Akamai Zero Trust Security

Akamai’s Intelligent Edge Platform offers a broad range of access management, threat protection, and application security services that will support you in your journey to Zero Trust, making it safe, scalable and easy to manage – delivered entirely from the cloud.

by Alexei Balaganski
ab@kuppingercole.com
September 2019

Content

1 Introduction ........................................................................................................................................... 2
2 Product Description ............................................................................................................................... 3
3 Strengths and Challenges ..................................................................................................................... 6
4 Copyright .............................................................................................................................................. 7

Related Research

Product Report: Akamai Intelligent Platform – 70874
Leadership Compass: Cloud Access Security Brokers – 72534
Leadership Compass: Dynamic Authorization Management – 70966
Advisory Note: Top Cyber Threats – 71032
Advisory Note: Connected Enterprise Step-by-step – 70999
1 Introduction

Akamai Technologies is a content delivery network and cloud service provider headquartered in Cambridge, Massachusetts, USA. Founded in 1998, the company is one of the veteran players on the market, providing a broad range of performance-, security- and even productivity-related services through their content delivery network (CDN), one of the world’s largest distributed computing platforms. Spanning over 250,000 servers and 1600 networks across 137 countries, the company’s Intelligent Edge Platform is within direct reach of over 90% Internet users around the world. With this global footprint, Akamai can serve numerous large enterprise customers of all industries, including such demanding technology giants as Microsoft, Apple or Facebook.

Although the company’s history predates even the very notion of “cloud”, over the last two decades Akamai’s platform has evolved from a traditional CDN to a full-featured Intelligent Edge Platform that not just competes with established cloud providers in multiple areas like web and mobile application delivery, enterprise security, and strategic services, but in fact complements them with a unified layer of defense for all IT systems, applications and services regardless of their location or platform, as well as with a universal integration platform for hybrid multi-cloud architectures.

As organizations continue embracing the digital transformation, trends such as mobility, the proliferation of SaaS applications and cloud infrastructure are driving up the number of connected entities and devices increasing the attack surface. A traditional corporate security perimeter has all but disappeared, and more and more people, applications, and sensitive data are moving outside of the “trusted network”. The Zero Trust paradigm is rapidly gaining popularity as a modern alternative to the traditional perimeter-based security, which can no longer provide sufficient protection against external and internal advanced cyberthreats. An IT infrastructure designed around this model treats every user, application or data source as untrusted and enforces strict security, access control, and comprehensive auditing to ensure visibility and accountability of all user activities.

Like many other popular security buzzwords, the notion of “Zero Trust” has many conflicting interpretations among experts, software vendors, and customers. Perhaps the biggest misconception is that the Zero Trust model can be purchased on a turn-key basis, instantly transforming a legacy network into a “next-generation perimeter”. This, of course, cannot be further from the truth.

Going Zero Trust is a transformational process that requires organizations to radically rethink not just their IT architectures and security policies, but to adapt their entire business processes for the modern mobile workforce where there no longer is a notion of a trusted “inside”. This includes implementing a fine-grained least-privilege, default deny access model for applications and data sources; designing a multilayered cyberthreat defense that works anywhere, not just behind the corporate firewall; dismantling the very notion of “the Intranet zone” to ensure consistent experience across all devices and locations; and, last but not least, avoid making your IT infrastructure unbearably complex.

And even though you still cannot simply “buy Zero Trust”, Akamai’s Intelligent Edge Platform offers a broad range of access management, threat protection, and application security services that will support you in your journey to Zero Trust, making it safe, scalable and easy to manage – delivered entirely from the cloud.
2 Product Description

Ever since it became clear that the traditional security perimeters of corporate networks are quickly disappearing, IT specialists have been frantically searching for a modern, more consistent and future-proof alternative approach. The adoption of the cloud meant that every organization now needed to manage multiple IT environments with completely different operational and security controls. Quickly growing mobile workforce meant that more and more employees and their devices constantly leave the safety of the office network or, worse, bring uncontrolled external devices into it. The business requirement to open the corporate network to partners, contractors, sometimes even customers was the final coffin into the traditional “castle wall” security mentality.

For some time, businesses tried to address the challenge by throwing money at it, allocating bigger budgets for additional cybersecurity tools. Unfortunately, the latest breach statistics indicate that further increasing complexity and cost of IT security does not translate into better overall security posture. It was clear that a radically different approach towards security is needed, and the concept of “Zero Trust” coined by Forrester Research and popularized by Google with their “BeyondCorp” project has quickly gained everyone’s attention. A simple idea that a corporate network should no longer have a “trusted LAN” zone and every user or device in it should be subjects of the same security and access control policies regardless of their location, sounded revolutionary, yet simple enough to be understood even by non-technical executives.

Unfortunately, the combination of a catchy name and marketing claims of various vendors has created somewhat unrealistic expectations among the general public. Yes, implementing Zero Trust can greatly reduce the overall complexity of corporate IT infrastructures, since it’s no longer necessary to maintain separate security stacks for each platform or network zone. Also, it substantially limits the potential for lateral movement within the network for malicious actors, dramatically reducing the impact of cyberattacks. Last but not least, it provides a unified user experience for users, offering greater flexibility and productivity for the staff and partners.

However, Zero Trust is not an off-the-shelf-product and not even something that IT alone can implement. It is a conceptual and architectural model that establishes basic principles for designing modern networks. Without substantially changing their existing organizational and sometimes even business processes, companies cannot expect to achieve Zero Trust. Even less realistic are the expectations of reaching the goal in one step using the “rip and replace” approach – especially from companies that still fail to implement the most basic security best practices.

Zero Trust is a journey that begins with a long-term business strategy and focuses on a step-by-step implementation using existing or readily available tools and technologies while maintaining the continuity of business processes and avoiding adding even more complexity to the existing architecture. Different companies will have different priorities in implementing individual requirements of the Zero Trust model, but for obvious reasons beyond the realm of IT, every one of them must ensure the continuity of their core business processes as well as the integrity and confidentiality of their sensitive corporate data. And this is exactly what Akamai’s Intelligent Edge Platform aims to provide to a company of any size, without the need to invest in additional infrastructure or security expertise.
The company’s approach towards achieving Zero Trust Security is to start the journey with enforcing the least-privilege access model consistently for all business applications using the **Enterprise Application Access** (EAA) service built on Akamai’s cloud platform. This ensures that every such application is completely hidden from “trusted” public exposure regardless of where it is hosted – in a corporate LAN, on-premises datacenter or in the public cloud. Thus, all users, internal or external, are forced to access the applications through an Identity Aware Proxy (IAP), which transparently handles all aspects of Zero Trust model such as multi-factor authentication (MFA), single sign-on (SSO) and enforcement of company-wide security and compliance policies.

Since the solution is completely offered as a service, there is no additional network hardware or security appliances to deploy and maintain. There is also no need for inbound VPN for external users – Akamai does not require any direct connection to the customer’s infrastructure at all. Every connection between users and applications is established from both ends and is always terminated in the Akamai’s platform. This not only significantly lowers the overall complexity of corporate network infrastructures, but also reinforces security best practices: any “implicit trust” giving users access to whole networks by traditional VPN tools is eliminated, and administrators are encouraged to block any inbound connections completely.

Typically for a SaaS solution, all management is performed through a single administration console in the cloud, including provisioning new applications, defining access policies, and monitoring their enforcement on users. Needless to say, these policies work seamlessly for any application deployed on-premises or in any cloud. Since EAA is an integral part of Akamai’s cloud platform, any other service offered by the company can be transparently applied to the application traffic as well. This includes performance capabilities like Akamai Application Acceleration and security functions like Akamai Web Application Firewall. Naturally, all monitoring, auditing and analytics capabilities of the platform are available to customers as well, just like it is prescribed by the Zero Trust model.

Although Akamai offers its own identity management services as well, the EAA service is designed to be identity-agnostic, supporting direct integrations with major on-prem and cloud-based identity stores like Active Directory, SAML or third party IAM vendors like Okta. On top of that, the platform incorporates a flexible MFA framework offering support for SMS, time-based OTP tokens and Duo Security.

From the user’s point of view, the new consistent user experience offers a major productivity boost compared to traditional VPNs: for web-based applications the process of establishing an authenticated and secured connection to an app is fully transparent and does not involve any additional hardware or software (a web-based application portal is provided for convenience, but Akamai can optionally integrate with existing application catalogs). To extend support for other protocols and ports, a single client must be deployed to the user’s device, which will automatically intercept any attempt to establish a direct, insecure connection to a backend and route it through the cloud platform transparently.

Once authenticated, users can “carry” their identities across multiple applications, even if those do not support this natively – the platform takes care of the needed transformations. It’s worth stressing explicitly, however, that the authentication is not a one-time event, but a continuous, adaptive process: for each request, the authorization platform will evaluate multiple contextual factors related to the identity of the user, geolocation, time of the day and so on to make a dynamic real-time access decision according to the active policy.
In the future, the company is planning to offer tighter integrations with its own and third-party security solutions to evaluate even more variables like the risk posture of the device or threat signals from protected applications. This dynamic policy-based authorization approach is again one of the core requirements of the Zero Trust model.

Harnessing the massive reach and performance of Akamai’s content delivery network, the EAA solution not only provides consistent secure access to business apps across hybrid IT environments, but enables other, less obvious use cases: for example, it can dramatically decrease the complexity of IT infrastructures after mergers & acquisitions; implement secure and compliant access of contractors and external admins to internal applications; or simply reducing bandwidth costs by getting rid of traffic backhauling from remote offices to a central security gateway (or by getting rid of the gateway completely).

To extend this protection from what used to be known as “corporate network” to the rest of the Internet, Akamai complements EAA with another service, Enterprise Threat Protector (ETP). Some experts may argue that protection from external threats is not the focus of the original Zero Trust concept, and to a certain extent, this is true. However, for most companies, the journey towards full Zero Trust may take years, and in the meantime, secured applications and data sources will have to co-exist with legacy systems, vulnerable endpoint devices and gullible users targeted by scam attacks.

The goal of the Enterprise Threat Protector is to ensure that all these users and devices are protected from external cyberthreats using the same cloud-based technology without additional performance overhead, administrative complexity or investments into additional infrastructure. Simply by changing DNS settings to redirect domain name resolution requests to ETP, customers can ensure that any such request will be validated against Akamai’s constantly updated threat intelligence database, and access to any known malicious destinations are automatically blocked. Additionally, risky web sites or even individual URLs can be forwarded to a cloud proxy within the Akamai’s platform that performs real-time analysis of the traffic using multiple antimalware engines: this allows the solution to detect and immediately block a wide range of malware, from executables to macros in office documents and even malicious scripts.

To ensure that even mobile workers are covered, companies may choose to deploy additional Enterprise Client Connectors to managed devices, which will ensure that traffic is forwarded to Akamai in any situation. One of the company’s short-term goals, however, is to integrate this functionality into the EAA agent.

Of course, the same technology can also be used for blocking inappropriate content or apply any other compliance policies to Internet traffic. All these policies are managed within the same administration console of Akamai’s Intelligent Edge platform. Additionally, customers can define their own threat categories, integrate custom threat intelligence feeds and, of course, utilize the comprehensive reporting and analytics capabilities. Activity logs and security events can be sent to an existing SIEM for further analysis.
3 Strengths and Challenges

With its impressive scale and a broad range of offered services, Akamai’s Intelligent Edge Platform goes way beyond just security or access management capabilities. On the other hand, in contrast to quite a few other security vendors, Akamai does not attempt to market its platform as the ultimate solution for all your Zero Trust needs.

And yet, while it is definitely not possible to buy Zero Trust, as we have hopefully demonstrated earlier in this paper, making Akamai a part of your long-term network modernization strategy would definitely make your Zero Trust journey shorter and more comfortable.

During the initial phase, thanks to the fully cloud-based architecture that does not require any infrastructure investments, you can start with smaller short-term goals and achieve quick wins, for example, by onboarding your partners or contractors first, gradually expanding user coverage as needed.

Further on, you’ll be able to incorporate additional security services to improve your security and compliance posture during the transitional period. Finally, the sheer scale and availability of the company’s cloud infrastructure in every corner of the world will ensure that even the largest multinational corporations will never face a performance or scalability bottleneck.

Strengths

- Massive scale and availability of Edge infrastructure in every region of the world
- No need to deploy and maintain any additional hardware infrastructures
- Consistent enforcement of secure access policies for hybrid environments, any network protocol
- Identity-agnostic, direct integrations with multiple on-prem or cloud IAM solutions
- Extends pure Zero Trust with threat protection, application performance and other security services

Challenges

- Does not cover all requirements of the Zero Trust model
- Multiple software agents required for consistent access control and threat protection beyond web apps
KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.


For further information, please contact clients@kuppingercole.com