PAINLESS, SECURE THIRD-PARTY ACCESS
It’s time to start restricting users to only have access to the enterprise applications they need to do their job, not the entire network.

As users are moving outside the traditional network perimeter and DMZ, threats are evolving and moving inside. According to the 2016/17 Kroll Annual Global Fraud and Risk Report,2 82% of executives surveyed reported that their company had suffered a cyber incident in the past year (a 7% increase year over year).

WHY IS THIS AN URGENT PROBLEM?

It is essential that users have access to the enterprise applications they need to get their job done. And it’s increasingly important that they can do this from anywhere, on any device. Traditionally, for IT this has meant providing VPN or VDI and a variety of other solutions including client-side hardware and/or software, security, IAM, and policy-related configuration to ensure each user has access to the network and the necessary applications. But traditional access technologies were created for the networks and business environment of yesterday. Most access systems are cobbled together by different technologies and are complex for IT to manage … not to mention unsecure. Traditional access solutions, like VPN, create points of entry to an organization’s network, thus often enabling lateral movement and increasing the overall risk of a security incident.

Today’s digital, global, and mobile businesses need a simple and secure approach to providing application access.
Traditional access solutions, like VPN, are linked to companies that have the highest number of major incidents from authorized and unauthorized employees, contractors, and vendors gaining access.²

THE CHALLENGE: APPLICATION ACCESS HAS BECOME OVERLY COMPLEX FOR IT

The growth of users accessing corporate applications behind the firewall, along with the skyrocketing growth of data breaches, has produced untenable operational demands on IT, network, and security teams. To securely enable application access, IT organizations must navigate and manage a complex maze of people, processes, and technologies. Deploying, configuring, and maintaining secure access technology is often a complex process that involves everything from network hardware and software to device software, directories to user provisioning and deprovisioning, security, etc.

The complexity of this process results in:

- **Strain on IT Resources:** Remote access system complexity reduces IT agility and often requires senior IT team members to manage on- and off-boarding users, rather than focus on other IT priorities.

- **Decreased User Productivity:** Contractors, suppliers, and employees lose productivity due to delays in on-boarding or application changes, or the inability to access enterprise applications from any device, anywhere.

- **Increased Security Risk:** The complexity of a remote access system means that if a step is missed or a user isn’t off-boarded after termination of employment, the potential for a security incident is much greater. Additionally, monitoring remote access systems is equally complex, which can mean that a network data breach could go undetected.

57% feel their company is vulnerable to an unauthorized remote access breach.³
AKAMAI TRANSFORMS APPLICATION ACCESS,
PUTTING YOU BACK IN CONTROL

Approaching the problem in a fundamentally different way, Akamai now offers Enterprise Application Access, a SaaS that delivers access to applications without providing user access to your entire network. With Enterprise Application Access, you get a service in the cloud that does not require external hardware or software. Managing and controlling access becomes simple and uncluttered, and with the elimination of complexity and unfettered network access comes fundamentally better security.

Enterprise Application Access removes the chronic pain suffered by IT teams associated with managing application access. It is easy to deploy, provision, change, and monitor. Enterprise Application Access removes all the complexity of traditional systems. There is no device software, no software upgrades or updates, and no additional hardware to manage. User management – from on-boarding to off-boarding – and additional security capabilities such as multi-factor authentication, are enabled with a single click. 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 a simple, secure application access solution.

SOURCES
1) http://money.cnn.com/2017/06/21/pf/jobs/working-from-home/index.html
2) Akamai/IDC sponsored research study “Remote Access and Security Challenges & Opportunities”
3) Ibid

As the world’s largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai’s massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai’s portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 08/17.