Enterprise Application Access

Secure, Simple, and Fast Application Access

Secure access to the right application, for the right user, at the right time has become difficult and complex because of the widely distributed nature of users and applications. The definition of a user has evolved to be much more than an employee; this can be a supplier, partner, customer, developer, or an employee of a newly acquired company. Applications now have wider definitions that include multiple types (legacy, web, or SaaS) and locations (data center, Internet, and public cloud).

A New Approach Is Needed to Deliver Zero Trust Access

Legacy network security tools, built for the outdated notion of a secure perimeter, have not kept pace with today's need for secure access. These traditional technologies leave organizations vulnerable to attack by bad actors who move laterally inside the network. The ideal solution to this problem is one that grants user access to specific applications and not to entire networks or network segments, as VPN tunnels do. A cloud-delivered, identity-aware, high-performance service is required to provide secure application access for users whenever and wherever they need it.

swisscom

Why Akamai for Zero Trust Access?

Akamai's edge platform enables your secure digital transformation. It gives you the scalability, visibility, and simplicity needed to adapt your business: Quickly onboard employees from a merger or acquired company, enable manufacturing or production in different markets or geographies, easily add and remove contractors to adapt to changing business needs, and move applications to the cloud cost-effectively without sacrificing security. Akamai's platform allows you to deploy IT staff to important business initiatives, rather than maintaining outdated legacy VPN security architecture.

Business Benefits

Eliminate the operational cost and risk involved in maintaining and patching VPNs, and other appliance-based solutions, for secure application access

Reduce your technical complexity and debt with a user/application-centric model for secure access, by building on the unmatched scalability of the Akamai Intelligent Edge platform

Reduce the risk of compromise from employees, third-party contractors, partners, and mobile users — regardless of their location — by delivering secure application access without the need for network access

Accelerate the pace of mergers and acquisitions by enabling shared access to applications, without complex or costly network consolidation or re-architecture

Deliver better-informed decision-making through enhanced visibility and a more granular understanding of users based on security signals, including device posture, threat intelligence, and endpoint compromise

Enable high performance at low cost in a branch environment by retiring Multi-Protocol Label Switching (MPLS) and using application access over the Internet as transport

Leverage the power of multiple clouds by enabling secure access to applications across AWS, Azure, and Google Cloud, as well as web and SaaS applications — using a single secure portal for access

Identity-Aware Security

How Enterpirse Application Access works

Akamai's Enterprise Application Access (EAA) is an Identity-Aware Proxy (IAP) in the cloud. It's a flexible and adaptable service with granular decision-making access based on real-time signals such as threat intelligence, device posture, and user information. The solution is part of Akamai's highly scalable performance edge platform and bypasses the need for network access, while also reducing application delivery risk, cost, and complexity. Enterprise Application Access integrates data path protection, identity and access management (IAM), application security, multi-factor authentication (MFA), single sign-on (SSO), and management visibility and control into a unified service across all application locations and types (on-premises, Internet, IaaS, SaaS, etc.). The edge-delivered solution supports clientless and client-required applications with one-click integrations for Active Directory, SAML providers, CDNs, forward proxies, SIEM tools, and other infrastructures. Scaling and deploying applications across public and private infrastructures are easy with built-in high-availability capabilities, server load balancing, and automatic application routing.

Scalability

Access Needs Change, But Security Must Be a Constant

User and application access requirements are always changing. Regardless of where the user is located (headquarters, branch office, home office, or on the road) or where the application resides (on premises, web, or cloud), Enterprise Application Access scales to meet your business needs. You can give contract developers access to mobile applications, grant full application access to a newly acquired division on another continent, or provide a third-party supplier access to a manufacturing application without network access. All with the load balancing, high availability, scalability, and reliability of the Akamai edge platform.

Visibility

Granular Insights to Easily Provision, Monitor and Manage Access

Enable more granular access decision-making with risk profiles based on visibility into user authenticity, identification, device security, and threat intelligence signals. Identity and contextual signals such as time of day, location, specific URL, and HTTP method can further inform access decisions. You can utilize device posture capabilities that allow for the capture of both device vulnerability signals, as well as threat intelligence signals. You can also leverage information about device compromised status collected from Akamai's Enterprise Threat Protector, as well as third-party endpoint detection policy enablement signals from Carbon Black.

Simplicity

Reduce Technical Complexity and Debt and Enable IT as a Business Partner to Drive Revenue

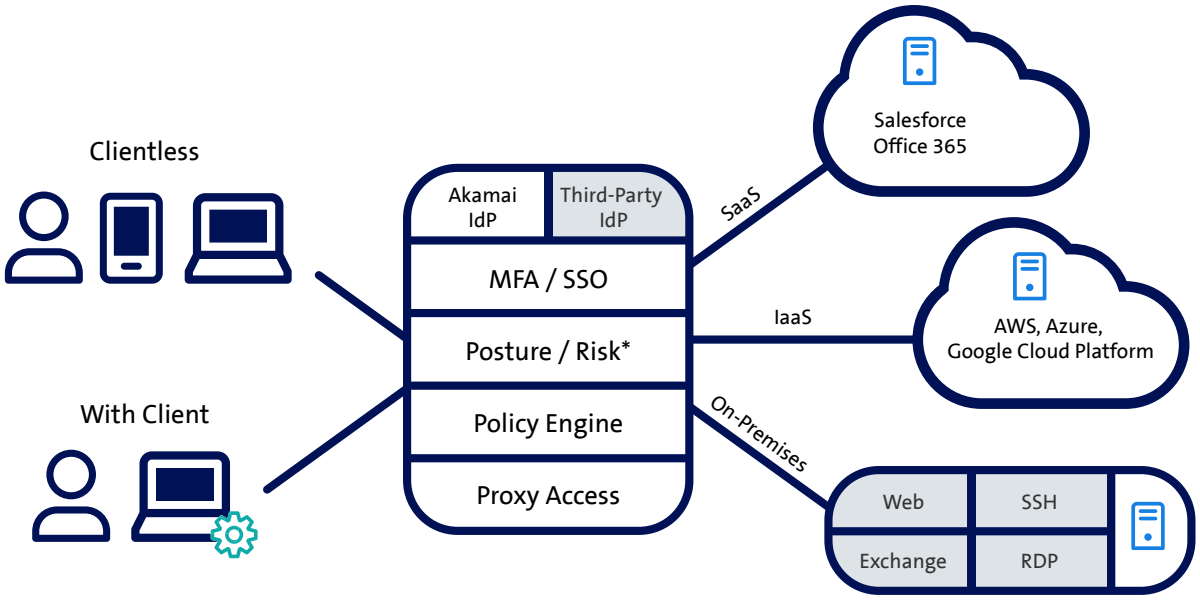
You have numerous and competing IT and security projects. You also have a limited staff and budget. With Akamai's support, you can deploy a user/application-centric service for secure access that allows your staff to focus on other imperatives. Enterprise Application Access is a cloud-native solution — there are no physical appliances to maintain. Akamai has been securely delivering services at the edge for more than 20 years. Our platform provides MFA, SSO, and IdP options, as well as interoperability with a multitude of third-party solutions. And with Akamai, you have the flexibility to work with your vendor/cloud provider of choice for IaaS, SaaS, and workloads.

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 an sign up for a free trial, visit akamai.com/eaa.

How the Enterprise Application Access works



Enterprise Application Access Client

Enterprise Application Access Connector

* Client needed

Application Access

- ✓ **Secure, clientless, and private application access** to nonbrowser TCP/UDP applications using a lightweight client
- ✓ **Secure, clientless, and private application access** to web applications and secure RDP/SSH/VDI application access via a clientless browser, without exposing the network or applications to the Internet
- ✓ **Unlimited connectors for load balancing** to deliver vertical and horizontal scaling deployment in data center, cloud, and hybrid environments, as well as to secure connectivity to applications
- ✓ **Granular, adaptive controls for granting intelligent access**, including IP address-based access and role/group, time, and location-based application access control and authorization
- ✓ **Enable more granular access decision-making through the capture of data for user authenticity** including key signals such as OS, browser and client versions, firewall, antivirus/malware status, and device/user certificate validation
- ✓ **Built-in identity functionality as well as the flexibility** to work with a variety of identity and SSO providers
- ✓ **Flexibility to create web application path-based policies** for user log in and on-premises network detection
- ✓ **Deep visibility into users and applications** including user login portal and workspace
- ✓ **Continuous application health monitoring** to ensure that ports are available and users can connect to the application
- ✓ **Scalable, high-availability edge platform** that includes application delivery controller, load balancers, failover, and high availability
- ✓ **Integrated real-time monitoring and reporting** about applications and users
- ✓ **Programmatically provision using API or SDK** with existing enterprise solutions for ease of use reporting functionality
- ✓ **Flexible SIEM log integration,** including an application with Splunk and 365-day log retention for better reporting

Platform

- ✓ **Additional application protection and services available** such as Kona Site Defender and Akamai's Web Application Firewall to protect applications and APIs from DDoS and application-layer attacks, exploits, and misuse
- ✓ **Accelerate application performance with additional layer** of services to provide fast and reliable corporate applications to end users with WAN acceleration from Akamai's global edge platform

Device posture Assessment

- ✓ **Device posture check of multiple signals** for better access decision-making for Mac and Windows laptop devices and iOS and Android mobile devices
- ✓ **Gain insight into the posture of all devices in your environment**, along with inventory reports with filtering capabilities, to identify devices that need attention
- ✓ **Ability to correlate threat detection signals from Akamai Enterprise Threat Protector** to assess the risk of a compromised device and disallow access based on that criteria
- ✓ **Leverage third-party endpoint detection policy signals** from Carbon Black to add event data recorder (EDR) information to application-access decision making
- ✓ **Classification of devices into risk assessment tiers** to apply access policies based on high-, medium-, or low-risk devices
- ✓ **Easier implementation of access rules** and creation of risk assessment device tags to apply requirements to subgroups of devices that meet defined sets of requirements
- ✓ **Remediation messages generated for mobile and laptop users** to assist with self-service when application access is denied

Identity

- ✓ **Native SAML identity support** for cloud, web, and on-premises applications to enable easy SSO for users
- ✓ **Support for internal applications** with authentication bridging and SSO, including protocol support for Kerberos, NT LAN Manager, or Open ID Connect
- ✓ **Seamless integration to third-party identity and MFA** solutions to support vendor choice
- ✓ **Flexible, native MFA** with policies by application, group, and directory
- ✓ **Identity support to enable different classes of users** including employees, third-party contractors, and partners
- ✓ **Choice of vendor-neutral, industry standard integration with LDAP**, as well as integration with Windows Active Directory

www.swisscom.com/digital-media
+41 800 22 40 40
digital.media@swisscom.com