Executive Summary

Businesses continue to evolve as digital technologies reshape industries. The workforce is mobile, and speed and efficiency are imperative, necessitating dynamic, cloud-based infrastructures and connectivity, as well as unhindered, secure application access — from anywhere, on any device, at any time. Leaders must remove hurdles to progress, but new business initiatives and processes increase the attack surface, potentially putting the company at risk.

Many businesses are embracing a zero trust security model to meet these challenges head on. A zero trust architecture assumes that everything on the network is hostile; gone are the days of “inside versus outside” and perimeter security, as too is the mantra of “trust, but verify.” In their place, organizations must adopt a “verify and never trust” outlook, authenticating and authorizing every device and user before delivering applications or data, and monitoring application access and network activity through logging and behavioral analytics.

One of the many use cases that supports a zero trust security strategy is enabling secure and unified single sign-on across all application types.

Enabling Single Sign-On Across All Application Types

Modern-day enterprise architecture is increasingly complex. Thousands of applications are utilized via on-premise, IaaS, and SaaS solutions for business-critical operations: communication, collaboration, infrastructure, business systems, analytics, and more. And the popularity of cloud applications is climbing. The average business uses more than 1,427 distinct cloud services, with the average employee actively using more than 36 at work daily. In addition to the myriad of application types that your users access, a staggering 79% of global knowledge workers are telecommuters — a number that has grown by 115% since 2005 — and IDC Research reports that this trend will continue to propagate. Additionally, the thread of your business is incredibly varied, consisting of employees, partners, contractors, supply chains, visitors, distribution channels, and others. All of these constituents need access from any device — mobile, connected “smart” device, or BYOD (Bring Your Own Device).

Providing this multifaceted and widely dispersed workforce with an efficient, consistent way to access the burgeoning number of increasingly distributed corporate applications is vital. Furthermore, a seamless single sign-on experience across these applications is a mounting concern for today’s enterprises. Traditional network architectures struggle to meet this challenge, at best delivering degraded application performance. And the risks associated with an inability to provide unified and convenient sign-on are significant:

- Increased password fatigue from excessive username and password combinations. Ultimately, this motivates users to adopt dangerous security habits, reusing passwords, using weak passwords, or writing down their credentials.
- High IT costs and wasted IT resources as users bombard the help desk with requests around forgotten passwords and/or locked devices and applications. Ultimately, this distracts and further taxes already-burdened IT and security departments, diverting efforts from more complex and serious tasks.
• Increased time spent re-entering passwords and/or troubleshooting with IT as individuals battle brittle and fragmented network stacks. Ultimately, this frustrates users and curtails productivity — and has the potential to negatively impact engagement. Notably, productivity improves by 20-25% in organizations with employees who feel “connected” to their work.4

As the scale and frequency of network breaches grows, many companies have turned to a least-privilege model, opting to segment access to networks. Better access governance is key; a process of identifying and analyzing specific roles and needs, and then segmenting users based on these characteristics, is prevailing. But this segmentation must come hand in hand with simple, unified, and secure single sign-on, which remains an enduring challenge with legacy network frameworks. Autonomous services and directories — Active Directory, LDAP, IdP, MFA — utilized across on-premise and cloud applications are complex and time-consuming for owners to manage and for users to navigate.

Take Action: Implement Zero Trust

The best answer is to deliver templated single sign-on integration for on-premise, SaaS, and IaaS applications via the Internet, while proactively employing a “verify and never trust” approach. As this framework is delivered through the cloud and behind the firewall, seamless, convenient, and performant sign-on for end users is coupled with security enabled by a zero trust architecture. Adopting a zero trust security model — authenticating and authorizing every request, device, and user before delivering applications or data, and monitoring application access and network activity through logging and behavioral analytics — can enable seamless single sign-on across all application types.

Read “Moving Beyond Perimeter Security” 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 to single sign-on across all application types.

SOURCES
1) https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/

Akamai

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 04/18.