The use of moats for perimeter defense started in ancient Egypt. Today, we’re all familiar with the enterprise security approach of treating an organization like a castle, and surrounding it with a moat. While the moat-and-castle enterprise security approach has worked well in the past, it’s starting to show its age.

The moat-and-castle approach is not only ancient, but also losing effectiveness in today’s mobile and cloud-first world. The evolution of enterprises, applications and the threat landscape is seeing to that.

Enterprises are evolving and turning inside out. Employees want to access enterprise applications anywhere and from any device. What’s more, the enterprise ecosystem has become a core ingredient in successful digital transformation. And everyone within this ecosystem of partners, contractors and even suppliers wants the same thing as employees: Secure access to enterprise applications from anywhere, on any device. As Akamai’s own Senior Director of Enterprise Security & Infrastructure Engineering points out: “There is no inside.”

Enterprise apps are also evolving. End users expect the same experience when submitting an expense report or a bug report as when they update their social media profile or check their bank balance on their mobile phone. This has left many IT teams scrambling. In many cases, lines of business are bypassing IT entirely, opting for SaaS and cloud instead. Providing the ability to work anywhere, from any device, quickly and efficiently, is clearly good for the bottom line, so it needs to be a priority. That often requires some revamping, which for most of us means cloud — specifically Internet, IaaS or SaaS.

Lastly the threat landscape is always evolving. The moat-and-castle approach to enterprise security is based on two simple assumptions. First, walls work. Second, once inside the walls, a person can pretty much do whatever they want. There might be some simple door locks for certain rooms, but for the most part they can move around freely, learning about the castle layout, where the locked rooms are, if they have open windows or a second, less protected door, etc. Sound familiar? That’s because it’s the blueprint for most modern cyber attacks. Get in, do reconnaissance, find the weak spots, get what’s needed and then get out, without anyone realizing until it’s too late.

Combine enterprise, application and threat landscape evolution and you can see why we are waking up to the fact that moats and castles belong in the past.
Whether it is Google and BeyondCorp, or Forrester’s Zero Trust model, they ultimately strive for the same thing, to treat end users the same, whether they are outside or inside the enterprise/castle walls.

At Akamai we’ve taken a new and better approach — the cloud perimeter. The cloud perimeter boils down to the user and the application they are trying to access. The cloud perimeter handles authentication, authorization and application delivery across devices and locations. The cloud perimeter obfuscates where the application is hosted, and automatically sends the user to the right location — but only if he or she has the appropriate privileges. The potential attack surface has now shifted to the Akamai Platform, which only provides application specific access to trusted and authenticated end users and their devices. No more network access. No more moats and castles. Everyone is untrusted, inside and outside.

This makes life easier for enterprise IT and security teams who ultimately remain responsible for visibility, security and performance even though enterprise data, apps and employees have moved outside the enterprise’s traditional zone of control. In fact, it allows teams to continue to drive towards greater IT agility and simpler infrastructure. Only inbound and outbound non-malicious enterprise traffic passes through the cloud perimeter, and everything else gets dropped.

What are the implications of not moving to a cloud perimeter? To start, you’ll won’t have the ability to embrace and benefit from enterprise and enterprise application evolution. If you are not moving forward, you are moving backwards. Perhaps more importantly, the increase in risk associated with proving full network access, without multi-factor authentication, or single sign-on integration, weighs on the minds of most IT and security professionals. Another way to look at the implications of not adopting a cloud perimeter approach is by using the people, process and technology framework.

So, how does the adoption of a cloud perimeter impact each of these areas? In terms of people it is all about expertise, man hours, and productivity. Process is all about streamlining and simplification. Lastly, technology is pretty simple. Instead building out your own infrastructure and cobbling together various access and optimization solutions, Akamai can make it easy and simple by providing cloud perimeter as a service. Enterprise Application Access (EAA), our first cloud perimeter solution, offers, simple, secure access to enterprise apps behind the firewall. Find out more about EAA now.

It’s time to put moats and castles behind us.