscaler is the largest security cloud in the world, and processes more than 120 billion transactions a day. By applying advanced machine-learning techniques to this massive traffic volume, ZDX identifies trends and patterns that can help IT teams take proactive steps to mitigate potential user experience issues before they happen.

ZDX set up is simple, and can be done in a matter of hours, with no need to deploy additional hardware or software. (Contrast that with an alternative monitoring-tool approach requiring IT to deploy huge storage clusters to store a lot of raw alerts of dubious value.)

6. Cyber threat protection

Threat actors exploit crises to advance their cause. The coronavirus outbreak was no exception, leading to COVID-19-themed cyberattacks designed to take advantage of the heightened sensitivity surrounding the pandemic. Zscaler's ThreatLabZ team reported a 30,000-percent increase in COVID-19-themed threats between January and March, 2020. That included 380,000 attacks in just one month. (See Figure 4-15.)

During the COVID-19 pandemic, sophisticated threat actors played upon target fears of the virus, employing scareware tactics to spread malware[27] like Emotet, LokiBot, RemcosRAT, TrickBot,[28] and FormBook. Some scams aim to trick unsuspecting users into downloading ransomware.[29] Others deliver phishing messages with "corona" or "covid" keywords in an attempt to solicit user credentials. COVID-19-related mobile apps hide malicious activity, and thousands of newly-registered-domain (NRDs) websites purport to sell safety masks or (fake) coronavirus test-kits, spreading misinformation along the way.[30] (See Figure 4-16.) There are even campaigns capitalizing on the increased demand for VPNs by targeting remote users, tricking them into downloading and installing malware masquerading as a legitimate VPN client.

Zscaler ThreatLabZ Insights

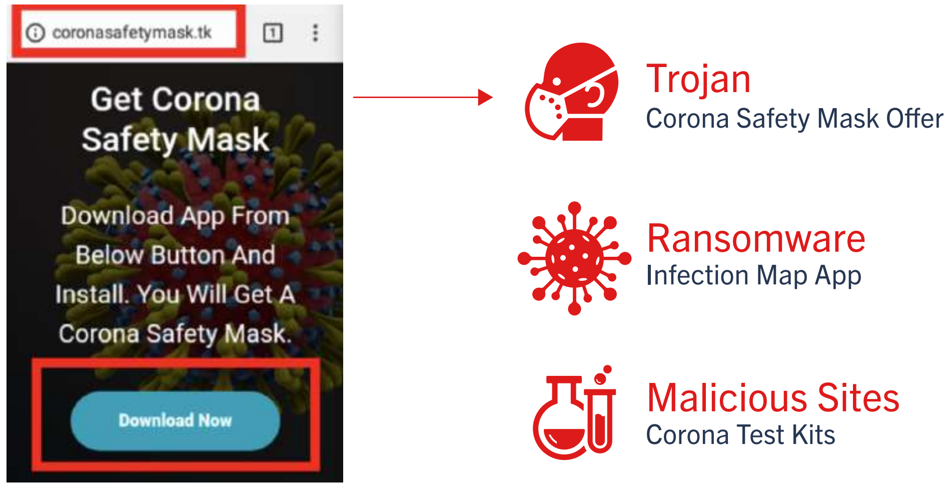
Threats seen in Zscaler Cloud, January vs. March 2020

85% increase	25% increase	17% increase
in phishing attacks targeting remote enterprise users	in malicious websites and malware files blocked	in threats targeting enterprise users

30,000% increase

in COVID-19-themed phishing, websites, and malware targeting remote users

Figure 4-14. COVID-19 security exploits increased 30,000 percent in March 2020.



coronasafetymask.tk

Get Corona Safety Mask

Download App From Below Button And Install. You Will Get A Corona Safety Mask.

Download Now

Figure 4-15. Rapid rise of COVID-19 ransomware, phishing and malware

[27] https://www.zscaler.com/blogs/research/emergence-coronavirus-and-olympics-scams

[28] https://www.zscaler.com/blogs/research/trickbot-emerges-few-new-tricks

[29] "CovidLock: Android Ransomware Walkthrough and Unlocking Routine": https://www.zscaler.com/blogs/research/covidlock-android-ransomware-walkthrough-and-unlocking-routine

[30] "The Emergence of Coronavirus and Olympics Scams": https://www.zscaler.com/blogs/research/emergence-coronavirus-and-olympics-scams

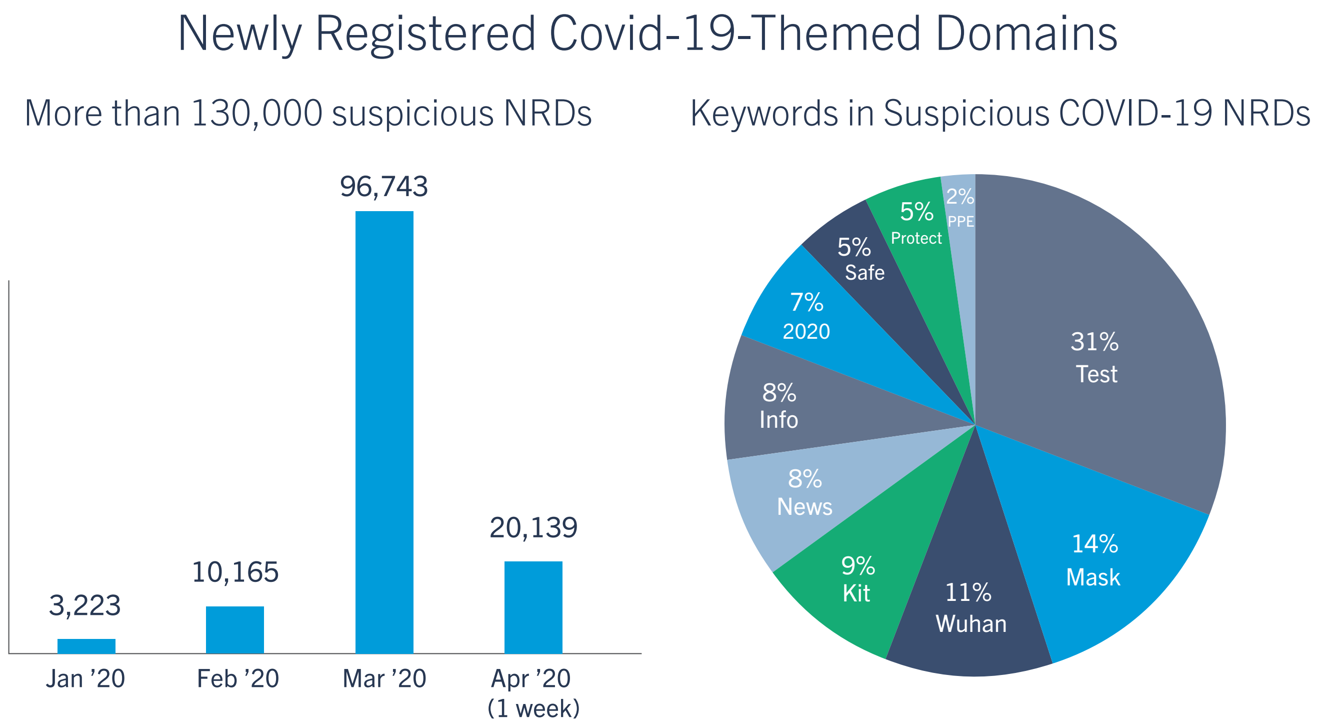


Figure 4-16: Increase in the number of Coronavirus/COVID-19 NRDs seen since the pandemic outbreak

Are your employees protected from cyber threats when they work remotely? (Probably not.)

When employees work in a corporate office on a legacy network, appliance-based security solutions deployed in data centers protect them from some cyber threats. To counter those threats, IT organizations bolt sandboxing solutions onto existing security stacks. Those sandboxing solutions provide a mechanism for isolating questionable data so it can be assessed for threat risk. This approach helps, at least marginally so, but adds complexity: The more point products added to a physical security stack, the greater the challenge to achieve a fully-integrated threat platform.

When employees work from home or from a remote location, they are not necessarily on the corporate network, and their activity may be conducted outside IT security control. Appliance-based sandboxing solutions installed to protect on-network users are now useless for securing them when they are remote and off-network. Without such security controls, remote employees are vulnerable to zero-day attacks or advanced persistent threats (APTs). That risk extends beyond just the individual user: When a compromised laptop rejoins the corporate network, malware can quickly propagate "east-west"[31] within the corporate topology, endangering systems throughout the network.

Hardware-based sandboxing acts as a "detective" control, and at its best can highlight malicious files that were downloaded but have not yet succeeded in compromising end-user machines. Hardware-based sandboxing solutions aim to identify malware based on known indicators. But modern attacks (including COVID-19-related scams) have become multi-part and sophisticated, sometimes *combining* APTs and zero-day threats. Often, threat actors hide malware-detonation payloads within encrypted code: Appliance-based sandboxes can limit throughput, and lack the ability to fully inspect SSL-encrypted traffic. If a security solution cannot inspect all incoming and outgoing data, how "complete" a solution is it?

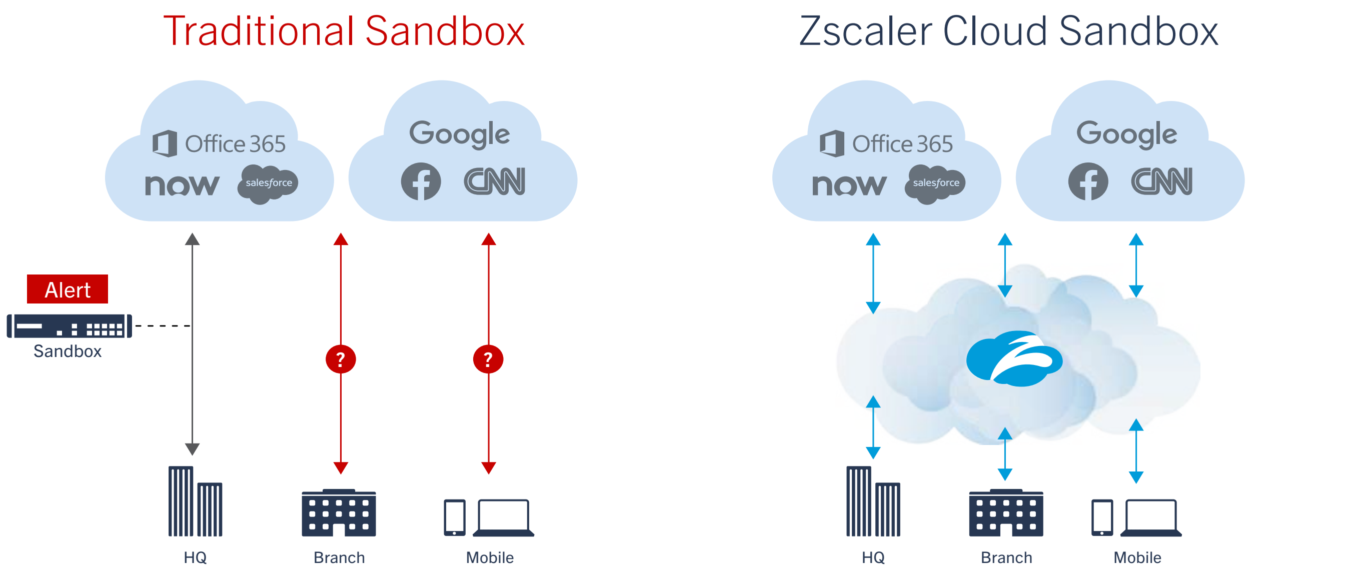
[31] https://www.forbes.com/sites/forbestechcouncil/2019/02/28/why-compass-thinking-bias-can-hinder-your-cloud-migration/

Leveraging a cloud-based architecture for full threat protection

The Zscaler Cloud Security Platform includes advanced sandboxing capabilities as part of a comprehensive and multi-faceted cloud security solution. (That's different from an appliance-based security-stack environment, where sandboxing is a separate, tacked-on point product for IT to manage.)

Zscaler leverages big data analysis, static analysis, and behavioral analysis to provide a fuller context for threat protection. Zscaler enhances traditional behavioral analysis techniques: Zscaler combines the benefits of behavioral analysis with the reach of a worldwide, SaaS-based service to collect binary files from global clouds, analyze them centrally, and ensure that all customers benefit when even a single malicious file is identified.

In traditional behavioral analysis (such as that offered with hardware-based sandboxing), a data sample is analyzed in isolation. In that scenario, behavioral analysis would uncover the fact that a given sample requested a specific URL when executed, but the behavioral analysis engine would have no way of knowing if the request was benign or malicious. Zscaler can further interrogate information by comparing it to all historical transactions: The Zscaler behavioral analysis engine is smarter than any one piece of hardware can be, because it benefits from the latest intelligence derived from mining *all* Zscaler Cloud Threat Intelligence.



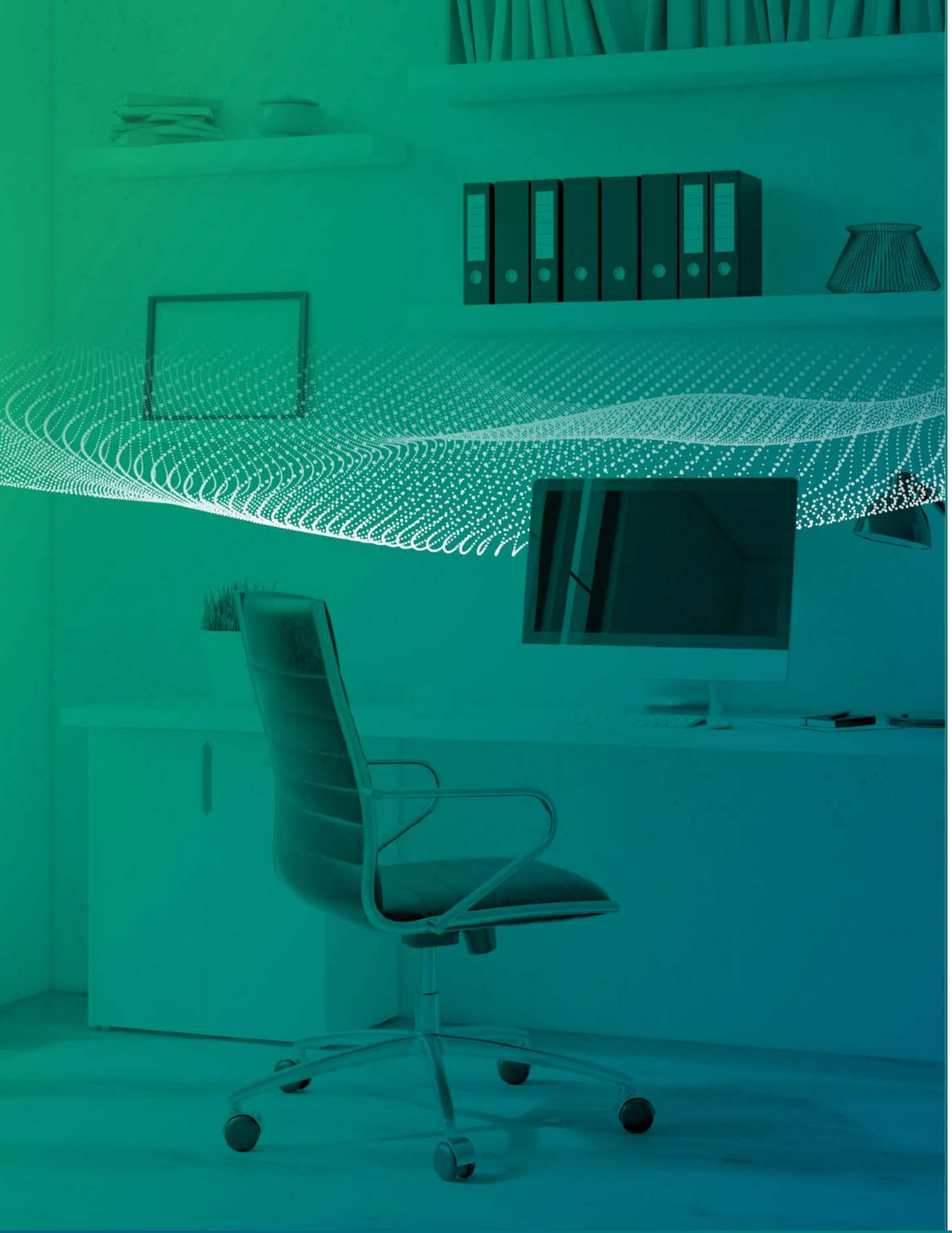
Limited Capacity with no SSL Inspection

- Users off network go unprotected
- Sandbox allows files to pass and infect
- Threat data is often localized and not shared

Unlimited Capacity with full SSL Inspection

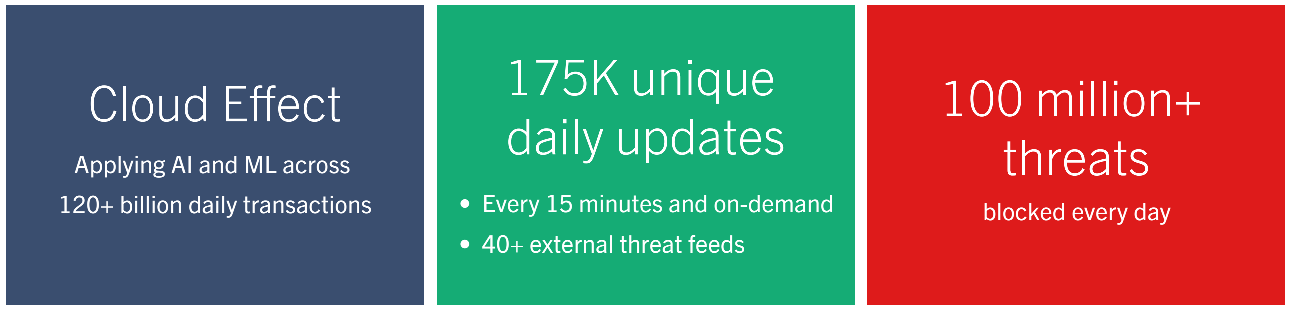
- Easily scale across all users/locations
- Inline architecture holds file until clean
- Cloud effect shares blocks with all customers

Figure 4-17. Traditional sandboxes are insufficient for protecting workers outside the corporate perimeter.



Zscaler's advanced security solution provides full SSL inspection and inline blocking. It provides continuous coverage for any user, anywhere, and Zscaler's advanced security solution scans every packet, every byte, every time — for both inbound and outbound traffic. It scans all communications to block botnets calling home, cookie-stealing, and anonymizers, and it provides full vulnerability-shielding. (AV-TEST GMBH provides independent third-party validation of Zscaler security protection.)[32]

Zscaler generates dynamic risk scores based on content and behavior, and establishes score thresholds to block zero-day threats. Zscaler has numerous industry partnerships for access to real-time intelligence feeds of known compromises, ensuring protection is updated dynamically. Every transaction is logged in detail for forensic analysis. Additionally, the Zscaler ThreatLabZ team continuously monitors online activity across more than 120 billion daily transactions to ensure that Zscaler customers are protected from the broad spectrum of known and unknown threats. (See Figure 4-18.)



Cloud Effect

Applying AI and ML across 120+ billion daily transactions

175K unique daily updates

- Every 15 minutes and on-demand
- 40+ external threat feeds

100 million+ threats

blocked every day

Figure 4-18. Zscaler protects remote users from cyber threats.

[32] https://www.zscaler.com/resources/avtest

7. Data protection

Corporate data volume can grow exponentially over time, and much of this data is highly sensitive and subject to regulatory oversight. Such sensitive data can include personal information related to customers and employees, financial information, and intellectual property that businesses must keep safe. In the past, private information was preserved in hard-copy form, perhaps secured in a locked file cabinet. These days, this data moves freely across multiple channels, and can be found on an endpoint, in storage, or in transit. The need to protect this data is an imperative responsibility for an organization entrusted to keep it safe.

To protect valuable data, some organizations implement comprehensive data-loss prevention (DLP) solutions. A DLP solution comprises technologies and processes to monitor and inspect data on the corporate network to ensure sensitive data is not lost or stolen. DLP solutions address three major organizational objectives: regulatory compliance, protection against data loss, and visibility.

On-prem DLP solutions cannot protect remote workers

In response to the COVID-19 global pandemic, organizations had to transition to a fully-remote workforce. Fast. So fast that security protocols couldn't keep up: Few if any employees received sufficient training or preparation on proper security practices when working remotely and leveraging the cloud and the internet. Remote users can access apps and work files from just about anywhere at any time. Bypassing productivity-lowering VPN connectivity lets remote users access vital company data directly (and unsecurely), and store files outside of the data center, where they are no longer protected by corporate DLP tools. IT can't monitor those activities, and this leaves the organization in the dark when it comes to that data, increasing the likelihood of data leakage and breaches with the remote employees' online actions.[33]

It is imperative that organizations implement appropriate security and DLP measures to secure a 100-percent remote workforce, and overcome the shortcomings of traditional DLP tools that fail to protect them. Hardware cannot scale fast enough nor does it offer sufficient security to address the challenge: Reconfiguring a traditional hardware stack for the cloud is inefficient and does not provide the protections and services of a cloud-native solution.

[33] "Data Breach Report: RigUp Exposes More Than 70,000 Private Files", *Security Magazine*: https://www.securitymagazine.com/articles/92098-data-breach-report-rigup-exposes-more-than-70000-private-files

Traditional DLP solutions fail in a mobile- and cloud-first world:

1. **Cannot offer the same level of protection for all users:** With traditional DLP solutions anchored in the data center, level of visibility and protection depends on where users are located. Remote users can go off-network and bypass inspection, connecting directly to cloud applications and circumventing VPN and data-protection measures. To provide comprehensive data protection, a DLP solution should provide identical protection to all users, regardless of their location, whether they connect from the office, an airport lounge, or home.

2. **Unable to inspect encrypted traffic:** With more than 90 percent of today's traffic using encryption,[34] it is incumbent upon organizations to inspect encrypted data. But traditional security solutions don't natively inspect encrypted traffic. And adding SSL appliances to improve security posture is prohibitively expensive and increases IT complexity. The only way to get visibility into encrypted traffic is to use a DLP solution that natively inspects SSL-encrypted data.

3. **Cannot scale for inline inspection:** The tremendous growth of internet traffic requires constant updates to traditional, appliance-based DLP solutions, as their finite inspection capacity is quickly drained when data volume climbs. In an attempt to overcome the complexity and cost of this endeavor, many organizations resist deploying a DLP solution inline from the start. Unfortunately, this limits organizations to damage control only *after* data has been compromised.

Zscaler keeps valuable data safe when employees work remotely

Zscaler has developed a comprehensive data-protection solution that keeps valuable data and assets safe, regardless of where employees work from — the corporate office, home office, or any other remote location. ZIA includes Cloud Sandbox, Next-Generation Firewall, and Cloud Application Visibility and Control capabilities. Zscaler keeps data safe by further augmenting that offering with Cloud DLP, Cloud Access Service Broker (CASB), Cloud Security Posture Management (CSPM), and Remote Browser Isolation capabilities, all in a single platform.

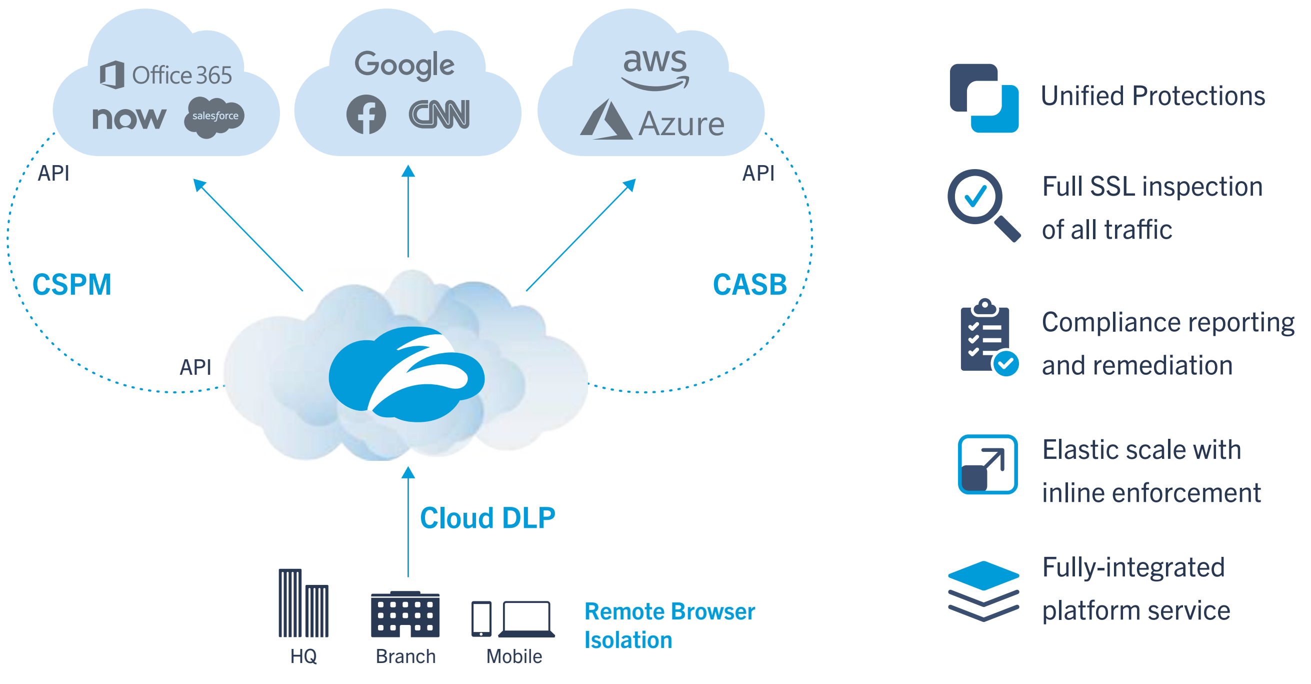

Office 365
now
salesforce
Google
CNN
aws
Azure
API
API
CSPM
CASB
API
Cloud DLP
HQ
Branch
Mobile
Remote Browser Isolation
Unified Protections
Full SSL inspection of all traffic
Compliance reporting and remediation
Elastic scale with inline enforcement
Fully-integrated platform service

Figure 4-19. Zscaler Data Protection

[34] https://transparencyreport.google.com/https/overview?hl=en&time_os_region=chrome-usage:1;series:time;groupby:os&lu=load_os_region&load_os_region=chrome-usage:1;series:page-load;groupby:os

Zscaler Data Protection comprises four service components:

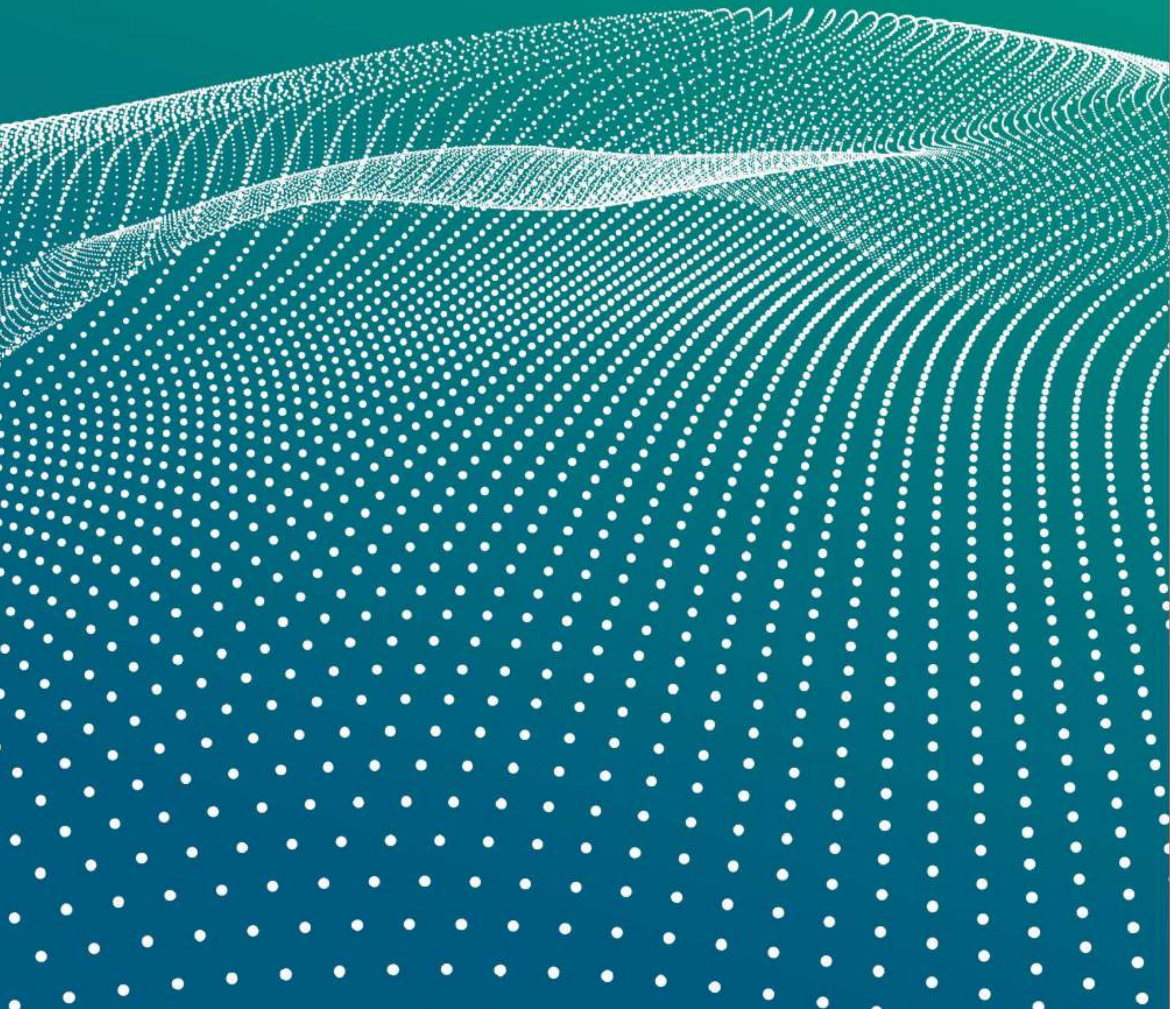
1. **Cloud DLP:** Zscaler provides complete data protection with full context and content inspection for all data (in motion and at rest), as well as advanced features, including Exact Data Match (EDM), machine-learning, and granular policies for optimal protection. Zscaler Cloud DLP protects an organization's mission-critical data and assets:
   - Cloud DLP policy follows users whether they work on- or off-network, and provides the same high level of protection to all users at all times.
   - Cloud DLP inspects all encrypted traffic. Unlike hardware-based alternatives, Zscaler Cloud DLP has no capacity constraints for enabling SSL interception at scale. The platform is a proxy by design, performing SSL inspection on all traffic without the inspection limitations of appliances.

2. **Cloud Access Service Broker (CASB):** Zscaler's cloud-native policy engine offers both inline and out-of-band CASB capabilities. All user traffic flows through the Zscaler Cloud Security Platform's in-line CASB before any cloud application is accessed. For traffic that cannot pass through a cloud policy engine or cannot be inspected inline, the platform's out-of-band CASB function looks inside the SaaS applications themselves (through API integrations) to identify data exposure (whether accidental or intentional) and compliance violations that would otherwise go unnoticed.

3. **Cloud Security Posture Management (CSPM):** This offering identifies and remediates cloud misconfigurations and compliance violations in SaaS, PaaS, and IaaS.

4. **Remote Browser Isolation:** Zscaler's Remote Browser Isolation functionality protects sensitive documents by blocking downloads on the endpoints when users access corporate-sanctioned cloud applications.

Key Takeaways



- There are seven key requirements to ensure a productive and secure remote workforce:
    1. Secure access to all applications
    2. Cloud identity access management
    3. Fast user experience
    4. Rapid deployment
    5. Visibility and troubleshooting
    6. Cyber threat protection
    7. Data protection

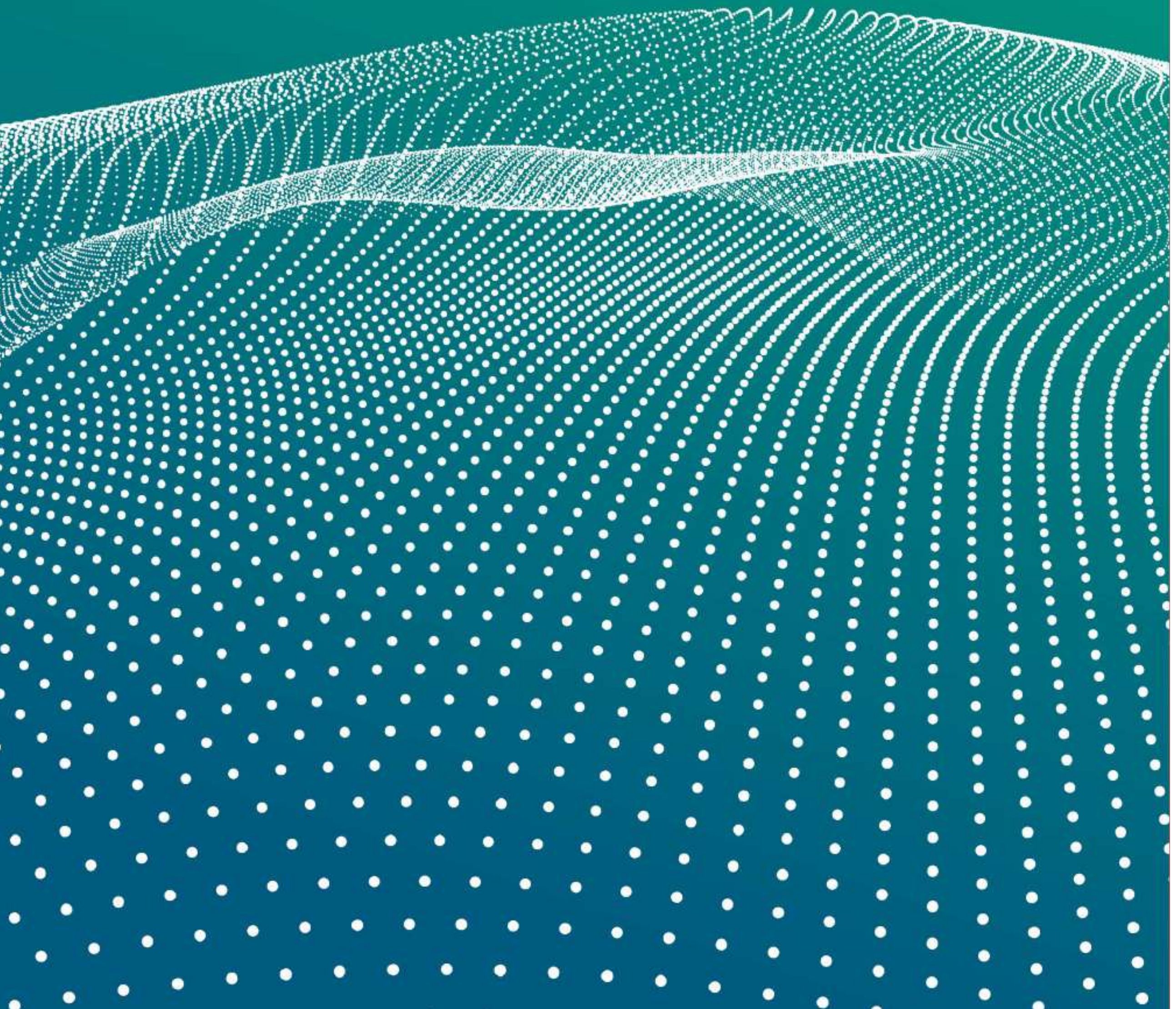
- Employees want, need, and deserve secure access to all internal and external applications required for them to work effectively.

- Having a proper cloud identity matters: Only authorized employees should be able to access specific applications and resources.

- Remote employees must be able to work without connection-speed limits. Ensuring a fast user experience can entail application prioritization and performance optimization for collaboration applications like Microsoft Teams or Zoom.

- In a crisis, an IT team must be able to roll out remote-access capabilities in days, not weeks.

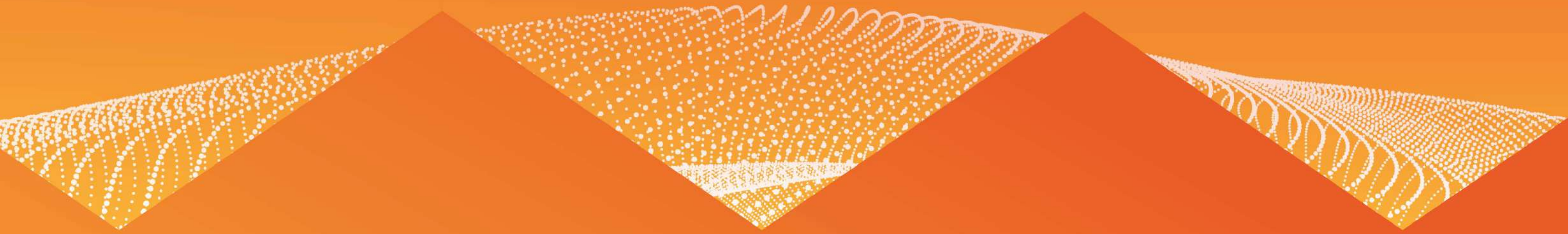
Key Takeaways



- IT teams need real-time visibility of users and applications to help troubleshoot and mitigate issues.

- Security and compliance must remain high priorities for IT, especially when every employee is working remotely.

- If remote work is not secured, organizations face data-breach risk when workers return to the office: When compromised machines rejoin a corporate network, they provide an entry point for threat actors to launch large-scale malware attacks.



CHAPTER 5

The rise of the cloud-first modern architecture: How COVID-19 is accelerating digital transformation

> *All eyes are on me. And I'm trying to deal with exploding online loads, people working remotely, new cyber threats. Every day it's something new.*[35]
>
> Banking Industry CIO, as quoted in "The CIO's moment: Leadership through the first wave of the coronavirus crisis," McKinsey & Company, 2020

The coronavirus pandemic has not only forced organizations around the world to transition to remote work at an emergency pace, it has cast an intense spotlight on every organization's preparedness to maintain business continuity during a crisis.

COVID-19 has put new pressures on IT leadership. "CIOs are facing the greatest challenge of their careers," note McKinsey & Company senior partners Aamer Baig, Klemens Hjartar, and Steve Van Kuiken in a *McKinsey Digital* article. "We are seeing infrastructure breakdowns, denial-of-service attacks, and sites going down because of traffic load," continue Baig, Hjartar, and Van Kuiken, "[e]ven as companies grapple with the implications of the COVID-19 pandemic, it is already clear that CIOs are playing a central role in navigating the crisis."[36]

This is a critical time for CIOs and CISOs as they reevaluate their current IT priorities, shift resources, and develop competitive differentation.[37] The COVID-19 crisis represents a turning point for IT leaders: an opportunity to create growth and competitive differentiation. CIOs and CISOs have been forced to take a longer-term view, and stay committed to the broader digital transformation initiatives like cloud, AI, and automation. Cloud transformation fosters agility, innovation, and cost efficiency. Those values are essential for short-term recovery, but also prepare organizations to be able to adapt to future pivots.

"This is a wake-up call for organizations that have placed too much focus on daily operational needs at the expense of investing in digital business and long-term resilience," says Gartner Research senior director Sandy Shen, as quoted by *TechRadar's* Dean Nicolls.[38] She continues, "Businesses that can shift technology capacity and investments to digital platforms will mitigate the impact of the outbreak and keep their companies running smoothly now, and over the long term." Shen makes an important point — one that progressive IT and business leaders have known for a while. The COVID-19 crisis has brought that view into sharp perspective.

The COVID-19 outbreak has propelled IT leaders into uncharted territory. But in crisis lies opportunity, and those IT leaders who can reevaluate and reprioritize their organizations' digital transformation will emerge on the other side of this with reinforced enterprise resilience, digital strength, and innovation. Responding to a crisis requires urgent attention, but CIOs and CISOs cannot afford to neglect longer-term initiatives and programs to help their businesses become tech-forward.

[35] Aamer Baig, Klemens Hjartar, and Steve Van Kuiken; "The CIO's moment: Leadership through the first wave of the coronavirus crisis," *McKinsey Digital*; March 18, 2020: https://www.mckinsey.com/about-us/covid-response-center/conversations/the-cio-moment-leadership-through-the-second-wave-of-the-coronavirus-crisis

[36] Ibid.

[37] Angus Loten, "CIOs Act as Companies' Glue During Coronavirus Disruptions": *Wall Street Journal*; March 2, 2020 (subscription required): https://www.wsj.com/articles/cios-act-as-companies-glue-during-coronavirus-disruptions-11583189119

[38] Dean Nicolls, "How Covid-19 is shaping digital transformation": *TechRadar*; April 7, 2020: https://www.techradar.com/news/how-covid-19-is-shaping-digital-transformation

Leveraging a work-from-anywhere solution beyond business continuity

Even after the coronavirus pandemic eases, companies can expect to sustain some level of remote work, says HR researcher Jeanne Meister. Writing in *Forbes*, she notes that employees may choose to stay away from the office: “The coronavirus is making companies, employees, and their managers more comfortable with working from home. From now on, we will question taking that flight to see a client if we can communicate on a new project using Zoom.”[39]

As organizations settle into the “next new normal,” the cloud-first modern architecture — the one that quickly transitioned the workforce to remote access to maintain business continuity — becomes the foundation of future IT strategy. In this new paradigm:

1. The internet is the new network.
2. The cloud is the new data center.
3. Any device can be a work device.
4. Identity is the new perimeter.

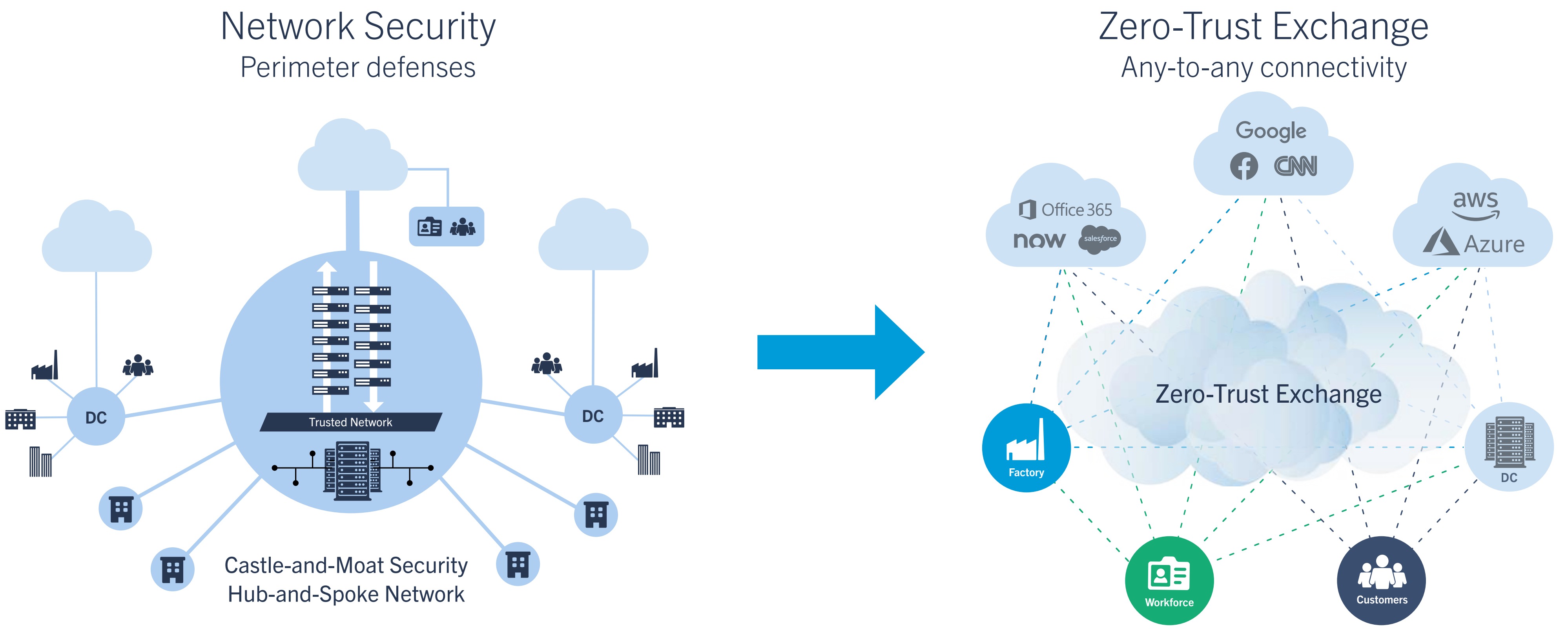


Figure 5-1. A Zero-Trust Exchange is required for secure remote work.

> *At TT Electronics we recently ditched traditional VPN technology and replaced it with Zscaler. Today people are telling me the response times are like being in the office, certainly didn’t get that feedback on the VPN! A huge thanks to Zscaler and the IT team at TT Electronics for helping us keep safe whilst working.*
>
> Steve Johns, Head of IT Operations, TT Electronics

[39] Jeanne Meister, “The Impact Of The Coronavirus On HR And The New Normal Of Work,” *Forbes*; March 31, 2020: https://www.forbes.com/sites/jeannemeister/2020/03/31/the-impact-of-the-coronavirus-on-hr-and-the-new-normal-of-work/

That same cloud-first modern architecture can be leveraged to accelerate enterprise digital transformation and drive critical initiatives. Cloud-first modern architectures deliver tangible future benefits:

- **Enabling digital transformation:** Crisis-response activities — optimizing office space, reducing travel — require IT teams to establish global shared services. Digital transformation supports that effort, and drives IT cost savings through the decommissioning or reduction of legacy infrastructure.

- **Driving a multi-cloud strategy:** Digital transformation supports access to multiple clouds (private or public, internal or external), ensuring apps can be moved seamlessly, connectivity is reliably uniform, and a superior user experience is delivered.

- **Accelerating IT integration for mergers and acquisitions:** Digital transformation simplifies secure application access. With no corporate networks to mesh, a cloud-based modern architecture speeds time to value following M&A or business growth/downturn activities.

- **Securing third-party and business-to-business access:** A cloud-first architecture enables IT teams to extend and secure connectivity to third parties. Unlike a legacy environment, there is no network exposure: With policy-based management, IT can control (and limit) that access to protect data, users, and applications.

Enable Digital Transformation

- Business process improvements
- Security as enabler for future initiatives
- Cost savings / avoidance via modernization

Drive Multi-Cloud Strategy

- Uniform connectivity for all users / locations
- Eliminate the need for virtual DMZs
- Seamless end-user experience

Accelerate M&A IT Integration

- Day-1 access — key users to critical apps
- Integrate companies without integrating networks
- Standardize security across companies

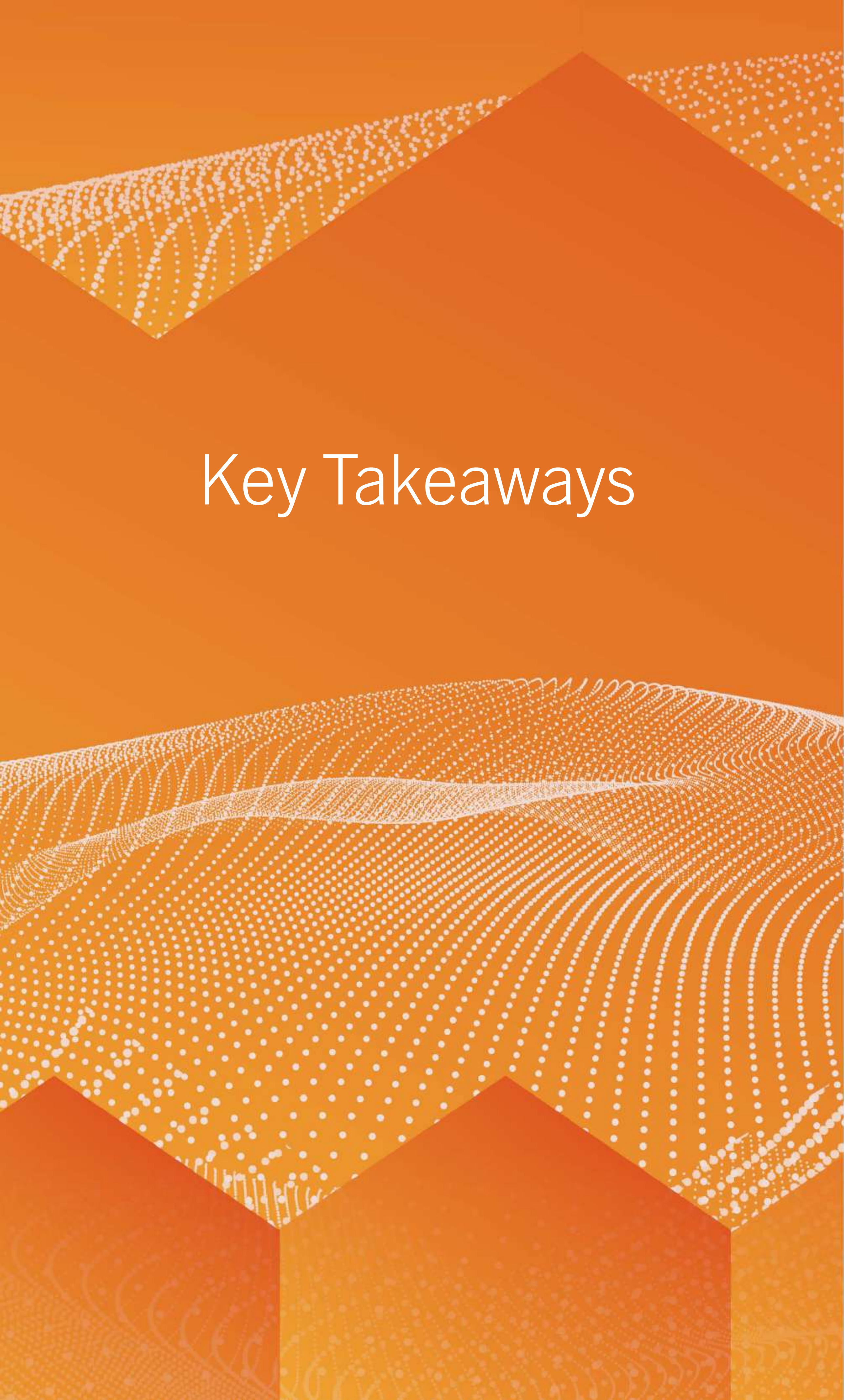
Secure Third-Party / B2B Access

- App access without network exposure
- Full granularity and visibility
- Protect data as well as applications

Figure 5-2. Leveraging a cloud-first architecture to drive strategic IT initiatives

Begin the journey

The best time to start a digital transformation journey is now. Leveraging a cloud-first architecture enables organizations to maintain business continuity through crisis and disruption. This architecture drives business profitability, innovation, and strategic IT (r)evolution while maintaining the safety of employees, customers, and resources. A future where the internet is the new corporate network, the cloud is the new data center, any device can be a work device, and identity is the new perimeter is a future where users can access the applications they need from anywhere in the world, quickly and securely.



Key Takeaways

- The COVID-19 crisis presents an opportunity for IT leaders to create growth and develop competitive differentiation with a cloud-first architecture.

- Even after the coronavirus pandemic eases, employees will continue to perform remote work.

- The future of connectivity depends on successful enterprise digital transformation. In the new enterprise, the internet must become the new corporate network, the cloud must become the new data center, users must be able to work on any device, and identity must become the new perimeter.

- Even with short-term focus on crisis response, IT must act now to enable digital transformation for long-term resilience, flexibility, and business continuity.

CHAPTER 6

Lessons Learned: CIO Journeys

Company Background

Company:	National Oilwell Varco
Sector:	Oil and Gas Manufacturing
Driver:	Alex Philips
Role:	CIO
Revenue:	$7.3 billion
Employees:	25,000 users
Countries:	65
Locations:	over 600

Company IT Footprint

National Oilwell Varco is a globally-distributed company with operations in over 600 locations. Of its large computing workforce of 25,000 employees, 70% are mobile with laptops.

“Smart” cloud migration in a hurry: How NOV accelerated its work-from-anywhere rollout

> *The situation for COVID-19 is very fluid. We need extreme flexibility. . .and it’s going to change the way that our company operates and works.*
>
> Alex Philips, Chief Information Officer, National Oilwell Varco

National Oilwell Varco — more commonly known by its acronym NOV — supplies technical equipment and services to the global oil-and-gas industry. NOV is a Fortune 500 company, and CIO Alex Philips espouses the company’s informal mantra: “We power the industry that powers the world.” Philips’ commitment to that mission was put to the test when the entire company had to move to remote access.

Getting used to doing more with less

Philips and his IT team are no strangers to dramatic business shifts: NOV’s fortunes are inexorably tied to fluctuating global commodities markets. After oil prices plummeted in the mid-2010s, Philips and team faced a straightforward challenge: Do more with less. Much less.

They sought to reduce the burden of legacy technical debt and lower historically high costs, while simultaneously adding more capabilities and improving security for their worldwide organization. NOV began its transformation in 2016 with a shift to the cloud, away from what Philips describes as “security appliance hell.”

NOV invested in Zscaler Internet Access (ZIA) and introduced (secure) local internet breakouts for its employees. The move was pragmatic: ZIA provided an optimal secure access service edge (SASE) model that optimized SaaS access, and in particular, helped accelerate its Microsoft 365 rollout. NOV replaced legacy hardware-based security appliances, saving the company money, delivering better security, and improving user experience. Philips describes this transformation as a “smart cloud usage approach”: moving NOV to the cloud where and when it made sense and on NOV’s own terms.

ZIA served NOV’s need for direct connectivity for internet egress and validated Philips’ commitment to “smart-cloud” migration. But there was still considerable data traffic going to its corporate data centers. In 2018, Philips and his IT stakeholders began rolling out Zscaler Private Access (ZPA) to secure remote access to internal applications.

NOV’s legacy on-prem remote-access solution was designed to handle up to 2000 users at any one time, volume that had only been neared during regional weather events like an ice storm or flood. Moving to ZPA opened up a world of future capacity.

ZIA and ZPA brought a new level of security to NOV connectivity, enabling protected remote access (for both employees and third-party contractors) and comprehensive inspection of incoming and outgoing SSL/TLS-encrypted data. “Many of our users work outside of our network,” notes Philips. “With Zscaler, we were able to deploy [the Zscaler Client Connector] on all these endpoints and those users were protected no matter where they were.”

The work-from-anywhere call to action: How a pandemic changed everything

“My team’s job is to enable our amazing colleagues to access their mission-critical applications and data securely anytime, anywhere, on almost any device,” explains Philips. And with NOV’s responsibility to “power the industry that powers the world,” preserving business stability was essential. “Being a critical supply chain partner to the energy industry means continuity is not a buzzword or checkbox,” he says, “but a necessity at all times.”

With a broad base of operations and 600+ offices, NOV was particularly vulnerable to global market ramifications of the coronavirus outbreak. Operationally, Philips and his IT team suddenly had to support a drastically different new reality: 27,500 employees around the world all needing remote access to work from anywhere. Immediately.

NOV had one major advantage in coping with the challenge posed by having to shutter offices. It’s inaccurate to suggest anyone was actually “prepared” to respond to the global pandemic of early 2020, but NOV’s investment in ZPA set the stage for the company’s shift to remote access.

“When COVID-19 broke out, we had to start thinking differently. How are we going to adapt?” says Philips. “Our China facilities were shut down…and we were really concerned: What’s going to happen if this goes worldwide? What do we need to do? How do we need to prepare?”

In February 2020, Philips assembled his now-remote team. They all expressed confidence in NOV’s ability to respond to the crisis. “They said, ‘Alex, I think that we’re okay,’” says Philips. “‘We’ve moved to ZPA, and Zscaler can handle this for us.’” The quickly-spreading pandemic meant that NOV was going to have more users using ZPA than they had ever had.

With Zscaler’s assurance that its globally-distributed SASE cloud could accommodate NOV’s secure-remote-access traffic volume, Philips updated his peers: “I was able to go to my leadership team and say all 27,500 of our users, if they need to work remotely, they can do it.” As for the execs, says Philips, “they were absolutely stunned.”

Creating a “desktop-based mobile workforce”

With remote-access readiness confirmed, Philips and team recognized an unexpected challenge. Sending employees who used laptops home would be practical enough, but some thirty percent of the company’s staff (engineers in particular) used powerful desktop machines. Often, these desktop systems contained expensive or proprietary software, making it harder to take work offsite.

The NOV CIO had to "face the reality that our engineers would have to take their engineering systems home with them to continue working — How are they going to connect back to corporate resources?" Many of the desktops lacked Wi-Fi capabilities, and few were equipped with the software to access needed remote resources.

"We quickly had to push out the ZPA client and instruct everyone 'Okay, take a long ethernet cable home or go grab a USB Wi-Fi adapter,'" says Philips. "We did this in a couple of locations, and it worked very, very well." Philips and team found themselves in an unexpected new operational environment: "That was a huge learning for us. Desktops would now be part of our mobile workforce, which we had never planned for or imagined. BYOD in reverse."

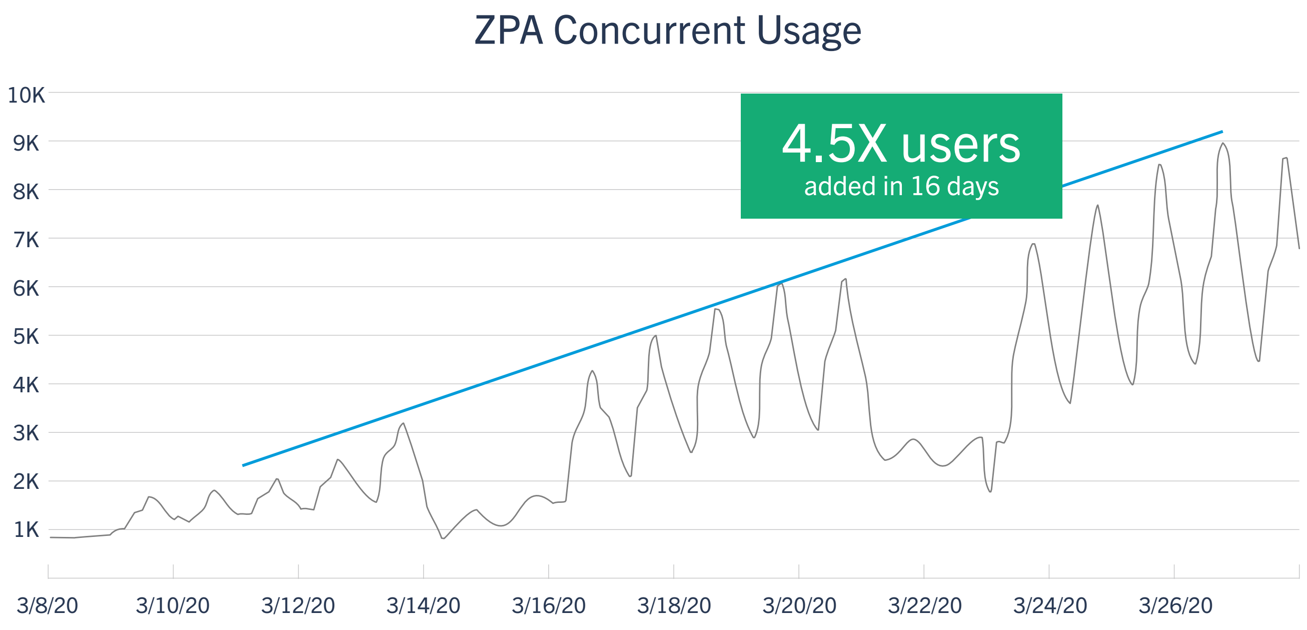


Figure 6-2. NOV increased its remote-access Zscaler workload more than fourfold in only sixteen days.

With its employees equipped with the necessary tools, NOV began its remote-access ramp-up. Philips and team held their collective breath, but despite a few initial connection hiccups, NOV's rapid transition to a remote-access workforce went smoothly.

"We have seen the number of ZPA concurrent user connections increase 4.5X over a sixteen-day period," notes Philips, who has seen operational performance spikes with more than 9,000 NOV employees connecting to corporate applications and data resources simultaneously.

"Zscaler was able to adapt quickly and increase capacity to more than satisfy our needs," says Philips. "As employee feedback from around the world has come in, I'm hearing exactly what I had hoped: 'It feels normal.'" For Philips, that response from NOV employees validates the company's secure cloud migration. As he notes, "That's very high praise considering the disaster we would have felt using our old solution!"

For Philips, NOV's remote-access effort — frantic though it might have seemed initially — has fostered NOV's longer-term operational agility.

"The situation for COVID-19 is very fluid," explains Philips. "We need extreme flexibility…and it's going to change the way that our company operates and works."

Concludes the CIO, "We're extremely excited about what lies ahead for us, and how we're actually helping prepare for our Zero-Trust journey. We have proved our employees can operate without being on the same network as their resources!"

Company Background

Company:	Takeda Pharmaceutical Company
Sector:	Pharmaceuticals
Driver:	Mike Towers
Role:	CISO
Revenue:	USD$32B
Employees:	52,000
Countries:	110
Locations:	575

Company IT Footprint

Tokyo-based Takeda Pharmaceutical Company is the oldest pharmaceutical firm in the world. Its 2019 acquisition of Shire PLC increased its footprint to more than sixty office and research locations around the world. Working out of Cambridge, Massachusetts, Takeda's IT team manages systems for its 70,000+-strong global workforce.

Finding business continuity in the cloud: How Takeda Pharmaceuticals Company scaled remote access

> “*One of the things we are providing is an app-by-app type of approach to giving folks what they need and not having to over-provision access. With the combo of ZIA and ZPA, we're much more flexible with what we can provide and since we're running all our traffic through it, we know it can scale.*”
>
> Mike Towers, Chief Information Security Officer, Takeda Pharmaceuticals

For CISO Mike Towers, it was a merger — a very big merger — that propelled Takeda Pharmaceutical Company's secure cloud transformation.

“We acquired Shire PLC in January 2019 and doubled the size of the company,” says Towers. Takeda's Shire acquisition grew its workforce significantly. Towers found himself having to integrate an incongruous patchwork of network hardware technologies.

Finding help in the cloud for a “disjointed” network

Fortunately for its CISO, Takeda had begun rolling out Zscaler Internet Access (ZIA) in late 2018, ostensibly to secure employee internet egress via the cloud and provide employees with a better, more consistent user experience wherever they might be, and for whatever device they might use. But ZIA proved particularly valuable when Towers and his team were confronted with integrating what he calls a “quite-disjointed” network architecture.

“We had about 320 or so firewalls that were in local sites, regional sites, core sites, et cetera,” says Towers. “It was a very, very traditional on-premise network appliance-based architecture. That was the predominant way that the perimeter and the network design was instituted, developed, rolled out.”

The merger accelerated Takeda's migration to the cloud: “We were ready to move toward a Zero Trust, user-to-destination type of model,” continues

Towers. “We wanted to do that as quickly as possible and we standardized on ZIA. By doing so, we can displace our ‘next-generation’ firewalls.”

ZIA gave Towers and Takeda greater flexibility in enabling secure employee connectivity — for every type of worker, notably — via local internet breakouts. Towers points out that Zscaler’s policy-based administrative controls help make Takeda more agile: “Seventy-thousand employees in 110 countries, but we had one policy,” he explains. “We can have the same policy regardless of where people travel, with a consistent experience whether you’re on-premise or off the network. When you think about challenging yourself to improve both user experience and better security, Zscaler allows us to do that because folks can be flexible.”

Deploying ZPA slowly. . .then very, very fast

In an industry built on research, Takeda Pharmaceutical Company relies heavily on internal development, and that requires extensive use of proprietary technologies, applications, and intellectual property. In the past, that dependence had slowed Takeda’s migration to the cloud.

Looking to a cloud future, Towers envisioned “a model of remote access for applications that have historically been on-premise.” He cites regulatory pressures and “machine proximity” for keeping resources in-house: “When you have a manufacturing plant or an R&D lab, there’s expensive equipment in those environments that require computers to run them. Those often have to stay on-premise, and we want folks to have access to those applications without having access to the full network.”

In 2019, Towers and team began rolling out Zscaler Private Access (ZPA) to deliver secure connectivity to internal resources, prioritizing its deployment by both application and user. Towers notes that Tokyo-headquartered Takeda — the oldest pharmaceutical firm in the world — is “values-driven,” and shifting to ZPA was a bit of a cultural change for the company.

Towers prioritized extending remote access and retiring VPN hardware. “Remote access historically has meant remote network access,” says Towers. “We no longer think that way.” ZPA changed the way Towers viewed VPN technology at Takeda: “Remote users are used to clicking on a VPN client to connect, but inherently, VPN is not about application access, but about network access. In our mind, this is more around the applications and the services folks need. . .and VPN really doesn’t do much because you’re coming into a network just to back out again.”

Towers had to reassess Takeda’s infrastructure, in particular its remaining use of VPN technologies in light of Takeda’s progress toward cloud transformation.

Today when he considers VPNs, Towers asks rhetorically, “What’s the point?” As he puts it, “We can provide that same level of assurance and control natively in the cloud. We want to remove as much friction as possible.” Zscaler helps Takeda remove that friction. Continues Towers, “ZPA allows us to have the application accessed without somebody having to ever think about whether they have to click some other window or some other emulation engine to get to it. . .We want to support that capability as quickly and with as little friction as possible.”

When working from home becomes the new normal

In early 2020, Towers and his team were progressing with a measured ZPA rollout at Takeda. And then the coronavirus outbreak hit. Like many multinational companies, Takeda saw its first operational impacts in China, where Towers notes branch offices were still using “legacy VPN infrastructure” on “dated network architectures that made

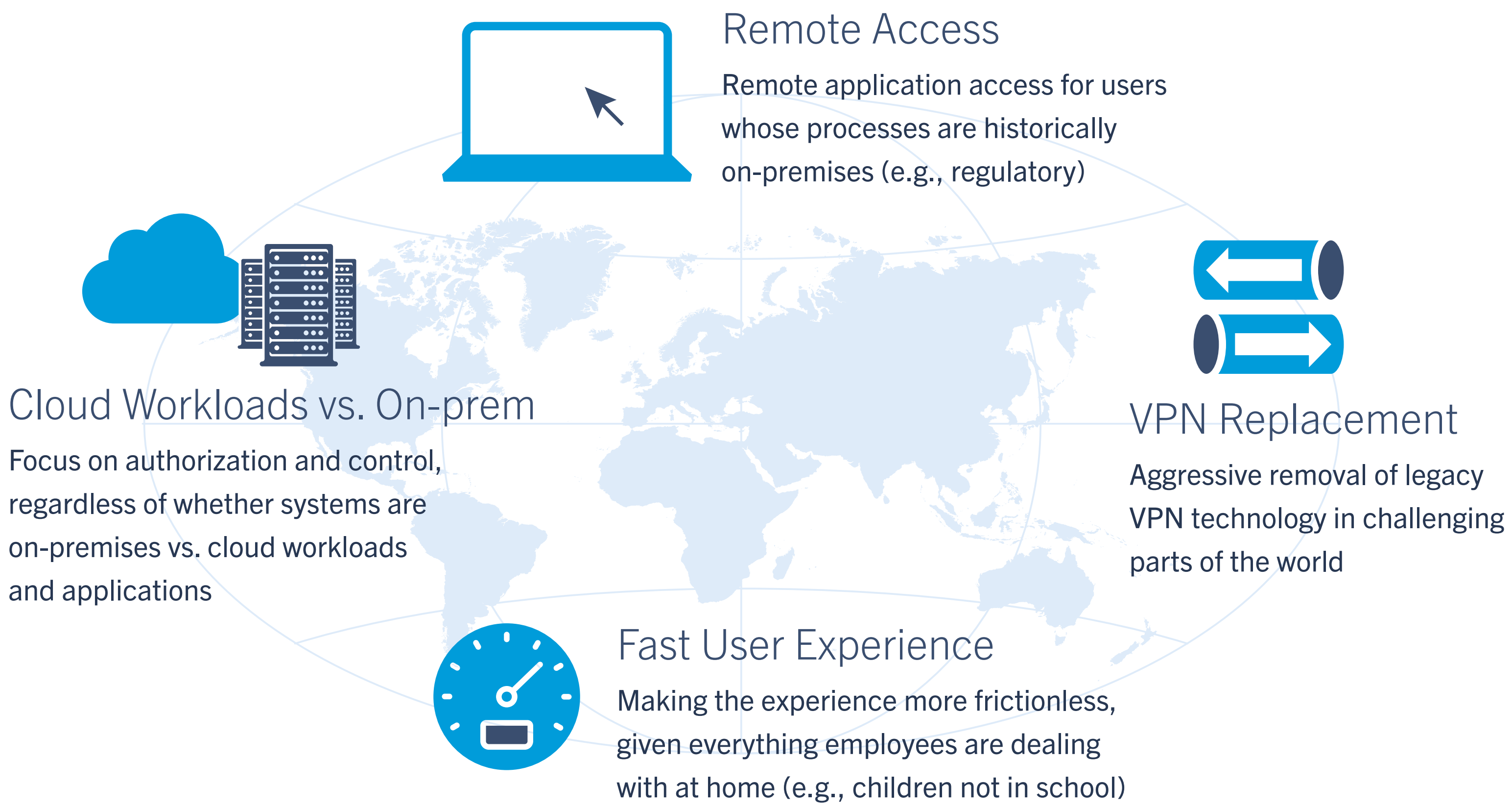

Remote Access
Remote application access for users whose processes are historically on-premises (e.g., regulatory)
Cloud Workloads vs. On-prem
Focus on authorization and control, regardless of whether systems are on-premises vs. cloud workloads and applications
VPN Replacement
Aggressive removal of legacy VPN technology in challenging parts of the world
Fast User Experience
Making the experience more frictionless, given everything employees are dealing with at home (e.g., children not in school)

Figure 6-3. CISO Mike Towers led Takeda's (accelerated) initiative to enable employees to work from anywhere. He prioritized four objectives: remote access, VPN replacement, better user experience, and a focus on control (regardless of whether the system is on-prem or in the cloud).

application access and performance quite slow." The solution? A "quick pivot to ZPA," led by Towers and team.

But as the urgent need for employee remote access grew, Towers had to figure out how he and his colleagues around the world could sustain business continuity given such "unprecedented" challenges. "We've never had a situation where we have so many people working from home," he says. "You practice for widespread work-from-home quite regularly, but no one practices with everyone doing it at the same time when all their children and families are home." Access was one thing, managing crowded bandwidth was quite another: "Every worker [at home] is competing with Netflix and Xbox from the kids at the same time, so performance optimization for internet access is something that we've had to focus on."

Towers and team looked at how Takeda users work with internal applications. They shifted Takeda's "control and provisioning approach" so users would be concerned with *which* applications they needed to get their work done, and not so much with *where* those applications might reside. "We don't want to think that way anymore," he explains, and now IT can instead provide "an app-by-app type of approach to giving folks what they need, and not having to over-provision access."

When working remotely means less hardware, not more

ZPA has enabled Towers and team to secure Takeda’s transition to fully-remote operations. As the company has adopted ZIA and ZPA, Takeda has achieved what Towers calls “significant cost savings” by retiring its firewall hardware. CISO Towers aims to get the number of corporate firewall appliances down from its high (320+!) to just a dozen.

Takeda’s realized benefits with Zscaler aren’t limited to VPN and firewall hardware. After struggling with “a lot of niche point solutions,” Towers is now leveraging Cloud Access Service Broker (CASB) capabilities via Zscaler’s inline-proxy security architecture: “Zscaler can help us do more with CASB controls,” explains Towers, “and help us be smarter with the data, and make security decisions based on data, and because it’s in the cloud, and we’re already sending our traffic through it, we know that it will scale [and] be operationally stable.”

As employees have shifted to local internet breakouts, Towers has been able to retire costly networks. “Ninety-eight percent of what [users are] going to is on the internet anyway,” he explains. “We can get rid of a lot of expensive WAN links.”

In the past two years, Towers and his IT team have had to adjust (much more adroitly than they could have imagined) to operational obstacles placed in their path. But though his company’s secure cloud transformation may be progressing at a faster-than-expected pace, Towers remains optimistic.

“With the combo of ZIA and ZPA, we’re much more flexible with what we can provide and since we’re running all our traffic through it, we know it can scale,” concludes Towers. “This is a good time to be a security professional because you don’t have to worry about trying to balance user experience and security anymore. You can do both!”

Company Background

Company:	National Australia Bank
Sector:	Financial Services
Driver:	Steve Day
Role:	Executive for Enterprise Technology
Revenue:	USD$12B[40]
Employees:	35,000
Countries:	8
Locations:	1600

Company IT Footprint

National Australia Bank (NAB) is one of Australia's "Big Four" financial institutions, and serves consumer and commercial interests in Australia, New Zealand, and across Asia. Its IT organization supports business operations for more than 1500 branches.

Moving financial services to the cloud: How National Australia Bank transitioned to working remotely

> *To go from where we were, to almost the entire bank working from home within four weeks…people are quite astounded. We're looking forward now, and I'm appreciative of this partnership.*
>
> Steve Day, Chief Information Security Officer, National Australia Bank

With more than nine million customers, National Australia Bank (NAB) is the largest business bank in Australia, not to mention a 160-year-old institution and a national icon.

Like most banks, NAB has adapted to new ways of doing business. "Cash is becoming less and less relevant in today's society," explains Steve Day, NAB executive for enterprise technology. "Transactions used to be performed within a branch, but now people are expecting a Google or Amazon-type experience when they work with their bank."

Day and his IT team have shepherded NAB towards an operational future that integrates online-transaction convenience with a relationship-driven development approach. Some transactions, large ones primarily, require "personal, direct engagement," notes Day, who observes that few people want to go online for say, "the biggest investment you make in your life." For Day, finding a balance between in-person and online communication is an ongoing objective. In practice, it means "moving to a business model where day-to-day online activities become seamless and easy while maintaining that personal relationship on bigger transactions."

Moving financial services forward in the cloud

When it comes to business evolution, the financial services industry can be staid: Strict data-privacy requirements, low risk tolerance, and regulatory constraints can all foster resistance to change. But

[40] FY2018 based on April 2020 exchange rates.

NAB hasn't let operating pressures slow its progressive approach to infrastructure innovation.

In the mid 2010s, NAB's leadership recognized the potential and value in migrating to the cloud, in particular to help strengthen its security posture. The company invested in Zscaler Internet Access (ZIA), rolling out local internet breakouts for users, and taking advantage of ZIA's Cloud Sandbox security technology.

"Cloud is integral to our future," says Day. He and NAB IT leaders have worked to transform NAB's application suite from on-premise to cloud-based, reducing the company's reliance on legacy architectures to take advantage of both application-containerizing functions and new application capabilities.

Moving a high-touch business to a work-from-anywhere model

NAB's shift to the cloud was driven by security priorities. "Part of the initial motivation was to get to Zero Trust," says Day. "We didn't need to run a separate corporate network, since that increases the number of places you can be attacked from."

"Many of our older financial systems were not designed for working anywhere but in an office, and on a low-latency connection," comments Day. With a dual focus on securely enabling the business and improving user experience, Day and team began evaluating Zscaler Private Access (ZPA) as a solution for connecting employees to internal resources.

And then in early 2020, the coronavirus outbreak hit. The first necessary adjustment NAB had to make was scaling to accommodate higher-than-normal customer call volumes. In the space of a few days, NAB found itself having to transact three-to-four times its normal commercial and consumer banking volume.

"The bank must play a role in enabling and sustaining the Australian economy through a crisis," explains Day. "We play a part in enabling the stimulus packages and support programs."

The second adjustment was a practical challenge: To ensure the safety of its employees and enable teams to be able to serve customers in a time of need, NAB had to enable its call-center staff employees to work remotely.

The third adjustment was sudden: An employee reported contracting coronavirus. To safeguard the health of the employee and the employee's coworkers, NAB immediately evacuated the building, meaning 4,500 people had to work remotely, though some were not yet enabled to do so.

Moving from constrained VPNs to scalable cloud

Day and the NAB IT team shifted into overdrive: "The amount of logistics that went over the days following…we worked 24/7 for four days to enable remote access for thousands of employees."

"We had been looking at modernizing our internal capabilities," says Day, "and as we moved applications to the public cloud, we could see that the current VPN wasn't providing the right outcomes."

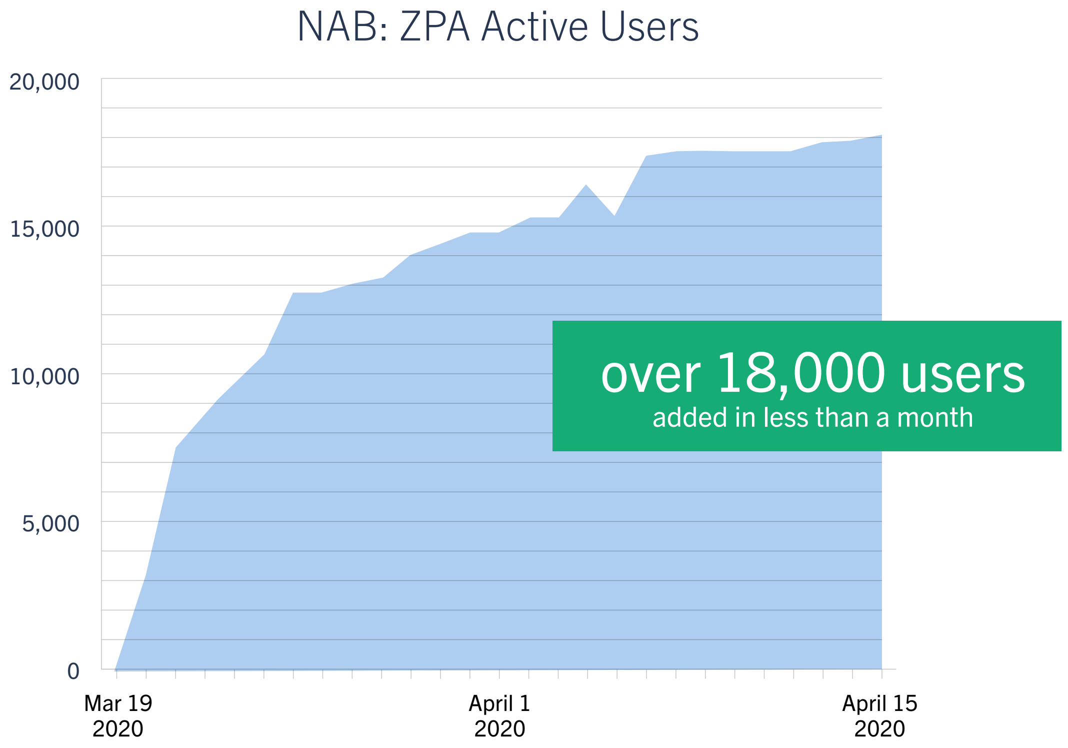


Figure 6-4. National Australia Bank (NAB) deployed ZPA to more than 15,000 users in only two weeks, enabling its workforce to work remotely during the COVID-19 crisis.

He and team realized they wouldn't be able to procure legacy connectivity hardware affordably, let alone expediently. "We couldn't scale up our existing VPN solution rapidly," explains Day. "We'd have to order equipment, and wait for it to be delivered, but you don't know when you're going to get anything since everything's clogged up in customs right now."

The alternative? An accelerated — *a very accelerated* — ZPA rollout

"We needed to pivot quickly," says Day, with unintentional understatement. Over the course of the next few weeks in March 2020, NAB shifted to a remote-access model, with only those required to work on premise remaining to do so. Day and his colleagues deployed ZPA for thousands of employees, enabling their access to corporate resources from remote locations.

Those ZPA-enabled employees included NAB's call-center staff around the world. "Before March 2020," comments Day, "we had never had a single customer call handled by someone working outside of one of our offices."

Moving away from a corporate network

"Today, we are happily working with 22,500 users on ZPA," says Day, who notes that NAB went from fewer than 150 users to full deployment in less than three weeks. "ZPA offered a seamless experience," he says. "Users would turn on their PCs and they connected exactly the same way as they did in the office. That was a real benefit for us."

Day's original intent with implementing ZIA and ZPA for local internet breakouts was to get to a Zero-Trust environment. Ultimately, COVID became the catalyst for accelerating scale up. According to Day, ZPA's ease of use and flexibility made fast rollout possible. He also credits the efforts and insourcing work of internal teams for the successful deployment.

"Zscaler enables us to save costs and reduce threat surface area," says Day. "Because Zscaler is a cloud-based service, it scales beautifully...we didn't need to build out additional infrastructure — It was the obvious solution."

DB SCHENKER

Company Background

Company:	DB Schenker
Sector:	Logistics
Drivers:	Markus Sontheimer, Gerold Nagel
Roles:	CIO/CDO Member of the Board of Management, SVP of Global Infrastructure Services
Revenue:	USD$18.5B
Employees:	76,000
Countries:	80
Locations:	1400

Company IT Footprint

Global logistics and freight-forwarding company DB Schenker provides contract shipping services over land, sea, and air. Its IT infrastructure team manages systems and solutions for its 76,000+ employee workforce in more than 1400 locations around the globe.

Agility in motion: How a commitment to the cloud facilitated remote access for DB Schenker's global workforce

> *Zscaler Private Access was the key enabler for DB Schenker to support our business continuity plans. And to keep our business ahead of our competitors in the market. Our employees don't want to go back to a traditional VPN connection anymore.*
>
> Markus Sontheimer, CIO/CDO Member of the Board of Management, DB Schenker

When the coronavirus outbreak began, multinational logistics company DB Schenker had to address an immediate concern: How do you enable the majority of your workforce to work remotely and keep them safe while ensuring business continuity? Fortunately for DB Schenker, the company had set the stage for its own business continuity years earlier.

"Global" operations in every sense of the word

Based out of Essen, Germany, DB Schenker is one of the world's leading logistics and freight-forwarding companies, providing contracted transport services over land, sea, and air. Its operations span more than 80 countries, and it employs more than 76,000 workers in 1400+ locations.

Markus Sontheimer, DB Schenker's CIO/CDO Member of the Board of Management, describes the worldwide nature of DB Schenker's business operations this way: "We have to cross borders. We have to ship from A to B, no matter what country it is, and no matter what it costs."

Committing to the cloud

Sontheimer had begun initiatives across DB Schenker to migrate workflows, resources, and applications to the cloud. The effort was partly to reduce infrastructure expense, but also to ease management and administrative complexity.

DB Schenker's secure cloud transformation began in 2017, when the company invested in Zscaler Internet Access (ZIA) to secure local internet breakouts for its employees' internet egress. It was part of a larger program launch within DB Schenker called "Global Workplace Management," prioritizing cloud-based solutions and SaaS use.

"We started what we call 'server-free branches,'" explains Sontheimer, "basically, cloud-first operations: authentication in the cloud, software distribution in the cloud, nothing on-premise anymore. And with [Microsoft 365], all our data is in the cloud, accessible at any time, from anywhere."

Starting in 2018, the next cloud-migration objective was to move DB Schenker away from its legacy network architecture. The IT team focused on two areas: First, as Sontheimer recalls, "We switched to a hybrid network, with internet connections all over the place, and Zscaler for bandwidth control."

The second task was to standardize on a software-based, global unified communications (UC) telephony platform: "No desk phones in the office and hardly any hardware," notes Sontheimer.

The constructive transition to "Global Workplace Management" – GWM for short – built the foundation for DB Schenker's successful cloud transformation. But it represented only the beginning of what would become the most agile operational pivot in company history.

An interruption in Chinese operations signals a broader global disruption

In January 2020, the coronavirus hit, immediately impacting DB Schenker's Chinese operations. The outbreak's business repercussions started during the Lunar New Year holidays, while many China-based DB Schenker employees were on vacation. That simple circumstance bought DB Schenker a little bit of time to figure out how to enable immediate remote access for its affected workers.

DB Schenker SVP of Global Infrastructure Services Gerold Nagel and his team moved quickly — Given what was happening in China, they recognized the extent of the threat COVID-19 posed to global business operations. To begin, Nagel assessed the legacy network hardware serving his Chinese colleagues and remote DB Schenker employees around the world. And the assessment wasn't positive.

"We had some very specific challenges we had to face in China," explains Nagel. "We had a small, dedicated VPN setup." Worldwide, DB Schenker allowed users to connect through VPN concentrators in four locations. Nagel quickly determined that sticking with DB Schenker's VPN hardware would constrain the company's ability to ramp up remote access for home-based workers. "We had a traditional VPN," says Nagel, "but it was very limited in how many concurrent users there could be." Scaling the VPN architecture would "require hardware, setup, ordering" and would mean "we wouldn't be able to do anything on time."

Nagel and team considered alternatives. They started with the cloud, and Zscaler Private Access (ZPA).

"The disruption led us right away to ZPA," explains Nagel, a solution that would allow "users to log on remotely and access applications with high scalability and ease of use."

In early February, Nagel and team ran a successful four-day ZPA pilot test phase, and then raced to deploy it for affected employees: When employees began returning from holiday travel, DB Schenker's IT infrastructure team was ready to put ZPA in production. Over two-and-a-half hectic weeks, DB Schenker rolled out ZPA, first for its employees in China, then to the broader workforce.

Nagel saw an immediate impact: that there was no impact to business continuity.

"ZPA is what we implemented," says Nagel, "and that enabled us to very quickly ramp up 8,000 users in our Asia/Pacific region, working from home, accessing everything in the cloud, accessing everything that is in our own premises, all of our own applications."

They expanded ZPA to DB Schenker's global operations. "By the end of February," notes Nagel, "we already had a huge workforce working remotely."

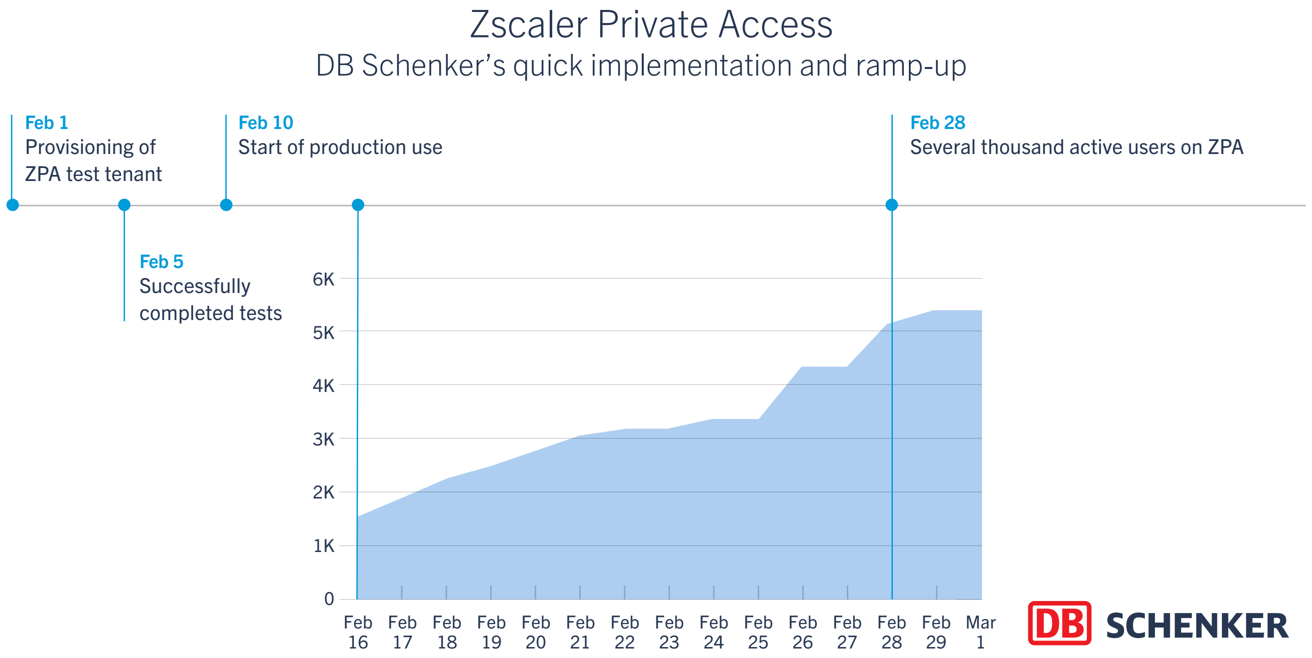


Figure 6-5. DB Schenker moved aggressively to deploy ZPA, transitioning its Chinese employees to remote access in the space of two-and-a-half weeks.

Lessons learned: Communicate, communicate, communicate

As more of its workforce has shifted to remote work, DB Schenker has continued to deploy ZPA to support them. The rapid ZPA adoption has gone smoothly, though not without some unexpected outcomes.

"From an IT infrastructure point of view," says Nagel, "we have been ahead of business divisions, many of which were slower to have continuity plans in place because things were changing every day."

ZPA contributed to Nagel and team's success in sustaining DB Schenker business continuity. To Nagel, having the GWM already in place "was one of the key principles that helped us." But it was a solid communication plan that helped guide DB Schenker through the crisis.

Even in the early days of the COVID-19 crisis, Nagel recognized the importance of clear, unambiguous communication. Says Nagel, "We had to tell employees very basic things like 'Take your laptop home! Don't leave it in the office. You might not get the chance to return to get it.'"

Nagel identifies the six components of DB Schenker's crisis communications plan: establishing a task force, leveraging collaboration tools (in DB Schenker's case, Microsoft Teams), performing daily status checks, ensuring accountability with detailed task-tracking, building (and using) communication channels, and ensuring continuous improvement with shared lessons learned.

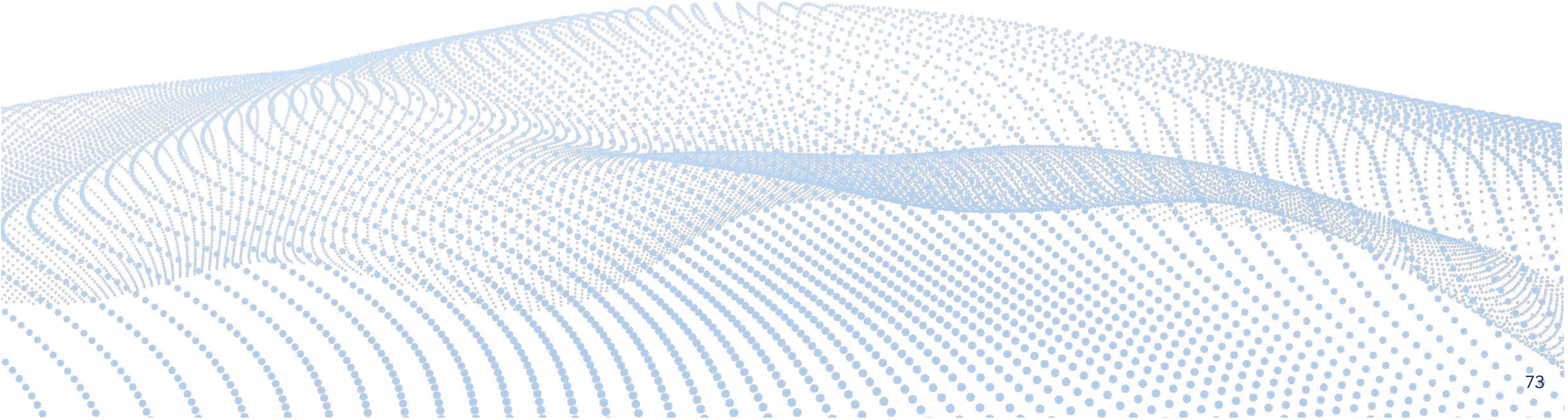
Remote access, no more VPNs, and a new competitive advantage

Adapting to an entire workforce needing to work remotely is an admittedly extreme example of DB Schenker's new operational agility. Sontheimer and Nagel both credit ZPA for that, and for what they hope will be a competitive advantage in the future.

"ZPA is very easy to use," Sontheimer explains. "The volume of people can grow. You don't have the limitations of a VPN. Zscaler Private Access was the key enabler for DB Schenker to support our business continuity plans. And to keep our business ahead of our competitors in the market."

The feedback from affected employees has been more than positive, notes Sontheimer: "They don't want to go back to a traditional VPN connection anymore. And that's something I can guarantee."

In the end, ZPA gives DB Schenker a direct-connection capability it didn't have before. In this case, it delivered that value under crisis circumstances. Nagel remains appreciative. "This is practical, not theoretical," he says. "It's actually really working! Easy to use and also very quick to ramp up. I must encourage enterprise IT leads: Look into ZPA if you have to get your workforce working from home."



Appendix

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 (C-staff, IT, customer support) can access the network when needed.	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 Client Connector 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; limiting network access 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 backhauling.	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 when they are outside of the corporate security boundaries.	Develop access-specific policies to apply to endpoints based on situation.	Deploy Zscaler Client Connector to all endpoints either through push, self-service portal, or the App Store or Play Store. Use ZIA to apply policy to those Zscaler Client Connector 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 risk profile allow for exclusions (such as PCI DSS or 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 (EDM) to more effectively restrict critical data movement.	Use canned and/or custom ZIA DLP rules to look for sensitive data in traffic flow.

About Zscaler

Zscaler was founded in 2007 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.