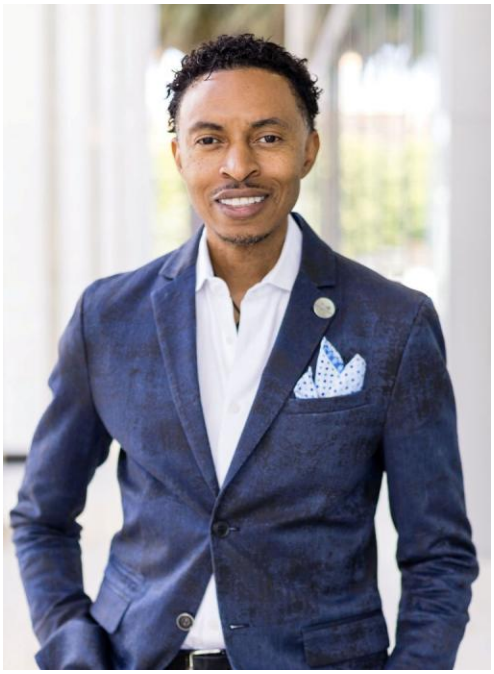
ceocfointerviews.com

Issue: March 24, 2025

Cyvatar – Providing the Gap Analysis, Training, Insurance, Compliance and Security Solutions with Proactive End-Point Management that Enables SMBs to Stay Cyber Secure – all in One Subscription for an Affordable Price



Corey White
Founder & CEO

Cyvatar

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. White, according to the Cyvatar website, "Cyvatar is the easiest system, the most cost-effective way to get and stay cyber secure." How do you accomplish that?***
Mr. White: One of the biggest challenges that companies have is they think there is a silver bullet where they can say, "I have antivirus, so I'm good," or "I have a firewall, so I'm good." Unfortunately when you think about a cyber attack, it is way more complicated than that today. For example, take a business email compromise that we all get, where you get that email sent to you and you click on a link, and the next thing you realize you are taken to a fake site and they steal your credentials or download malware onto to your system. No is no one solution solves that. You have to have multiple layers of security in place to stop that type of attack. What that means is with a business email compromise phishing attack, you want to start with security awareness training. You want to make sure hopefully you are not clicking on a link, to begin with.

When you think about security awareness training, three to five percent are still going to click anyway. You want to put email phishing in place to stop that phishing email from getting in. However, what happens now is hackers are using AI and Grammarly, so it still gets through. Therefore, if someone were to click on that link, what happens after the click is, although it may try to download malware onto your system, you want to block that from executing, and if you don't have antivirus you are not going to stop it from executing. It may also take you to a fake compromised website so if you don't have DNS or web filtering, you are going to go to that site and it is going to look just like your site, so you will put in your credential and you will be compromised. All of those scenarios need to be stopped by tools. Cybersecurity is not just one step and done.

CEOCFO: ***Are you surprised so many people still think there is a one-step solution?***
Mr. White: Yes I am. When you think about physical security, security for your home or your car, it is equated to when you go home you close and lock your door behind you. Maybe you have an alarm system and have all your doors and windows locked, but for your computer and your business, you do not have anti-virus or anti-phishing or any kind of firewalls in place. I think you have to think about it from the perspective of you doing all those things to secure your home or car, so why wouldn't you do it for your business?

Cyvatar interview continued on page 3.

Click on the images below to watch video ads:

CEOCFO: ***Why the focus on SMB startups and supply chains; did you recognize that market from the beginning?***
Mr. White: The Fortune 2000 companies already have a Chief Information Security office or a security team with some controls in place. However, that is only 2000 of the 32 million companies and businesses that need to be secured. Just last year alone there were six million new startups or starting businesses, and 99.9% of all businesses out there are small to medium sized businesses. Therefore, it is a huge opportunity in the underserved community.

The big challenge is small businesses if they want to buy the best products, these large enterprise based security solutions, they only do not sell to small businesses. If you have under 100 employees, you cannot even buy the product.

CEOCFO: ***How are you solving the problem? I see on your website that Cyvatar is the first Cybersecurity as a service provide;, would you tell us how that makes you different from others?***
Mr. White: I have been in the cybersecurity industry for thirty years, and in those thirty years, I have seen some of the largest global cyber incidents in the world. I have done penetration tracking and run hacking teams to help secure companies and implement products of multiple companies and even worked at Microsoft. So I have seen and done a lot.

When you think about how to stop a cyberattack, I know what that formula is. What we have done with our team, is instead of just coming in and saying we are going to sell one product or one service, let's sell only solutions that are tied to an outcome. What I mean by that is to stop a ransomware attack you need best-in-breed products, someone who knows how to install and configure and set it up into a blocking preventative state, you need someone monitoring 24/7 and then you need to make sure it is all tied in together in one simple solution.

"The biggest myth in cybersecurity is that one tool can protect your business. The reality? It takes layered security, expert implementation, and constant vigilance — all of which we bundle into Cyvatar's subscription." Corey White

When you think about cybersecurity, a lot of companies are selling all the individual components, which may not stop the attack. We have bundled it into one subscription, so you get secure end-point management in one subscription for one affordable price. We took that same model and applied it to vulnerability management, multifactor authentication, email security, DNS security, and cybersecurity training.

We built the model into affordable bundles and we figure out what gaps the company has to solve the whole problem. On top of that, once we solve that whole problem, we map out our solutions to compliant requirements like SOC 2, so a company can come to us and get insurance, compliance and proactive preventative cybersecurity all for one affordable price.

CEOCFO: ***Do potential customers understand the difference?***
Mr. White: That is one of the biggest challenges. Unfortunately, the average buyer does not understand the complexity, so if someone comes to you and says "We are going to give you a MDR service and monitor all your endpoints and make sure everything is locked down and secure," it sounds great. However, really what they are saying is we are not going to proactively prevent anything. We are just going to monitor and will alert you when something bad happens, which when you think about it, it is absurd and not useful at all.

Most do not know the difference between getting some monitoring and getting a lower, cheaper solution that does not have the ability to stop a sophisticated AI cyberattack. They do not know. We spend a lot of time here educating the market but unfortunately, the best education is when they are compromised. They realized what they were doing was not sufficient.

Cyvatar interview continued on page 5.

Click on the images below to watch video ads:

Comfort First Introduction and Installation

CEOCFO: ***How do you reach out to the millions of potential customers?***
Mr. White: We built a Freemium model, where we truly believe in serving the underserved SMBs, whereas we do not believe you should be spending money on big expensive gap assessments. We do that free on our platform because if you have nothing in place, there is nothing to gap on because you have nothing of very little in place. We are partnered with MasterCard, we have our external risk exposure product built into our solution. You get your risk scans done for free, you get external scans done for free and you get policies done for free. You get a ton of value. Today we have almost 1200 companies in our platform leveraging that value. When it is time for them to secure themselves, then they can leverage our platform they can call us and we will bring in the right solutions to secure them based on the gaps we have identified.

The other way is we have quite a few strategic partnerships with large global organizations. When you think about a cyberattack and you want to attack an organization, don't attack them, attack their partnerships or their third parties. From a third-party risk management perspective, those are small businesses, some are large businesses, but they have access to large businesses and large companies. We partner with these large global companies to secure their ecosystem. Those are the two most useful ways we get our customers. We get impounds, and a lot of impounds come to us understand that they need a one-stop-shop for all of it and they see us.

CEOCFO: ***What is the key to staying ahead of the new threats?***
Mr. White: It is a constant challenge because when you think about how fast technology is moving today, every three months technology is evolving. When you think about what you can do with AI as it relates to a cyberattack, a lot of the phishing attacks need to be manual, a lot of the creation of the fake phishing websites had to be manual, and it would take forever. There are AI-based tools out there that will automatically create your phishing campaign, the fake websites, target lists, everything just with a click of a button.

What people need to realize is that AI-based attacks are not necessarily a category. All of the attacks that were working before, your ransomware or phishing or basic hacking attacks were already working and working well. We were losing this battle, and now with AI on top of it, they are that much further ahead with AI. And it is much worst for SMBs that have nothing in place. At Cyvatar we leverage AI in all of our tools, we are using enterprise grade products and we are proactive and preventative in everything we do for our customers.

CEOCFO: ***Would you tell us about the insurance aspect?***
Mr. White: Insurance is probably one of the most misunderstood pieces within the cybersecurity industry, especially for the buyers. What people don't realize is when you fill out a traditional questionnaire and the underwriters send that over to you, they are asking all these questions about your security program. If you say yes we apply patches every week, and yes we have endpoint protection, the bugs, malware, ransomware, yes we do backups every week, and on and on, but then you have a breach and a claim. That insurance company then sends out their forensics team and they help you get back up and going but at the same time, they are looking to see how the attack happened. Once they realized it happened because they didn't apply patches and didn't have a backup, but in the questionnaire you said you did apply patches, but it came out six months ago. Then the insurance company may or may not pay that claim because you violated what you said you were doing, you weren't doing the basic best practices that you agreed to when filling out the questionnaire.

Some companies get hacked and they have been paying insurance for years and then when they get hacked find out the insurance company does not, but that is not the insurance company's fault. The insurance company has always worked that way, and you have to meet certain requirements. Ultimately the company needs to understand that the only way to do this properly is to be proactive and preventative. Once you can prevent a cyberattack, then you have the proper controls in place. However, if someone still gets in while you have these proper controls in place, then you will get paid back out by the insurance company. Unfortunately, there are still attacks that you just can't prevent.

CEOCFO: ***Are there different levels of service that people can purchase from you or is it one-size-fits-all?***
Mr. White: It is never one-size-fits-all. It all comes down to what your needs are. We will get on the phone with a customer and they could do the initial gap analysis in our platform, which will tell them where their gaps are, but in many cases these are uninformed buyers. They have never bought cybersecurity before, so they do not know. Therefore, we will spend some time asking if they have a vulnerability management program in place or endpoint protection, multi-

factor authentication, some of the basic table stakes solutions. If the answer is no, we will know those are some of the solutions they need.

In that conversation we are also mapping to their business, what their business requires, and the reason they are trying to do cybersecurity now. They may need to be compliant, insurance questionnaire questions, or third-party mismanagement questionnaires as well. They have all these things coming their way and they need cybersecurity. We can then build a more comprehensive solution to match the gaps that they have in their organization.

CEOCFO: ***What do you look for in your people so that they not only have the technical skills but also the personal skills they need to speak with people, explain your services and technology and not sound like pushy salespeople?***
Mr. White: That is near and dear to me because I want to make sure I have people that care first. When you think about cybersecurity, it is more than that. You have the internet and books. From the technical side, we want the highest and most technical abilities but you could be the smartest technical person but not care about that customer, not do the extra level needed to make sure they are well taken care of and in a preventative state. From our technical delivery team up to our member experience team who has a slightly different role, they are looking at every single customer trying to make sure that holistically they are taken care of The team makes sure to fill any gaps.

Our sales team diagnoses what their problems are, not just their technical problems but their business challenges. Throughout the organization, it is about solving business challenges for our customers and making sure that those problems are resolved for them so that they can grow their businesses. Cybersecurity is a business enabler.

CEOCFO: ***What is your geographic reach?***
Mr. White: We are in North America, the United States, Canada, and Puerto Rico, and we will be expanding internationally in the next eighteen months.

CEOCFO: ***What is the takeaway for our readers; what makes Cyvatar an important company?***
Mr. White: Cyvatar is the future of cybersecurity because gone are the days when a company if they wanted to be secure had to Google around and find a product, find someone to implement it, get insurance. You come to one place with Cyvatar and you can get your initial gap analysis done, and you can get your external scans done. Then when it is time to get your organization, meet compliance, meet insurance needs, you have one partner. We are that outsourced cybersecurity partner for you as opposed to you having to figure it out yourselves. We want to make your lives easier.