AKAMAI SOLUTIONS BRIEF

PAINLESS, SECURE THIRD-PARTY REMOTE ACCESS

Akamai
FASTER FORWARD

Restrict contractors, suppliers, partners, and customers to only the internal corporate applications they need to do their job.

In today's connected mobile world, companies use outside resources more than ever to stay competitive. According to the Bureau of Labor and Statistics, more than 15.5 million people in the U.S. are self-employed, an increase of roughly 1 million since May 2014. That number is expected to grow at a steady clip. A separate study by software company Intuit estimates that by 2020, more than 40% of the American workforce (or 60 million people) will be independent workers, i.e., freelancers, contractors, and temporary employees.

Today's environment has another trend: the growing number of enterprise breaches, and their risks and costs, 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. 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.

Why this is an Urgent Problem?

It is essential that outside contractors and suppliers have access to specific enterprise applications to be productive. This usually means giving them VPN or VDI access so they can get to those applications. It also means the IT staff must jump through hoops with respect to network, device, software, and policy-related configuration and management tasks to securely enable that access. But any kind of third-party remote access creates additional points of entry to an organization's network, thus increasing the overall risk that critical corporate information — such as proprietary documents or customer data — could fall into the wrong hands. Unfortunately, abuse of third-party access accounts now constitutes a majority of breaches today, including:

- 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
- PwC reported that outside suppliers were contributing to an increase in cybersecurity incidents among manufacturing companies. In their survey, they found these incidents increased by 17% while the cost of the breaches jumped 38%.

The Challenge: Managing Third-Party Remote Access is Painfully Complex

The growth of third-party suppliers and contractors accessing corporate applications, together with the skyrocketing growth of data breaches caused by third parties, has also produced untenable operational demands on IT, network, and security teams. To securely enable vital information sharing, IT organizations must navigate and manage a complex maze of people, processes, and technologies. Deploying, configuring, and maintaining secure access technology is a chronic pain — from network hardware and software to device software, directories to user provisioning and de-provisioning, security, etc.

IT must touch many moving parts to ensure third parties can access the enterprise applications their jobs require. The implications to any organization are huge, with the complexity and increased risk resulting in lost:

- **Time –** IT, security, and management teams preoccupied with the monitoring and management of third-party access
- **Productivity –** Contractors and suppliers lose productivity due to delays in on-boarding or application changes
- **Data –** Lack of effective third-party monitoring can easily lead to a network data breach
- **Money –** According to the 2014 report commissioned by HP, each data-breach loss averages approximately $2M
- **Corporate Reputation –** A 2014 Ponemon Survey found data breaches are in the top 3 of incidents that affect reputation

A recent survey estimated that 63% of all data breaches were caused by "security vulnerabilities introduced by a third party". The massive data compromise at Target, for instance, began when a hacker gained access to one of the retailer's systems via a remote access account belonging to a heating, ventilation, and air-conditioning company. Hackers were able to use that access to gain a foothold on an internal system and then use that to leapfrog to other systems inside Target's network.

Akamai Transforms Remote Access, Putting you Back in Control

Approaching the problem in a fundamentally different way, Akamai now offers Enterprise Application Access, a SaaS service that delivers access to applications without providing user access to your entire network. With EAA, 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, and with the elimination of the complexity comes fundamentally better security.

EAA removes the chronic pain suffered by IT teams associated with managing remote 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 on boarding to off boarding – are a breeze. As a central point of entry and control, EAA provides a single management pane for detailed audit, visibility, control, and compliance reporting. The result is painless secure remote access.

Top U.S. banks and credit companies average nearly 20,000 third-party suppliers.
— McKinsey and Company, 2013

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.