Patrick Gray:
Hi, everyone, and welcome to this special Soap Box edition of the Risky Business podcast. My name's Patrick Gray. These Soap Box podcasts we do here at Risky.biz are wholly sponsored. That means everyone you hear on a Soap Box edition of this show paid to be here. But that's okay because we pick interesting and great sponsors who generally have very interesting things to say.

This edition of the Soap Box podcast is brought to you by Akamai. And yeah, it's funny because they booked this podcast slot last year. And you know, here we are all of a sudden, months later, in the middle of this terrible crisis, and Akamai is right in the thick of it. Obviously, there are some massive shifts happening right now. So many people are stuck at home and on the Internet right now. So much traffic being pushed around. And yeah, Akamai's series of tubes are getting a pretty serious workout.

In addition to doing CDN and DDoS mitigation stuff, Akamai was one of the earlier companies to offer an identity-aware proxy. So a whole bunch of organizations are using identity-aware proxies right now to serve internal applications to newly external users. There's a bit of a mad rush on to do that. So naturally we're going to talk a bit about that in this podcast. I mean, there are clear advantages to this approach over just provisioning everyone VPN access and sort of dumping them onto your LAN, in a weird free-for-all. As you'll hear, these identity-aware proxies are great for serving up anything that's normally accessed with a browser, including internal applications.

[00:01:45.29]
It does get a little bit more complicated with non-web-based applications, like thick client applications. We're going to talk about that. But yeah, look, another nice thing about using these types of proxies over a VPN concentrator — *your* VPN gateway, *your* VPN concentrator — it's easy to DDoS. But taking down Akamai, that's going to be a little bit harder. So a little bit harder to knock you offline for ransom. So, yeah, we'll get into all of that in the interview. And look, sadly, I suspect that knocking people's VPN gateways off for ransom is going to be a thing if this crisis keeps drawing out the way it is. We get into all of that in this interview, and I suppose I should tell you who it's with at this point.

Today's guest is Patrick Sullivan, who is Akamai's CTO of Security Strategy. He joined me for this interview and started off by telling me what an identity-aware proxy actually is. Here is Patrick Sullivan.

[00:02:38.64]
Patrick Sullivan (Akamai):
The central goal is to move users off of a privileged network segment. That has proven time and time again to be very difficult to defend. So rather than —

Patrick Gray:
These things are designed to kill VPN access, basically. That's the idea, isn't it?

[00:02:55.41]
Patrick Sullivan (Akamai):
Yeah, it is. It's a different access model. So rather than having where you are in the network topology be the primary key for access, here, it's irrelevant where you are in terms of network topology.

What matters is your identity, your ability to strong authentication, the posture of your device, and then least-privilege role in the organization. So for example, me as a technical user, I would be granted indirect access. The proxy that's inspecting and logging all my requests to maybe some software

delivery, a productivity suite, but I wouldn't have reachability to sensitive HR applications within corporate or financial applications that my role doesn't grant me any viable reason to access.

So to boil it down, if you're on a typical VPN and you run a port scan, you're going to see lots of ports open and lots of potentially bad IP addresses connecting to your network all kinds of returns that represent risk. With the EAA model, you run a port scan and you see basically the IP address of a proxy that understands your identity and will grant you indirect access to the applications that your role warrants.

[00:04:12.11]
Patrick Gray:
So this is like identity aware and kind of application aware. So the idea being, me as a user, I can Duo authenticate to my Okta single sign-on (SSO), which then tells this Akamai identity-aware proxy to connect me to various applications which might even reside on the LAN, right? So this is a way to get those legacy applications from inside an organization to the outside in a way that isn't going to get you hacked immediately. I mean, that's the summary here, isn't it?

[00:04:42.0]
Patrick Sullivan (Akamai):
It really is, yes. So the nuts and bolts, you would publish applications by installing a bit of software, you know a connector that runs on a VM sort of in application hosting LAN, whether that's your own co-location, your infrastructure as a service provider — that connector is a diode. So it dials out, basically leaving you with a micro-perimeter that need not accept inbound connections.

You just re-use that outbound connection and then end users would connect in to the identity-aware proxy at the very edge of the network, which would first ensure strong authentication before any connection is made. And that could be either native or third-party multi-factor authentication (MFA).

We would then understand where to derive identity information. So that could be IDaaS (identity as a service), it could be a local directory, and then from there enforce least-privilege, indirect access to those applications. So now in this model, you're not on the network. No privilege on the network. Even as an authenticated user. You've been externalized. Really trying to cut down on that whole threat of lateral movement for the soft underbelly of corporate applications.

[00:05:57.27]
Patrick Gray:
Now, one of the things that I really like about this is that it is a 2020 approach. It's a modern day approach to accessing legacy applications while still using some of those other wonderful things that we like, like, you know, modern-based CASB, risk-scored authentication, and stuff like that.

I mean, you're probably getting better — if you're doing this with those sorts of technologies — you're probably getting better authentication and trust in users, even when they're connecting from the outside of an organization.

But let's talk nuts and bolts, right? Because the problem with this sort of technology has always been that it's not necessarily as easy as it sounds to just make this all automatically work. Now, this product that you're talking about, I think you've had it in Akamai's portfolio for something like four years. There's a lot more competition now in that space. Everyone from Microsoft to CloudFlare to F5 — there's a lot of

people doing this stuff. But why don't you sell me on how easy this is to do? And I imagine you would have kicked off quite a few projects in the last few weeks. Sell me on that.

[00:07:06.84]
Patrick Sullivan (Akamai):
Yeah, it certainly has been busy. You know, I think you often will talk to organizations that are aspirationally saying, "We want to use the Internet as our corporate WAN and move security up to the application layer." I think many people find themselves in that situation in 2020 where, like it or not, kind of that remote access extension *is* the critical part of that access model.

So I think the key for Akamai is we're building this on a pretty unique platform where we can intercept those requests right at the very edge of the network, where the most capacity exists. We can do all of our 20 years plus of accelerating those transactions for end-user performance, availability, scale, all of those types of things. And then also, port and protocol support. So not just supporting web applications and RDP, but also supporting arbitrary ports and protocols in the same model.

[00:08:04.68]
Patrick Gray:
Now that's where it gets a bit interesting, right? Because anyone can sort of glue together something that's going to web proxy and tie in with all of these CASB brokers, because that's all web stuff, right? Like anything that's served over web — web, web, web, easy, easy, easy. But when it starts getting to these weird legacy, thick-client enterprise applications, that's where it all starts going a little bit odd, right? And I'd imagine that's where, probably, most of the friction is when you're trying to do this. Is that right?

[00:08:31.97]
Patrick Sullivan (Akamai):
Yeah. Those can be — they typically are. You typically want to take out your web applications or RDP applications first, because those are, as you say, quite easy to do these days. When you get into 30 or 40 year-old thick client applications with vintage authentication, that's often where we push a client down to the endpoint, so we can intercept those odd ports and protocols and speak all of the right languages internally in terms of other authentication protocols while presenting more of a SAML front-end to the to the client. So hiding some of that complexity on the internal side of the proxy. So the proxy gives you that ability to break the session sort of in two, allowing you to sort of keep everybody happy on either side of the proxy.

[00:09:23.42]
Patrick Gray:
Are you going to be doing stuff like serving people RDP session windows that are accessing this application in like a window and you serve them that window? Or is it really that you're going to have to push that thick client to the endpoints that are on the outside of the network so that they can then tunnel in through this proxy? Like, it just sounds like it starts getting a bit messy at that point.

[00:09:47.14]
Patrick Sullivan (Akamai):
Yeah, so any of these kinds of legacy applications, in some cases, if they are a thick client, you're going to want to retain that thick client. You could present RDP in a browser window if that is a viable alternative for you. So you do have some architectural flexibility there. It depends on the approach that you want to take.

[00:10:05.76]
Patrick Gray:
Yeah. And what sort of approach have people taken in the past and what are they sort of doing now? Because I'd imagine here would be some projects in the works, happening right now, doing this stuff.

[00:10:16.39]
Patrick Sullivan (Akamai):
There are and I think that's kind of, you know, as remote work has increased, that has led to a big increase in people looking at this model. You do have to kind of relook your remote access strategy. So that's, I think in some cases it's an acceleration of a strategy that people had already. And in other cases, it's, you know, people trying to supplement maybe what they're doing with the VPN to get a surge of remote access capacity, to get around some of the bottlenecks just in terms of sheer capacity at the corporate data center, right? It's a pretty easy way to avail yourself of a cloud model where there's usage-based capacity there. You don't necessarily have to plan for what percentage of your users are going to be coming in via remote access. That capacity planning challenge really is not as significant in this model.

[00:11:11.88]
Patrick Gray:
Now, when we talk about DDoS, you know, because that was something that came up earlier. I'm guessing that just by nature of this thing going through Akamai — you're just connecting to Akamai's Edge and then into the core of your network — I'm guessing that gives you some inherent DDoS protection right off the bat? Because in order to block my access to your edge, I'd need to take you down. And that's kind of hard because Akamai is big.

Patrick Sullivan (Akamai):
Yeah. I mean, we're seeing a lot of traffic as people are working from home and stuck in the home for recreation.

Just in terms of the outbound traffic that we're seeing, I think Q1 of last year was close to 70 terabytes a second. This Q1, we've seen closer to 160 terabytes a second. So we're pushing all of that on the outbound, which means on the inbound asymmetric side, we've got quite a bit of capacity there to absorb DDoS.

And then we can also intercept routes via BGP, should you need to protect some remote access solution that you have there as well, so we can scrub out DDoS from clean traffic that's coming in to really whatever remote access suite that you have. So it's certainly something that people are keeping in mind as the remote access is such a vital part of the business right now with everything going on.

Patrick Gray:
Yeah. Now, look, you've got access to a lot of traffic, right? You see a lot. Akamai sees a lot. What's it like out there at the moment? I mean, are you seeing a lot of attacks? Are you seeing attacker behavior change? People dropping off a bit? What can you tell us about what's happening right now?

Patrick Sullivan (Akamai):
Business as usual. You know, for the most part, I think the attacks persist. I think some of the techniques sort of have differed. I think there's been a lot of coverage around using the crisis as phish bait for malware distribution. I think a lot of the conversations we've had are with savvy security teams that know to think like an attacker.

There've been some early reports of some businesses that are dependent on remote access getting hit. But I think it's mostly just proactive. Organizations are just trying to understand, given the heavy dependence on remote access right now, what does that attack surface look like? Do we need to take another look at what it looks like and what tools are in place to prevent it or block those threats? So those are some of the exercises we've been going through in recent weeks.

Patrick Gray:
Do you get the sense that's there's going to be some positives to come out of this with regard to how people are actually just sort of running their businesses? Because I feel like this is one of those events where, a year from now, things are going to be different and they're going to stay different and some of it's going to be bad. You know, a lot of it's going to be bad, but some of it's going to be good as well. Do you feel like there might be some weird positive impacts on the way we all work? On the way that we run our organizations? Not just the technology, but more broadly speaking. It just feels like a time of great change right now.

Patrick Sullivan (Akamai):
Absolutely. So I think on the technology side, many organizations have directionally been heading toward, call it Zero Trust Access or whatever that may be. So I think some of those security decisions that are already long-term architecture may be accelerated. So maybe that's a positive that comes out of this. I do think that our systems will be more robust on the other side as people work through these challenges and enable people to be really productive from a remote access perspective. It's going to cause some IT headaches in the short term, but you have to be optimistic that that's a potential benefit coming out of the other end.

Patrick Gray:
Now, look, one of the things we're seeing now is a whole group of people working from home who previously didn't work from home. And while a lot of organizations have been able to go out and secure supplies of new hardware, like whether that's just buying a whole bunch of Chromebooks or just refurbished laptops, whatever it is — there's kind of been a run on hardware. So it's my feeling that a lot of people out there are going to be accessing company resources using their own hardware, their own systems. Is that something that's happening out there at the moment? Is that something that you're hearing much about?

Patrick Sullivan (Akamai):
I think it is, right. So we have heard a lot of desire to RDP into, you know, the machine that's in the office, something along those lines. And I think one of the keys here to the identity-aware proxy is the ability to have kind of a contextual security decision, right?

So, part of it, as we discussed, is your identity, your need to have access to a given application. But along with that, some of the other decisions you can make are:

- "What is the posture of the device that we're willing to accept, either passively or more actively if the operating system (OS) firewall is disengaged?"
- "Are you willing to grant access, maybe to a message from HR around work from home policy? But then, if you go to a more sensitive financial application, maybe at that point you would be prevented from taking that step?"

Patrick Gray:

So you're saying, yes, people are provisioning access to company resources from BYOD and that you're somehow measuring system health of those devices.

[00:16:29.45] How are you doing that if you're not running a client on those systems? The way Duo does it is they capture browser agent strings and sort of look at that as a proxy for overall system health. But what's Akamai's approach to this? Is it similar?

[00:16:42.83]
Patrick Sullivan (Akamai):
It is, yeah. So it would be passive in the case where you don't have a client. And obviously those things are spoofable. When you do have a client, you can get in there and gain much more rigorous understanding of more variables there. So the ability to have a client does allow you to burrow deeper there and gain a better understanding. But in the absence of anything else, you go with the passive elements that come across in the session.

[00:17:08.3]
Patrick Gray:
So do you have customers who are pushing Akamai's clients out to employee-owned hardware? Is that something that's happening right now?

Patrick Sullivan (Akamai):
I think that's a decision that a business would have to make — are they willing to push that via mobile device management (MDM)? I haven't seen a ton of that. You know, I think at this point, you still sort of have the traditional managed versus unmanaged.

Patrick Gray:
But before they can push it through MDM, they need to actually push MDM to a user's own personal device. If I'm an employee, I can imagine installing an Akamai client as an employee on my own hardware. But no way am I installing MDM.

Patrick Sullivan (Akamai):
Yes. So not seeing a ton of that. I mean, other than the, you know — many corporations on your mobile device, you have that already. But I'm not seeing a huge departure yet from your personal workstation, where you're MDMing those devices, to your point.

[00:18:04.66]
Patrick Gray:
And are you seeing success at the moment? Can you think of a couple of case studies you've been involved in where organizations had to pivot very quickly to work from home and they've been able to do it with these technologies? Like what's the quickest someone's been able to move?

[00:18:18.86]
Patrick Sullivan (Akamai):
Yes. So I think web applications, to your point. Typically people take those on first. So that's the first thing you do. And there you can move quite quickly. I think for thick client applications, that's going to take a bit longer.

[00:18:31.92] And typically that's a phase two type of a project that we would see, coming on the heels of the quick wins you can get with those more transparent web and RDP type of applications.

[00:18:43.73]
Patrick Gray:
So what are the sticking points with the thick client stuff? You've got those different approaches where you can actually put the thick client software onto the endpoint and then, sort of, that endpoint is provisioned access to that network resource and then can go direct from the endpoint right into the gut, to the enterprise, and access what it needs to make that thick client application work. That's one way. Another way, the way that I like and that you've discussed, is you set up some sort of RDP gateway where client authenticates to that, it authenticates onwards to that thick client application.

[00:19:21.23]
How long does it take? Is there a uniform approach to making that work and making it work quickly? Or is this just a case-by-case basis and it's really fiddly and requires some development work? Or is it the case that, if you're prepared to go to an RDP sort of translation layer, that it's just very easily done? But you've got to spend a little bit of time setting it up?

[00:19:44.63]
Patrick Sullivan (Akamai):
You know, there's a lot of variability in organizations, but I think what we're seeing is, in a lot of those cases, people are pushing the client out to their managed devices as kind of the — that's really the most frequent strategy that we see.

[00:19:56.66]
Patrick Gray:
Well, that's going to be that's going to get you there the quickest, isn't it?

Patrick Sullivan (Akamai):
I think so, yeah. At least for managed devices.

[00:20:01.64]
Patrick Gray:
Now, earlier on in this interview, you described a massive increase in traffic across Akamai's network as compared to last year.

[00:20:11.21] What's that been like? Because I imagine you would have had to add a lot of capacity, right? And you're not the sort of organization that's just going to spin up some cloud resources because you are kind of one of those companies. You are actually a company that's going to operate its own hardware. What's that looked like from an Akamai perspective, trying to spin up all of these extra resources in the middle of a crisis?

[00:20:35.09]
Patrick Sullivan (Akamai):
Yes. So I think the good news is that we were in the midst of a pretty significant ramp up. This year there were a lot of OTT video services that are launching. That's driving more traffic than anything else. And then also, this was a peak year for presidential elections, Olympics. So all those things are big traffic drivers. So we've been pushing to get in front of those for some time. So that's part of the business — being there to scale in the event that we do see the expected traffic for OTT releases, for gaming releases that come out, and similar type of events.

[00:21:18.89]
Patrick Gray:
So you were rolling out extra capacity anyway, basically. But I'm guessing it'll bring forward additional capacity planning now because you probably have got less headroom now against DDoS attacks, you would think, right?

[00:21:31.67]
Patrick Sullivan (Akamai):
Well, I mean, the symmetric nature of the traffic, typically things like — as people come to view their bank balance, go to e-commerce, leverage an OTT service, those are highly outbound. The inbound is quite a bit less. So in some ways, if you have a symmetric platform as we do, the inbound is a little bit of a free lunch there, right? So we're building for peak on the egress side, which leaves us quite a bit of ingress to absorb those type of things. But to your point, I think we're always building, always trying to stay well out in front of not only the threats on DDoS, but also just the peak traffic flows, which typically are events.

[00:22:15.02]
Patrick Gray:
So Akamai, I guess, probably best known as an early CDN, DDoS mitigation, stuff like that.

[00:22:22.49]
But Akamai has been around a long time. I believe you used to host Facebook or Facebook images. I don't know if you still do, but you know, that's been the sort of traditional history of Akamai. But it seems like you're doing an awful lot more now. What would you say Akamai's business actually is? Because it feels like it's got a dozen things that it does now. What are the big things? What would you say the top three or four are?

[00:22:47.09]
Patrick Sullivan (Akamai):
Yeah, so we look at our business across three business units. So the first is CDN. And then the second one would be accelerating dynamic web applications.

[00:22:58.79] And then the third would be security. So protecting web applications, DDoS, API protection, as well as this identity-aware proxy model that we spoke about. Of those, those are roughly give or take sort of a billion dollars each with security growing the fastest. So if trends continue, security will be our largest business unit in short order, just given the growth trajectory there.

[00:23:29.03] So I guess the answer is, primarily a security company, would be the way we look at ourselves.

[00:23:34.94] Well, it also makes you already one of the largest security companies in the world. I'm wondering, though, I'm curious, if you're already doing a billion dollars in security, what else are we going to see? Because that's up there from an infosec company point of view. What sort of other services are we going to see you launch? Are you going to start going into email delivery, messaging security, what else can we expect to see?

[00:23:59.6]
Patrick Sullivan (Akamai):
Yeah, absolutely. So a lot of focus on web applications. I think that's where Akamai is probably best known.

[00:24:07.33] So we continue to expand what we're doing with web application protection. I think a shift that we're seeing there is, now we are instrumenting the client to get in front of the web supply chain. So a modern web application. Certainly there are some calls that go back to your data center. But half of your calls could go to your third-party widgets — all the formjacking that we see there. So that's kind of a newer service that we have in 2020, monitoring the behavior of JavaScripts from the perspective of the runtime on the client. So getting in front of that other series of threats there that come from your web supply chain. So that's a really interesting area that we're focused on in 2020.

[00:24:59.02]
Patrick Gray:
All right. Well, Patrick Sullivan, thank you so much for joining us on Risky Business on the Soap Box to have a bit of a chat with us at this time of crisis. I'm glad that we've seen these emerging services, these emerging platforms, kind of come along at a time that we actually need them.

[00:25:16.63] I look forward to finding out from you how 2020 went, in a year from now, when this all starts ratcheting down. When it all starts winding down, it will be interesting to see where we're at. Again, thank you very much for joining us. And we'll chat to you again soon, I'm sure.

Patrick Sullivan (Akamai):
Thank you, Patrick.

Patrick Gray:
That was Patrick Sullivan there from Akamai. Big thanks to him for that. And huge thanks to Akamai for sponsoring this edition of the Soap Box podcast from Risky.biz. I do hope you've enjoyed it. And that is it from me this week. I will be back next week with more risky biz. But until then, I've been Patrick Gray. Thanks for listening.