Everything You Always Wanted to Know About Security at the Edge, But Were Afraid to Ask.
Introduction

Whether you’re focused on public-facing websites or your company’s assets and users, as someone who cares about digital security, your life is dominated by these trends that characterize the state of all things security in 2019:

Attacks are growing, evolving, and becoming more sophisticated. And the types of attacks we see are proliferating.

Business depends on flawless digital experiences. This is true for the enterprise — to communicate, collaborate, and produce at the highest level. And it’s true of core business offerings like seamless online retail and financial transactions, OTT video delivery, online healthcare portals, and for connected devices on the manufacturing floor.

There used to exist the idea of a constant immovable security perimeter. You could put a wall around and protect anything inside your data center. Nothing in. Nothing out. The problem is, the perimeter as we know it is dissolving. How do you protect your crown jewels when the castle has no walls?

The answer is at the edge.

When you deploy security at the edge, you are protecting your changing assets closer to the attack itself and moving digital experiences closer to users. In essence, you’re deploying a single pane of glass, an extension of your infrastructure, that sits between you — your users, your digital experiences — and the always-changing nature of today’s digital environment.
What we mean when we say "edge."
Bob Gill of Gartner wrote that edge is simply “the physical location where things and people connect with the networked digital world.”*

In a sense, it’s a question of physical topology. At a time when users expect seamless digital experiences on demand, pushing interactions to the edge, closer to the source of the data being generated, not only provides better experiences, but it is also the best location to construct safeguards between your business and your widely distributed users and consumers of digital experiences.

The shift in focus to the edge has been driven by several factors:

- Consumers’ growing intolerance for latency.
- The rising consumption of bandwidth-gobbling rich content.
- The sheer enormity of content being delivered and consumed.
- The realization that centralized data centers aren’t ideal for delivering or securing the kind of engaging content we’ve all come to expect from our digital experiences.

While some data centers have become larger and more centralized than ever before, as we look to the future, the topology is trending toward smaller and more distributed edge data centers. By moving to the edge, many analysts predict, businesses will be able to create entirely new markets based on the benefits it offers.

This is an opportunity for security and information services teams to leverage a simple, agile security platform to move beyond merely being a cost center, and instead becoming a strategic partner that empowers business and drives revenue.


Everything You Always Wanted to Know About Security at the Edge, But Were Afraid to Ask
What we mean when we say "security at the edge."
With processing happening so close to where data is generated, edge architecture can provide a better experience, better efficiency, and better security, and ultimately allow companies to save money and concentrate resources on additional revenue opportunities.

Along with the benefits the edge brings, there also comes the opportunity to look at security anew. The network perimeter as we know it is dissolving, so approaches to securing it must adapt.

Enter security at the edge.

Security at the edge is an approach to defending your business, your customers — all of your users — from security threats by deploying defense measures closer to the point of attack and as far away from your assets (your people, applications, or infrastructure) as possible. Security at the edge is dynamic and adaptive. It allows you to surround and protect your users or consumers wherever they are — at the core, in the cloud, or on the edge, and everywhere in between.
What you're protecting isn't what you used to protect.
Whether adapting to the shifting nature of the perimeter or endeavoring to protect evolving public-facing applications, it’s clear that what you are protecting has fundamentally changed, and will continue to do so. The attack surface isn’t what it used to be. For example:

- **Applications are constantly updating** with new versions, new functionality, and new microservices.
- **Applications are continually moving** from on premises to the cloud, and back again.
- **Websites are in a state of transformation** from traditional, legacy infrastructure to mobile-first and API-based back ends.
- **Data centers are perpetually being expanded or consolidated.**
- **Infrastructure is regularly being added to or removed.**
- **Employees are always on the go.** Rarely does the 9-to-5 paradigm exist and, increasingly, neither does a centralized brick-and-mortar workplace.

In such an environment, you’re protecting a mix of applications: on premises, in the cloud, or in multiple clouds. At the same time, the teams within your organization are composed of different groups of people with varying priorities making independent decisions. They may all be sound business decisions, but the unpredictable nature of the process presents great challenges.

The answer lies in a cloud-agnostic security practice that can respond to your business when it changes directions or uses multiple cloud solutions simultaneously. Your solution lies at the edge.
How do I deploy security at the edge?
Your mission is to protect applications wherever they are. Deploying a single security solution at the edge minimizes the time and resources spent training on that solution. And with that one solution — that single pane of glass — you can protect applications anywhere on any platform.

The exact combination of security solutions appropriate for each organization may vary, but the following measures are critical pieces of an effective edge security strategy:

**DDoS Protection**
It’s not uncommon for organizations to be hit with hundreds if not thousands of DDoS attacks a month. It’s critical to keep applications and IT services available even through the largest of these attacks.

**Web Application Firewall**
Websites and web applications are increasing in complexity and risk, with new vulnerabilities discovered daily. A superior firewall can offer protection and performance.

**Bot Management**
Bots can represent 30 to 70% of an organization’s website traffic, with impacts ranging from poor performance to lost customers to fraud. It’s incumbent on the organization to deploy a capable and adaptive bot strategy to bring scrapers under control and mitigate credential stuffing.

**Secure Enterprise Application Access**
Business models have changed. Enterprise digital ecosystems, cloud applications, and distributed users mean that IT needs agility — and your users need safe but seamless access. Simple, secure remote access management needs to be easy for IT, provides inherently better security, and delivers an exceptional user experience.

**DNS**
Protect your authoritative DNS service and stay connected with your users and employees. Architected for performance and availability, our solution maintains a fast and available DNS experience even through the largest DDoS attacks, and can also protect against DNS forgery and manipulation.

**Malware Prevention**
Ensure that your users and their devices can safely connect to the Internet anytime, anywhere, by proactively identifying and blocking targeted threats such as malware, ransomware, phishing, DNS data exfiltration, and zero-day attacks.
Maintain trust with security at the edge.
Consumers of digital experiences expect their data and transactions to be secure and their privacy to be protected. And companies need to protect their workforce from incursion attempts. When you protect your assets and your people from the outside in — and the inside out — you’ve taken an important step in cultivating trust as a core brand value.

And don’t underestimate trust: According to research conducted by Frost & Sullivan, 86% of customers surveyed said they prefer security over convenience, and the more trust placed with a company, the more money they would be willing to spend with that organization. In fact, as Forrester reports, the mere whiff of suspicion of a company’s data use practices can cut revenue by up to 25%.

The security landscape is shifting. Today’s security professionals are faced with persistent attackers, sophisticated bots, and advanced command and control software, along with an enterprise perimeter that is increasingly difficult to enforce. To maintain users’ trust, organizations need security at the edge that surrounds and protects the entire architecture — clouds, sites, content, apps, and users.
Conclusion

The laws of physics — the speed of light, data gravity, limitations in bandwidth — require a change in the way we think about security. The demand for more real-time interactions between things, people, and their digital experiences is pushing us all toward the edge. Which is a good thing. It’s already expanding business opportunities, and fundamentally changing how we live, interact, shop, and work.

But along with this evolution, attack surfaces will continue to shift and become highly distributed. Attacks will continue to grow and target with more precision. Trust based on a single network location will no longer be relevant. These trends, and the ever more complex systems in digital business, ultimately will result in even more risk. But they also provide security teams considerable opportunity — the opportunity to become a business partner and a driver of value for their organization.

You can do this by employing an edge security strategy — one that is adaptive, in-depth, and designed to preempt the expanding attack surface and simplify security controls. One that brings users closer to the digital experiences and knocks down attacks where they’re generated. One that breeds trust and puts the confidence and control back in your hands.

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, 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 24/7/365 monitoring. To learn why the top financial institutions, online retail leaders, media and entertainment providers, and government organizations trust Akamai, please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. Published 05/19.