Avast Business

White paper

The Security Impact of Digital Transformation

Avast Business' David Ryder on How to Thrive in 'End of Box' Era

16 September 2021

ISMG INFORMATION SECURITY MEDIA GROUP

Avast Business

About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

Introduction

Cloud solutions, the mobile workforce, the skills gap – these are among the security impacts that don't get enough attention when discussing digital transformation. **David Ryder** of Avast Business opens up on these topics.

David Ryder

Ryder is the director of SMB & MSSP at Avast Business, where he is responsible for North American development and adoption of an industry-first cloud network security subscription model tailored for the managed security service partner. He has over 15 years' experience in network security in a diverse range of verticals and security partners.

In an interview with Tom Field of Information Security Media Group, Ryder discusses:

- Security topics that don't get enough attention;
- New security gaps created by the impact;
- What it means to be in the "end of the box" era.

Cloud Challenges

Tom Field: So, we're going to talk about digital transformation. There are some areas I particularly want to talk about – some of the security impacts that we don't discuss enough. And the first is cloud solutions. What can you tell me about it?

David Ryder: The world is moving to a cloud model ... as part of a digital transformation. In the past, we polished up security starting at the perimeter. Workers came to an organization and they were secured behind a firewall as well as other layers of security.... But as more employees work remotely, the perimeter moves with the remote worker now. That presents an incredible challenge to the conventional security model.

In order to provide true security, we have to acknowledge the reality that today's modern worker is typically remote, and traditional solutions do not address that in terms of perimeter security.

Avast Business

Skills Gap

Tom Field: Regarding the mobile workforce and its impact on security, how do we address the skills and the personnel gap?

David Ryder: Organizations ... used to have the technical staff that were able to provide a fairly high level of security. That's actually gone away in recent years. There's an enormous crunch when it comes to technically proficient people who can manage your security.... A lot of the people that are managing security are fundamentally unsuited and untrained.

This is causing a vast amount of problems. One of the biggest issues that has not been addressed is that we're doing business over the cloud, we're doing business on the internet, but the internet is now virtually fully encrypted.... The traffic is going through the security appliances complete uninspected. Which means that all the other security features – the IPS, the anti-virus, that cloud sandboxing – none of it actually works. It is only pseudosecurity.

Now put that failure in conjunction with the personnel who are unable to manage to inspect the encrypted security on these appliances. To manage security on these appliances is borderline impossible to extremely challenging. It almost requires a one-to-one approach in terms of personnel to the appliances. But between the lack of qualified personnel and the difficulty of managing security today, we have a crisis.

'Screen of Blindness'

Tom Field: David, when you consider all these factors – cloud solutions, mobile workforce, the skills gap –what new security gaps do you see created?

David Ryder: It's not so much a security gap as a massive screen of blindness. Now, we also have to look at the fact that everybody is mobile, so how are we going to fix it? We can identify what the problems are. We know there is a lack of skilled personnel out there. We know that there's a lack of resources. The traditional appliances are having a very, very hard time providing basic security that people are actually buying and acquiring and buying them for. So that's the gap.

The news is full of examples of breaches ... including breaches at the National Health Service in Britain and Equifax, just to name some of the big ones. But this stuff happens on a daily basis in terms of ransomware infecting the city of Baltimore, Atlanta ... and other cities as well as hundreds if not thousands of small businesses that are badly affected by these threats as well on a daily basis.

We have to be able to provide the highest level of security across the board because everybody does business on the same cloud solutions. So the gap out there is personnel and technology. That's what we're looking to address; that's what I believe we have successfully addressed here with the Avast network security solution. It's an "always on" SSL inspection with full cloud sandbox technology, meaning that 100 percent of traffic will be inspected 100 percent of the time without specific traffic that you're going to exclude from inspection.... That's the major issue that we're fixing.

The other issue that we fixed is that we make it easy to provision, and it's on all the time for all the remote workers. Every remote worker never leaves the security perimeter; there's a full inspection all the time. So, it's not a case that we have to go and inspect the device, make sure the certificate's up to date. The device, regardless of where it is in the world, is always behind our network security platform.

Current Shortcomings

Tom Field: Why do traditional security solutions fail to fill the gaps that you've talked about?

David Ryder: Maybe because they are not inspecting encrypted traffic. ... If you were to go and ask your security provider or your employees in charge of security for your organization, "Are you inspecting the encrypted traffic coming into our network?"... the answer in most cases would be, "No we're not." That's ... an incredible hole in security. It's also a major challenge because they're not inspecting the encrypted traffic; other security means that are put in place do not work. The sandbox cannot inspect what it cannot see. Sandboxes are effective at finding zero day threats if they can see them.

Equifax had a very sophisticated sandbox in place, but the sandbox was unable to do anything to protect them from the breach because it could not see if the traffic was encrypted. That means people are relying on the endpoints to bail them out today. Now, depending on whose threat reports you read, you're going to see ... more than 100,000 threats throughout every day....

On a daily basis, you're exposed to thousands of threats that will just eat the endpoint. To be truly secure, we have to have an "always on" perimeter that moves with everybody, inspecting crooked traffic. That removes an enormous amount of threats right there.

Once we run it through the sandbox, we reduce the threats down to a manageable level. And now the endpoint isn't forced to do all the heavy lifting by itself. You provide a very, very nicely layered solution to provide security for your always on enterprise, which are employees everywhere. That's the major gap – the lack of inspection. What we have is the fix for that for the network as well as the remote work.

Ransomware

Tom Field: David, you mentioned Equifax. More recently, we've seen incidents like Capital One, and there been the ransomware outbreaks throughout government and elsewhere. Are there any specific immediate security events that you consider to be very significant to what we're talking about today?

> "Between the lack of qualified personnel and the difficulty of managing security today, we have a crisis.

Avast Business

David Ryder: Well, the ongoing security events we talk about all the time that are getting the most media attention are ransomware attacks. Ransomware has moved in from an occasional thing to a very, very specific targeted attack. People aren't just accidentally getting hit. It's not a "to whom it concerns" approach so much. Ransomware is a valuable commodity when its developed, and it's targets specifically are individual people within an organization. Its an ongoing stress. As you can see, the damage it's done to large cities is absolutely enormous in terms of loss of productivity, loss of records, detrimental effects on law enforcement, tax collection, as well as providing services to the citizens of that city.

I would regard that as one of the most significant threats that's ongoing these days. It shows no sign of decreasing, and the security needs to be up to par to deal with it.

> "What we really want to do is make access to the security very, very flexible and very, very easy.

'End of the Box'

Tom Field: David, in past conversations you've talked with me about us being in the "end of the box" era. How is this likely to change how we approach cybersecurity in the coming year?

David Ryder: I do believe we are in the "end of the box" era. The customer premises equipment, the box, has reached the end of its useful life.... It's too restrictive. You put into place a security policy that's based on what you anticipate will happen for the next few years. Typically people are tied in financially to the appliance, and then you run into a situation that you're going to have the conflict between business and security. Business will frequently win out at the expense of security. We're in an era when bandwidth is becoming massively inexpensive and very widely available. The boxes simply can't deal with that in terms of sizing them.

They also, like I said, require very, very heavy management. They're difficult to deploy. They're very rigid in their performance in what you can do. They do not scale very well. For an example, we have a lot organizations... in the tech business that might have one, two gigs of data coming into their network as well as having the remote workers. If they were to size an appliance deal with two gigs, especially trying to inspect the encrypted traffic, they would be in tens of thousands of dollars, sometimes it's financially unviable for an organization to get that.

This alternative right-sizes them immediately, provides some of that infinite scalability for whatever kind of bandwidth they want. It makes it always-on security for the remote workers. That, by comparison, to what the appliance is bringing in rigidity means that the box is going to go the way of the Dodo bird very, very quickly.

Avast Business

Avast's Role

Tom Field: So, David, to bring it back to Avast, how are you helping customers to prepare to make this transformation securely?

David Ryder: Well, in terms of managed service providers, we're providing them with a product with always-on SSL inspection and data security features. But what we really want to do is make access to the security very, very flexible and very, very easy. We built the financial model around a no commitment, month-to-month model. We know when people use our product, they'll want to stick with it.... We want to make sure that security will always remain flexible.

One of the things that we are absolutely committed to here is making sure that somebody can always access the best security without any financial penalty, even if that means somebody moving away from us.... That's perhaps one of the most significant things we believe in ... access to enterprise-level security that's used to secure some of most critical enterprises on the planet and bringing it down to the level that any company can afford to have it and have ease of management in a financial model that's very, very easy to adopt and very, very painless

About Avast Business

Avast Business provides integrated, enterprise-grade endpoint and network security solutions for SMBs and IT service providers Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. The result is superior protection that businesses can count on. For more information about our managed services and cybersecurity solutions, visit **www.avast.com/business**.