A shift has taken place. The majority of organizations now empower their employees to work remotely. In fact, the number of non-self-employed, at-home workers has grown by 140% since 2005, and employees are not at their desks 50–60% of the time. Globally, Fortune 1000 companies are drastically revamping their physical workplaces in response.

Additionally, businesses increasingly rely on contract workers, partners, suppliers, developers, customers, and other third-party entities to support their corporate imperatives. It’s predicted that by 2027, more than 50% of the U.S. workforce — over 86 million people — will be freelance, and that’s if the current adoption rate holds instead of continuing to rise.

The corporate space — once easily defined by concrete and network perimeters, and unilateral credentials and access — must extend far beyond office walls to accommodate a varied, mobile, hyperconnected, and evolving employee ecosystem. Regardless of locale or affiliation, every member of the workforce needs secure access to the enterprise applications they require in order to perform their jobs. And vitally, this access must be simple.

Providing customized access to a diversified employee body cannot complicate or confuse the end user. Rather, users must have a streamlined single sign-on (SSO) experience that is expedient and efficient across all devices and corporate tools. In other words, enterprise applications must meet the same expectations of ease and performance as consumer applications to ensure adoption and user productivity.

While this requirement has broadly created greater flexibility, it has also caused complexity and a growing number of daily functions, management responsibilities, and support tickets for IT and InfoSec. These teams must reevaluate and reconsider the access they allow to internal applications and systems. Configuring, testing, troubleshooting, and — when it’s all over — decommissioning access for users can take hours, if not days. Due to the intricacy and importance of the task, it often falls to senior IT managers to execute, taking highly skilled professionals away from other business-critical and revenue-impacting initiatives.

So, how can IT remove the intricacy of application access on the back end while also satisfying users on the front end?

An access model that meets the requirements of today’s workforce is needed.
Akamai’s Enterprise Application Access is a proven solution, designed to enable IT to:

1. **Consolidate and Streamline Access Technologies**
   Provide seamless single sign-on for users across all enterprise applications, whether they’re on-premise, IaaS, or SaaS. Collapse your application delivery controllers (ADCs), WAN optimization technologies, VPNs, and multi-factor authentication (MFA) into a single tool that doesn’t require internal hardware or network changes (such as firewall rules, IP address whitelisting, etc.) to set up. Additionally, enable your users to access applications from any device without additional software, including VPNs and browser plugins.

2. **Advance End-User Satisfaction**
   Eliminate multiple passwords and provide application access through a single web portal. Users will experience seamless sign-on to all applications to which they have access, on any device, and from anywhere in the world. Reduce latency for higher application adoption and fewer IT help desk ticket requests. Your users will no longer experience delays as a result of waiting for specifically equipped hardware to be sent to them from IT.

3. **Drastically Improve Security**
   Keep all users off of your network with application-level access versus broad network-level access. Lock down your firewall or security group to all inbound traffic and make your application IP addresses invisible to the Internet. Easily add multi-factor authentication to any application with the click of a button.

4. **Simplify Reporting**
   Get a single management portal for detailed audit, visibility, control, and compliance reporting — available as built-in reports or integrated with your existing SIEM tools.

5. **Maximize Time**
   Set up new users and applications in minutes, not days. Through a web-based portal, you can bridge multiple IdPs, integrating your existing solutions or a native option. This enables you to set up users with the click of a button, rather than having to work across multiple hardware/software devices to provide access.

6. **Stop Configuring Devices**
   Discontinue management of client-side configuration with a tool that requires no software updates or upgrades, and no hardware to provision access.

The result is a simpler method of secure application access for all of your users.

To learn more about Enterprise Application Access and to start a free trial, visit akamai.com/eaa.

**SOURCES**