COLEMAN
VISASQ

Cybersecurity

Our Expert :
Brad Bussie

SVP & Virtual CISO – Entisys360

- SVP & Virtual Chief Information Security Officer at Entisys360
- Managing Director of Security Strategy at Trace3, Inc. (April 2017 – May 2020)

Brad holds more than 18 years of experience in the cybersecurity industry with deep specialization in Endpoint Security, AI, Identity, and Cloud. He currently serves as a leader and specialist at a leading cybersecurity advisory and value-added reseller of cybersecurity products. At Entsys360, he is the key decision-maker who evaluates, negotiates, and selects partner cybersecurity vendors including companies such as PANW, CRWD, SentinelOne, Okta, Zscaler and others. Previously, he held an executive position at Trace3, Inc where he led their security advisory, strategy, and architecture. In this role, he helped C-level executives better understand security initiatives like CCPA, Zero Trust, and IAM among other security focused responsibilities.

Moderator:
Max Le Sieur

Founder & Managing Partner at Rosemont Legacy

- MBA, Harvard Business School
- Investment Banking Associate at BMO Capital Markets (07/2016 – 08/2020)

Expert Insights On:

- Overview of what comprises a cybersecurity threat for enterprises. Vectors of vulnerability.
- Changes in vulnerability over the years and outlook.
- Endpoint security overview. Endpoint security vs Network security
- The role of the CISO today vs the past
- Products and services that exist today for endpoint security and network security
- Competitive dynamics in the space and key players
- How has artificial intelligence and machine learning impacted cybersecurity?
- How companies may be leveraging Copilot and cybersecurity and whether and how Copilot AI can learn to protect systems?
- How do cybersecurity budgets fare in uncertain economic times?
- Key trends and future outlook of the broader cybersecurity market

Introduction -

Max: So Brad, thank you very much for taking the time. My name is Max, and I'll be leading this call on behalf of Coleman Research. And so as you know, the purpose of the discussion is to learn about cybersecurity, including endpoint security, network security, key players, and key industry trends.
Before we begin, I want to remind you that we are in no way soliciting any material non-public information or any information that is confidential related to any company or organization you are currently or have ever been affiliated with. Does that make sense?

Brad: Understood. Agreed.

Max: Awesome. If you feel as though the answer to any question would involve non-public information, please tell me right away and I'll take us in a different direction. Does that make sense? Cool.

Brad: Cool. It does, yeah.

Max: Perfect. So Brad, do you have any questions before we hop in?

Brad: I don't.

Overview of the Cybersecurity Landscape -

Max: Okay, perfect. And so I think we're ready to hop in. What I'd like to start with, Brad, is just endpoint security and network security. And where I think we should start is just high level what comprises a cybersecurity threat for enterprises.

Brad: Absolutely. So let me walk you through what I would call the anatomy of an attack and how attackers really think about compromising a environment. So when you look at cybersecurity and you think about what a threat actually is, think of it along the lines of what could potentially happen to your environment. And traditionally, organizations have thought of this as, how do I defend my network, my people, my data, my endpoints?

And really if you boil it down, those threats that most organizations are concerned with tend to revolve around a couple of different things. First and foremost is vulnerabilities. Because a lot of the time a vulnerability is something that an organization either can't do a lot about or maybe isn't as well equipped to do something about. And vulnerabilities come in a lot of different flavors.

Typically, it can be a deficiency in some kind of software that they have, whether it's something stemming from Microsoft Office, whether it's a vulnerability that you find in a web browser or some other kind of application. Some of the ones that organizations really don't have a lot of protection from are things that we call zero days. So a zero day, all that really means is it's a vulnerability that's being exploited that there isn't currently a fix or a patch or some way of defending against it.

So I'd say the third piece of threat tends to revolve around users. So users either having too much access or users that are targeted specifically because they have more access than they could potentially need. And credentials, so my username, my password, my multifactor authenticator key/token, those are things that all of the attackers are going after. So those are threats to organizations.

So there's a lot more, but honestly, I think that's a good way of setting the stage because it does cover applications, endpoints, the network and the users. And I would say what are all of those things pointing towards? Really that's data. What are the attackers after? What's the biggest threat to an organization? It's either someone getting their data, somebody holding their data hostage or someone destroying their data.

And then there's another one that's emerging, which is someone changing the data in such a way that it no longer looks how it did before and you can't distinguish what's different about it. And that's very much a threat when it comes to things like healthcare where you could be tinkering as an attacker with medical records and you could change potassium on a chart for a patient, or you could double, triple, quadruple the medication.

Brad: And in some cases no one would know. They would administer the medicine and the next thing you know you're having a bad day. So those are some of the threats that I think you could easily wrap your brain around.

Max: Got it. So Brad, I just want to summarize. So the application layer, there's the application, there's the user, and then what was the third one? You mentioned three, right?

Brad: Network and then data.

Max: So there's four places or four vectors of vulnerability for an enterprise.

Brad: Correct.

Max: Got it. Just so I understand, what are attackers trying to do? So what's the point of messing around with data is to hold the company ransom? So I guess holding the company ransom for a ransom payment is a very straightforward way to monetize your effort in terms of being a bad actor. Is that the gist of what people are trying to accomplish here is just get paid by exploiting a vulnerability? Or is there some other kind of motivation to these bad actors?

Brad: Yeah, yeah, I'd say the monetary side of it is still the most popular. And there's actually a chart that you can look at on Google that starts to break down early '90s through early 2000s where everybody was worried about viruses because what were viruses doing, they were destructive. They would get into a system and they would destroy.
There was no like, hey, let's monetize this. It was just people behaving badly and bringing systems down, crashing networks, doing things, whether it was mischievous or whether it was taking something offline for some other reason. But attacks have definitely morphed into more of a business and they are pretty heavy towards the ransom side of things.

Brad: But there is still, I'd say if you were looking at the second style of attack, similar to, and most people know what happened with Stuxnet where a virus was engineered to attack a very specific thing inside of nuclear power plant. And once inside, it either spun some of the centrifuges too fast, others too slow, and ultimately it crippled another nation's nuclear capabilities. So that's the other side of it; instead of demanding a ransom, there is destroying something for another reason. And it depends on what that reason would be, but there's a bunch of different ones, but I don't think that's super important.
So I would say those are the two main things besides the third, which is stealing data. And in some cases when you steal data, what are you wanting to do? While you're wanting to ransom and get paid for it. Alternately, you want that data because you want to build a better airplane or a better naval vessel or an advanced missile system. So you're stealing the information to, in essence, make one of your capabilities better.

Max: Got it. Got it. And so we talked about the four vectors of vulnerability for enterprises. How has that changed over the last decade? And where do you think that's going? What are kind of the areas where enterprise are going to be the most vulnerable moving forward over the next five years, let's say?

Brad: Yeah. I mean there's a pretty firm statement that I definitely believe in now after watching how attackers have changed up their methods. So it used to be the old adage, your attackers are breaking in. Well, now your attackers are actually logging in. So the style of attacks have definitely shifted from that brute force kind of, I'm going to keep attacking and guessing and trying to figure it out to how about I just steal credentials and I try using those.
So one of the things that attackers have gotten pretty good at is they have their own version of the internet. So there's the dark web and the deep web, and there's a whole commerce kind of business out there where all of these data breaches that are happening, I mean, everybody's gotten that letter, we're so sorry, your personal information is now for sale or it has been stolen.

Brad:

And then they give you a list of all the things that they take it. And in some cases it's just your username. Sometimes it's your first name, last name, date of birth. Other times it's your social, sometimes it's your bank account information. The list is pretty long and it's kind of scary when you start to look at what they actually have.

So then it's up to the attacker to decide what kind of an attack are they going to create. Are they going to do a phishing style attack where they're going to take the email address of yours and they're going to email you with something that looks pretty legit, like, "Hey, you should get credit monitoring because you just got compromised. Go here and sign up and put in your credit card, put in your information, download this application." Which then infects your system.

And while some of this can target just the individual user, next thing you know you are hopping from your personal machine over to a business machine. And these attackers are getting into businesses in seemingly legitimate ways because they're on "trusted device" but people are really not doing a very good job of keeping work and home separate, especially with what's happened from the pandemic. Some people got to go home and stay home, or as I like to say, they got to go anywhere and stay anywhere.

And the attackers have pretty much figured out that the old network defenses and the perimeter, that kind of stuff really doesn't exist anymore. And the person's identity has really become that new perimeter. Some organizations are doing a good job, others aren't. So that's where the attacks have just completely changed. It used to be, "Hey, here's a virus. I'm going to try to infect a system." And it's gone much more towards the social engineering, the phishing, the spear phishing, the ransom, and it's not so much destruction anymore, it's more of monetary. I'm either going to make some money from this, I'm going to take some pictures that you had on your cloud or device that you don't want others to see, and I'm going to extort you for it.

Brad: It's gotten a heck of a lot more of that, and I don't see that slowing down. I see that continuing. I see that accelerating, and I think that those style of attacks are going to continue to get more and more advanced. And part of that is because of artificial intelligence, and a lot of it has to do with some of the phishing emails and style of attacks that we would get. We knew it wasn't a Nubian print that was trying to get us to click on something because you couldn't really read half the email. It was completely broken, couldn't understand it. Was very obvious that it wasn't something where you were inheriting the millions.
With AI, the attacks have gotten really pretty well done, clever. I actually did a little call it round table with a bunch of executives, and in that round table we created some very compelling letterhead, same colors as an organization, really had the same look and feel because we had given the AI a sample, and next thing you know we had a phishing email designed that was incredibly difficult to determine if it was real or not.

Max: So your contention is that individual users are the area where an enterprise is the most vulnerable moving forward.

Brad: Correct.

Endpoint & Network Security -

Max: Got it. That's super helpful. That's interesting. And so that brings us to endpoint security. And so what are enterprises trying to accomplish when they put in place endpoint security measures? What are the broad strokes of how to think about endpoint security?

Brad: Sure. Yeah. I mean, broad strokes, endpoint security is trying to do a couple of things, trying to prevent viruses because those still exist. They're still floating around. There's preventing rootkits, there's identifying pattern based and behavior-based style of attacks. That's the first level of endpoint.

Brad: But really the next piece of it is making sure that there is a firewall. And that's always been a thing. But what you're finding is most of these endpoint solutions have a software firewall that goes beyond just the Windows or the Mac based firewalls. They're centrally controlled and they look very similar to what an old network firewall protecting an organization would've looked like.
And a lot of this has to do with the fact that the users aren't behind the four walls of a building/organization anymore. They're kind of wherever they are. So the realization was we have to protect from the virus's, ransomware, all that kind of stuff, but then we also need to make sure that we're protecting the ports and really looking at traffic and making sure we understand what it is, if it's good, bad, allowed, all that kind of stuff.
So you're also starting to see inside of endpoint security, things like browser isolation. And you're going to start to see, as I'm talking through this, like there's a bleed between endpoint and network security now. And there's this next piece that we'll get to, which is what we call the SSE or the SSE. So it's a security edge and just think of it as a big proxy in the cloud, but I'll stay on endpoint for now.
So essentially we've got the antivirus endpoint detection response side of things. We've got the firewall component, and then we have, think of it as an application runtime. So what applications are allowed to run on a system, what's allowed to be installed? And there's a way of really locking down what is allowed on your endpoints. That's typically the focus right now of most endpoint security platforms.

Max: Got it. Got it. And so you touched on this overlap with network security measures. How are network security measures different and where are they applied and how is that distinct from endpoint security measures?

Brad:

Yeah. Sure. So there's this whole concept, and this was the buzzword of last year. The buzzword of this year is AI, but the buzzword of last year was ZTNA or Zero Trust Network Access or Architecture, depending on how you look at it. So really what's happened is with the dissolving of the perimeter is what we're calling it, because people aren't in the office anymore, they're kind of wherever. You're having to bring your protection closer to the application, closer to the endpoint and closer to the user. And the way that we as an industry have done this is through that zero trust architecture. And just think of it as you're trying to understand what is your protect surface. You're making sure you map all of your data flows. The way that we've done this is through that secure access service edge. There's a bunch of different products we can talk about, and I think we'll talk about that a little bit.

But from an architecture standpoint, picture this, okay? You install an agent on, we're just going to use a laptop, for instance. You install an agent on a laptop, it takes whatever identity that your organization uses. Let's just say we use Azure. So when I log onto my workstation, I have to authenticate, I'll use my token or my face or my finger or whatever it is to make sure it is Brad. And then I have a connection, which is an always on connection to the cloud.
And all of my browsing, all of my reaching back into my organization to get a file, printing or accessing Salesforce or ServiceNow or whatever my applications are, all of that passes through a proxy. And that is what we call the SSE. And what that proxy does is it encrypts and decrypts network traffic. It does data loss prevention, it intercepts malware that could be in flight from exchange online or from Google. It enforces zone control. So let's say for instance, I live in Denver. I authenticate in Denver, but then maybe an hour later it shows that I'm trying to authenticate from New York City. That is an improbable travel event, and something like that would not be allowed. It would be flagged and then it would be reported.
So in essence, I'm taking this security layer that used to exist. This was something that was in a data center back in the '90s, early 2000s. But the only way to take advantage of it was if I was on that network. Well, that's not the case anymore because that network is everywhere. So I have to treat everything like the internet. So what I've done is I've centralized all of this traffic in one place, which is this proxy, and that is how the network has evolved.

Brad: And give it another three to five years, and in most instances, you won't have a firewall as an organization anymore. It's all going to be this kind of technology that I'm describing. And maybe I'll have firewall functionality coming from my big platform player like Google GCP, Azure or AWS. Maybe in some cases it would be Oracle, but in essence it's going to upend a lot of the things that we've been doing as a IT/security vertical because it just doesn't make sense to do it that way anymore because our business is fundamentally changed and continues to change.

The Role of CISO -

Max: Got it. Super helpful. Super helpful. How would you describe the role of a CISO today? And how has that changed over the last decade?

Brad: Yeah. Well, I think that in a lot of organizations, the role of CISO has become a bit of a revolving chair. And what that means is organizations haven't done a very good job of funding security programs or funding that CISO position.

Max: What makes you say that? Why do you say that?

Brad: It really comes down to, I'll use a car insurance analogy. Some people really like the full coverage. They want the comprehensive and the liability. They want the low deductible. They want to make sure that if somebody's injured in their vehicle, they'll be covered. They like all of these things. And then they look at what the premium's going to cost. Then they go, well, that's really pretty expensive for something that may not even happen.

So they start to lose a couple things like, well, I guess I could probably do without that, or maybe I'll take a little bit of a higher deductible plan, and they start to do some unnatural things. Same thing happens with health insurance. In a lot of organizations, cybersecurity gets looked at as “a nice to have”. I think it's shifting, but it's still not there yet. Cyber is still a component of or a subset of an IT budget in a lot of cases.

Brad: Now, granted, there are some organizations where some of cyber gets funded from legal or risk or other areas, but by and large, in my experience, it's still a CISO reporting up to a CIO and they get just a piece of the IT budget. So cyber defenders are trying to do a lot with not a lot of budget, and there are so many different types of attack. There's those four entry points, but then once you're in, there's a lot of different places you can go. And it's definitely not cheap to end up doing it right.

And from my own experience being A, practitioner, but being a CISO and defending my own organization, there's really never enough from a dollars perspective because I am there to mitigate risk, but I'm not typically viewed as something that makes the company money. Granted, if I can keep the organization from getting compromised, I am in essence making money. But there are enough organizations that are just trying to slip under the radar that there's just this kind of, can we do just enough to get by? And that is why.

And I will definitely go out on a limb and say that this is fact why we continue to have so many large data breaches and why people keep getting letters because there is a way to combat and stop 80% of this. But most organizations are not doing the foundational components. And a lot of the time it's because they simply can't afford it. And the CISO becomes the scapegoat and next thing you know, they're out.

You could see this just happened with Microsoft, this has happened with a lot of other organizations. Just if you pay attention, one of the first thing that happens, they've gotten breached, the CISO's out. And in a lot of cases that's probably not the right decision or the best decision. Because they know the network and the systems and how to defend everything better than anybody else because they've been doing it. But the problem tends to be they're not supported, they're not funded well enough.

Max: Got it. So you're suggesting that's what happened with Microsoft recently because they weren't funded well enough?

Brad: So with Microsoft, I think that's definitely a big piece of it, but I also think that they have some organizational challenges as far as a security arm that has the right, I don't want to say like heath or you have to listen to them or true enforcement. What I see in a lot of very large organizations is the business and the business initiative will trump cybersecurity every time where cybersecurity will say, you need to make sure your code practices are as follows, and the business says that will add six to nine months to our release cycle. We can't do that, we're not going to do that. And then cybersecurity says that you have to, that is the mandate. And then it goes all the way up to the top of the business and the business says, just get it done.

And next thing you know, something goes out the door, it's vulnerable, or there's something in an identity and access management system that was not well tested, it was not well understood, and you're left with the same thing. But fundamentally, it does come back to not having enough of something in organization, whether it's money, whether it's clout, or whether it is truly saying from a compliance perspective, this software or this update cannot release because we haven't done all of the things that we are supposed to do. So I see that pretty much everywhere.

Max: Brad, is it true that funding is directly correlated to level of defense? Like if something happens and a vulnerability is exploited, is it always because there was not enough funding really, or can it be because things weren't properly organized? Just to press on this a little bit, to your earlier point, to the extent users are the ultimate vulnerability, you could put in all of the software, all of the checks and balances, all of the protection you want. If you have an employee that clicks on the wrong phishing email because they're not paying attention, the level of funding may not have helped there, right?

Brad: So I will say, as in most things, that's 80% I would say yes. Now, there are ways as far as browser isolation as well as a couple of other things where I could have a user that is just read to compromise me and they click on everything. And if I've got the right defensive measures in place, then I start to mitigate the weakness of the actual user.

Brad: So I think it's something that, there's been a lot of philosophical debate about this, whether security awareness training actually works and helps to mitigate some of those things, or whether we should just say what our users are fallible. And no matter how much we train them, it's just not going to do any good.
I think organizations should have a bit more of a balance than they do. I think some organizations look at security awareness and that's their first line of defense, and then they go a little cheap in some of the other areas. But again, the business tends to, I'm not going to say complain, but maybe complain that, well, wait a second, this browser isolation, it's very inconvenient because now I can't get my files the way that I used to.
I go into my email and I click on that and I can't actually download it because an isolated browser, I have to go a different way to get my file and it takes longer or it's too cumbersome so they don't end up doing it. And yes, that would mitigate all phishing, but it slows the business down to the point where they don't end up doing that and they say it's too hard or doesn't work for the business.

Max: Yeah, I get that. I mean, just as a user, if you have to re-log into everything every 30 seconds, it can be annoying just as a rudimentary example.

Brad: Totally.

Overview of the Products and Services -

Max: Yeah. Okay. That makes sense. Okay, so we'd love to hear you comment on the products and services that exist today for endpoint security. I know the space can be a little bit of alphabet soup, but there's the identity exit management, privileged access management. So there's a number of area or types of products out there. I would love for you to just comment on the overarching tools available from an endpoint security perspective.

Brad: So if I'm looking at endpoint security, as you said, alphabet soup, that's a great way of describing it because I think if you were to type in endpoint security and pull a list, you would have 50 different options. But I think truly there are only a few that actually matter in the grand scheme of things. For endpoint security, I think some of the names that you could assign to this space would be CrowdStrike. I think another fair one would be SentinelOne.

I feel that when you look at this from a platform perspective as well, that ends up being something that is like your Palo Alto Networks, your Cisco, Microsoft, because they all have endpoint security components to them. And if you break down, what does Microsoft have? Well, they got Microsoft Defender for endpoint, Cisco has AMP, Palo Alto has Cortex XDR.

But if I'm looking at this from my pure play, really the ones that make the most sense and I see the most often is CrowdStrike, SentinelOne. And then there's always one of those platforms that are being considered. There's a bunch of smaller ones, but I don't think they're really even worth spending a lot of time on because they don't perform as well in any of the tests. And I think most organizations are going to gravitate towards one of those others.

Max: Got it. Super helpful. What about network security? Would love if you could provide just an overview of the products or services available for network security?

Brad: Yeah, network security is another one that I think what you're starting to see is a lot more gravitation towards that secure service edge, the always on approach. So that would be your Zscaler, Netscope, Cato Networks, and Microsoft as well is jumping into that. So their new Entra line and of the identity component, but there's also the network component for Entra, which is going to challenge Zscaler and some of the others.

So those are really that next three to five years that are going to, I think replace some of the things that we're still doing in data centers, whether the data centers in the cloud or wherever else.

Max: So Brad, endpoint security is easier to conceptualize for me anyways, because it's like logins assigning different levels of authorization for different users and for how deep they can go or what they can access, just cycling through credentials and automating and then doing the same thing for APIs because it's not always humans that need access to things, but it's computers and so that makes sense. And like logging into a work laptop or work phone, et cetera. But what do these network security tools do exactly?

Brad: So really they do some of the fundamentals that you would expect from before, which is they're preventing a style of attack, which is called man in the middle, where there's a way of capturing and replaying information and maybe even decrypting some of that. And what they're doing is they're ensuring that integrity of information from point A to point B to point C and back to point A.
So think of network just as it always has been, it's a transport layer and you're ensuring that the transport is encrypted, it's been encrypted and decrypted in the right way. The information is the same as when it left as when it arrives. So that's kind of one of the core tenets of all of this. And there's even the piece of making sure that there's no malware. That is because as a defender, the best way to prevent or the best way to combat malware is to prevent it in the first place.
So if I don't ever have to have CrowdStrike do its job, that's even better. So if I can stop that malware at the network layer before it even gets to the system or the endpoint, that is the best way as a cyber defender to make sure that that stuff is good. So I think that's one way of thinking about it.
And then it is the intersection between identity and network, because I think you hit it on the head already, it's identity and endpoint, but then there's identity and network where I made one of those kind of a, hey, I'm Brad in Denver, but all of a sudden I'm Brad somewhere else. So that's one of those things I think that is definitely network focused. So hopefully that makes sense on how that looks.

Max: Okay, great. And so now I want to talk a little bit about the competitive dynamics in the space and who the key players may be. You've alluded to some already. Is endpoint security and network security still the right way to break it down? Or how would you segment the market?

Brad: All right, can you repeat that just one second for me?

Max: I would like us to talk about the key players in the cybersecurity space. How should we segment the market? Should we still just talk about network security versus endpoint security or is there a different way to break it down?

Brad: Yeah, I just want to make sure I unpack that correctly. So I think there are four ways that I would look at the market that make sense. Network security is one, endpoint security is two. I would look at identity as three, and then I would look at data as number four. And there's argument that is, well, where its cloud in all of this? And I feel that cloud can be made up of any of those ones that we just talked about.
I would say one that may or may not get picked up in the ones that we've referenced is application security or DevSecOps. And the reason for that is if I'm going to build secure applications and I'm going to prevent some of those vulnerabilities in zero days that we talked about at the very beginning of this call, I need something like application security to make sure my libraries are secure, my coding practices are secure and I am building a resilient application. That I think is the way that really those cover, I think everything within cybersecurity.

Max: Got it. Okay. That's helpful. And so who are the key players in each?

Brad: Yeah, so if I'm looking at identity and access management, I would say SailPoint, Okta, Microsoft, Ping and ForgeRock. Those are my picks. They're the ones that I'm typically talking with clients about. I would say if I'm looking at data security, it's Varonis, it is Netrakes. You've got some of the same players. SailPoint has a data governance part of their solution. I would say you've got Concentric AI is another one. There's a bunch that are emerging in the data space. So that's one that I would definitely watch.
I think endpoint, we hit all the ones already. And then in network security we definitely hit. There's a subset of network which is more focused around detection response where you'll find Vectra, Cisco and some others. So I don't want you to think that space doesn't exist anymore, it's just not as focused right now. I think a lot of that other stuff that we've talked about is more applicable.

Brad: And then if I'm looking at the application security that is, you just actually watched CrowdStrike make an acquisition here, so that's kind of a space where there's a few that you'd recognize like WiZ and I think Palo Alto Networks, I think this is the right way. And they looked at it early.
And you were able to see Twistlock and a couple of others get acquired. But that's definitely an area that there's a lot of players. So I think the one that I was looking for is BIONIC. BIONIC is in there and a few others, but I think I hit most of the others. I think that's probably most of them.

Max: Got it.

Brad: I don't think I missed one. Did I miss one?

Max: No, I think that's helpful. That's helpful. Do CISOs want more or less vendors? Yeah, I'll just leave it at that.

Brad: Yeah. As a CISO, I want less vendors, but I want what's called defense in depth. So I want fewer vendors that have more capabilities that I can leverage. Think of it as like a backup or a fail-safe. I want to be able to have a initial protect surface and then I want something backing that up should it fail for any given reason.
So I think one of the veins of a CISO's existence is complexity. And the more we can simplify... I know this sounds kind of funny because I've had this discussion with a lot of different people over the years where they're like, "Wow, security is so complicated." And I said, "To be honest, security done right is actually more simple than you would think. It's just done right, it's effective." And I don't know, as a CISO, that's what I'm looking for.
And if I can get everything done with one platform, so for instance, the station you'll have with CISOs is Microsoft, because Microsoft has made so many investments into their security product platform, not necessarily their internal security, but their platforms that others can use as part of their E5 licensing.
You've got identity, you've got endpoint, you've got data security, you've got network security. The only thing you don't really have out of the box typically is application security, but you've got all of these different components and you're getting it from one place. The argument is, well, what if there is a vulnerability in the Microsoft stack and all of a sudden your entire Security protect suite is taken down? I agree with that.

Brad: So what do I do? Well, I'll just say for example, I've got Defender for endpoint, but I also have CrowdStrike. So in some cases I will have two alerts that fire at the same time and two actions that try to take place at the same time. One of them is going to win. Sometimes it's CrowdStrike, sometimes it's Defender. But essentially if one of those were to go down, I have a feeling of security, it's a funny word in this, but I have a feeling of security that I will still have that layered protection.
So do I want 12 best of breed products? I don't. I think that there's a place for something like that. You have to have a very specific use case. You have to build something, you've got a widget, you're a business that does one thing really well, and maybe it makes sense to bring in best of breed, but for most organizations, we're looking for platforms. We're not looking for best of breed.

Max: Super helpful. As a CISO, do you see this space just... So cybersecurity in general, especially endpoint management and identity seems like something that would be straightforward for the CSPs to bundle, and in fact, they already have in a lot of instances. And so is that where this ends up whereby single cloud or multi-cloud and just all of the cybersecurity solutions are baked into your cloud provider?

Brad: I could see that. And it's interesting because this exact kind of approach, Max has actually come out of the network side too, where there are a lot of network players that are doing this exact same thing. So I'm just going to make one up. I'm going to say Verizon.
All of a sudden Verizon is like, "Hey, why don't you just subscribe to our service and you'll get the Verizon endpoint, which does antivirus protection?" No one's going to tell you that's actually they just rebranded it or it's somebody else that they rebrand, but it becomes part of your contract with that network provider. I think the clouds are doing the same thing. So if I'm watching Mandiant... Say that again?

Max: Sorry, go ahead Brad, you cut out for a second, but then came right back. Apologies didn't mean to interrupt. Please keep going.

Brad: No, that's all good. No, you're good. So look at Google. They just acquired Mandiant and they also have acquired a couple of others like Chronicle, VirusTotal, a few others. So they're starting to build a very solid cybersecurity foundation. Microsoft, they've built their own, they acquired a few companies, but a lot of this is their own that they've built. AWS, they've got all of theirs that they've created, and pretty much anything you want is in that stack.

So I think it's a fair statement that that is going to become more and more common. I also think it's going to become more common for organizations to acquire their software through the CSPs. So you're going to see these big providers with their marketplaces, and instead of going and getting something from CrowdStrike or from a reseller, you're actually just going to go onto your marketplace, you're going to click CrowdStrike, you're going to put in how many of the things and you're going to click submit. And next thing you know you've got the licensing, you're downloading, you're installing, and you're off and running. I think that's going to be the stop gap while all of this gets baked into the big providers. I think there's always going to be options, but I do know that this pay monthly service going to continue to grow, but I can say a lot of Ciscos are wishing they could go back to more of the capital model as opposed to the operating model. Because if you look at some of those operating models, it's pretty rough on a business now.

Before that was kind of the way, but then it's like, wait a second, I'm just going to use a number. I'm spending 50,000 a month on my security stack, where before it was like two million bucks, but it was that for three years and I could capitalize that whole thing as opposed to just as a service. So I don't know, I think there's a lot that's going to happen next couple of years. And that's definitely one of the merging points is endpoint network identity program provider.

AI and Cybersecurity -

Max: Got it. Super helpful. Super helpful. And so Brad, you alluded to it earlier, but I'd like to formalize your view. How has artificial intelligence and machine learning impacted cyber security generally?

Brad: Well, I think it's in progress and I think you can get a really good view of this right now with... So since endpoint was the focus here and network too, look at what's coming out of CrowdStrike right now. Look at what's coming out of SentinelOne with their Purple AI and ChatGPT and really the whole large language model. What does that mean? That's in essence going to help cyber teams make decisions faster and it's going to automate detection, remediation, automation, predictions.

I think the impact, we've been watching it the last couple of years in machine learning, especially around security operations, orchestration, remediation. So you've heard people talk about SIM and then now the big thing is talking about Soar. I think you're going to find most of AI's impact in Soar right now, but I think you're also going to see it in identity and access. A good example of this would be CrowdStrike, their acquisition they made a couple of years ago in Preempt.

That identity piece, it's active directory focused, but it's going to demonstrate some of the things that we're talking about where for instance, I'm Brad, I've got access to pretty much everything, but my normal pattern says I only log into a certain number of systems. But all of a sudden I'm trying to access five servers that I've never accessed before, even though I'm allowed, I have the permissions, but I haven't done that before.

And all of this is going to be an algorithm that says, well, just because you can doesn't mean you should. So I am going to actually ask for a second level of either authentication or I'm going to ask Brad's boss, I'm going to ask the CEO, "Hey, should he be accessing these systems? Do you allow that?" "Oh yeah, that's fine." Or it's going to become more of a behavior thing that's going to say, well, all of the other things leading up to that moment say I should not give Brad access because I think he's going to take something. He's going to leave. He looks like he's looking for another job and he is looking like he's going to bounce, so I'm going to deny that.

Brad: And that is a very real thing that can come out of artificial intelligence because it's looking at patterns. And they've already shown studies that an AI can detect a pattern much faster than a person and they can tie together five million data points that points to Brad's looking for another job. So I think that's the kind of stuff you're going to start to see early.

What the next five years is like with AI is, I don't think it's as scary as people think. I mean, everybody that I've talked to, they're saying that initial layer of cyber defenders, that whole layer is going to go away. And then so how are we going to get our level two and level three type people if there's never a level one? I don't think that's going to be the case.

I think what's going to happen is these AIs, and I think I say this all the time, we do not have an artificial intelligence yet. Hands down, I will argue this all day with anybody. We do not have a true sentient thinking AI. We've got the advanced machine learning algorithms that can predict based on a vast amount of information, but I think the next three years is going to be a different stage called augmented intelligence.

I still need to give our AI some form of input, and based on that, I'm going to get a wealth thought out output. But without that initial input, there's really nothing. So I think it's going to augment us. I think it's needed because there's not enough cyber people. I mean there's three million shortage of individuals. This is going to help out a little bit. It's definitely not going to replace. I think it's just going to make room for those level one people to do other stuff and in some cases things that humans are much better at. So that's high level what I think.

Max: Awesome. Can you discuss how companies may be leveraging Copilot and cybersecurity and whether and how Copilot AI can learn to protect systems?

Brad: Yeah. Well, Copilot's interesting because it has access and it has all of the... Think of them as street that a car can drive down. Copilot already has all of that inside of Microsoft products and solutions. So really it's like any other language model. It's using some of the ChatGPT. It's basically, if I'm looking at, it's like the first GPT. And it is going to be the great aggregator, I think risks associated with Copilot from a data perspective.

Brad: And that's because organizations haven't done a very good job of data security and making sure they know who has access to what, they have that access and should they still have that access to. So I think Copilot is going to allow for bigger breach scenarios than existed before. So to answer the question, in order for us to leverage Copilot to better defend, we need to be able to ask it some questions like, Hey, how vulnerable am I? And where is my unstructured data? Where is my sensitive data? And where is my PII?
And asking the question, now, where is it? Copilot will tell you, can you help me defend it? Copilot will show you, and then can you do it for me? And then Copilot will do it for you. So where are we right now with Copilot? We're in the first stage. I'm going to show you where all of this stuff is. Until the rest of it is ready it's actually not so much a security helper as an inhibitor.
And there's a lot of organizations right now that are trying to just do the foundational AI security policies to say what is allowed. And I think Copilot in a way, jumped the gun because it basically got tendrils into everything. And for most companies that are office worker focused companies, 90% of what is in a Microsoft product, it's in that office layer. So I think it's just exposing a problem that was already there, but it's amplifying it. And I think without the right ability to configure Copilot, we are actually in more of a security vulnerability than helping spot right now.

Max: Super helpful. Really insightful stuff. Okay. And then I know we're going over, I think Alex alluded to this potentially taking 10, 15 more minutes. Are you okay with that?

Brad: Yeah, I'm good.

Max: Okay, perfect. Can you comment, is the impact of AI going to be different or how is the impact of AI going to be different for network security versus endpoint security in your opinion?

Brad: I don't know if it's going to be much different. And I say that because if I'm looking at network, I'm thinking of this still as a transport mechanism and making sure that what I am sending across reaches where it's supposed to go in the same condition that it left and it hasn't been tampered with. And it knows that basically all those things are encrypted.

So I would say if there are some things that are added from an AI perspective, it would be is this stuff that's coming across the network expected? I think it could enhance one very specific piece of our daily lives, which is email security. Because sure, email gets to the end point, but I'm sure you're like me and you're sitting there going, how does half of this information to my inbox? This is obviously spam and it doesn't matter how many times I click junk, that thing appears some other way.

So if I could maybe do something at the network layer and prevent some of that from ever even getting to my system, I think AI could help with that. And I think it could look at and start to learn behavior. And this is where I think you would find endpoint and network kind of a happy marriage together where you look at that message and you go, would that even be something that Matt or Brad would even want to look at?

Is this something that's even applicable to the years and years of collected data that I have? Or how about I just summarize all 80 of those things and then I give them a digest at the end of the day? My AI pops in and says," Hey, there was like 80 messages that looked like wouldn't really care about them. Here's a synopsis of what they were." And then you could ask the AI, well, could you maybe summarize or tell me which five would I maybe want to know more about? And it would tell you. And I see that a lot with LLMs today where I give it, so there's a PDF I get from somebody and there's 25 pages. As a CISO, I don't have time. I want the gist of it. I want to know what's foundationally important in that document. Well, I'm going to take it, give it to my ChatGPT or my LLM or my copilot and say, would you read this for me and give me a one page summary and it'll do that.

And then I'll say, could you give me maybe a little more detail on one of the points? And it'll do that. So I think that if I'm looking at this objectively, the only real value that AI will have to networking is going to be more on the transport encrypt, decrypt and malware defense, inline DLP, creating policies on behalf of looking at patterns and then suggesting policies. That's the kind of stuff you're going to see from your AI.

Cybersecurity Budgets in uncertain economic times -

Max: Super helpful. Super helpful. A little bit of a different question here, but how do cybersecurity budgets fare in uncertain economic times? Are they insulated from vendor rationalization efforts or not?

Brad: Not. Not. I watched this happen during the pandemic. And in some cases cybersecurity it looked great, but the reason was as everybody was trying to solve this, everyone is everywhere problem in a very rapid timeframe, but seen as a cybersecurity budget is typically just a fraction or a percentage of the overall IT budget. When that goes down, which happens in the hard economic times, the cybersecurity budget also shrinks.
And so what I've noticed is organizations start to make some decisions of, like so they would come to me, like they'd come to their CISO and they would go, "Hey, I need to cut the cyber budget 10%. What could we live without and how would that impact us from a risk standpoint?" And if I'm trying to mitigate risk, I would say, okay, well these are the eight things I can't live without.
And then from there, I would make a decision where I would, maybe I wouldn't drop my network security, but maybe I would drop one or two of the modules and I would say, well, like I said earlier, I want to have my A and B defense for a while. Maybe I would drop my B defense and I would just be running on my A to save money. So I think it's all on the table. I wish it wasn't that way, but cybersecurity is a lot like insurance, and sometimes when times are tough, you still have insurance, it just won't be as good as it normally is.

Max: Got it. Similar to the CSP consolidation question, what's your take on just consolidation in this space generally, and should observers expect to see more, and who would be the consolidators?

Brad: Yeah, expect to see a lot more. I think if there's any indicator, people have been hinting about this for ages and it's still not done done, but Cisco acquiring Splunk was that shot across the bow of if Splunk can be acquired, then that could happen to anyone. I know a lot of people are paying attention, so if you look at what CrowdStrike is doing, they're trying to build something similar to what Palo Alto Networks haS, to what Cisco has, to what Microsoft has.

Brad: So there's a lot of consolidation happening. CrowdStrike just acquired BIONIC, so application security posture management, they're pulling that in. I think the next one that's going to make sense for somebody is like a network security player, like a Zscaler or a Netscaler. Cisco already acquired one that was out there.
So I think if this whole market is ripe for action, consolidation, and I think you're going to see in the next couple of years, some of these players go the way of the buffalo and they're just going to start disappearing, whether through acquisition or just closing up from, not like an insolvency standpoint, but just a lack of customers and a lack of continued funding.

What's Next for the Market? -

Max: Got it. Super helpful. Super helpful. Brad, I just want to open it up for a final question here. What are some other key trends that we haven't touched on but that you think are particularly important when it comes to cybersecurity today and in the near term?

Brad: I mean, I think we covered a lot of ground today for sure. I mean, I think just reiterate the importance of identity is now the new perimeter. I think one thing we didn't touch on that's going to become even more important is passwordless authentication and authorization. I think what everyone needs to be looking at and thinking about is 80% of attacks are still credential based, and the most stolen thing from an organization tends to be anything having to do with credentials: passwords, passphrases, anything like that.
So I think that is going to be something hot for the next couple of years is the eventual death of the password and moving towards something that is truly passwordless, whether it's an application on a phone, which is generally the direction that it's going to be going, because that's the one device pretty much everybody has that can do the three things that you need an identity.
Something you have, something you know and something you are, whether it's your fingerprint or your facial recognition, it's already there. It's already built in. This is something that we were asking for 10 years ago and now it's everywhere. So that's going to become the next hot thing. Everybody's been talking about cloud, AI, zero trust, the next one's going to be passwordless. So that I think would be what I believe.

Max: Awesome. That's a great way to end. Brad, thank you so much. I can't think of a better person with whom to have this conversation. This was fantastic. We really appreciate you taking the time and look forward to chatting with you again.

Brad: Absolutely. Yeah, happy to do it. Have a great day, evening, morning, whenever you listen to this. Have a good one.

Max: All right. Perfect. Brad. Enjoy the rest of your evening. Bye.

Brad: You too. Bye.