USE CASE

Providing Simple, Safe Contractor Access to Internal Applications

Executive Summary

Digital transformation continues to reshape businesses globally. The workforce ecosystem is becoming wider, and many companies are providing third parties — such as contractors, suppliers, and partners — access to enterprise applications that sit behind the firewall. The reasons behind this are varied, but one thing is imperative: Access needs to be secure since these user groups are outside of your zone of control.

CONTRACT WORKERS ACCOUNT FOR **20-60%** OF THE WORKFORCE AT NEARLY **ONE OUT OF EVERY TWO** COMPANIES.[1]

Historically, 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 that each user has access to the network and the necessary applications. Additionally, many IT departments took the extra step of physically sending hardware to a contractor or supplier in an effort to strengthen security controls. But, this practice is unscalable and unsustainable for most enterprises, and many breaches still occur through lost, stolen, or misused credentials by third parties.

Because of this, many businesses are embracing a zero trust security model, which assumes a "verify and never trust" policy. In this approach, every device and user is authenticated and authorized before applications or data are delivered, and access is provided only at the application level versus the network level. Additionally, application access is monitored through logging and behavioral analytics.

Risks of Traditional Access Technologies: Why Is This an Urgent Problem?

Conventional 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. Legacy access solutions, like VPN, create points of entry to an organization's network by creating a hole in the firewall. In the event of a breach, this allows for lateral movement and for a user to go beyond the application(s) they have access to.

20% **OF COMPANIES** REPORT BREACHES COMING FROM AUTHORIZED CONTRACTORS OR VENDORS GAINING UNAUTHORIZED ACCESS.[2]

VPNs also lack intelligence. It takes a VPN combined with a number of additional systems to actually deliver connectivity and manage the complexity of everyday onboarding, offboarding, and general tracking. And there aren't validations on who is entering. It's simply correct or incorrect user credentials.

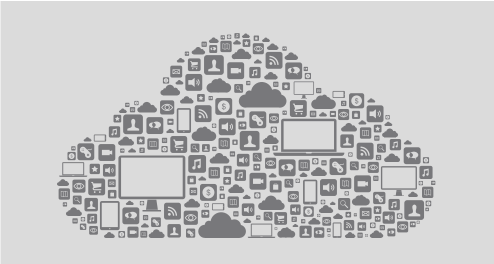
ABOUT ONE IN FOUR BUSINESS LEADERS (23%) DON'T HAVE A CLEAR LINE OF SIGHT INTO HOW MANY CONTRACT WORKERS THEIR COMPANY ENGAGES.[3]

As a result of the security risks, complexity of setup, and lack of visibility into user access for compliance and reporting purposes, traditional access technologies must be retired. Businesses need to transition to a system that enables easy implementation of remote restrictions for tailor-made application access that frees up both valuable IT resources and obstructive budget constraints.

Using Cloud for Simple, Secure Contractor Access

Faster, simpler, and more secure access solutions that can help you move to a zero trust security model already exist in the cloud. A cloud-native access solution can close all inbound firewall ports, while ensuring that only authorized users and devices have access to the internal applications they need, and not the entire network. This means that no one can access applications directly because they are hidden from the Internet and public exposure.

Cloud-native solutions can also collapse your existing, complicated access technology stack. A sole service offers data path protection, single sign-on, identity access, application security, visibility, and administration. Through a unified portal with a single point of control, cloud access services can be deployed in minutes in any network environment, and at a fraction of the cost of traditional solutions. The result is a highly secure access model for contractors that offers reduced management complexity as well as easier reporting and tracking for your IT department.



Read **"Why Akamai for Zero Trust"** to learn more about adopting a zero trust security model, or visit **akamai.com/eaa** to learn more about Akamai's cloud-based, centrally managed, and easily scalable solution for delivering simple and safe contractor access to enterprise applications.

SOURCES

1) http://workforce-solutions.workmarket.com/rs/908-UMC-610/images/2017_Workforce_Compliance_Report.pdf

2) IDC Remote Access and Security Report https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf

3) http://workforce-solutions.workmarket.com/rs/908-UMC-610/images/2017_Workforce_Compliance_Report.pdf

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 09/18.