ceocfointerviews.com

Issue: September 10, 2018

CEOCFO Magazine

Vericlave uses intelligence-grade security solution to prevent destructive and costly attacks on critical assets

Joel Bagnal
President and COO

Vericlave
www.vericlave.com

Contact:
Helena Krusec
800.766.2026 x 410
helena.krusec@vericlave.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Bagnal, what is the approach to security at Vericlave?***
Mr. Bagnal: At Vericlave, we believe in a design principle emphasizing prevention over reaction. In the current cyber security product landscape, there are about 1700 companies in the US today that develop security point solutions for specific problems that occur once an adversary is already inside an enterprise network. Most of those solutions are software-based and responsive in nature. They operate within the assumption that the threat is already in the network, and provide solutions to analyze the threat and its nature. They then respond to the threat in a certain way, or they provide alerts to the type of vulnerabilities in the network, and then leave it up to the operators analyzing the information to decide what to do about it.

Vericlave's approach is to minimize the attack surface, starting at the very edge of the network where the initial connection to the internet is established, where we provide a cloaking, obfuscation technology that hides the network from plain view and only validates the entities that have authorized access into the network. By minimizing that attack surface and making a network's content invisible, we can immediately mitigate the majority of complications associated with internet connectivity. After all, you can't hack what you can't see. If you are unauthorized, unknown or deemed a potential threat to the host network we are protecting, that host network is not accessible to you, and cannot be seen by any outsiders.

CEOCFO: ***Is the reason people have not been making prevention based solutions because they have not figured out a way to do it or just have not thought about it? How have you come up with a much better idea?***
Mr. Bagnal: The solutions developed over the past fifteen to twenty years have focused mainly on protecting networks, and not on dealing with the type of specific, sophisticated and harder to detect advanced threats that are seen today. The technologies that we have observed in the recent past are focused on known malware viruses, based on signatures that can be identified by an algorithm or machine identity. Our approach is instead to focus on protecting the network edge itself, using a technology that combines hardware, software, and encryption as opposed to just software.

To answer the second part of your question, the preventative technology behind Vericlave was originally discovered by our founders while serving in United States national security organizations, where it was used to protect deployed forces of the US Armed Forces and components of the intelligence community. In our service offering, we have taken a similar approach to that which was used to protect classified environments, unclassified it, and made it a commercial application for use specifically by critical infrastructure operators – which is our target market right now.

CEOCFO: ***When you are speaking with a company, do they immediately understand the benefit or are people skeptical it can actually be done?***
Mr. Bagnal: People have reservations because there are so many companies in the cyber security solution space today that claim "prevention" as their capability and design principle, when in fact they are really focused on "reactivity". We find oftentimes in discussion that the audience is initially rather skeptical until we offer our technical demonstration or proof of value. We do not offer proof of concept because we believe that our technology is proven and have seen it in operation over the past twenty years without a known hack or breach. Generally, in presenting our offerings, we do a live demonstration, during which the audience immediately recognizes that from any unauthorized perspective, their network is totally hidden, providing a level of protection and reduction of the attack surface unlike any of the other solutions they currently have deployed on their network.

CEOCFO: ***Your site indicates that simplicity is one of Vericlave's many hallmarks. How are you able to seamlessly provide this kind of service?***
Mr. Bagnal: We have a number of executives in our company that have formerly served in roles as Chief Information Security Officers and IT Security Directors, who understand the extraordinary frustration of integrating additional complex solutions onto their networks. We understand the second and third order ramifications of adding a security technology into a network that is intended for efficiency and a business operation. When you typically apply security protocol or technology, it will require some level of bandwidth and network efficiency to run that security solution. Information security officers, as well as information technology officers, are very frustrated with each other because security requirements often mean a degradation or disruption of some sort in the network, and a level of difficultly to integrate. We took those frustrations in mind when we developed the commercial solutions that we offer today, so that all you have to do is plug our system-agnostic device into the network and it begins to operate immediately. All the provisioning and integration of our solution is done ahead of time, and once our solution is ready for application, it takes less than a minute to boot up and deliver the effects of the intended solution.

"Vericlave's approach is to minimize the attack surface, starting at the very edge of the network where the initial connection to the internet is established, where we provide a cloaking, obfuscation technology that hides the network from plain view and only validates the entities that have authorized access into the network. By minimizing that attack surface and making a network's content invisible, we can immediately mitigate the majority of complications associated with internet connectivity. After all, you can't hack what you can't see."- Joel Bagnal

CEOCFO: ***Who is using Vericlave today?***
Mr. Bagnal: We have a good balance of government and commercial customers today. We focus intentionally on medium-sized businesses that do not have the current ability to afford millions of dollars' worth of cyber security solutions, nor the ability to afford a Chief Information Security Officer and a large security staff. If your business is in the $25 million to $500 million annual revenue range, Vericlave is a perfect fit for you because of our niche ability to provide intelligence-grade security at medium-sized company prices. That is where we are focused right now. Having said that, we do have some substantial enterprise customers, as well as large government customers.

CEOCFO: ***What have you learned about navigating the challenges?***
Mr. Bagnal: Since the technology behind Vericlave was born from a government environment, we find ourselves with a natural affinity towards working with them. We have certainly had a smoother experience than some of our competitors who might have less experience working with the government or understanding of how the federal procurement process works. We come from that space, and know it well. Having said that, there is still a natural skepticism among information security officers even at the government level because of the variety of options, so we still deploy operational demonstrations across government networks – usually for a two- to four- week period.

Again, we have found that after a period of time, when an operational demonstration is conducted to an organization, that eliminates doubt in the efficacy, which usually leads to a contract.

CEOCFO: ***Is there one solution for every organization or are there some tweaks or subtleties depending on whom you are working with?***
Mr. Bagnal: We have learned through experience that every single network is like an individual – the design, the architecture, the tools, and all the different software running on the network is different based upon that organization's needs and requirements. We do an awful lot of work up front, before our solution is applied, to customize each

deployment and ensure that we are providing a solution that abates their concerns and delivers a risk mitigated profile in accordance with the business objectives of the companies that we are serving.

CEOCFO: *Would you tell us about the change of name from Entegra to Vericlave?*
Mr. Bagnal: Entegra Technologies has been in operation for a little over seven years, and it started out as a tablet business. We were focused on the federal contracting community, specifically delivering hardened, ruggedized, secure tablets to the US Armed Forces. We built a very effective capability and delivered it to those components, but could not scale to meet the requirements of large organizations like the United States Army. Our competitors like Toshiba, IBM, Dell, Apple, and others quickly came into the tablet market and were able to mass produce very capable tablets. In fact, they were able to overtake us, so we needed to find a different path to revenue and a different market to serve. We decided to take the ruggedized nature of our solution and its security emphasis to focus on building a device that was able to secure networks at the edge, as oppose to an integrated computer system and a tablet. It took about two years to make that transition and we came out with our first set of solutions about four months ago. With that in mind, we decided it was appropriate to rebrand.

CEOCFO: *What will be different under your leadership?*
Mr. Bagnal: In terms of any organization that goes through a substantial change like we have, you have a strategy that you want to achieve, so you have to organize your staff to complement that strategy.

Since the solution came from the federal community with the intention of commercialization, we wanted our staff to have a healthy balance of federal and commercial leaders, all involved in the security space, that had experience starting and growing cyber security companies, and had a good understanding of how to apply security solutions in both the commercial and the government space. That is what we have done. We have assembled a team of people that fit that description well, and I'm confident that they will lead this team to success.

CEOCFO: *How is business?*
Mr. Bagnal: It is going well. We launched the new set of solutions about four months ago and we have a number of proofs-of-value in operation right now, which we expect to convert to full time contracts, and we are meeting the initial business objectives that we set for ourselves, so we are very pleased.

CEOCFO: *How do you get attention with so many companies in the space?*
Mr. Bagnal: We are taking a focused approach to go after customers in the medium-sized business space that are going through a deliberate security review to take on a strategic transaction such as going public on NASDAQ, S&P or going through some sort of merger and acquisition process. When a company goes through that kind of transition, they have to undergo audits and meet regulatory requirements that are associated with information systems and security. We find that this is an opportune time to approach a firm that needs help with cyber security, because we provide the solution that simplifies multiple products into one single capability and addresses the majority of common cyber security challenges. It makes much more financial sense to replace a variety of complex solutions with one, especially when that solution is as battle hardened as Vericlave's, and can solve a host of problems across spheres of security, networking, and compliance with one singular, system agnostic deployment.

CEOCFO: *Why choose Vericlave?*
Mr. Bagnal: The threats that face the critical infrastructure of our nation today are more severe than ever before in the history of computing. We have a solution that is designed to prevent the threat from ever even entering your network in the first place. That seems to be attractive enough in and of itself. No company wants to be above the fold on a major national newspaper talking about how they've been forced to publicly mitigate a significant cyber security hack, and is having to deal with the business reputation risks and business operational loss associated with the hack. As opposed to spending a lot of money on a bunch of different solutions and integrating them, taking a Vericlave solution and putting it on the end of your network and protecting yourself from the threat to begin with is a pretty strong value proposition.

About Vericlave
Vericlave is a cybersecurity technology and managed services company focused on preventing increasingly destructive and costly attacks on the critical assets of enterprise and government entities. At the edge of a customer's network, Vericlave implements a zero-trust stealth design that verifies access and hides the network from unwanted and unknown actors. The solution is comprised of a unique combination of a hardware root of trust, key management algorithms and encryption of all communications starting with the first packet to create isolated and secure enclaves that may be integrated into any network architecture. Proven in the U.S. intelligence community, with no known security breaches to date, the solution is easy to deploy and requires minimal to no disruption. For more information, visit www.vericlave.com/.