WHITE PAPER

Application Access Redefined: Managing the Modern Workforce

Akamai

Executive Summary

The paradigm shift sweeping enterprise technology and business gets more palpable by the day. The transition to cloud computing is near its tipping point. Mergers and acquisitions have burgeoned. And with a growing number of end users outside the corporate environment, IT departments need to serve an increasingly diverse, distributed, and demanding user ecosystem.

Providing secure, application-specific access to enterprise systems and data has become more important than ever. And more challenging.

The traditional, centralized security stack (e.g., VPNs, RDPs, proxies) exposes organizations to risks, increases complexity, and causes performance issues. And integration challenges, when addressed through quick, short-term configurations, pull your IT resources away from forward-looking initiatives and compound technical debt.

This white paper:

- *Details how the workforce, business environment, and IT are changing*
- *Examines the challenges of delivering secure application access using existing technologies*
- *Discusses why a Zero Trust security architecture can minimize your attack surface in the modern IT environment*

With a cloud-based Zero Trust platform, delivered at the Edge, you can provide users with appropriate, intelligent, and adaptive access with the simplicity they demand – on the device of their choice, regardless of whether their device is in the enterprise's sphere of governance. At the same time, your organization can shrink its attack surface, and simplify user provisioning/deprovisioning, troubleshooting, management, and administration.

> *"Cloud computing is at a major inflection point in its evolution. While 20% of business processes have already moved to the cloud, 80% of mission-critical workloads and sensitive data are still running on on-premises business systems because of performance and regulatory requirements. In 2019, the percentage of these workloads running in the cloud will increase to over 40%…"*
>
> *– Roy Illsley, Distinguished Analyst, Ovum[1]*

Enterprises Must Find New Ways to Provide Application Access

Enterprises today face a massive disruption to the way they deliver IT services, the makeup of their workforce, and their corporate structures. They must provide a diverse user ecosystem with calibrated access to enterprise applications and data located both on premises and, increasingly, in the cloud. These new IT and workforce structures mean enterprises can no longer rely on existing perimeter-based application and data access architectures and solutions.

Legacy access solutions and "trust, but verify" adages are problematic. Traditional VPNs, proxies, and remote desktops innately require trust on the part of the enterprise: A user or device is verified, but once authorized, can access the entire network. The perimeter takes on the entire burden of security while users are implicitly trusted once inside. But applications, data, users, and devices have moved outside the traditional network perimeter. A perimeter-centric security framework is woefully insufficient.

And while users and devices requesting access to the corporate network should always be verified, they should also never be unilaterally trusted or granted full network access simply because they are inside the firewall. There's too much at stake. Organizations need a new access model that supports a Zero Trust framework.

Multiple forces are at work, each with implications to enterprise application and data security:

Evolving Technologies

Adoption of cloud-based solutions has reached critical mass. Organizations of all sizes and types benefit from the advantages of the cloud and the ability to use services anytime, anywhere, from any device, on a subscription basis. They are grateful not to pay high software license and maintenance fees, purchase hardware, or hire large IT staffs to perform system implementation, configuration, ongoing maintenance and administration, and upgrades.

> *73% of enterprises have at least one application or a portion of their enterprise computing infrastructure in the cloud."*[2]

At the same time, organizations have yet to abandon their on-premises solutions. The vast majority of organizations are using a hybrid, multi-cloud environment with a combination of on-premises, private cloud, and public cloud architectures, with best-in-class resources from different cloud vendors. Application access strategies need to keep pace.

Companies using legacy systems often backhaul cloud traffic over the WAN through a centralized security stack, then reroute it through direct connects or VPNs back to the IaaS and the Internet. This model degrades application and user experience, increases enterprise security risk, and drives up costs — especially as businesses duplicate their stacks across geographies and vendors. Organizations need access solutions that simplify and enable the technology stack to support adoption of cloud-based solutions.

A Changing Workforce

Decades have passed since individuals remained with a single company for the duration of their careers and worked from 9 AM to 5 PM within an organization's four walls. Many staffers are no longer even employees. Labor today is a mix of in-house and outside resources that work both onsite and remotely.

Workers are increasingly:

Mobile: *Workers are no longer confined to desks in offices. They connect to the corporate network from home, the airport, on a plane or train, while on vacation, at a hotel, from a coffee shop — wherever their lives or business may take them.*

Remote: *More employees are working remotely for a larger percentage of the work week. A 2018 study by IWG found that 70% of professionals telecommute at least one day a week while 53% work remotely for at least half of the week.[3] In fact, Glassdoor reports that a number of companies now have a 100% virtual workforce.[4] And this culture has become expected; many would not take a job that required them to wholly work from an office without a very significant pay raise.*

Contingent: *Many workers aren't employees at all. A 2018 study estimates that 56.7 million Americans freelance — an increase of 3.7 million in just the past five years.[5] These contingent workers enable businesses to scale and bring in specialized talent quickly to meet business goals.*

Third-Party: *Many organizations rely on a digital ecosystem of vendors, suppliers, partners, and even customers to deliver their goods and services. Some might be located in regions that pose an access or security challenge, such as China, while others might also work with an organization's competitor.*

All of these groups are considered enterprise users and need access to corporate applications and data, regardless of their location, the device they use, or whether they are within IT's zone of control. But organizations cannot afford to provide unrestricted access to such users once they're inside the network. They must only provide access to the specific applications and data necessary for a given job.

Demanding Users

Even as the workforce has become more diverse, the consumerization of IT has made end users more demanding.

The modern workforce increasingly blurs the line between their personal and professional lives. Users research, select, and purchase their own devices, and they expect to use these devices to access the enterprise's applications and data. Corporate devices and personal consumer electronics that connect to the corporate network are also used to access unmanaged online services such as web-based email, data storage platforms, collaboration and file sharing tools, instant messaging services, and social media networks – all outside of the control and visibility of IT teams.

Furthermore, workers expect corporate applications to deliver the same simple, convenient experiences that their consumer applications provide. To meet these user demands, IT must deliver seamless, efficient, and secure access to their applications and data, from any device, without enveloping the user in complex processes.

Mergers and Acquisitions

Businesses are scaling and pivoting rapidly. Mergers and acquisitions are increasing in the current corporate landscape. In fact, 79% of executives expect the number of deals to grow and the size of transactions to be larger in the coming year.[6] To enable and simplify these mergers and acquisitions, organizations must be empowered to quickly and easily consolidate their infrastructures. Cloud-based architectures and solutions make this growth and change possible, reducing complexity and costs rather than requiring drastic updates to IT stacks: hardware, software, network stacks, IAM platforms, user access configurations, and more. At the same time, organizations need to apply standard security controls to all existing and newly acquired assets.

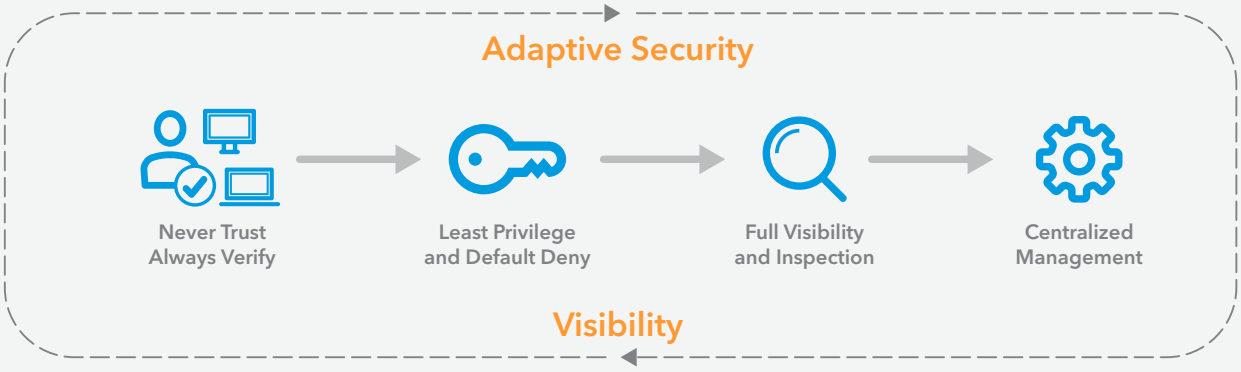
79% of executives believe the number and size of M&A transactions will increase next year.

The Need for a Zero Trust Security Architecture

As we've seen, an enterprise access solution must give every member of the workforce secure access to relevant enterprise applications and data, regardless of environmental factors. But owing to the diversity of your user ecosystem and the realities of today's threat landscape, that access can no longer be an all-or-nothing proposition.

While an executive should have permissions to access sensitive forecasts and plans, a third-party vendor or junior-level contractor should not. And if malware breaches external firewall defenses, the attacker should not be able to access systems and data across the organization. Your business must fine-tune control of applications and data.

Meeting the demands of modern access requires a Zero Trust security approach. Zero Trust implements a "verify and never trust" policy. It ensures that only authorized users and devices have access to the internal applications they need — and not to the entire network. Every access request is authenticated and authorized before applications or data are delivered, and this application-level access is transient. Unlike legacy systems such as traditional VPNs, a Zero Trust security framework controls all direct paths to applications.



The Limits of Traditional Access Control

Organizations often use VPNs and a variety of virtual or hardware appliances, such as load balancers, VPN concentrators, application delivery controllers, and proxies to control the workforce's access. Trying to provide access through this outdated centralized security stack is inefficient, exposes the enterprise to more threats due to integration challenges, and pulls IT resources away from forward-looking initiatives.

Businesses that rely on a perimeter to safeguard corporate applications are tempting fate; today's attackers are adept at penetrating the enterprise through hacking or social engineering. And stolen credentials allow easy entry for criminals. Once inside the network, they can take advantage of rules that place implicit trust in users based on location. Furthermore, traditional perimeter resources cannot protect users and devices that operate outside of the enterprise's zone of control or adequately secure cloud-based applications.

Traditional appliance-based firewalls and gateways were never designed with the cloud in mind. The lack of cloud-native security and access controls has caused IT teams to be very conservative about giving partners, suppliers, and customers — even employees — access to emerging cloud services. Doing so could mean providing broad, lateral network access.

These traditional access solutions present the following challenges:

Integration Complexity and Expense

Organizations need a stack consisting of many systems to support the VPN and deliver connectivity, onboarding, offboarding, and general monitoring. All of these components can be difficult to integrate. Businesses that use quick, easy, and makeshift configurations to perform short-term incorporation run the risk of requiring extensive — and costly — management and reintegration in the long run. Alternatively, they can invest upfront to configure a more cohesive stack that may remain operational longer, avoiding some technical debt — but ultimately, they have still sunk time and money into a security solution that inherently exposes the business to risk.

Moreover, in this scenario, each stack must be repeated for redundancy and high availability across regions and data centers. You must purchase, install, configure, and deploy each one of these components separately, in each locale, thus increasing capital and operating costs. To extend protection to cloud applications, organizations often backhaul cloud traffic over the WAN through a centralized security stack, only to reroute it through direct connects or VPNs, back to the IaaS and the Internet. In addition to further driving up complexity and cost, this degrades performance.

64%

of global IT budget increases will be spent upgrading outdated IT infrastructure.[7]

Time-Consuming Management

As the number of applications to be protected grows and the number of distributed, demanding users increases, management overhead swells. Administrators must spend more time managing their complex security stack in house, taking charge of ongoing monitoring, troubleshooting, patching, and upgrading. Each time they change the network or update a firewall rule, IT must battle a brittle network stack. And of course, IT resources are finite; time spent administering traditional, unwieldy access stacks distracts from other initiatives.

Poor User Experience

Traditional VPNs and other legacy technologies are subject to connectivity failures, latency, and timeouts, causing low adoption of applications and an influx of help desk tickets. Lack of seamless single sign-on (SSO) across all applications, including SaaS, frustrates users and hinders productivity as individuals reenter passwords. When disjointed authentication and authorization processes erroneously deny users access, both the users and IT teams are sidelined troubleshooting, or the users seek workarounds, potentially exposing the enterprise to additional risk.

Poor Security

By their very nature, traditional VPNs put a hole in the network firewall. They were designed primarily to connect an organization's internal infrastructure through external, untrusted networks – not for corporate security and privacy. They typically provide unfettered network access. So, when a breach occurs, attackers can move laterally to access applications and data beyond what organizational policies might deem admissible.

Furthermore, traditional VPNs lack intelligence. They're often unable to provide a continuously adaptive go/no go based on multi-factor authentication (MFA). Rather, they look at whether the user credentials are correct or incorrect. And VPNs can't check device posture, so they are unable to confirm that the device adheres to health standards before allowing it to connect to the network.

Device posture must be validated before access is granted.

What to Look for in a Solution

Organizations need an access solution that scales frictionlessly and can be configured and deployed quickly. A cloud-based solution delivered at the Edge is a natural fit. It should easily integrate with other security solutions and deliver a simple-to-use, consistent user experience. Additionally, a modern access solution must reduce security risk, provide visibility into network activity, and simplify ongoing management and administration.

Security as a Service Delivered at the Edge

A cloud-native solution that closes all inbound firewall ports and has a single point of control will isolate all applications from the Internet and public exposure. When security capabilities are delivered at the Edge, they not only scale, but are closer to users than a centralized cloud solution. This mitigates threats nearer to their origin point, improving end-user performance and security.

This security functionality should use a mutually authenticated Transport Layer Security (TLS) connection from within your data center or cloud to bring permitted applications directly to the user — without insecure tunnels or a clear path for malware to infiltrate. Users should be permitted to access applications using any browser and their device of choice.

Cloud deployment means your organization no longer needs to install a complex stack of equipment to protect each data center or backhaul traffic to a central location for authentication. You can simply use a single service in the cloud to secure all your applications, data, users, and devices. This streamlines operations so you can do more with your existing IT resources.

Simple Integration with Other Security Solutions

To enhance security while providing access, the solution should collapse the access technology stack into a single service that offers data path protection, SSO, identity and access management, application security, visibility, and administration. Such an integrated solution eliminates the need to install and maintain a complex amalgamation of equipment to secure each data center. It also enables users to access applications from any device without additional software, such as VPNs and browser plug-ins.

Seamless SSO and MFA, as well as a consistent user interface, will help to meet the demands of the modern workforce.

Ease of Use and a Consistent User Experience

When dealing with demanding users, you must remove unwieldy processes. Look for a solution that eliminates multiple passwords and provides application access through a single web portal. Users should have seamless SSO to all applications they require, on any device, from anywhere. You should also have the option to deploy simple, convenient MFA to strengthen security without requiring users to recall and reenter labyrinthine credentials. An easy-to-use solution with a consistent user interface will accelerate time to user productivity and increase application adoption while also reducing help desk tickets.

Reduce Security Risk

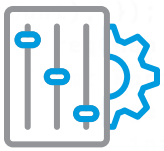
The application access each user needs is typically a fraction of what a legacy VPN actually grants. This extraneous access creates considerable preventable peril. Making matters worse, users rarely access the network from just one device, which further expands the attack surface.

The solution should not only authenticate and authorize the individual requesting access to each application, but also the device and the context in which they're requesting that access. The solution should first lock down the firewall or security group to all inbound traffic and make application IP addresses invisible to the Internet. MFA should then ensure the identity of each user/device, and device posture of the endpoint should be validated. Finally, trust should continually be assessed based on identity, device, and contextual signals such as location, time of day, authentication state, group membership of the user, and so on. These methods significantly lower your organization's security risks by minimizing the attack surface.

Improve Visibility

Your organization needs to know who is accessing your network and when. This simplifies the identification of real threats and reduces false positives that consume already strained security resources. The management portal should provide visibility by giving IT a single location where they can access detailed audit, control, and compliance reports, or it should integrate with your existing security information and event management (SIEM) tools.

80%



of IT professionals report that they spend half their time reworking software projects.[8]

Simplify Ongoing Management and Administration

The ideal solution reduces the load on IT, giving them time for other strategic initiatives. To this end, device-agnostic access eliminates the need for IT to install additional software, including VPNs and browser plug-ins. Optimized authentication and authorization processes for users and devices through seamless SSO and MFA can minimize help desk requests around forgotten passwords, locked devices, or application access issues. Improved network visibility accelerates the identification of real threats and reduces false positives. These capabilities all help IT respond more rapidly to security incidents.

Speed User Provisioning and Deprovisioning

Every day, enterprises must provide their diverse user ecosystem with very specific application access. Additionally, organizations undergoing mergers and acquisitions need to quickly onboard large groups of users to their existing and newly acquired assets while ensuring adequate security controls.

To reduce the burden on IT, a solution should allow security practitioners to stand up new applications and provision users in minutes through a single web portal, without changes to network attributes such as firewall rules or IP address whitelists.

The solution should empower IT to simply and quickly set policies that bind users to specific applications and devices without making hardware upgrades and laborious blanket changes to the network. To provide optimal security, policies should consider environmental factors (location, time of day, etc.), as well as device posture (i.e., whether antivirus protection is current, or endpoint detection and response ([EDR]/endpoint protection platform [EPP] technologies are employed). Simple user provisioning and deprovisioning eliminates the burdens of implementing all hardware and software components required for provisioning access to a VPN.

Conclusion

As organizations evolve their application platforms and workforce — and their very structure — they need an access solution that keeps pace. Enterprises can no longer afford to give all authenticated users the run of the network.

A Zero Trust security architecture operating at the Edge can provide your diverse, distributed, and demanding workforce with correctly calibrated access, as well as a convenient and streamlined user experience — on any device, from any location, inside or outside of IT's sphere of control. And because the solution minimizes help desk tickets, simplifies user provisioning/deprovisioning, speeds threat identification, and simplifies ongoing management and administration, IT will have more time for forward-looking strategic initiatives.

To learn more about securing application access in the modern enterprise and how Akamai's cloud-based solution delivered at the Edge can help, visit akamai.com/eaa.

Learn More

SOURCES

1) https://www.prnewswire.com/news-releases/ibm-unveils-worlds-first-multicloud-management-technology-300731206.html
2) https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/
3) https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html
4) https://www.glassdoor.com/blog/100-percent-remote-companies/
5) https://www.slideshare.net/upwork/freelancing-in-america-2018-120288770/1
6) https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-mna-trends-report-2019-us-dealmaker-optimism-hits-three-year-high.html
7) https://www.spiceworks.com/marketing/state-of-it/report/
8) https://www.geneca.com/why-up-to-75-of-software-projects-will-fail/