SUMMARY KEYWORDS
network, blue ridge, trust, risk management, architecture, john, approach, federal, address, capabilities, guard, data, mission, protect, nist, breach, multi factor authentication, technology, built, organizations

Welcome to the federal tech podcast. My name is John Gilroy, and I'll be your moderator. Our guest today is John Higginbotham, Chairman and CEO of Blue Ridge networks. And network is the phrase that pays because today, we're going to talk about the role of networks in the federal transition to zero trust architecture. Now, I've known John a while Blue Ridge networks has been around for 20 years before I was born. So maybe you give us a real thumbnail sketch, John before beginning about Blue Ridge and you and then we'll jump into the zero trust.

01:39
Sure, John, and good morning. Thanks for having us on your show. Always a pleasure to see you. Blue Ridge networks is pretty simple. We're an advanced cybersecurity company that develops specialized capabilities for what we used to call on trustable networks, which everybody today cause zero trust network. So we've been doing this a while. Up until the last few years, we were largely captive to federal government missions. In the last four or five years, we've been expanding to support protecting networks for critical infrastructure, block commercial enterprises, both here in US and abroad. where it makes sense. So I've been doing this a while. And hopefully you have something of utility to help address the zero trust needs of the marketplace. And that's

02:33
about two thirds of my list is going to be gummies federal information. And a lot of these people, they hear these buzzwords, and they roll their eyes and they go oh, I want to hear this again and back and forth. And and because John, you've been beat up and knocked around and you got the t shirt that says I've been beat and got a hold on that T shirt by the way, I've been knocked around. So zero trust this brand new something last few years. I mean, you you're you set it up to be No, this is just a new phrase for an old architecture no approach. So So why did it suddenly popular and and what may be mitigated the sudden phraseology?

03:06
Well, you know, it's good question and and the concept of how to approach risk management on a network is has been, you know, actively pursued for many years. The new news is the ultimate recognition that networks are untrustable. If you think about mentally, how we approached the old days, you know, calm sexy again, you can put all these these words and buzzwords. The concept was Trust, but verify. I mean, that was the the mental picture. And after all these years of spending ridiculous amounts of money and still getting breached. Finally, people said, Wait a minute, this is inherently untrustable. These networks, we've gone global, got cloud services, you got distributed workforce, you've got you know, all kinds of interconnectivity issues. OT it, all this stuff is getting networked, to a point where you say, wait a minute, I don't have the visibility or the control anymore. So by definition, it's an untrustable network, which requires, you know, a constant verification that

you're operating in some type of efficacy. So it's a recognition of reality that has finally worked its way into other the perspective about how to address risk management and complex networks.

04:44
Well, it's worked its way into an executive order recently. And and because of that, many organizations are standing up in front of the class and saying, Hey, this is a DOD this is how you should use your trust. You know, at NIST, this is i and this is Sissa and this So, just so so I think if I were a Federal Information Technology Professional, I'd be trying to figure out what, you know, which bird to fly? I mean, Which one, which one works and which ones to go with? I mean, it's it's difficult Did you rely? I mean, who do you rely on? And what about these frameworks? Are they valuable at all?

05:21
Well, they are. And you reference the executive order that the President put out a little over a year ago, which, you know, I would have to say, actually helped galvanize the issue, which, which was a positive thing. And it galvanized these organizations to really start to address it. You're quite right, there's been a lot of frameworks, you know, NSA has their perspective, DOD, CIS, NIST, OMB, these are agencies that are trying to put definition on it, and, and are addressing different aspects of the network. If you look, across the construct, a commonality among all these different approaches to frameworks are some fundamentals where you're starting to focus on mission outcomes, you know, what am I trying to protect, it's a recognition that all data is not equal. And some data is more sensitive than the next, it's a recognition that you've got to segment and authenticate in a more aggressive manner, to be able to produce the kind of results of resilient protection that we're looking for, develop the policies, whether it's administratively network policies, whatever, to be able to implement that and then monitored continuously to make sure you're verifying. You know, it's, it will continue to evolve our understanding, but the fundamentals built around, you know, fundamentally, protecting data in a risk management contract, in a way that you can can verify the authentication of that data is under underscores all of these approaches to framework.

07:19
So is the first step and some will say, is multi factor authentication. So really, John, what you want to do maybe, little baby step, you want to do that Boston marathon next year, maybe run around the house a couple times? I mean, is that reasonable first step?

07:36
Well, certainly multi factor authentication is essential. It's a foundational approach. It's in and of itself, it's it's not a panacea. But clearly, one has to have multi factor authentication. And let me point out, you know, all multi factor authentication is an equal, there's a lot of different methodologies. And the trick becomes applying the technical characteristics, the protocols and techniques. Again, back in this context of your mission objectives to make sure that you've got the level of authentication that you need, you know, most breaches occur from credential theft, in some estimates, or as much as 90% of all breaches ultimately find our way back to credential theft. Authentication is about maintaining the efficacy of what's authorized or not authorized. So it's foundational, I get it, I would submit in and of itself. Even though it's a foundational component, you've got to

look to the overall architecture, how you're segmenting your net network, do you understand your operations and understand what data needs to be sequestered versus what data needs to be public. So you've got to take these techniques and apply them in the context of the objective that you're trying to achieve. And then make the technical trades for the different types of methodologies available in any one of these constructs like multi factor authentication, to ensure that you've got the the level of risk management you're seeking, and that is compatible with with your mission objectives or the architectures that you've inherited, you know, we've inherited all this. So how do you take legacy infrastructure and get assured comms on it? I mean, that's what this is all about.

09:39
I think the best quote when it comes to hackers, is that used to be hackers would break in, but when it comes to stolen credentials today, hackers login that's, that's how I am. I like setting aggressive goals for myself, especially in sports and athletic things. And whatever I wind up doing mostly swimming I see this goal has been set for federal agencies that, hey, by the end of 2024, this zero trust better be in place. I think that's kind of that's kind of a reach. So what is the the Blue Ridge networks approach this this is this is a fantasy land or is this real? Or some agencies? Yes, sir.

10:18
I, you know, I one, one has to respect trying to set goals to force organizations to to change. So I put deadlines like this, in that context as an organizational imperative, rather than an outcome. In some ways, we're already there. Zero trust is a is a mentality, it's a process. It's not an outcome. And if you put it in the context of risk management, I think all of us would say that risk management is a continuous function in any organization. So the achievement by 2024, of integrating concepts of, of a risk management of our networks, in an approach is never trust, always verify, which is what zero trust is about. That's a worthy goal. And that is achievable in terms of a an organizational objective. Now, if you take that to the next level, that means achieving zero trust isn't an outcome, it's a process. And you're integrating a process where you're continually maintaining and evaluating your networks to ensure that you are achieving the risk management protection that you're seeking, that becomes a permanent part of the operation of the network. When this is all day. That's kind of how we see it.

11:51
I'm at your website, Blue Ridge networks.com. And there's examples from the government and examples in the commercial world to some of the work you've done. And so is the cart link to horse the horse laying the card? I mean, so what role is the federal government has been driving commercial adaption?

12:08
Oh, clearly, you know, some of the initiatives that had this Sissa, NIST, others are definitely worthwhile for helping commercial industry, particularly critical infrastructure, to to come to grips with how to deal with this. They're setting framework standards, approaches that that any organization could assist with, I will say there are others impacting the insurance industry, and starting to kick out on this, you know, state and local, are starting to kick in on this. So federal, the federal leadership on this very definitely has helped play a role to get

focused on this issue. The good news is, whether it's the the industry standards, bodies, insurance community and others, organizations themselves, companies boards are starting to wake up and focus on this and insisting that their their strategies for IT management and cybersecurity, you know, adopt this mentality of risk management that we're talking about?

13:20
Well, John, I have a question about CES. But first, one of the best ways to keep up with the fast changing world of technology is to attend webinars, you learn your schedule, and you get continuing education credits. The best webinars are from Fed insider.com. And they're free. Just last week they had on Dr. Ernest Moy from the VA talking about technology and equity for veteran care. Well, we talked about the VA, let's go back to the CI S A, instead of the VA Sissa. March, just a couple months ago, march 2022, they came up with some guidance to meet the executive offices, zero strategy. They talked about five pillars, identity devices, applications, governance and networks. So you're in the middle of the fight there, buddy, whether you like it or not, aren't you networks are right in the middle?

14:07
Well, they are and you know, in order to address network security, you must also address these other areas. So I applaud system for late, simply explaining the breadth and the interdependency of a of a cybersecurity approach that cuts for zottoli across all of these different components of a network and not just vertically. So that's point number one, point number two, you know, their focus has been to look at the technologies for the mobile world operating systems, hardware, ancillary systems, and really start to define how to protect across these different components of a network. You know, why do we have networks it's so we users can use applications in order to communicate. And we do that with certain protocols, which are governance structure. So it's it's giving a very clear picture of the nature of the challenge. To achieve network security, one must be thoughtful of these other areas, and how they either enhance or detract from that security. Which is, which is why we have Blue Ridge, you know, have focused not just on the network side, but the endpoint side, the user side, ultimately, you're talking about bringing an entire architecture in a play, that addresses all these constituents and stakeholders, whether it's devices or people or data, and doing it in a way where you have, you know, roots of trust and confidence across the entire universe of who's using a network, and what that network is. So this is a piece this mark, was incredibly insightful, actually, to be able to try and communicate the nature of the problem.

16:07
Well, I'm glad you brought up edge and edge computing, because when my addled brain thinks of networks, I think of maybe a data center in Ashburn, then maybe in Texas and California and wait, whoa, wait a minute, wait a minute. What about the 5000 people that are within a mile of Ashburn on their phones? Right? Oh, well, you got to worry about that. So the network is, it's not your father's network. It's not a server in two different cities. It's, it's John Higginbotham, at the golf course, hitting a piece of email with, you know, trigger some malicious attack. So

16:43

I read this one, yeah, Golf is a distant memory. And I want strokes job next time we play.

16:55
Well, I went to a website and I looked around, I poked around and read a bunch of stuff. And there's something called App guard or something on your site. So we didn't talk about the last time we're in the year. So So what the heck is this? And what's this got to do with zero trust for my listeners,

17:10
of course, you know, again, it goes back to the point we're just making about CES, I mean, Blue Ridge, cut its teeth on network security. We're isolation containment, high assurance network solution for data, high, highly sensitive data, they've just gone across the disparate and trustful environment. But as we looked at the problem, we realized with with more and more happening at the edge, and more and more happening in a distributed environment, whether it's cloud distributed enterprise ops, you know, whatever global marketplace, in order to present the efficacy that we needed to present to protect data from point A to point B, we had to be thoughtful of, you know, what was happening in a distributed user base, and what was happening in the applications that were operational across the disparate edge devices or endpoints. So we brought out a series of capabilities built from our technology, that go network to user to application, that's link guard, app guard, edge guard, right? So it doesn't, if we're doing our job of protecting your data, cradle to grave over a network, we have to integrate the realities of how you're trying to operate your network, which is distributed applications with a distributed workforce over a complex network. So our three product lines are designed to deliver what we call cyber clubs. Our our viewpoint is for the portion of the network that that we have visibility, we have a lot of different tools. The problem is that's only about half the network. And then you can go to Gartner. Anybody, you know, federal reports. Getting visibility into a global cloud environment is basically a bascome. So if we don't have visibility on the other half of the network, how are we going to operate high assurance zero trust architectures across an environment where we don't have the kind of visibility to use our traditional tools. That's where Link guard edge guard and app guard come in. They are perfect to extend zero trust into the half of the universe, where we don't have the ability to apply the kind of monitoring detection and analysis tools that work well for us in an IT environment. In doing that, we're essentially bringing a no protection lag architecture It maps perfectly to the operational technology world, which is a big challenge for the IT community to address the complexities of, you know, the industrial world, transportation, water treatment, oil, gas, all of this industrial infrastructure, which by design is different than the IT infrastructure that we deal with every day to do sessions like yours today, bringing those into an interoperable zero trust environment is very challenging. We optimized link guard, as guard and app guard to be able to address that problem and bring that interoperability with with the IT networks that we've deployed, do it in a way that seamless, easy to deploy. low overhead. That meant we had to build autonomous capabilities, we had to build in, you know, autonomous multi factor authentication capabilities, we had to build in, you know, network segmentation capabilities, it's an integrated approach to take a comprehensive architecture into the world where we don't have visibility. That's why it's been so successful is it marries up nicely with in a comprehensive architecture, particularly for for your high value missions and critical infrastructure operations.

21:32

So the takeaway from this interview is that app guard could be a solution for many federal listeners, I did some research on it. And it seems like it's a an intermediary, I'm trying to think of the word a, like a container, a containment strategy, or a sandbox or some kind of a gateway out that gateways, they got all kinds of technical implications. But think of the old fashioned gateway with, you know, with cheap going on a farm or something. So is that

21:59
now you said something, our gateways would be the White Guard side? Ah, AP guard, is the process control that goes on? In software, it goes on a computer or server something? And the answer is, it's all the above, it's an isolate, it's a fully integrated capability. That is establishing containers, containerized policies and enforcing those autonomously, at the process level. It's doing at a process level, the same thing we do at a network level with Link guard. And all edge guard is doing is doing it for the users in a distributed environment. So the fundamental approach to delivering zero trust, and we like to call it zero breach for zero trust. I mean, reality is, in our 20 plus year history, we have yet to report a breach bull vulnerability. And then this stuff works. It's a sort of thing where you're bringing a comprehensive architecture where we have pre thought, privileged access management, identity controls, authentication, segmentation, and brought it together in an integrated capability, either at the network, the user or the endpoint level, as lingered edge guard.

23:23
So the practical question I have to you stems from my classroom experience, I teach at Georgetown. And when my students walk out of classroom, there's like recruiters there with nets and trap doors and, and hard to get talent there. How did you find the talent in the last three years? I mean, what are you offering? Like free parachute? Right? I mean, I don't know what you can offer anymore. But when every time you said that, I said, Okay, that's another developer. Okay. That's someone who really understands gateways. Okay, that's someone. I mean, this is not, you know, hey, on the way home from work to get a loaf of bread and come up with some app guard. I mean, this is tricky. This difficult.

23:59
Yeah, you're, we have been fortunate, I've been fortunate to be colleagues with an incredible group of professionals that are highly committed to this mission. And we've generally been able to attract the talent we want because the nature of the problems we work on, are some of the most advanced in the industry, which is intellectually exciting. We have a successful company. So it's a stable platform for a professional in building his or her career. And we're fun place to work. I mean, we it's just a great group of people. We've been fortunate to have good good attraction and very high retention. Because you know, we we have a great compensation package, we take care of our employees. And it's these are the most exciting problems on the planet with cybersecurity. So, if that's your interest in life, Life where this is a great place to be get an inside look, and be involved in the cutting edge technologies that can protect us not only today but well into the future.

25:12
You know, it's the mission I talked to, you probably know Brigadier General Greg to Hillman. He's over in Pittsburgh now. And, and I said, Greg, I mean, you know, you could work at any McDonald's in town. You can

work anywhere. And why there, it's the mission. It's no, he really, I mean, he's, he's serious about, you know, he goes, I don't care. It's the mission. And he's serious about it, if he's voting with his paycheck right there. So it is about the mission, that's, well, we've

25:38
got some of that built into our culture. I mean, most of us in Blue Ridge, have had the privilege of serving missions, that serve us all. And I think that, you know, it really is about the mission, and with an attitude that, you know, if we're doing our job, that money will flow.

25:59
So John, your mission is to give me a five year prediction here of zero trust the federal government speed bumps, I think we got a lot of motivation here. And we got mandates, we got initiatives, we got people beating drums, so five years from now, what's gonna happen?

26:17
Well, we will make incredible amount of progress over the next five years. Point number one, point number two, this is a mission that's permanent, because in the context of risk management, every time we bring a new IoT technology in the equation, it has an impact on everything else we've done. So again, this is a process, not an outcome. Which means five years from now, hopefully, this this zero trust mentality toward risk management of our networks is built into our enterprises. The whole conversation about how we address legacy challenges with new innovation will now become SOP. The one thing that's constantly changing is the threat environment. So in order to address future threats, we're going to have to develop future technologies and future constructs to be able to address those, you know, quantum computing is probably number one on the risk mean, basically practical quantum computing as a relatively good chances of breaking any crypto algorithm out there, at least the ones that are predominantly used, I mean, what's the implication of that? You know, brute force attacks with a quantum computer are no brainer. So as as we have technical developments and advancements in it. In all its related forms, you know, it's going to have implications for how we evolve in a cybersecurity context to protect, you know, our most valuable data. And we really feel strongly about this, because the the nature of competitive advantage, either as an individual company or country is increasingly based on on the quality and value of the data. And what that means is, we've got to, we have to get more and more serious about protecting, access to and utilization of the critical intellectual properties that we developed. Because, you know, one of the challenges we're dealing with in the current crisis is a lot of the intellectual properties that have under underpin their capabilities to do harm they stole from us, through, you know, many, so So the nature of competitive advantage is going to be built around protecting our most valuable data for utilization by those that are authorized and operating within the rules of civilized nations is going to become increasingly important.

29:08
That's that's pretty serious. I have to give you a transcript of that. That's some serious talk. So John, unfortunately, we're running out of time here. You've been listening to federal tech podcast with John Gilroy. I'd like to thank my guest John Higginbotham, Chairman and CEO of Blue Ridge Networks