

# SECURE ACCESS TO ENTERPRISE APPLICATIONS IN THE CLOUD

## EXECUTIVE SUMMARY

Enterprise applications are evolving to match the realities of modern businesses.

For the majority of organizations, this means a transition to the cloud. But as workloads move outside of the enterprise's traditional sphere of control, there are risks to consider. Whether using a lift and shift approach to an infrastructure as a service (IaaS) environment, or the ability to consume the required functionality as software as a service (SaaS), the question remains the same. How should security and IT teams provide access to cloud applications without losing control and exposing them to the dangers of the public Internet?

## THE CHALLENGE

### Applications are moving to the cloud, but what about access controls?

While some enterprise workloads will continue to remain on-premises, an increasing number of corporate applications are migrating to the cloud. In fact, IDG reports that 73% of enterprises have at least one application or a portion of their computing infrastructure in the cloud.<sup>1</sup> And by 2020, it's projected that 83% of all workloads will be in the cloud.<sup>2</sup> Clearly, adoption of cloud-based applications has hit critical mass.



The global cloud computing market will exceed \$278 billion in 2021, up from \$145 billion in 2017.<sup>3</sup>

Organizations of all sizes and types are hooked on the cloud's advantages of simple, scalable infrastructure or application functionality for a low monthly subscription. Moreover, they are grateful to not have to pay high software license and maintenance fees, purchase hardware, or hire large IT teams to perform system implementation, configuration, ongoing maintenance and administration, and upgrades.

But how is access to these cloud applications being managed?

One option for IaaS applications is to build out a private network connection to the appropriate cloud provider and application. Companies using legacy architectures often backhaul cloud traffic over the WAN through a centralized security stack, then reroute it through direct connections or VPNs, back to the IaaS provider. 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 the technology stack to support adoption of cloud-based solutions.

Another option for application access is to use virtualized appliances in the IaaS environment. However, organizations have found that trying to piece together traditional appliance-based access controls that were never designed with the cloud in mind usually results in increased complexity, cost, and overhead, as well as a lack of agility.



The third access option is to expose the SaaS or corporate IaaS application on the Internet. This is the path with the highest inherent risk, requiring the same protections afforded to hardened public-facing web applications. It also demands expanded resources to actively manage an application that is vulnerable on the open and often hostile Internet.

None of the options outlined above are ideal from a visibility, user experience, and security perspective. Internal applications exposed to the Internet generally represent a risk profile that few organizations are willing to accept. Direct connections and virtual appliances are often complex, result in poor user experiences, and are expensive to deploy and maintain. A different approach is clearly needed: Instead of 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 applications in the cloud.

### THE SOLUTION

## Secure access as a service.

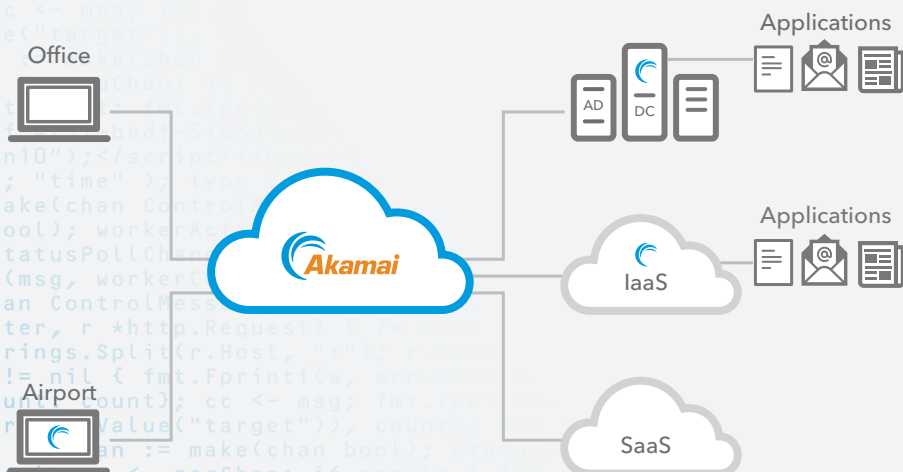
At Akamai, we believe that services to provide access to applications that reside in the cloud should be born in the cloud and delivered at the Edge – without ever exposing the application to the threats intrinsic to the open Internet. Akamai Enterprise Application Access is a cloud-based solution that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

Akamai's solution is architected to ensure that only authorized users and devices have access to cloud applications. No one can access applications directly because they are hidden from the Internet and public exposure. Enterprise Application Access is designed to minimize risk and allow IT to scale finite resources to meet the demands of the business in any environment, enabling IT to stand up new applications and users in a matter of minutes through a single portal. The technology supports clientless and client-required applications, making access fast and intuitive for end users. And it reduces support calls for poor application performance, VPN connectivity issues, and device incompatibilities.



There's a reason that Gartner Research published a report titled "It's Time to Isolate Your Services From the Internet Cesspool."

## Adaptive Application Access Through an Identity-Aware Proxy at the Edge



- **Inline application access**
  - Client and clientless
  - On-premises and IaaS
- **Identity**
  - Akamai, on-premises, or cloud-based identity stores
- **Single sign-on**
  - On-premises, IaaS, and SaaS
- **Multi-factor authentication**
  - Email, SMS, TOTP, or Duo Security
- **Application performance and security**
  - Akamai web application firewall and application acceleration




Enterprise Application Access supports multi-factor authentication while enabling adaptive access based on device posture and other security signals. It allows for insertion of data path protection, identity, application access, and management visibility and control into a single service across all application types (on-premises, IaaS, and SaaS). The technology also integrates single sign-on (SSO), supporting a wide range of SaaS applications and a number of virtual environments such as Amazon Web Services (AWS) EC2/VPC, Docker, Google Compute Engine, Microsoft Azure/Hyper-V, OpenStack, and VMware. To facilitate deployment across various environments, Akamai provides prepackaged connectors such as an Amazon Machine Image (AMI) to deploy in your AWS environment.

Better still, Akamai Enterprise Application Access enables IT to embrace a Zero Trust security strategy for critical workloads deployed in any environment, including IaaS. Upon providing user identity and authentication, it grants permissions on a per-application basis to only those cloud applications that 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. The solution only ever dials out through a secure, mutually authenticated transport layer security (TLS) connection from within your cloud environment to the Akamai Intelligent Edge Platform.

All user connections are inspected at the Edge and terminated on Akamai's globally distributed identity-aware proxies (IAPs), enabling the insertion of additional application performance and security controls. Specifically, Akamai provides broad protection for corporate web applications against the largest and most sophisticated DDoS and web application attacks. Our web application firewall includes robust security protections for websites, updated by the industry's best threat research team, to help organizations keep up with ever-evolving security threats.

Furthermore, Akamai's IAP architecture enables enterprises to deliver applications that are fast, reliable, and secure using Akamai's proven application acceleration solutions. This empowers enterprises to overcome the challenges related to delivering business applications over the Internet by placing application delivery capabilities within the Akamai Intelligent Edge Platform – closer to users, the cloud, and on-premises workloads. Anywhere in the world.



Visit [akamai.com/eea](https://www.akamai.com/eea) to learn more about Akamai's Enterprise Application Access solution and how it can help you accelerate, simplify, and secure your application migration to the cloud.

#### SOURCES

- 1) <https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/>
- 2) <https://www.forbes.com/sites/louiscolombus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#260d54656261>
- 3) <https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019>



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](https://www.akamai.com), [blogs.akamai.com](https://blogs.akamai.com), or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at [www.akamai.com/locations](https://www.akamai.com/locations). Published 06/19.