WHITE PAPER

The 4 Benefits of VPN Elimination

Executive Summary

The corporate perimeter as you know it no longer exists. Virtual private network (VPN) vulnerabilities are pervasive, and outdated access solutions are not only cumbersome and time consuming, but also allow for unprotected access to enterprise networks and applications. Management and IT practitioners have long recognized this, yet effective alternatives were either scarce or intimidating in scope and cost. Thankfully, that market has now changed.

As more day-to-day operations migrate to the cloud, internal corporate applications are, too. IT must support, maintain, and replicate stacks of hardware and software across different environments and multiple geographies to operationalize this, and the task of delivering access to IaaS, SaaS, and on-premise applications is proving too complex. By adopting a zero trust security model as a first line of defense, businesses can not only dramatically reduce risk, but also minimize IT hours and money spent.

Cloud-based access solutions use the ubiquity of the Internet to offer simple, more scalable means of application-level access for all users — regardless of their device or location — while also streamlining IT's provisioning processes. Today's businesses now have an opportunity to reduce the attack surface created by VPN and full network access, and adopt a solution that not only provides detailed logging and reporting of activity, but also keeps users off of the actual network.

In this paper, you'll discover the four advantages to VPN elimination, and how to identify and apply modern solutions to archaic remote access processes — all while ultimately creating more efficient and effective everyday operations.

An Introduction to VPN Elimination

While the term "elimination" can often have negative connotations, when it comes to your VPN, it is anything but. Outdated remote access technologies that consist of a variety of cobbled-together hardware and software are no longer an option in today's threat landscape. Think about it: VPNs were introduced during a time when most people were working in an office each day. Clear access parameters *and* IT perimeters were set. There were certainly fewer devices from which to choose. And attacks, in general, were considerably less sophisticated and frequent.

What worked 20 years ago simply cannot be trusted today. This has repeatedly been proven by an increasing number of data breaches that occur as a result of lateral network movement via privilege escalation and trusted credentials. With growing mobile and remote workforces around the world, providing users with easy, secure access to only those applications they require to perform their jobs — regardless of locale — is more important than ever.

This may feel like an intimidating task; any transformation in business-wide systems or processes can be daunting. However, once you gain a clearer understanding of the availability and features of simpler, more cost-efficient solutions, most organizations will wonder — why didn't we eliminate our outdated VPN sooner?

General Inefficiencies of VPN

We likely don't need to tell you what's wrong with your VPN from a management and performance perspective. These grievances are typically top of mind and top of list for IT and users alike. Support is costly and requires continuous IT bandwidth. Cumbersome hardware is vulnerable and often obsolete. And an unfriendly end-user experience creates headaches and frustration, and ultimately decreases overall productivity.

However, these generalizations merely sit at the tip of the proverbial VPN iceberg. What you might not want to concede is that VPNs pose a very real threat to enterprise security. By their very nature, they punch a hole in the network firewall and typically provide unfettered network access. They also lack intelligence; VPNs can't accurately confirm the identities of those who are trying to access your network or provide a continuously adaptive go/no go based on multi-factor authentication (MFA).

Furthermore, VPNs monopolize senior IT resources. Users rarely have visibility into the number of hours dedicated to, and the superfluous systems involved in, supporting a VPN — both to deliver connectivity and to facilitate the complexity of everyday onboarding, offboarding, and general auditing.

> “In a recent survey conducted by IDC, 50%+ of IT practitioners report that they still use more than 10 network and application components to add a new external user group to an organization.[1]”

Configuration, deployment, use, and decommissioning of access should be simple, for both IT and users. Modern, progressive organizations might understand the trappings and tribulations of a VPN, but the question becomes: what to do about it? How can businesses implement tailor-made application access that secures the enterprise and frees up valuable IT assets, while also considering budget constraints?

Why Change, Why Now?

Eliminating your VPN is not only a viable option, but it is becoming imperative due to four modern realities: workforce mobility, varied digital ecosystems, cloud migration, and the threat landscape.

MOBILITY

Enterprise users are increasingly scattered. The majority of organizations now empower their employees to work remotely — and daily, users connect to the corporate network from home, the airport, a conference, a train, a hotel, a coffee shop, and even at 30,000 feet when traveling. Employees are not at their desks 50-60% of the time.[2] And a staggering 79% of global knowledge workers are full-time telecommuters.[3] The number of non-self-employed, at-home workers has grown by 140% since 2005,[4] a trend that IDC Research reports will continue to propagate.[5] But regardless of locale, every member of the workforce needs secure, straightforward access to the enterprise applications they require in order to perform their jobs.

DIGITAL ECOSYSTEM

The composition of today's workforce is incredibly varied. Enterprises increasingly rely on contract workers, partners, suppliers, developers, customers, distribution channels, and other third-party entities to support their initiatives. It's predicted that by 2027, more than 50% of the U.S. workforce — over 86 million people — will be freelance, and that's if the current rate of adoption stays static.[6]

Not only is the ecosystem diverse, but it is globally dispersed as well as subject to rapid scaling. Mergers and acquisitions are commonplace in today's corporate landscape, and an acceleration of these activities is projected through 2018, as is an increase in merger size.[7] Additionally, this growing number of constituents access the corporate network from an increasing number of devices — desktop computers, laptops, mobile phones, tablets, connected "smart" devices, and BYOD (bring your own device). Access technologies must be able to keep pace with these demands.

CLOUD TRANSFORMATION

Enterprise architecture is increasingly complex, and applications are increasingly distributed (i.e., on-premise, IaaS, and SaaS). And the popularity of cloud applications is climbing. The average business uses more than 1,427 distinct cloud services, with the average employee actively using more than 36 at work daily.[8] Companies using legacy systems often backhaul this cloud traffic over the WAN through a centralized security stack, then reroute it through direct connects or VPNs, back to IaaS and the Internet. But this model degrades application performance and user experience, increases enterprise security risk, and drives up costs, especially as businesses duplicate their stacks across geos and vendors.

SECURITY

Cybercrime is a trillion-dollar business. Malicious actors are patient and highly incentivized, attacks are customized and targeted, and the threats themselves are widely available for sale. On average, a data breach costs an organization $3.86 million, though worst-case "mega breaches" can carry a price tag of $40 million to $350 million.[9] Perhaps more startling is the fact that more than 40% of breaches are linked to authorized users.[10] As the locations, types, and methods of access expand, segmentation of users and qualification of all requests is imperative. Unilateral network-level permissions must be superseded by case-by-case, application-level, customized access.

THE AVERAGE DATA BREACH COSTS

$3.86 MILLION

A MEGA BREACH CAN COST

$40-$350 MILLION

VPN and its plethora of complexities don't align well with the requirements of today's mobile, diverse, and distributed businesses. Agility and simplicity can't come at the cost of security. Cloud-based access solutions can combine intelligence into decision making and look at users, devices, and locations, as well as patterns of access, which uplevels security.

The Way Forward

Faster, simpler, and more secure alternatives to VPN already exist. And more organizations are realizing that they are at a critical juncture when it comes to reducing costs, restricting gratuitous application access, and gaining visibility into *who* exactly is using *what*.

The days of set-it-and-forget-it VPN systems that create more inconveniences and inefficiencies down the road are a thing of the past. A cloud-based service enables IT to implement a zero trust security framework by closing all inbound firewall ports and keeping users off the network, while simultaneously providing users the instant, vital application access they require to do their jobs — and all of this can be executed with considerable ease by IT through a single portal in minutes instead of days.

How Does a Cloud Framework for Application Access Work?

View an application access cloud architecture as your universal portal into one out-of-the-box solution for everything your VPN once provided and more, without any of the common problems or complexities. That means you'll have data path protection, identity and access management (IAM), application security and acceleration, and single sign-on (SSO) — as well as clear visibility and control — in one service across all applications. You'll accumulate less technical debt and consolidate your stack, all while simplifying the process and saving time (and potentially dollars).

This, in turn, provides secure service to all users, remote or otherwise, with no direct path into your network. Instead, it delivers a mutually authenticated Transport Layer Security (TLS) connection from within your data center or cloud, thus bringing the permitted applications directly to the user. No insecure tunnels. No clear path for malware to infiltrate. And no way for malware to spread to sensitive systems.

Maybe best of all, the applications are now presented in any browser on the user's device of choice. By utilizing both an enterprise-wide SSO and MFA, IT gains additional controls, the end-users' experience is vastly simplified and immensely improved, and ultimately, security is no longer the predominant issue.

Last, but certainly not least, custom scripting and integration are virtually eradicated, as a wide variety of enterprise infrastructures are seamlessly amalgamated in just one click. The result is a single-source, secure access delivery model that enables a zero trust framework for critical workloads deployed in any environment — anywhere your users may need to gain entry to essential applications.

The 4 Benefits of VPN Elimination

Determining the explicit applications that a user needs, and limiting access accordingly, is paramount to modern-day enterprise security and user experience. It's increasingly vital for businesses to not only identify users' devices, but to also verify the identity of the specific individual requesting access.

This is no small task, but the advantages of eliminating a VPN and moving to a unified application workspace and portal are compelling. IT teams, end users, and businesses as a whole will notice that cloud-based access delivers four key improvements across the organization — almost instantly.

BACK-END BENEFITS TO CLOUD-BASED SECURE ACCESS

IMPROVED SECURITY

Keep your network void of unwanted traffic by locking down the firewall, making application IP addresses invisible, and adding MFA with just a click of a button.

REDUCED IT COMPLEXITIES

With no additional software, easily consolidate VPN and MFA functions into one seamless SSO across all applications.

IN-DEPTH REPORTING

Gain complete auditing and recording of all user activity, available as built-in reports or effortlessly integrated with existing tools.

SIMPLIFIED ADOPTION

Deliver applications to any device type – anywhere in the world – thus increasing ease of adoption and reducing time-consuming IT tickets.

1. SIMPLER, MORE SPECIFIC REMOTE ACCESS

Challenge: Unnecessary Full-Network Access

Organizations should strive to reduce their attack surface by identifying only the applications needed per user. This sounds obvious, but the reality is that superfluous application access is the bane of a VPN's existence. Yet once you eliminate a VPN, you are also eliminating redundancies and gratuitous permissions — along with needless, time-consuming security monitoring.

Solution: Identify the End User, Device, and Context

A user's IP address tells less than half the story. Basing trust on IP ranges inside of a network is a fallacy. Rather, trust should be continually assessed based on identity, device, and contextual signals in terms of location, time of day, authentication state, group membership of user, and more. Ultimately, adopting a security posture of default deny and least privilege illustrates that the specific application access needed per user is probably just a fraction of what your current VPN actually grants that user. This creates a tremendous amount of preventable risk, and given today's mobile and digital workforce, users are rarely accessing your network from just one device. As such, it becomes imperative to not only authenticate and authorize the individual who is requesting access, but also the device and the context in which they are requesting it.

Through their device of choice, users can then log in, prove their identity, and access those applications to which they have permissions — assuming their context does not demand step-up verification or revocation of permissions. It's a simple, fast, and secure provision of service that provides instant, scalable value.

2. REDUCTION IN MANAGEMENT AND IT SECURITY BURDENS

Challenge: Permissions for Non-Employees

If best practice is to limit access for your employees, it's certainly necessary to qualify and restrict access to the other members of your ecosystem as well, such as contractors and clients. According to recent IDC Research, 46% of IT professionals estimate that their organizations experience major incidents a few times each year.[11] As your user base becomes increasingly mobile, varied, distributed, and cloud-first, the probability of these security episodes only increases. And as access controls are based on identity versus IP address, the next logical step would be to empower IT to simply and quickly set policies that bind a user to a given application, without making hardware upgrades and laborious, blanket changes to the network. The overlying problem is that VPNs don't — and can't — work in this fashion.

Solution: Set Secure Authorization Parameters

Establish one centralized control point for both authentication and monitoring to curtail access and reduce the risk of a potential malicious actor acquiring network credentials. This not only provides essential agility for management and IT to rapidly respond to those aforementioned security incidents, it also delivers peace of mind to those same individuals.

Typically, contractors, partners, suppliers, and other part-time users only need access for short stints. Projects/assignments might vary, yet the hours and resources required to configure, manage, monitor, and deploy this access via a VPN are significant and constant. IT professionals are already taxed; by eliminating the burden of VPN and migrating remote access to the cloud, you will be saving the business time and money.

BOTTOM-LINE BUSINESS BENEFITS

SAVE TIME

Empower IT, security, and management teams to focus on higher-priority projects instead of monitoring and managing user access.

INCREASE PRODUCTIVITY

Eliminate inconsistent and poor-performing applications so that users can do their jobs faster.

SECURE DATA

Effectively monitor real-time activity to prevent loss of company data, customer information, and other intellectual property.

REDUCE COSTS

Decrease budget dollars spent on expensive hardware and installations, while minimizing loss from unexpected breaches.

3. STREAMLINED SECURITY POLICIES

Challenge: Digital Transformation Increases Risk Exposure

A "trust but verify" methodology is no longer a secure option given the sophistication of today's threats and the risk that unfettered cross-network access poses — 40% of breaches are linked to authorized users.[12] But access demands still climb in number, intricacy, device type, and origin point. Multiple VPN gateways can lead to multiple headaches for your IT team and your business in general, and a virtual private cloud (VPC) doesn't meet all your needs. Fragmented security policies are inevitable with VPNs or VPCs, and they will eventually increase your company's exposure due to ongoing routing environment complexities and manual deployment. It's no wonder that more than 50% of survey respondents agreed that all aspects of securing remote access are difficult.[13]

Solution: Adopt a Zero Trust Strategy

Nothing is truly internal anymore. Moving to a cloud-based model for enterprise IT and security simplifies back-end processes and makes applications invisible to the public, while also adding multi-factor authentication as an auxiliary layer to reduce risk. New applications can be stood up in mere minutes, saving hundreds, if not thousands, of IT and management hours per application. And when you need to set or adjust a policy, you can quickly and simply configure a new user without additional installations.

But the benefits of a zero trust strategy don't end there. Complete auditing and reporting of user activity will be at your fingertips on the back end as well. Whether those are built-in reports or integrated with your existing tools, you can customize them as you choose.

4. ERADICATION OF END-USER FRUSTRATIONS WITH SEAMLESS ACCESS

Challenge: Eliminate Unwieldy Processes

Successful organizations must keep ease of use in mind to ensure adoption and advocacy. If this is accomplished, users will welcome an end to slow servers, frequent service drops, sluggish onboarding processes, and general connectivity frustration. In turn, your IT security team will celebrate an end to cumbersome stacks and the ongoing maintenance of laboring hardware. And executives will appreciate the savings, the liberated bandwidth of senior IT resources, and the increased productivity of the workforce.

Solution: Adapt in the Cloud

Cloud-based solutions are the surest way to achieve seamless, universal access to customized applications, complete with preferred device compatibility and reduced management complexities. And data path protection, IAM, application security and acceleration, SSO, MFA, and more are easily and immediately integrated, managed, monitored, and updated through this cloud architecture. In today's increasingly competitive global market, this fast, simple, and secure solution is critical to the progression of your business and empowering the people who help make it a success.

CRITICAL STEPS TO VPN ELIMINATION

So, what are next steps to implement a worry-free remote access solution? New and innovative approaches are emerging every day, but first you must adopt an effective strategy based on a zero trust security philosophy. The best way to do so is to keep it simple:

- **DIFFERENTIATE YOUR DATA** between what is for public consumption and what you'd classify as sensitive information
- **IDENTIFY THE APPLICATION** and exactly who needs to access it.
- **SCALE AND DEPLOY APPLICATIONS** fronted by a globally distributed, identity-aware proxy platform across your public and private infrastructures to enable high-availability capabilities.
- **ADOPT CLOUD-BASED ARCHITECTURE** where everyone – even those in the home office who are considered "remote employees" – one and the same.
- **MONITOR, MONITOR, AND MONITOR** with MFA and SSO for every user and device while using real-time reporting to ensure every application is always secure.
- **OPTIONAL: IMPLEMENT NETWORK SEGMENTATION TECHNIQUES** that will compartmentalize east-west traffic within a subnet.

Conclusion

Global organizations are no longer bound by the inefficiencies and vulnerabilities of antiquated VPNs hosted in various data centers or hybrid cloud environments. Faster, simpler, and more secure solutions are available to lock down all inbound firewall ports while providing end users with remote access to only the specific applications they need. Gone are the days of unnecessary broad network-wide access.

It's time to separate your organization's infrastructure from the Internet. Minimize the attack surface. Hide applications from public Internet exposure. And deploy a modern, cloud-based solution in minutes as your first line of defense — all at a fraction of the cost of build-it-yourself substitutes.

To learn more about Akamai's zero trust methodology, our secure delivery model, and cloud-based access solutions, please visit akamai.com/eaa.

SOURCES
1) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
2) http://globalworkplaceanalytics.com/telecommuting-statistics
3) PGi Global Telework Survey, http://go.pgi.com/gen-genspec-15telesur-SC1129
4) http://globalworkplaceanalytics.com/telecommuting-statistics
5) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
6) https://www.upwork.com/press/2017/10/17/freelancing-in-america-2017
7) Deloitte Mergers and Acquisitons Trends report 2018, https://www.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-mergers-acquisitions-2018-trends-report.pdf
8) https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise
9) Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, https://www.ibm.com/security/data-breach
10) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
11) Ibid.
12) Ibid.
13) Ibid.

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 10/18.