No.18
5th December 2018

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

Akamai's Traction in Enterprise Security

HardenStance attended Akamai's Edge EMEA Forum in Barcelona last month. Here's an update on how the company is doing in the enterprise security space it is targeting now:

- Akamai has solid-looking proof-points for traction in enterprise security but not yet enough to demonstrate decisively that it can replicate its success in cloud security.
- Akamai has a valid enterprise security strategy but faces challenges grafting it onto legacy environments and supporting faster adoption of applications and devices.

With Akamai exiting Q3 at a run rate of nearly $700 million a year in security revenues across its business units, CEO Tom Leighton told last month's EMEA EDGE Forum in Barcelona that "security is going to be our biggest business based on current trends."

The Zero Trust portfolio pitches Akamai into securing an enterprise's own users and applications.

To get to a billion-dollar-a-year security business and beyond, Akamai launched a Zero Trust portfolio 18 months ago. Having almost surprised itself with its success in protecting its customers' own customer-facing assets in the cloud, the Zero Trust product line pitches Akamai into securing an enterprise's own users and applications.

The two products – Enterprise Application Access (EAA) and Enterprise Threat Protector (ETP) – and the underlying 'Zero Trust' branding that underpins them – are described in **Figure 1**. Combined with other public data, insights shared during the Forum by the company and some of its security partners and customers, point to five key take-aways as regards the traction Akamai is seeing in enterprise security:

1. In its Q3 investor call at the end of October, Akamai stated that Q3 bookings for EAA and ETP services were four times those of Q3 2017 and up 30% sequentially.
2. Akamai states it now has more than two hundred EAA/ETP customers in production. Eighteen months since launch, that sounds good rather than remarkable.
3. One of the largest UK banks; a $10 billion travel company; and a $4 billion luxury fashion brand are all cited as EAA/ETP customers.

Figure 1: Three Pillars of Akamai's Enterprise Security Strategy

Pillar	Name	Brand or product	Description
# 1	Zero Trust	Brand	Tightly controlled access and inspection of everything. Network layer access is dangerous. Retire VPNs and micro-segmentation.
#2	Enterprise Application Access	Product	Identity-aware proxy tied to Akamai or third party Multi Factor Authentication (MFA) or Single Sign On (SSO) giving users access only to the applications they need rather than to the whole network.
#3	Enterprise Threat Protector	Product	Recursive DNS service that protects against complex targeted threats like malware, ransomware, phishing and DNS-based data exfiltration. Allows employees to be blocked from accessing infected sites as well as providing protection against DNS exfiltration attacks.

Source: HardenStance

4. T-Systems, the IT services arm of Deutsche Telekom, is re-selling ETP (and Kona Site Defender) as part of a multi-layered partnership with Akamai. T-Systems' ambition is no less than to become Europe's largest cyber security provider. Having built an ecosystem of forty-nine security vendor partners, T-Systems is actually on a mission to significantly reduce that number. Adding another new security partner at this time suggests that T-Systems thinks highly of these Akamai products.

5. Peter Hecko, Head of IT Security for Helios Kliniken, shared his company's experience as an early adopter of ETP during the Forum. Helios is a German hospital provider with 100,000 employees worldwide. Hecko relayed the following in his talk:

Helios appreciates being offered ETP as a stand-alone service and without requiring any hardware investment.

   - Sending all of Helios' DNS traffic into the ETP cloud was considered very high risk by Helios admins but the outcome has proven highly satisfactory;
   - Helios had three business objectives in evaluating its options for a recursive DNS security service. It wanted an extra layer of defence against malware, ransomware, phishing and DNS data exfiltration; it wanted to minimize risk by reacting faster and earlier to mitigate threats; and it wanted to provide malware protection for all network devices including connected medical devices (bearing in mind that European regulations prohibit installation of any software on medical devices);
   - Hecko stated that ETP offers the ability to "easily detect malware-infected devices". Akamai's threat intelligence provides "the highest level of protection against complex cyber attacks" and delivers "very low levels" of false positives;
   - Helios has been able to extend protection to medical devices and other IoT 'things' that weren't previously protected;
   - Compared with other solutions on the market, Helios greatly appreciated being offered ETP as a stand-alone DNS threat protection service. Helios liked being offered this independently of the rest of Akamai's DNS and DNS security products - and without requiring any hardware investment.

The Challenge of Selling Zero Trust into Enterprise Customers

In IT security terms, Akamai's push into enterprise security is a classic case of a big fish in a small pond seeking to make it as a small fish in a bigger pond. That can go spectacularly well. It can go spectacularly badly. Or it can succeed but fall short of expectations. The above proof-points offer ample evidence that a spectacular flop is unlikely. They don't demonstrate decisively that Akamai is on track to achieve its goal of being even more successful in enterprise security than it has been in cloud security.

Here are some of the challenges that Akamai's product, sales and marketing teams are either encountering already or will encounter in the market place:

- **Inertia**. More than ten years after people first started recognizing that the security perimeter was fatally compromised, some organizations have yet to refresh their architectures to reflect that. Likewise, many will resist the proposition that the remote access VPN and micro-segmentation should be phased out just because "that's how we've always done things."
- **When it's what you know, not who you know**. It's one thing for an enterprise security team to receive Akamai's Zero Trust pitch having been recommended to them as security leaders by their own colleagues in the developer team. Absent that internal recommendation from the other side of the wall, Akamai's sales folks will be starting on the ground floor along with a variety of well-established enterprise security vendors. Even then, enterprise security and web security folks do tend to fit different demographic profiles: it's a broad generalization but the former are more likely to be older and from networking backgrounds whereas the latter are

more likely to be younger and from software backgrounds. The recommendation from across the other side of the wall is sometimes valued, sometimes not.

- **Real networks come in many shades of grey**. Perspectives on the risks of VPN access vary significantly according to the type of VPN access you're talking about. A high level of security coupled with an intelligent client that supports a variety of secure connectivity options, irrespective of the user's location, is very different from a solution lacking those attributes. Akamai also states that EAA is designed to co-exist with existing remote-user VPN technologies to ease the phasing in of applicants and user populations. Has the ease of push-button micro-segmentation via solutions like VMWare's NSX come with the double-edged sword that many enterprises have over-segmented their networks causing too much complexity? Yes, for sure. But for many organizations, that should just mean limiting segmentation to truly critical applications rather than doing away with it altogether.

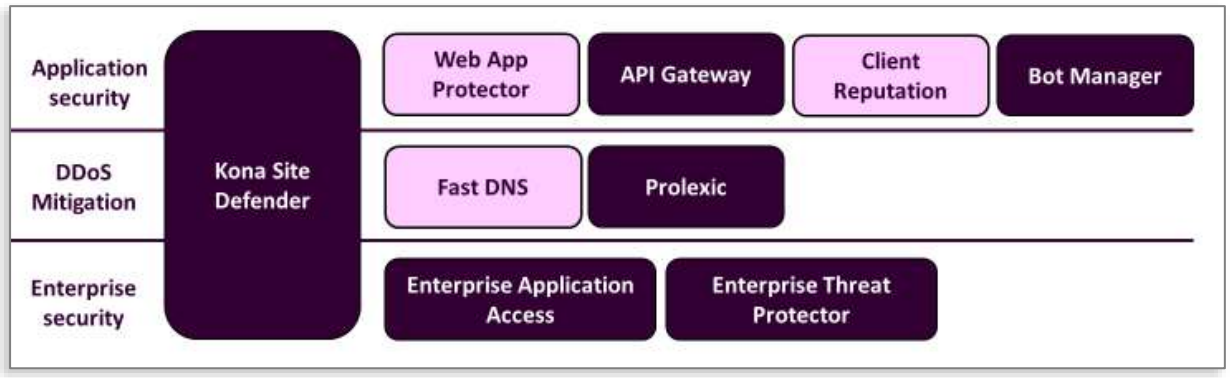
Best of breed buyers expect EAA and ETP to each stand on their own two feet without having to lean on one another.

- **Best of breed buyers**. One of Akamai's strengths is that it offers both pieces of a Zero Trust approach – the tightly controlled access and the inspection of everything. This is certainly valuable for enterprises that are focused on consolidating their security vendors, as many are. Best-of-breed buyers, however, expect EAA and ETP to each stand up on their own two feet without having to lean on one another.
- **Controlling access with accelerating velocity of consumption**. Ensuring that authorized users and devices only have access to the applications they need rather than the whole network is a sound enough security objective. Where it is liable to get complex, however, is as organizations progress through phases of digital transformation. This adds more and more applications and devices into the enterprise network. At the same time, organizational and individual user tolerance of delay in accessing the applications they need is lessening. Akamai needs to be able to demonstrate that EAA's way of pre-determining what a user or device does or does not legitimately need can maintain speed and accuracy of outcomes as application consumption and diversity scale up. It needs to demonstrate that EAA doesn't risk forcing the security team back into the role of "Dr No", imposing unnecessary restrictions on an organization's operational agility. Akamai points to a number of features of EAA as addressing that. Perhaps the most important is that EAA supports a range of configuration options that allows access to be extremely strict, or wider, depending on the individual enterprise's risk tolerance.

How far can Akamai go from here?

The jury is still out on exactly how far Akamai can make inroads into the enterprise security market. The approach is disruptive, credible and clearly seeing some amount of traction with some high end customers and partners. The buying environment is nevertheless very different. It's early days but expect investor pressure to drive the release of more detailed numbers before long.

Figure 2: Akamai's Security Portfolio



Source: HardenStance/Akamai

More Information

- November 2017 Briefing: "What Akamai will do with Nominum"
- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- Register for free email notifications when HardenStance publishes new content.
- www.hardenstance.com
- HardenStance received no payment for publishing this Briefing.

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.