5 Reasons Enterprises Need a New Application Access Model

Executive Summary

To thrive in today's competitive corporate environment, enterprises must deliver services and experiences that are innovative, effective, agile, and secure. Digital transformation, and the technologies that enable it, are central to this evolution. The most successful companies continuously evaluate and refine their technology stack to best enable their organization's imperatives and retain their market share.

Why then do so many companies rely on technologies that are antiquated, complex, and most importantly, insecure, for application access?

Legacy application access solutions such as traditional VPNs, proxies, and remote desktops innately require trust on the part of the enterprise. A user or device must be verified, but once authorized, that user or device can access the entire network. The onus of security is placed on a perimeter that allows for implicit trust once inside.

But this framework is no longer viable because most contemporary businesses have users, devices, applications, and data outside of the traditional network perimeter. And while users and devices requesting access to the corporate network should still always be verified, they should also never be unilaterally trusted nor granted full network access simply as a result of their "inside" locale.

A new application access model that supports a Zero Trust framework is needed for this business landscape. This adoption is critical and urgent because of five modern realities:

1. An increasingly hostile threat landscape
2. The speed and scale of business
3. A widening and increasingly distributed ecosystem
4. The cloudification and SaaSification of corporate applications
5. The IT skills shortage

1 Cybercrime Is on the Rise and Unlikely to Slow Down

Worldwide, cybercrime is estimated to cost $600 billion a year, up $100 billion since 2014.[1] Malicious actors are increasingly patient and persistent — and highly monetarily incentivized. Attacks are customized and targeted at specific companies. And the threats themselves are widely available for purchase through growing cybercrime-as-a-service schemes. Additionally, there is little deterrence for cybercriminals as utilization of anonymous browsers and cryptocurrency is prevalent, and international response remains disjointed.

Daily, more than 350,000 new malicious programs are registered[2] and computer and Internet users face 80 billion malicious scans.[3] And, in just the first half of 2018, a total of 3,353,172,708 records were compromised, up 72% from H1 2017.[4] But perhaps most startling is the fact that more than 40% of security breaches are linked to authorized users.[5]

The consequences for compromised companies are growing as well. 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.[6] According to 90% of CEOs, rebuilding trust among stakeholders after a breach is one of the most difficult tasks to achieve, and over 70% of businesses that experiencea major incident either do not reopen or fail within three years.[7] No vertical is off limits — global titans of industry, as well as governments and military forces, have all experienced crippling assaults in the last several years.

MORE THAN

40%

of security breaches are linked to authorized users

OVER

70%

of businesses that experience a major incident either do not reopen or fail within

3 years

Given these facts, not using every means available to shore up your enterprise's security posture is simply irresponsible. But traditional access solutions such as VPNs, proxies, and remote desktops were designed to punch a hole in the network firewall, typically providing unrestricted network access. This is highly problematic for today's business models.

In the event of a breach, this access allows lateral movement and permits access to applications and data beyond those authorized per the user credentials. These legacy access technologies also lack intelligence and detailed logging. They can't accurately confirm or validate the identities of those who are trying to access specific applications. Nor do traditional VPNs integrate with other security mechanisms such as data path protection, application security and acceleration, and single sign-on (SSO).

As cybercrime continues to proliferate and access requirements expand to broader user groups, like contractors and partners, a new application access model that supports a Zero Trust security framework is essential. Providing application versus network access, as well as authentication and authorization of all requests is imperative; unilateral network-level permissions must be superseded by case-by-case, custom, application-level access.

2 The Speed and Scale of Business Are Unprecedented

Everything is getting faster; thus the importance of speed as a means to the success of a business cannot be overstated in today's climate. Your customers and employees expect it and every one of your competitors is striving for it. Leaders across all industries are therefore charged with driving their organizations to greater agility by removing hurdles to progress, empowering their workforce, encouraging productivity, and balancing infrastructure needs with low overhead costs.

2018 had the second-highest global value for M&A on record:

$2.72 trillion

across 13,575 deals

In addition to an overarching focus on improving time to market, businesses are scaling and pivoting rapidly. Mergers and acquisitions are commonplace in today's corporate landscape. In fact, 2018 had the second-highest global value for M&A on record: $2.72 trillion across 13,575 deals.[8] And according to Deloitte's 2019 M&A Trends report, continued acceleration of these activities is projected, as is an increase in deal size.[9] Simultaneously, divestitures will persist, with 80% of respondents stating plans to sell assets in the coming year.[10]

Given these realities, application access solutions must be efficient, convenient, and scalable. Yet outdated access technologies hardly meet these requirements, often consisting of cumbersome and cobbled-together hardware and software. As a result of these fragmented architectures, provisioning and deprovisioning access, especially to large groups of users, is time consuming and complicated for IT. From an end-user perspective, it often results in connectivity failures, latency, and timeouts, causing frustrating low adoption of applications and an influx of help desk tickets.

Poorly integrated solutions also hold up time to market; the business pauses while IT battles a fragile and brittle network stack each time a network change or firewall rule update is needed. This wastes business resources and depreciates productivity. The lack of a seamless single sign-on experience also frustrates users and waylays progress as individuals re-enter passwords and troubleshoot with IT. And erroneous access denials, as a result of disjointed authentication and authorization measures, add to corporate deceleration.

Additionally, onboarding and decommissioning via traditional access models can mean configuring or dismantling more than 10 network and application components per user.[11] And some IT departments with legacy application access solutions physically send hardware to third parties in an effort to strengthen security controls. This is a painstakingly slow process.

As the pace of innovation and disruption continues to ramp, an updated and cloud-based application access model that delivers immediacy, performance, convenience, and flexibility is critical. An enterprise's technologies and infrastructure must be able to fluctuate, transition, and keep stride with the demands of doing business today.

3 Ecosystems Are Growing Wider and More Distributed

The composition of today's workforce is varied. Enterprises increasingly rely on contractors, partners, suppliers, developers, distribution channels, and other third-party entities to support their initiatives. In fact, salaried employees are the majority at only 42% of organizations, and globally, there are 77 million freelancers — that's a 36% increase in just the past five years.[12] This trend is only expected to become more prominent in the coming decade.[13]

Not only is the ecosystem diverse, but it is mobile and globally dispersed. The majority of organizations now empower their employees to work remotely. The non-self-employed, work-at-home population has grown by 140% since 2005, and employees are not at their desks 50–60% of the time[14] — a trend that will likely continue to propagate as knowledge workers are more productive, motivated, and loyal to their company if given the option to work remotely.[15]

The non-self-employed, work-at-home population has grown by

140%

since 2005

Employees are not at their desks

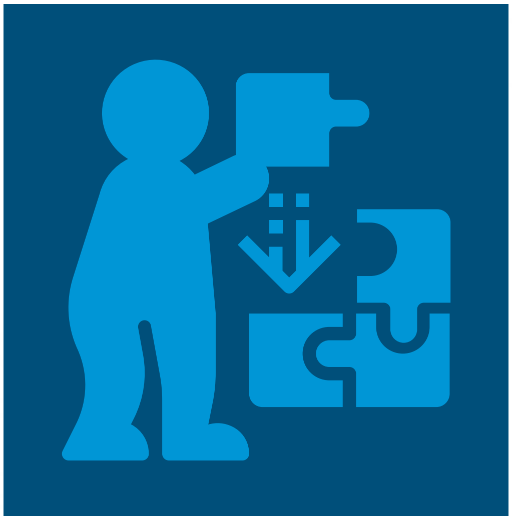
50–60%

of the time

And of course, in today's hyperconnected world, businesses have branches and satellite offices as well as individual remote workers physically spread all over the globe. As if a dynamic and distributed workforce ecosystem doesn't sufficiently complicate access, these constituents are connecting to the corporate network via an increasing number of devices — desktop computers, laptops, mobile phones, tablets, and BYOD (bring your own device). These trends demand more permeable and accessible infrastructure.

Access technologies must be able to provide calibrated application access to any user, in any location, on any device — without compromising security. Traditional application access models fall short. Outdated access solutions also allow unfettered lateral movement, meaning that once a malicious actor gets on to the corporate network, he or she can move about unhindered and easily steal material. And legacy technologies often provide one-tiered, blanket access to the network, bluntly disclosing information and operations regardless of user needs, affiliation, department, or seniority. This means that an executive and a third-party HVAC repairman might be privy to the same corporate applications and data.

Configuration, deployment, and decommissioning of antiquated access architecture to this mobile, diverse, and ever-evolving workforce requires hours of IT attention — providing VPN or VDI and a variety of other solutions, including client-side hardware and/or software, security, IAM, and policy-related configuration. As previously discussed, IT might even mail hardware pre-loaded with access requirements to remote and third-party users for an added layer of security, but this is also inefficient and impractical. And replicating network and security stacks across multiple environments and geographies to support a global workforce is complex and often prohibitively expensive. Additionally, legacy access technologies can't easily integrate with the plethora of device types used by today's workforce.



Given the variety of users and access points, the prevalence of third-party employees, and the rate of attrition, this access onboarding and offboarding is a massive resource sink and untenable in the long run. As modern employee ecosystems continue to expand and scatter, a new application access model that accommodates open business infrastructure as well as increased identity awareness is imperative. A Zero Trust security architecture that provides case-by-case validation and access is the path forward.

4 Cloud Migration and the SaaSification of Enterprise Applications Will Perpetuate

Corporate applications are increasingly distributed, accessed on premises and in the cloud for business-critical operations. While on-premises infrastructure will endure, it's also true that there hasn't been an on-premises software company funded in the last decade.[16] Cloud is front and center — and the popularity of cloud applications is only climbing. The average business uses more than 1,427 distinct cloud services, with the average employee actively using more than 36 at work daily.[17] And in the public cloud market, software as a service (SaaS) is king.

BY 2020

the SaaS market is projected to reach

$76 billion

Fifty-nine percent of all cloud workflows will be delivered as SaaS by the end of 2018.[18] Companies use 16 SaaS applications on average today, and by 2020, the SaaS market is projected to reach $76 billion, with 73% of organizations using almost exclusively SaaS applications.[19] This makes sense when you consider that, as consumers, we live in a SaaS world. Witness LinkedIn, Facebook, Instagram, and Uber — applications that can be readily accessed on any device, anywhere, with high performance. Enterprise users want the same experience when accessing their corporate applications: simple and unified access from any location, on the device of their choosing, with no VPN or client software required.

While this trend is well underway — led by Salesforce.com, Microsoft Office 365, Box, Amazon Web Services, Slack, Google G Suite, and others — delivering this SaaS experience in an enterprise environment is far easier said than done. Traditional corporate network architectures and the castle-and-moat security frameworks they utilize aren't amenable for today's cloud-first world.

To cope with the shifting landscape, many companies rely on the previously mentioned cobbled-together hardware and software appliances to provide enterprise network access. They backhaul cloud traffic over the WAN through a centralized security stack, only to reroute it through direct connects or VPNs back to infrastructure as a service (IaaS) and the Internet. This is complex and expensive to duplicate globally, across different environments and geographies. This model also degrades application performance and user experience, and drives up overhead and associated costs.

But most significantly, traditional access models increase the enterprise's attack surface, exposing users, devices, and applications to the security risks inherent to the public Internet. In response to these vulnerabilities and inefficiencies, companies have had to front-end their applications with Internet-scale protections from DDoS attacks, add acceleration to mitigate performance and latency issues, and add specific application-layer attack protections. These one-off, piecemeal approaches simply don't make operational or financial sense. A new application access model is needed — one that is cloud-based and provides users with a simple and convenient application interface, while also shoring up the enterprise's security posture through adaptive, identity-aware access.

5 IT Resources Are Increasingly Strained

Currently, there is a global shortage of 2.9 million cybersecurity professionals.[20] In a recent survey, 70% of organizations reported that this shortage was negatively impacting their business.[21] And while the number of qualified security practitioners dwindles, the demand for this skill set climbs as a result of the prevalence and sophistication of cyberthreats. Many attribute this gulf to a steady decline in the study of science, technology, engineering, and mathematics (STEM); despite a significant effort spent promoting STEM education in the past several years, its popularity continues to wane.[22]

global shortage of 2.9 million cybersecurity professionals

70% **of organizations reported that this shortage was negatively impacting their business**

BY 2021

the number of unfilled security jobs will swell to

3.5 million

It is projected that by 2021, the number of unfilled security jobs will swell to 3.5 million.[23] To manage this trend, business leaders must strive to empower and enable their IT resources to be hyperefficient. But the dearth of security practitioners is not uniquely an issue of STEM graduate volume. The reality is that there are challenging internal operational factors at play that enterprise executives must address: IT and security experts are being sidelined, kept from critical and future-looking enterprise imperatives, as well as innovative strategy and training efforts, by security incidents precipitated by aging and poorly integrated technology stacks, including legacy access solutions.

Antiquated application access models and their laborious, cumbersome technology require significant and continuous IT bandwidth. Supporting these broken access models monopolizes IT resources, and it's often a matter of hours, if not days, that are required to provision and/or decommission a single user or device, as well as to handle basic maintenance and system updates. Legacy application access solutions also make auditing complex or nearly impossible as they often fail to provide IT with visibility or aggregated reporting of network access and activity.

Increasingly, IT is bombarded by help desk requests as a result of fragmented sign-on experiences and erroneous access denials — forgotten passwords, locked devices and applications, and permission requests from users missing what should be templated access per their role. This lack of unified access also causes increased password fatigue and motivates users to adopt dangerous security habits — reusing passwords, using weak passwords, or writing down their credentials — further limiting IT's ability to limit and secure network access.

Unfortunately, the majority of these frustrations consume the most senior of IT resources given the number and intricacy of overlaid and interdependent systems, further distracting the most capable security professionals from strategic and revenue-impacting initiatives.

As the rift between available cybersecurity professionals and demand continues to expand, an updated and cloud-based application access model is needed to provide immediate, secure, and simple access through a unified and easy-to-manage portal. A solution that enables painless implementation of remote restrictions for tailor-made application access will free up valuable IT resources and have business-wide impact.

The New Application Access Model

It's now clear that, in order to address these five modern realities, enterprises need a new architecture for providing access to their corporate applications. This new model must meet today's challenges by:

1. Eliminating dependencies on the infrastructure between the user and corporate resources while also integrating data path protection, identity and access management (IAM), application security and acceleration, single sign-on (SSO), and other advanced security measures.

2. Moving to a model where access is agile, locale- and device-independent, and transient.

3. Separating and isolating access to the underlying network and providing access to only the applications that users need to get their work done.

4. Meeting the high-performance and simple UX expectations of users, delivering enterprise applications via a SaaS model.

5. Enabling IT to easily and quickly provision identity-aware access, freeing up valuable corporate cybersecurity resources.

Access must be agile, flexible, scalable, and adaptable — and most importantly, it can't come at the cost of security. A cloud-based access solution is the answer, combining intelligence into decision making and examining users, devices, and locations, as well as patterns of access, at each and every request.

To learn about Akamai's solution for simple, unified, and secure enterprise application access, visit akamai.com/eaa.

Sources

1) McAfee 2018 Report: Economic Impact of Cybercrime, No Slowing Down, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&

2) https://www.av-test.org/en/statistics/malware/

3) McAfee 2018 Report: Economic Impact of Cybercrime, No Slowing Down, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&

4) https://breachlevelindex.com/

5) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf

6) Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, https://www.ibm.com/security/data-breach

7) https://dataconomy.com/2018/03/12-scenarios-of-data-breaches/

8) https://www.forbes.com/sites/suntrust/2018/12/06/the-5-biggest-trends-in-mergers--acquisitions-for-2019/#73056e321ca1

9) Deloitte 2019 Report: Mergers and Acquisitions Trends, https://www2.deloitte.com/us/en/pages/mergers-and-acquisitions/articles/ma-trends-report.html

10) Ibid.

11) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf

12) https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2018/contingent-workforce-management.html

13) https://www.upwork.com/press/2017/10/17/freelancing-in-america-2017

14) http://globalworkplaceanalytics.com/telecommuting-statistics

15) https://www.ciphr.com/advice/10-essential-remote-working-statistics/

16) https://searchcloudcomputing.techtarget.com/feature/SaaS-apps-reshaping-face-of-enterprise-IT

17) https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/

18) https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#cloud-forecast

19) https://www.bettercloud.com/monitor/state-of-the-saas-powered-workplace-report/

20) https://www.isc2.org/

21) https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse

22) http://www.govtech.com/education/k-12/New-Research-Shows-Declining-Interest-in-STEM.html

23) https://cybersecurityventures.com/cybersecurity-market-report/

Akamai

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7/365 monitoring. To learn why the top financial institutions, online retail leaders, media and entertainment providers, and government organizations trust Akamai, please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. Published 02/19.