ENTERPRISE APPLICATION ACCESS

Secure, Simple, and Fast Application Access

Increased mobility and a growing utilization of the cloud have driven the need to monitor, control, and secure access to enterprise applications without hindering workforce productivity. Enterprises must also deal with the risky 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-premises 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. Akamai's 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 secure, simple, 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. This access model enables a Zero Trust security framework by closing all inbound firewall ports, while also providing user identity and authentication so that permissions are granted on a per-application, versus network-level, basis. Enterprise Application Access also facilitates monitoring of endpoint security posture based on device signals, securing access to the corporate network without hindering workforce productivity.

It is an identity-aware proxy in the cloud that integrates data path protection, IAM, application security, multi-factor authentication (MFA), single sign-on (SSO), and management visibility and control into a unified service across all application types (on-premises, IaaS, and SaaS). It can be deployed and can stand up new applications and users in a matter of minutes through a single 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

The solution provides secure access as a service (AaaS) that eliminates the need to punch holes in a network firewall. All user connections are stopped in the cloud, terminating on proxies while applying strong authentication and security controls. 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.

Enterprise Application Access supports clientless and client-required applications, 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 applications and presents them in any browser on any user device – with enterprise-grade SSO and intelligent MFA.

The complexity of traditional enterprise networks is no longer an impediment: With one-click integrations for Active Directory, SAML providers, CDNs, forward proxies, SIEM tools, and other infrastructures, custom scripting and integration is 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.

BUSINESS BENEFITS

Improve security posture by enabling a Zero Trust architecture

- Transform cloud and access architecture
- Protect the network with access that is granted on a per-application/per-user/per-device basis
- Lock down the firewall or security group to inbound traffic
- Simplify network architectures – and no longer backhaul VPN traffic to central data centers for authentication
- Enable application access quickly and easily after mergers and acquisitions
- Conceal application IP addresses from the public Internet

Reduce complexity for IT

- Stand up new applications and provision users in minutes through a single web portal, without network changes such as firewall rules and IP address whitelisting
- Facilitate seamless SSO across all applications – on-premises, IaaS, or SaaS
- Bridge user authentication between IdPs and the application, regardless of what the application expects in terms of identification
- Integrate with other Zero Trust ecosystem security solutions and consolidate individual solutions for ADCs, WAN optimization, VPN, and MFA
- Enable device-agnostic access – without requiring additional software, including VPNs and browser plugins
- Leverage information about compromised or infected devices, and certain third-party endpoint security vendors, with device posture
- Empower auditing and reporting of user activity; available as built-in reports or can be integrated with existing tools

Provide a fast, seamless user experience

- Eliminate multiple passwords and login windows
- Reduce latency for improved productivity and higher application adoption – and fewer IT help desk tickets
- Deliver applications securely to any device type, anywhere in the world, with consistent user experience

ENTERPRISE APPLICATION ACCESS

WHY A ZERO TRUST SECURITY MODEL IS NEEDED

Users, devices, applications, and data have moved outside the network perimeter. Digital transformation is driving applications beyond the corporate data center, to the cloud. Employees, remote workers, contractors, suppliers, customers, and developers need access to internal and private applications to be productive. All of these factors increase the overall risk to critical corporate information and data. 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. Enterprise Application Access supports a Zero Trust security model built on least-privilege application access, with full visibility and controls on a per-user/device/application basis.

TRADITIONAL VPN ELIMINATION

VPN elimination is a core tenet of a Zero Trust network. VPNs, by design, are complex to manage and require a high level of understanding of the configurations. And as organizations change to support a growing number of remote and mobile users, the VPN infrastructure can become costly to upgrade and scale. This increase in access from numerous and various devices and locations via a VPN also adds security drawbacks, including the increased risk of unauthorized access to data.

Traditional VPNs have become an antiquated access technology that allow for too much lateral movement across the network. Enterprise Application Access helps organizations to transition away from the VPN to an adaptive risk and security model with no implicit trust, providing granular access control and reducing the lateral attack surface. The elimination of the complex access stack results in fundamentally better security and streamlined administration.

KEY CAPABILITIES

- Keep users off of the corporate network: Lock down your firewall to all inbound traffic while making your infrastructure invisible
- Centralize security and access control: Enable intelligent access decisions for users and devices, as well as the applications – cloud and on-premises – that they are authorized to use, with enhanced security signals
- Multi-factor authentication for enterprise applications: Minimize unauthorized access by authenticating users using MFA across email, SMS, TOTP, or Duo Security
- Single sign-on for all enterprise applications: Seamlessly access on-prem, IaaS, and SaaS applications
- Authentication chaining: Take advantage of unique authentication bridging by separating user authentication from application authentication
- Complete auditing of user activity: Log all users' client information and actions taken, as well as contextual signals and device vulnerability
- Local server load balancing: Balance traffic across internal infrastructure using a variety of load balancing algorithms
- Simplified access management: A central point of entry and control through a single management portal
- User risk assessment: Create risk profiles through the capture of device vulnerability and threat intelligence signals

THE AKAMAI ECOSYSTEM

The Akamai Intelligent Edge Platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Our comprehensive solutions are managed through the unified, customizable Akamai 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.

To learn more about Enterprise Application Access and sign up for a free trial, visit **akamai.com/eaa.**

ENTERPRISE APPLICATION ACCESS

Secure, Simple, and Fast Application Access

APPLICATION ACCESS	
Secure access to applications while maintaining the principles of Zero Trust	√
Clientless web, RDP, and SSH application access	√
Unlimited proxied/least-privilege application limit (excluding wildcard application access)	√
Access non-browser-based services using the Akamai EAA Client	√
Unlimited connectors included	√
Adaptive access controls (Role/group-, time-, and location-based application access control and authorization)	√
Load balancing across application servers	√
Continuous application health monitoring	√
Infrastructure isolation (via dial-out)	√
DDoS protection on management node	√
Custom domain names and certificate upload per application	√
Web application path-based policies (e.g., send app.company.com/login to a different place than app.company.com/home)	√
User login portal and workspace	√
ICAP for AV and DLP integration	√
Application discovery	√
IP address-based access	√
On-premises network detection	√
Captive portal	√
IDENTITY	
Native SAML IdP for application SSO (IaaS, SaaS, and on-premises applications)	√
Authentication bridging and SSO to internal applications (Kerberos, NTLM, password, SAML)	√
Native MFA with per application, group, and directory policies	√
Unlimited SaaS application access	√
Seamless integration to third-party IdP/MFA solutions	√
AD/LDAP integration	√
Cross-origin resource sharing support	√
Integrated directory in the cloud	√
Multiple IdP support for different user classes (employees, third parties, etc.)	√
Basic user-to-service account mapping (PAM)	√
MANAGED DEVICE AND POSTURE	
Clientless posture check (user agent validation and geolocation)	√
Access policies based on device trust (certificate authorization)	√
Vulnerability signals (i.e., endpoint firewall status), incorporated into device risk profile	√
Capture of endpoint detection policy threat intelligence signals from third-party vendors, such as Carbon Black	√
MANAGEMENT	
SIEM log streaming plus a certified Splunk application	√
Integrated real-time monitoring and reporting (real-time transaction)	√
Log retention (number of days)	365