ZERO TRUST

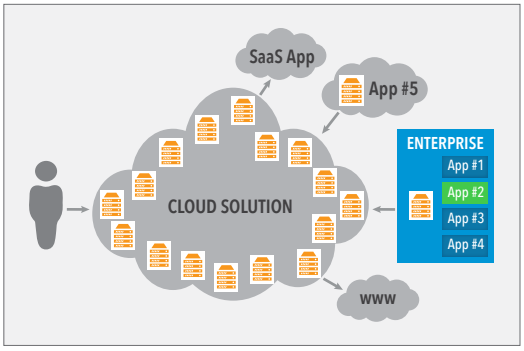
WHY YOU NEED CLOUD-BASED SECURITY FOR AGILE, INNOVATIVE, AND LEAN IT

Digital transformation isn't just a buzzworthy trend or a finite phase for today's businesses. Rolling adaptation to an ever-changing environment and continuous digital evolution has become the new normal for enterprises — the key to success in this agile, demanding, and hyper-connected age.

To deliver standout digital experiences to your customers and workforce, your business needs to operate with agility and speed to drive simplicity and innovation. As a result, business leaders are increasingly being tasked with removing hurdles to efficiency and acceleration for their employees, business partners, supply chains, distribution chains, and others. This necessitates more dynamic infrastructure, increased connectivity, open lines of communication, and unhindered secure application access — from anywhere, on any device, at any time.

At the same time, the threat landscape is becoming increasingly hostile. The days of generic threats are over. Cybercriminals are refining and personalizing their attacks, targeting specific companies, and probing security perimeters and enterprise resources for vulnerabilities with a distinct purpose. These malicious actors are skilled, patient, and persistent, forcing business leaders to prioritize security to defend against this onslaught, and prevent incidents that can impact share prices and their jobs.

So, how do you balance these conflicting charters? It's clear that the traditional enterprise network, security, and application delivery architectures must evolve. In their place, consider adopting a cloud-based security architecture to achieve agile, innovative, and lean IT.



With an inherent focus on users and devices, and applications and data, cloud security is simple and reduces risk. It uses the Internet as its core network, can be consumed as a service in the cloud, and embraces "verify and never trust" (i.e., the Zero Trust security model) as a guiding principle. Additionally, cloud-based security enables the abstraction of the complexity that enterprises traditionally deal with regarding appliance deployment, management, patching, license counts, and more.

A cloud security solution's full visibility and logging can enable your enterprise to look not only at positive and negative security models, but also predictive analytics and behavioral analysis in order to effectively apply security policy, enforce compliance, and reduce risk. With SIEM integration and visibility, the cloud security architecture can also provide you with insight across users and applications, independent of whether they reside in the cloud or on-premises.

Finally, an integrated system in the cloud needs to support single sign-on across all applications — SaaS, on-premise, and IaaS — to provide the same level of visibility, security, and performance. Figuring into the authentication path as well as the data path means that adding additional security and performance capabilities, such as advanced threat protection or application acceleration, can be easily achieved.

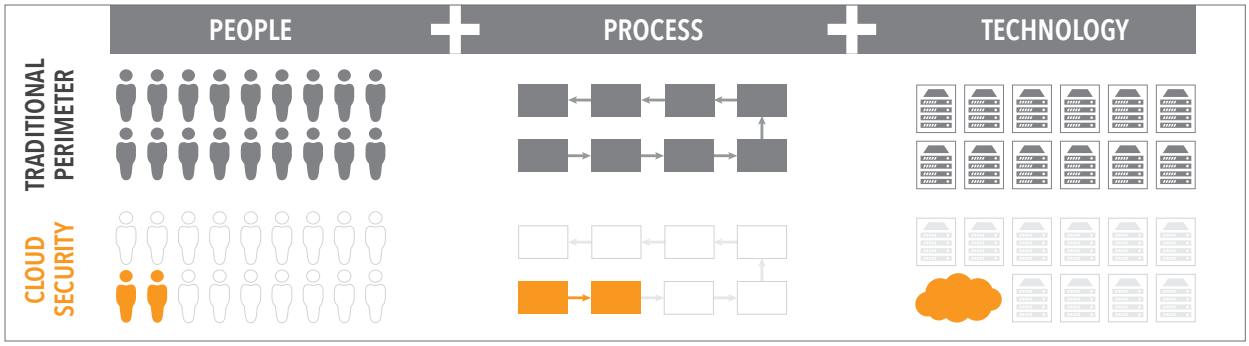
Migrating to a cloud-based security will not happen in the blink of an eye; it is a process and a commitment. So why start this journey now? Neglecting to do so only delays the inevitable:

- Your employees are not likely to stop working from home and while on the road
- The need for vendor, supplier, and partner access to your applications is not going to abate
- Your ecosystem will not discontinue using mobile devices, connected IoT devices, and Bring Your Own Device policies both on and off of your network
- Malicious actors will not slow the evolution of their assaults as your attack surface grows

Enterprises need to embrace the cloud architecture to successfully transform the business, enabling innovation and agility, without compromising security.

WHY YOU NEED CLOUD-BASED SECURITY FOR AGILE, INNOVATIVE, AND LEAN IT

So what would be the day-to-day impact on your resources and output? The most dramatic — and real — differences will be noticed when you look across people, process, and technology.

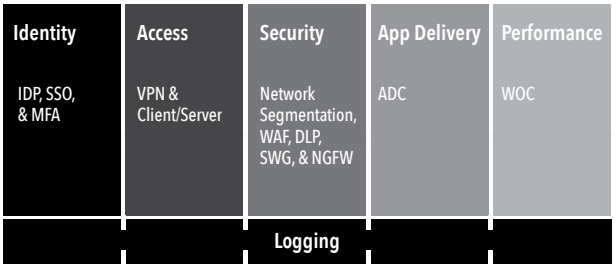


Let's start with people. Would a CIO want a team of senior engineers and architects spending their valuable time managing sophisticated, but cumbersome security appliances? Or would they prefer them to focus on other areas, and let a helpdesk support person — or the application owner — handle rolling out access on their own, in a secure and performant manner? With cloud security, your IT and security teams can focus on what is important and forward looking, rather than battle daily the complex and brittle systems in place. With an ever-growing deficit of skill in the security space, this impact has never been more critical.

When it comes to process, IT is currently charged with the inevitable, unenviable questions and actions surrounding changes made to or on the network. Alternatively, as seen with DevOps and continuous deployment, the option to embrace a process that is simple, streamlined, and focused on ownership and accountability is far preferable. Additionally, being able to integrate cloud security solutions, through open APIs, into a DevOps and continuous integration workflow will help drive a simple and streamlined process.

Finally, on the technology side, the habit of racking and stacking shiny new hardware endures with some long-enamored fans. However, at this point in the IT and technology evolution, this hardware model no longer makes sense. Even the staunchest proponents of this type of configuration are looking toward tomorrow, silently moving into software and attempting to migrate to the cloud.

TRADITIONAL PERIMETER / DMZ



> "With traditional perimeters, 50%+ of people surveyed reported that they use more than 10 network and application components to add access to a new user."
>
> *— IDC InfoBrief, Sponsored by Akamai, Remote Access and Security, September 2017*

In a business world defined by the necessity and speed of digital transformation, as well as an ever-increasing and intensifying threat landscape, enterprises must evaluate their current perimeter security approach. Are you positioning your people, processes, and technology to successfully transform, enabling innovation and agility, while not compromising your company's security?

To learn more about how Akamai can help you move toward a cloud-base security architecture to secure and accelerate your business, visit akamai.com/zerotrust.

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 01/18.