No.1
29th November 2017

HardenStance Briefing

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

What Akamai Will Do With Nominum

Akamai's acquisition of leading DNS provider, Nominum, closed earlier this week.

- Akamai will sell its whole portfolio into Nominum's global telecom operator accounts.
- Akamai will leverage Nominum's threat and security intelligence across the business including on the Akamai Intelligent Platform and across its security portfolio.

Akamai's strategy

The highly distributed Akamai Intelligent Platform now consists of more than 240,000 servers in more than 3,700 locations installed in more than 1,600 networks in 131 countries. Akamai is also planning for 'beyond the edge" - end device software enabling peer to peer networking. According to its latest corporate messaging, Akamai is committed to being "the world's largest and most trusted cloud delivery platform, making it easier for companies to provide the best, most secure, digital experiences today and in the future."

"Akamai's annual revenues from telcos will still only be $100 million once the acquisition completes"

In the first part of 2017 investors were rattled by declining revenue in Akamai's media business arising from the big cloud providers like Google and AWS accelerating investment in building their own CDNs. This bearish sentiment contributed to Akamai's stock price sliding steadily from around $70 in January to around $45 in September.

Once 25% of Akamai's revenues, the cloud giants now account for just 8%. As that change in the revenue mix has rippled through the business, Akamai generated $2.3 billion in revenues in 2016, up 6.5% on 2015. For the quarter ending September 30th 2017, Akamai reported 6% revenue growth Year on Year (since when the stock has recovered to around $55).

Some highlights around the company's growth strategy:

- Lead in meeting the scalability and performance requirements of the growing OTT Internet video market, including "better than broadcast" OTT for broadcasters;
- Double the size of its security business to $1 billion in 4-5 years;
- Increased focus on selling to – as well as selling through - the telco market;
- Double down on investing in web performance as web pages get ever more complex;
- Close the gap on competitors like AWS on allowing customers to interact with its platforms with their own DevOps models and open APIs.

Nominum helps with the key telco market

Even with Nominum now formally acquired, Akamai's annual revenues from telcos are only $100 million. Akamai wants to grow that number aggressively for several reasons:

- to backfill the decline in revenues from webscale cloud providers;
- to exploit the anticipated growth in the OTT Internet video market,
- to exploit the tilting of the regulatory playing field in the U.S in favour of telcos, as evidenced by the FCC's recent decision to roll back the principle of net neutrality.

A sense of the telco sector's increased importance in Akamai's strategy can be gleaned from the recent restructuring of its reporting divisions into four. The carrier and enterprise business has been split into two stand-alone units. And whereas separate individuals now head up the web and enterprise businesses, one individual purposely heads up both the carrier and media businesses. For an explanation of that, look no further than BT Sport. And for a bet on which of the four business units are most likely to merge over time look no further than carrier and media.

The acquisition creates strong cross-selling opportunities

Akamai already has partnerships with big tier ones like BT, AT&T, Bell Canada and others but it's still only scratching the surface. With its global account footprint of more than 130 telecom operators in more than forty countries serving 500 million subscribers, Nominum gives Akamai far greater account access to the telco market.

"Nominum gives Akamai a core DNS value proposition which aligns with the traditional buying patterns of most telcos"

Everything on the Internet needs to go through DNS. It is critical infrastructure that cannot fail. It is also the control point and business intelligence tool from which Akamai drives key configuration changes for customers. This conjunction of key control point with large global footprint of telco accounts looks like one of the two most important drivers behind the acquisition.

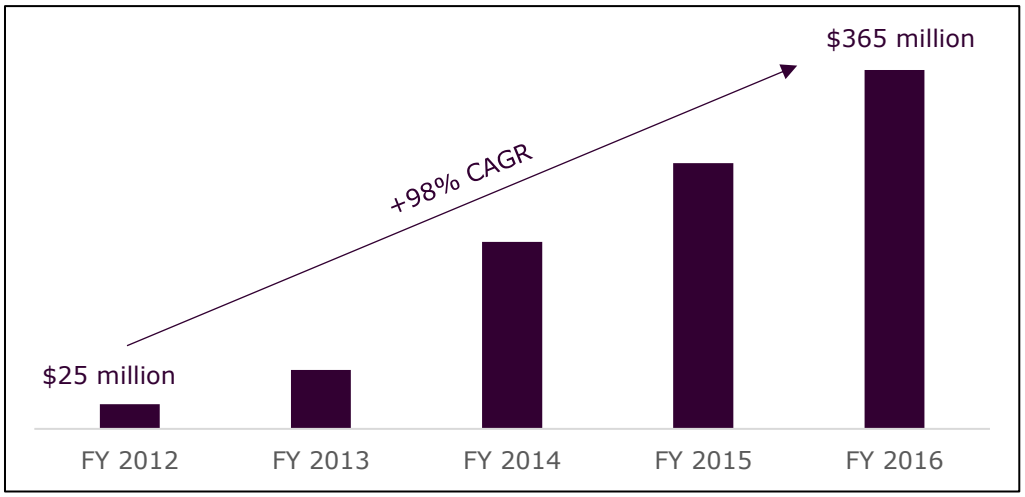
The main prize is the substantial cross-selling opportunity for Akamai's whole portfolio of services into telecom operators. That's primarily core web, media and enterprise services. There are also key upsell opportunities like security. Virgin Media is a good example of the cross-selling opportunities here. Virgin is an established customer for Akamai's DDoS protection as well as Nominum's parental protection services.

Nominum's core business still consists of shipping DNS server products into telcos for them to operate themselves. Hence Nominum also gives Akamai a core DNS value proposition which aligns with historical telco buying patterns better than Akamai's mostly cloud based DNS services. Assuming management wants to continue investing in Nominum's DNS server product line for at least the medium term, Akamai's sales model into the telco sector will have to adjust accordingly.

Nominum enhances the security portfolio

Having grown its security business from $25 million in 2012 to $365 million in 2016 (see **Figure 1**) Akamai now pitches itself as "the world's largest pure-play cloud security provider". This year the company will hit around $500 million in security revenues and wants to grow the security business to $1 billion in four to five years.

Figure 1: Akamai's Security Revenues 2012-2016



Source: Akamai

The largest share of this year's $500 million comes from the Cloud Security portfolio. This sits in the Web division, centring on protecting customer websites against external attacks. In Q3 2017 the Cloud Security portfolio was the fastest-growing part of Akamai's whole business. It grew 27% year-over-year during the quarter to $121 million or about 20% of total revenue. **Akamai sees still greater growth potential in the enterprise security market, recently launching two new products into that space, including Enterprise Threat Protector (see below).**

DNS is a primary target as well as a primary source of cyber-attacks. As well as being the critical control point for customer configuration changes, DNS is also an excellent control point from which to insert security. Hence, leveraging Nominum's assets to drive the security business to its $1 billion target – as well as underpin the broader business – looks like the second key driver of the acquisition.

"DNS is a primary target and a primary source of cyber attacks. It's also an excellent control point from which to insert security."

Nominum Security Research is considered key

The opportunity to drive DNS threat intelligence derived from Nominum Security Research – formerly Nominum Data Sciences – across its cloud and enterprise security portfolio is especially prized by the Akamai management team. This should augment Akamai's security portfolio and enhance its "most trusted" brand positioning.

With Nominum processing 1.7 trillion DNS queries per day, Nominum Security Research lays claim to seeing a unique volume of DNS traffic from which to extract and curate high value threat intelligence. Nominum Security Research also cites leading edge data analytics capabilities including the application of proprietary (unsupervised) machine learning algorithms to the vast lake of DNS data that it sees.

The global market in threat intelligence remains highly fragmented. Many ecosystem players continue to seek to differentiate based on the unique view of the threat landscape that they see. In that context, acquiring Nominum doubtless lifts Akamai onto a new level from a threat intelligence perspective. The question is by how much?

Threat intel sharing has always been a little bit like world peace: easily formulated into top-table communiques; thorny to implement on the ground. These days, though, the momentum is with the sharers and with those that want to make high end DNS security in particular widely available and free of charge.

In a general sense, you can see sharing at work in the Cyber Threat Alliance (CTA) which has managed to bring together Cisco, Check Point, Palo Alto Networks, Fortinet, Symantec, McAfee, Sophos, RSA and others. Its strong governance structure compels member companies to contribute a high level of threat intelligence as a condition of continued membership. Some CTA members even cite their collaboration as having driven faster alignment around industry-wide understanding of the WannaCry outbreak.

You can see specific efforts around making DNS threat protection freely available by other big beasts of the cybersecurity world.

- **The Global Cyber Alliance (GCA) has just launched Quad9, a free DNS resolver service.** Built out with Packet Clearing House (PCH), Quad9 automatically checks DNS queries against IBM Security's X-Force's threat intelligence database. Accurately comparing the DNS threat intel of IBM Security and Nominum is beyond the scope of this briefing paper. Intuitively, though, the probability that Nominum beats IBM Security out of sight – even on DNS security – feels like a bit of a stretch.
- **The UK's National Cyber Security Centre (NCSC) is working with Nominet to make free DNS threat protection services available** to public and private sector organizations**.** The NCSC might not see 1.7 trillion DNS queries a day but it is still part of GCHQ, one of the world's premiere intelligence agencies.

If the momentum around threat intelligence sharing builds rapidly– as many would like it to – Akamai may not get quite as much differentiation from Nominum as management

expects. The other way of looking at that, though, is that in an environment of increasing threat sharing, the Nominum assets still serve to secure a position at the top table of threat intel sharing which Akamai alone might not have been be able to land.

New threat intelligence across the DNS portfolio

With the acquisition complete, Akamai has a newly refreshed portfolio of no less than seven different recursive and authoritative DNS products and services. The new line-up can be viewed here: Akamai's newly enhanced DNS portfolio.

Nominum's threat intelligence will be leveraged to take the security features of the whole portfolio to the next level. The four secure DNS and pure-play security product lines that stand to benefit most from Nominum's assets are AnswerX; Fast DNS; Enterprise Threat Protector (ETP) and Kona Site Defender (KSD).

"Akamai has high hopes of even stronger performance in enterprise security than in its traditional web security business"

AnswerX

AnswerX is Akamai's recursive DNS solution, enabled by the March 2015 acquisition of Xerocole. AnswerX comes as a highly scalable DNS Cloud Resolver solution; an in-source carrier grade DNS resolver solution for telcos; as well as DNS resolver engines for telco architectures as they virtualize. Until now AnswerX has tended to be pitched in competition with open source DNS on the one hand and with DNS product vendors (like Nominum) on the other. A core part of the value proposition of AnswerX for telcos and other customers is the ability to build their own customized version of a service according to a DevOps model.

There are specific opportunities for specific parts of Akamai's DNS portfolio to be combined with Nominum's in pursuit of enhanced security outcomes. One that Akamai is known to favour is combining attack data with the Nominum and AnswerX capabilities to notify telco customers that have been infected and get them cleaned up.

Fast DNS

Akamai's Fast DNS authoritative services are optimized for attack resilience for those organizations who cannot have their domain go down from an attack. It competes in the market in cloud-based managed DNS services with the likes of Dyn (part of Oracle); Google; AWS and others.

Leveraging the highly distributed character of the Akamai Intelligent Platform, Fast DNS is architected for performance and availability even through the largest DDoS attacks and is available as a primary or secondary solution. DNSSEC is available as an optional add-on to protect against DNS protocol manipulation.

Akamai is committed to ongoing upgrades to its internally developed Fast DNS servers so that they will always have substantially more capacity than the largest DDoS attack yet seen. There's the potential for Nominum's own server products to feature in the evolution of the Fast DNS roadmap at some point. Whether they will or not hasn't been communicated yet.

Enterprise Threat Protector

With high hopes of even stronger performance in enterprise security than in its traditional web security business, Akamai launched new enterprise products earlier year, one of which is Enterprise Threat Protector (ETP). Built on the AnswerX cloud, ETP is a recursive DNS service that provides enterprises and carriers additional network based end point protection against complex targeted threats like malware, ransomware, phishing and DNS-based data exfiltration. Specifically it allows employees to be blocked from accessing infected sites as well as providing protection against DNS exfiltration attacks.

Akamai reckons that its highly distributed number of clusters of DNS resolvers around the world gives ETP a competitive differentiator. Akamai also guarantees under SLA that

100% of DNS queries will be resolved. After less than six months in service, ETP is "only" handling 150 billion DNS queries per day. Insight from Nominum's 1.7 trillion should enhance ETP's competitive positioning.

In the initial RFPs it has contested, Akamai reports ETP going up most frequently against Cisco's "Umbrella" product. Umbrella combines Cisco's acquisition of Open DNS and its Advanced Malware Protection (AMP) product, with additional extensions to other Cisco capabilities like the acquired Cloudlock assets. Cisco provides another example of how Nominum's threat intelligence prowess will be tested. At over $2 billion, Cisco's security business is four times bigger than Akamai's. As well as OpenDNS, Cisco also acquired threat intel specialist, TALOS, in 2015 and is a member of the Cyber Threat Alliance.

Kona Site Defender

"The Akamai team shows no sign of wanting to alter the company's positioning with respect to DHCP or IPAM"

Kona Site Defender (KSD) was the primary driver of the Cloud Security business' stellar performance in Q3. Kona leverages the Akamai platform's huge distributed capacity to protect its customers from large web-based DDoS and targeted web application attacks.

Kona also examines all traffic coming to a customer's websites, apps and APIs, blocking malicious traffic. In the wake of the Equifax attacks, market messaging around Kona emphasizes its role as "a virtual patching layer" in front of websites and applications – "allowing customers to be protected even when they haven't patched everything".

Having been positioned as protecting customers' externally-facing websites for many years, the latest 5.0 Kona release adds support for APIs and measures to protect the enterprise's internal applications. Recent enhancements include the extension of protection to attacks that target APIs like SQL injections as well as out of the box and API-based integration with leading SIEMs.

"Business as usual" on the DDI front?

The Akamai team shows no sign of wanting to alter the company's position with respect to Dynamic Host Configuration Protocol (DHCP) and IP Address Management (IPAM). The combination of DNS, DHCP and IPAM into an integrated DDI solution is an established product space, pitched primarily at the enterprise market. Akamai already partners Men&Mice, one of the smaller DDI players, where needed. This is typically for on-prem authoritative DNS.

Being telco-focused, Nominum's forays into the DDI space have been confined to a partnership with FusionLayer to develop an integrated management solution across the DNS and DHCP domains. Nominum Configuration Manager (NCM), based on FusionLayer software, is still available to customers. That seems to focus largely on the centralized management of Nominum's DNS engines. The partnership also operates where customers have Nominum's DNS engines and want to expand the solution towards IPAM.

Interest in EDNS

One notable interest that Akamai has is in Extension Mechanisms for DNS (EDNS). Of particular interest is EDNS Client Subnets (ECS), a draft IETF standard which yields more granular end user detail from DNS servers as the basis for determining which specific servers should be attached to which specific end users. Akamai can be expected to look into the case for accelerating efforts to drive industry adoption of ECS.

HardenStance Ltd Disclaimer of Warranty and Liability

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.