Edge Delivery Services
powered by Akamai

Enterprise Application Access

Secure, Simple, and Fast Application Access

Providing employees with secure access to enterprise applications deployed behind the firewall is a core requirement for all businesses. Enterprises must also deal with the riskier proposition of providing access to a varied list of contractors, suppliers, partners, customers, and developers. Regardless of where these applications are hosted — whether in a public cloud or private data center — this is a complex, cumbersome task requiring on-premise hardware and software such as application delivery controllers (ADC), virtual private networks (VPN), identity and access management (IAM) systems, and more. Yet with all of these technologies, enterprises are still exposed to a variety of security risks stemming from the fact that access to internal applications opens up the entire network to attack. Our Enterprise Application Access (EAA) solution solves these problems, helping businesses transform application access to meet today's mobile- and cloud-centric requirements while improving their overall security posture.

Enterprise Application Access

Enterprise Application Access provides a simple, secure, and fast alternative to traditional access technologies such as VPN, remote desktop protocol (RDP), and proxies. With Enterprise Application Access, applications are hidden from the Internet and public exposure. It enables a zero trust architecture by closing all inbound firewall ports, while also providing identity and authentication for users so that permissions are granted to only those specific applications required by a given role, versus full network access.

Enterprise Application Access integrates data path protection, IAM, application security, seamless single sign-on (SSO), and management visibility and control into a unified service across all application types (on-premise, IaaS, and SaaS). It can be deployed and stand up new applications and users in a matter of minutes through a unified portal, at a fraction of the cost of traditional solutions. The result is a secure-access delivery model that enables a zero trust framework for critical workloads deployed in any environment.

How It Works

Enterprise Application Access provides secure access-as-a-service that eliminates the need to punch holes in the network perimeter. Instead, users access applications through the cloud, which stops and secures user access far outside your network. With Enterprise Application Access, there is no direct path into your applications; the solution dials out a secure, mutually authenticated TLS connection from within your network or cloud and brings the application to the user.

No tunnels means that there is no direct path for malware to land inside your network and potentially spread to sensitive or privileged systems. All user connections are stopped in the cloud, terminating on secure proxies while applying strong authentication and security controls. You can add your own security controls for increased protection across all sensitive applications. Enterprise Application Access makes accessing applications fast and intuitive for end users, and reduces support calls for poor application performance, VPN connectivity issues, and device incompatibilities. Enterprise Application Access optimizes

Business Benefits

Drastically improve your security posture by enabling a zero trust architecture

- Keep all users off of your network with application-level access vs. network-level access
- Lock down your firewall or security group to all inbound traffic
- Make your application IP addresses invisible to the Internet
- Easily add MFA to any application with the click of a button

Reduce complexity for IT

- Seamless SSO across all applications, whether they're on-premise, IaaS, or SaaS
- Consolidates ADCs, WAN optimization, VPN, and MFA
- No internal hardware or network changes required, such as firewall rules, IP address whitelisting, etc.
- Users access applications from any device — without any additional software, including VPNs and browser plugins
- Stand up new applications and provision users in minutes
- Automatically integrates with other zero trust ecosystem security solutions

Provide a fast, seamless user experience

- Complete auditing and reporting of user activity
- Available as built-in reports or can be integrated with your existing tools
- Eliminate multiple passwords and provide application access through a single web portal
- Reduce latency for higher application adoption and fewer IT help desk ticket requests
- Deliver applications to any device type, anywhere in the world, with a consistent user experience

applications and presents them in any browser on any user device — and with enterprise-grade SSO and intelligent multi-factor authentication (MFA), security is no longer a burden for users or IT.

Enterprise networks are not an impediment: With one-click integrations for Active Directory, SAML providers, CDNs, forward proxies, SIEM tools, and other infrastructures, custom scripting and integration are eliminated. Scaling and deploying applications across public and private infrastructures is easy with built-in high-availability capabilities, server load balancing, and automatic application routing.

Market Conditions: The Rise and Risks of Distributed Workers

It is essential that employees, remote workers, contractors, suppliers, customers, and developers have access to specific internal and private corporate applications to be productive. Today, this usually means giving them VPN access. But providing internal access creates additional points of entry to an organization's network, increasing the overall risk to critical corporate information. This new paradigm for application access requires a revised view into enterprise security.

"Trust but verify" is no longer an option. There should be no access distinction between internal and external networks or users; trust is not an attribute of location as abuse of access is a significant and rising source of data breaches.

The Challenge: Managing Application Access is Painfully Complex

The growing complexity of today's enterprise infrastructure, combined with the skyrocketing growth of data breaches, has led to massive, untenable operational demands on IT, network, and security teams. To securely enable access to the applications users need to do their jobs, IT organizations must navigate and manage a complex maze of people, processes, and technologies. Deploying, configuring, and maintaining secure-access technology is cumbersome and time consuming.

These systems are currently dealt with on a piecemeal basis, requiring constant maintenance updates and human intervention. There is no one central place to manage and control the technologies associated with application access. There is no simple approach to manage the software, hardware, policies, and security associated with keeping valuable data secure. There is no central visibility as to what users are doing on your network. All of these fragmented factors lead to increased risk for your organization.

The implications to your business are enormous, with complexity and increased risk resulting in lost:

- **Time** – IT, security, and management teams are losing time — which could be spent on higher-priority projects — because they are preoccupied with the monitoring and management of employee and third-party access.
- **Productivity** – Employees, remote users, partners, and contractors lose productivity as a result of inconsistent application delivery and poor application performance due to their wide distribution and new hosting environments. Your workforce should have the customized applications and access they need to do their jobs in minutes, not days or weeks.
- **Data** – The inability to effectively monitor activity on your network can easily lead to a network breach, potentially resulting in the loss of company data, customer information, and intellectual property.
- **Money** – In an IDC Study, "Remote Access and Security Challenges and Opportunities," companies reported that the average expected loss from breaches per year was $6.5M. Companies that provided network access to more third-party users reported an even higher amount at $8.2M.

Transform Internal Application Access and Take Back Control
Approaching the problem with a zero trust security model, Enterprise Application Access provides fast, secure access to applications without allowing users on your network. Enterprise Application Access is a SaaS solution that provides a centralized management portal that does not require additional hardware or software to deploy. The elimination of the complex access stack results in fundamentally better security and streamlined administration.

Enterprise Application Access also improves user access management. It is fast and easy to deploy, provision, change, and monitor users — making onboarding to offboarding a breeze. As a central point of entry and control, Enterprise Application Access provides a single management portal for detailed audit, visibility, control, and compliance reporting.

IBM® Edge Delivery Services and the Akamai Ecosystem

We make the Internet fast, reliable, and secure. Our comprehensive solutions are built on the globally distributed Akamai Intelligent Edge Platform™, managed through the unified, customizable Luna Control Center for visibility and control, and supported by Professional Services experts who get you up and running easily, and inspire innovation as your strategies evolve.