ENTERPRISE APPLICATION ACCESS

Simple, Safe, and Secure

Providing employees with secure access to enterprise applications deployed behind the firewall is a core requirement for all businesses. Increasingly, enterprises must also deal with the riskier proposition of providing this same access to third parties, including their contractors, partners, suppliers, and customers. Enabling secure application access, whether hosted in a public cloud or private data center, is a complex, cumbersome task requiring on-premise hardware and software such as Application Delivery Controllers (ADCs), Virtual Private Networks (VPN), Identity Management Systems (IAM), and more. Yet with all of these technologies, enterprises are exposed to a variety of security risks, now compounded by the growing network presence of untrusted third-party users. Fortunately, Akamai's Enterprise Application Access solves these problems and helps enterprises transform remote access to meet today's mobile and cloud-centric requirements while improving an organization's overall security posture.

Enterprise Application Access

Enterprise Application Access is a new approach to remote access. It provides a unique, secure, and more convenient alternative to traditional remote-access technologies such as VPNs, RDP, and proxies. With Enterprise Application Access, no one can get to applications directly because they are hidden from the Internet and public exposure. A unique cloud architecture closes all inbound firewall ports while providing authenticated end users access to only their specific applications. Enterprise Application Access integrates data path protection, identity access, application security, and management visibility and control into a single service.

Enterprise Application Access can be deployed in minutes through a unified portal with a single point of control, in any network environment, and at a fraction of the cost of traditional solutions. The result is a secure-access delivery model that enables a zero CapEx, low OpEx model 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. Instead, Enterprise Application Access dials out a secure, mutually authenticated TLS connection from within your network or cloud and brings the application to the user.

Since there are no tunnels, there is no 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 of highly sensitive applications.

Enterprise Application Access makes accessing applications fast and intuitive for end users. Forget the 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 — and with enterprise-grade single-sign-on and intelligent multi-factor authentication, security is no longer a burden for users or IT.

Enterprise networks are not a problem for Enterprise Application Access. 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 apps across public and private infrastructures is a snap with built-in high-availability capabilities, server load balancing, and automatic application routing.

BENEFITS

Convenient

- Users access applications from any device on any browser – without any additional software, including VPNs and browser plugins
- Stand up new applications and provision users in minutes
- Use a service that consolidates ADCs, Wan Optimization, VPN, & 2FA
- No hardware or network changes required – firewall rules, IP address white listing, etc.

Secure

- Keep all users off of your network
- Lock down your firewall or security group to all inbound traffic
- Make your applications invisible to the Internet
- Easily add MFA to any app with the click of a button

Visibility

- Complete auditing and reporting of user activity
- Available as built-in reports or can be integrated with your existing tools

ENTERPRISE APPLICATION ACCESS

The Rise and Risks of Independent Workers: Why this is an Urgent Problem

Why is this new paradigm for application access required? It is essential that outside contractors and suppliers have access to specific internal private corporate applications to be productive. Today, this usually means giving them VPN access. But any kind of third-party access creates additional points of entry to an organization's network, increasing the overall risk that critical corporate information – proprietary documents or customer data – could fall into the wrong hands. Unfortunately, the abuse of third-party access is a significant source of data breaches today, including:

- Last year Trustwave estimated that 63% of all of data breaches were caused by "security vulnerabilities introduced by a third party"
- CyberArk's 2014 Threat Landscape Survey found that 60% of organizations allow third-party vendors remote access to internal networks
- In 2013, McKinsey and Company reported top U.S. banks and credit companies average nearly 20,000 third-party suppliers
- According to Booz Allen Hamilton, third parties were the number-one security risk to financial services firms in 2015
- PwC reported that outside suppliers were contributing to an increase in cybersecurity incidents among manufacturing companies. In their 2014 survey, they found these incidents increased by 17%, while the cost of the breaches jumped 38%

The Challenge: Managing Remote Application Access is Painfully Complex

The growth of third parties, employees, and even customers accessing corporate applications, combined with the skyrocketing growth of data breaches, has also lead to massive, untenable operational demands on IT, network, and security teams. To securely enable vital information sharing, IT organizations have to navigate and manage a complex maze of people, processes, and technologies. Deploying, configuring, and maintaining secure-access technology is a chronic pain.

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 convenient, simple, and fast approach to manage the software, hardware, technologies, policies, and security associated with keeping consultants and supply-chain partners secure. There is no central visibility as to what third parties are doing on your network. All of these fragmented factors lead to increased risk for your organization.

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

- **Time –** IT, security, and management teams are losing time — time that could be spent on higher-priority projects — because they are preoccupied with the monitoring and management of employee and third-party access
- **Productivity –** Employees and contractors lose productivity due to delays in onboarding and subsequent changes, such as adding access to new applications. You want your workers productive in minutes, not days or weeks
- **Data –** The inability to effectively monitor access activity on your network could easily lead to a network breach, resulting in the loss of data or intellectual property
- **Money –** According to the 2014 Executive Breach Preparedness Research Report commissioned by HP, each data-breach loss averages approximately $2 million
- **Corporate Reputation –** According to a 2014 Ponemon Survey on "The Aftermath of a Data Breach", data breaches are in the top 3 incidents that affect company reputation

MARKET CONDITIONS

In today's connected mobile world, companies are using outside resources more than ever to help stay competitive. For example:

- The Bureau of Labor Statistics classifies more than 10 million workers, comprising 7.4% of the U.S. workforce, as independent contractors.
- According to a study conducted by software company Intuit, by 2020 more than 40% of the U.S. workforce — or 60 million people — will be contingent workers.
- In 2014, companies increased their purchases of supply-chain software by almost 11%, spending $9.9 billion dollars.
- Today's environment also has another truth: the number of enterprise breaches — and their risks and costs —continues to grow, seemingly unabated.
- U.S. data breaches tracked by the Identity Theft Resource Center (ITRC) totaled 781 in 2015, the second-highest year on record since tracking began in 2005.
- IBM's 10th annual Cost of Data Breach Study published in 2015 found the average total cost of a data breach was $3.8 million, representing a 23% increase since 2013.
- According to a 2014 report from credit agency Experian, the risk of businesses experiencing a data breach is higher than ever, with almost half of organizations suffering at least one security incident in the last 12 months.

ENTERPRISE APPLICATION ACCESS

Akamai Transforms Remote Access, Putting you Back in Control

Approaching the problem in a fundamentally different way, Akamai now offers Enterprise Application Access — an SaaS service that delivers access to applications without providing users access to your entire network. With Enterprise Application Access, you get a centralized, managed solution that does not require external hardware or software. Managing and controlling third-party — as well as customer and employee — access becomes simple and uncluttered. The elimination of the complexity results in fundamentally better security.

Enterprise Application Access removes the chronic pain suffered by IT teams associated with managing third-party access. It is easy to deploy, provision, change, and monitor. Enterprise Application Access removes all the complexity: no device software, no software upgrades or updates, and no additional hardware. User management difficulties — from onboarding to offboarding — are a breeze. As a central point of entry and control, Enterprise Application Access provides a single management pane for detailed audit, visibility, control, and compliance reporting. The result is painless, secure application access.

The Akamai Ecosystem

Akamai makes the Internet fast, reliable and secure. Our comprehensive solutions are built on the globally distributed Akamai Intelligent 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.

Akamai FASTER FORWARD

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable, and secure for its customers. The company's advanced web performance, mobile performance, cloud security, and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise, and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.