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 companies at risk.

Many businesses are embracing a zero trust security model to meet these challenges head on. A zero trust architecture assumes that 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 associated with a zero trust security strategy is delivering fast and secure enterprise applications.

Delivering Fast and Secure Enterprise Applications

Enterprise users are becoming increasingly scattered; business no longer happens solely within the four walls of an office building. Employees, contractors, partners, suppliers, customers, and other members of the enterprise ecosystem are on the go, connecting to the corporate network remotely, from home, the airport, a conference, a train, a hotel, a coffee shop, and even at 30,000 feet when traveling. 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.

Simultaneously, enterprise applications are becoming increasingly distributed, accessed on-premise and in the cloud for business-critical operations. And the popularity of cloud applications is only climbing. The average business uses more than 1,427 distinct cloud services, with the average employee actively using more than 36 at work daily.

To cope with this shifting landscape, many companies rely on a variety of hardware and software appliances cobbled together to provide enterprise network access, backhauling cloud traffic over the WAN through a centralized security stack, only to reroute it through direct connects or VPNs back to Infrastructure as a Service (IaaS) and the Internet. But these approaches no longer make operational or financial sense, especially as many businesses are required to duplicate these stacks across geos or cloud vendors. This model degrades application performance and user experience, increases enterprise security risk, and drives up overhead and associated costs.

Congestion and latency consume the valuable time of employees, partners, and other users as they wait for critical applications to load, ultimately wasting business resources — including IT help desk bandwidth — and depreciating corporate productivity. Backhauling application traffic and relying on ill-fitting and complex overhead configurations exposes corporate infrastructure and data to cyber attacks.

Furthermore, this taxed framework often provides no off-network protection and allows unfettered lateral network access, bluntly disclosing sensitive information and operations to any user. This brittle, excessive, and indirect structure drives up overhead and expenditures.
Take Action: Implement Zero Trust

Clearly, the existing techniques and transport choices are no longer sufficient. The best answer to providing accelerated, performant, and secure enterprise application access in today’s hybrid landscape is to deliver corporate infrastructure via the Internet while proactively employing a “verify and never trust” approach. This transport method is significantly faster than backhauling traffic to the corporate network and the zero trust architecture means that every request, device, and user is authenticated and authorized before applications or data are revealed. As this framework is delivered via the cloud and behind the firewall, your IaaS, SaaS, data center infrastructure, endpoint clients, and IP addresses are not exposed on the public Internet.

Given that capabilities such as Internet route and protocol optimization combined with content caching as well as identity integration, single sign-on, and multi-factor authentication can be consumed as a service from the cloud, there’s no need to worry about applications, global performance, or ongoing infrastructure management. This means seamless cross-device performance across the globe both for in-country and international use cases, and with the benefit of cellular optimizations.

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 quickly and safely deliver enterprise applications across your network.

Read “Moving Beyond Perimeter Security” to learn more about adopting a zero trust security model, or visit akamai.com/eea to learn more about Akamai’s cloud-based, centrally managed, and easily scalable solution to delivering fast and secure enterprise applications.

SOURCES

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.