USE CASE

REDEFINE APPLICATION ACCESS TO SIMPLIFY Mergers AND ACQUISITIONS

EXECUTIVE SUMMARY

Businesses are scaling and pivoting rapidly.
Worldwide, over 50,000 mergers and acquisitions (M&A) take place each year. As the speed at which enterprises operate and execute often dictates success in today’s ultracompetitive corporate environment, it is imperative that efficient integration and swift return on investment (ROI) are realized after such transactions.

This poses a challenging task for IT: How to realize this from an infrastructure and application access perspective, without impacting end-user productivity, without increasing complexity and technical debt, and – most important – without compromising enterprise security?

Historically, given the difficulty of achieving intercompany communication, many organizations granted application access unilaterally to streamline this one component of integration. As a result, trust in users and devices was afforded simply by virtue of location – a risky precedent. While we’ve moved beyond putting users and devices directly on the internal corporate LAN, most other corporate network best practices have not sufficiently evolved.

Many modern organizations continue to rely on ill-suited legacy access technologies — virtual private networks (VPNs), remote desktop protocols (RDPs), and proxies — as well as multiple identity stores, all cobbled together into an intricate and temperamental infrastructure. On its best day, this outdated and brittle framework likely can’t deliver secure, granular, and authenticated application access. When asked to quickly scale, to configure an expanding workforce with corporate application access after a merger or acquisition – or expediently decommission access in the case of a divestiture – this jumble of technologies will fall short.

WHAT’S THE URGENCY?

Integration at speed is paramount to a deal’s success.
Companies that can’t coalesce efficiently are vulnerable, both financially and competitively. It’s critical that IT enables this velocity. Yet configuring, deploying, and decommissioning antiquated access architecture to a previously unknown, untrusted, and fluid workforce requires days and often months of IT attention.

IT teams need to provide VPN or virtual desktop infrastructure (VDI) and a variety of other solutions, including client-side hardware and/or software, security, identity access management (IAM), and policy-related configuration. Onboarding and decommissioning, via traditional access models, can mean configuring or dismantling more than 10 network and application components per user.1

Faced with this, IT might try replicating network, identity, and security stacks across multiple environments and geographies to support the new workforce. But this is increasingly complex and often prohibitively expensive in terms of effort and required upgrades. To provide some semblance of limited access control, IT might physically mail hardware preloaded with access requirements to the new users. But this is inefficient and impractical, often resulting in employees using multiple laptops and systems.

A sizeable number of M&A transactions fall short of achieving the results initially envisioned.2
At best, this approach frustrates new employees or hinders their productivity with availability and performance issues, as well as consumes IT resources. At worst, access retrofitted by legacy technology will expose the enterprise to a security breach – during a critical and vulnerable moment. Even after 2018 saw the second-highest global value for M&A on record, projections call for an increase in both the number and size of these deals. Facilitating and securing these transactions is vital for enterprise success.

We must redefine the application access model to simplify and facilitate – even accelerate – M&A while securing the business against modern threats with a Zero Trust security strategy. Instead of placing users on the network and delivering workloads via a VPN or other legacy services, IT teams must leverage a cloud-native and simple adaptive access solution delivered at the edge to support successful M&A.

**THE SOLUTION**

Secure and scalable access as a service.

At Akamai, we believe that services to provide access to modern corporate applications – that largely reside in the cloud – should be born in the cloud and delivered at the edge, without ever exposing the application to the threats inherent to the open Internet. Akamai Enterprise Application Access is a cloud-based solution that helps IT teams provision and protect application access with a single set of security and access controls.

Akamai’s solution is designed to simplify management and allow IT to scale finite resources to meet the demands of the business in any environment. Enterprise Application Access enables IT to stand up new applications and users in a matter of minutes through a single portal. The technology supports modern web and legacy thick client applications, making access fast and intuitive for end users. And it reduces support calls for poor application performance, VPN connectivity issues, or device incompatibilities.

Enterprise Application Access also supports multi-factor authentication while enabling adaptive access based on device posture and other security signals. It integrates data path protection, single sign-on, identity, application access, and management visibility and control into a single service across all application types (on-premises, IaaS, and SaaS).

Better still, Akamai Enterprise Application Access enables IT to embrace a Zero Trust security strategy. It is architected to ensure that only authorized users and devices have access to applications. Upon providing user identity and authentication, it grants permissions on a per-application basis to only those applications the user needs. No network-level access. With Enterprise Application Access, IT teams can close inbound firewall ports and isolate applications from the Internet and public exposure. There is no direct path into your applications. The solution only ever dials out through a secure, mutually authenticated TLS connection from within your cloud or on-premises environment to the Akamai Intelligent Edge.

Furthermore, Akamai’s Identity-Aware Proxy architecture enables proven application acceleration, empowering enterprises to overcome the challenge of delivering business applications over the Internet to, say, a newly acquired branch location. It does this by placing application delivery capabilities within the Akamai Intelligent Edge Platform – closer to users, the cloud, and on-premises workloads. Anywhere in the world.

Learn how Akamai Enterprise Application Access can reduce complexity and accelerate integration, empowering IT to deliver M&A success. Visit [akamai.com/eaa](https://akamai.com/eaa) to learn more and get a free trial.
SOURCES
3) Ibid.
4) 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 06/19.