ceocfointerviews.com

Issue: September 18, 2023

Endor Labs – Helping Organizations and Developers Secure Their Open Source Software and Applications while Eliminating the Developer Productivity Tax

Varun Badhwar
Founder and CEO

Endor Labs

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Badhwar, what is the concept behind Endor Labs?***
Mr. Badhwar: Endor Labs focuses on helping organizations secure the software that they develop. In the last few years, most software teams have gone from writing much of their code themselves, to relying most heavily on open-source ecosystems written by other people. Software applications rely on how you as an organization effectively embrace that shift. It is about enabling and empowering your developers to use more open source confidently to foster innovation but do it with the right guardrails where code can remain secure and operationally healthy.

CEOCFO: ***How does Endor Labs help an organization do all those things?***
Mr. Badhwar: Endor Labs focuses on a foundational problem that exists in cybersecurity and software development. We call this the developer productivity tax. Recently, a McKinsey report found that software engineers are spending only about 30% of their time producing code and 70% of their time on these taxed areas like meetings, security, and compliance initiatives. The biggest problem driving this tax is that application security tools create too many false positives. They generate far too much noise and their accuracy level is low.

Endor Labs helps organizations focus on the 20% of the issues that are causing 80% of the risk in the enterprise. We developed our technology by focusing on understanding the root of this problem of why security tools generate so much noise, and coming up with a unique approach that focuses on truly understanding how organizations are building their applications, writing their software, and relying on open source software, and uncovering only the issues that truly affect the enterprise so that you can safely deprioritize most of the noise security tools are creating for you. We eliminate up to 80% of false positive vulnerability alerts.

We then take that a step further. The right way to solve this problem is to help software engineers early in the process when they are selecting which software to rely on and give them feedback early to avoid any surprises that would prevent them from shipping their software into production because a tool is flagging an issue that may or may not be true. We help developers avoid surprises at all costs, select the most high-quality sustainable software, and maintain and manage the entire lifecycle of software development without introducing unnecessary risks.

CEOCFO: ***Are developers ready for you, are they looking for a better way?***
Mr. Badhwar: There are two parts to the problem. Are developers extremely frustrated using security tools and processes? Absolutely! As a developer, there is nothing more valuable than being able to build great features and functionality in software and ship it. Anything holding them back from focusing on that is a tax, and none of us like taxes.

On the security side, security teams are finding themselves being discredited because five or ten years ago we lived in a world where security tended to be heavy-handed. Today, the most successful security leaders consider engineers their internal customers. They want to empower them with better tooling and enable them to move fast. For security teams, we stir up a conversation and tell them we can give them much more actionable information with less information they need to act on. They can prioritize the information, and go to their developers with evidence of why they need to drop everything and fix it. They are interested and excited about pursuing that technology.

CEOCFO: ***What goes into how Endor decides what should be a priority for any given company, industry, or type of application?***
Mr. Badhwar: Let's first look at the genesis of how this came about. As an industry, we all created a community-driven concept for tracking vulnerabilities in a common vulnerability exchange format. All vulnerabilities for any application universally fall into what is called CVE (Common Vulnerabilities and Exposures). This worked for the intent that it started with, but that was decades ago. The idea was to score vulnerabilities as critical, high, medium, or low. Guess who decides those ratings? There is a combination of the person recording it plus the developer who owns the property. However, the universal truth is that what is critical for one organization may be very different for another because they have different businesses. One use case of using that particular software component could have a vulnerability that is different, and how it's used is different. One organization may also have compensating controls, while the other doesn't.

"Endor Labs focuses on a foundational problem that exists in cybersecurity and software development. We call this the developer productivity tax." Varun Badhwar

At Endor Labs, we provide all of those parameters specifically for you by inspecting how you use that code with your particular application. First, I want to know what environment it is in. Is it in test, or is it actually in production and deployed? I want to understand if part of the code that has that critical vulnerability is even being used in your application at this very moment or not. I would understand if that particular vulnerability is being exploited. If there are signals and if it is being exploited and we know about it, there are sources of information for that, and we want to track that and know if we can even do anything about it. If the developer has not created a fix for this problem, then what can I do about it at the moment?

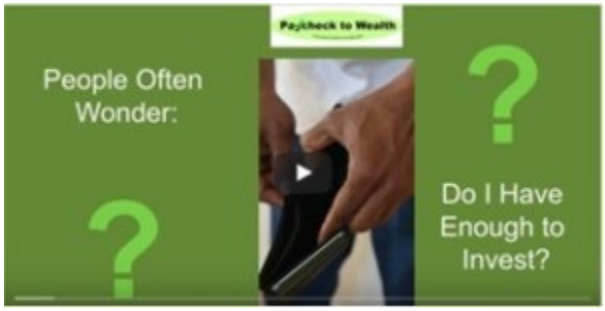
We look at these different parameters to understand how you use the code, if there is something in the app that could go wrong, or if there are attackers in the wild exploiting this today. We look at all the data points and how developers and security teams prioritize what I call the now, next, or never -- what needs attention now, what needs a fix tomorrow, and which issues you don't need to address at all.

CEOCFO: ***How do you interact with your clients?***
Mr. Badhwar: Our typical clients vary from modern-age cloud native companies of several hundred employees to some of the largest banks in the country that have tens of thousands of employees. Every company is a software company today, so everybody is writing software whether it is for your smart car, smart vacuum, or Fintech. The way we typically

engage our customers is a combination of application security leaders, and/or engineering platform leaders. They are typically facing the frustration of using a lot of open source and they either do not know exactly what the developers are bringing in, and how secure or insecure it is, or they know what they are using but the current tools are generating far too much noise for them to build actionable programs to reduce their risk.

We start with conversation and propositions and move into value engagement where the customer will bring a couple of their applications, and we will produce the results by scanning them quickly. Then we will surface to them what the current state-of-the-art tools they are using are doing in terms of risk reduction, vulnerability noise, and what we can do. It is a very clear comparison. It is the analogy of a car; you are buying a car and I can tell you why my engine is better and I will prove it to you when I do a road test and it drives better. I will show you the statistics on how fuel-efficient it is and how comfortable it is. Then it makes it an easy decision on our client's part to ask themselves if they want to make the switch with the existing tool, or maybe they do not have a tool at all and they want to adopt Endor Labs, and they ask about return on investment.

We work with our clients to build a total economic impact assessment that says the way they are doing things today costs them this much, and the way they can do things with Endor Labs, brings in this many savings a year. In this day and age where we are running with pretty tight economic budgets and conditions -- having that ROI calculator is very critical.



CEOCFO: ***Who do you typically engage with at an organization?***
Mr. Badhwar: We typically engage the Chief Information Security Officer or the head of the application security team and the engineering platform leaders. This could be the CTO, a Director of Engineering Productivity, or a VP of Platforms. Those are the types of titles that this technology is most relevant to.

CEOCFO: ***How do you get a foot in the door and how are you reaching out?***
Mr. Badhwar: We have a combination of components. We are building a digital presence and brand presence. We do a lot of educational content that helps people understand the problems in the space of cybersecurity and open source software. People find us through the valuable content that we publish. We will have a free certification which people can sign up for online and learn more, so digital is one mechanism. Direct enterprise sales is another where we are targeting the right kind of customer clientele profiles that would make sense for us in our business.

The third piece is channel partners – we work with value-added resellers and managed security providers that are already engaged with our target customers and have a very good understanding of our prospective customers. Channel partners that have a good understanding of the needs, wants, and challenges of organizations play a pivotal role in connecting us with enterprises who need our technology.

CEOCFO: ***What have you learned from your customers since you started Endor, and what are you doing differently today?***
Mr. Badhwar: We've learned that up to 50% of software engineering time is being spent on security. There is a high degree of frustration because of that. The need to focus on developer productivity is one big lesson we've learned from customers. The other big lesson is a transition you see in the industry -- security teams no longer want to purchase tools

in a silo and shove them down the engineer's throat because engineering teams have more voice and more opinions and can push back. If the engineering teams do not adopt and embrace these security tools, security teams are not really poised for success.

We have built capabilities that are not only relevant for the security teams but also help engineers do their jobs better. We are in a current economic situation where organizations only want to take on projects that will have very significant direct or indirect cost-savings to the business. The value proposition is very important.

CEOCFO: ***Would you tell us about your recent funding and what your plans are for the money?***
Mr. Badhwar: We have raised $70 million in a Series A financing, an amount traditionally unheard of, but most importantly, unheard of in the current global economic situation. We're also backed by Tier 1 investors, not just venture firms, but also CEOs and operators of very large companies. We are proud of the investors we brought along.

We are happy for the market opportunity for the problem we are solving -- it is a massive problem and a massive need that we can solve in an untapped market. We have built successful businesses before in cybersecurity and people are confident we can do it again.

Third is the traction we have demonstrated in a short amount of time that normally takes several years for startups to get to. In terms of where we invest the capital, we expect it will be on both research and development and continuing to further the technical differentiation we bring to the market on our product, but also in our go-to-market reach and how we get to customers faster and make them aware of our existence and help them solve key challenges.

CEOCFO: ***What is the key to staying if not ahead at least in tune with challenges in security?***
Mr. Badhwar: I have been in cybersecurity now for sixteen years and the reason I keep going and what makes it exciting is it's like a cat and mouse real-world video game. You are never quite done. We listen to our customers about the new challenges they face, and we build technologies to help them solve those challenges.

The second piece is investing in security research to look at what is ahead and see the patterns that are just starting to emerge that maybe even our customers are not seeing yet. We are seeing the wild playout and what is going to be the next frontier of cybersecurity attacks.

As founder and CEO, my job is to pay attention to what is around the corner and emerging challenges.

CEOCFO: ***Endor Labs has received recognition from many sources in your industry. What is most meaningful for you?***
Mr. Badhwar: There are three things to call out. One is being a top ten finalist for the RSAC Innovation Sandbox. Hundreds and hundreds of companies apply each year and we were one of the top ten finalists. The second was Black Hat, which is a very prestigious international security conference where we were one of the four selected spotlights out of hundreds. The third is Gartner®, choosing us as a Cool Vendor in cybersecurity. All this was in one year.

None of these awards are pay-to-play. There is a lot of controversy around where you can pay a few thousand dollars and be recognized for an award, but none of these were that. These were truly industry leaders, customers, judges, and luminaries in the cybersecurity space picking us for what we do and recognizing that we solve meaningful challenges. For me that is the most important thing I am proud of -- the team and the technology that we have built here is recognized already by meaningful industry analysts and accolades from the industry.

CEOCFO: ***What if anything might someone miss when they are looking at Endor Labs and why is Endor Labs an important company?***
Mr. Badhwar: Today the biggest technology transformation we are seeing is artificial intelligence (AI). Every week in the blink of an eye we see something new and something completely disruptive in the industry. You have seen statements from companies like Google and Microsoft saying what will win in this AI movement is open source. Fundamentally, open source is leading a lot of this AI enterprise movement. The main thing is open source is here to stay. If your organization does not embrace open source software, you will be left behind.

And if you are to embrace open source software, you have to understand the risks. Nothing is free in this world. You have to invest in the right governance, guardrails and measures to make sure you are bringing in high-quality software that is reliable and secure. That is where Endor Labs comes in and that is where we can partner with organizations to help in that journey, where they can embrace all of the innovations in this space, which is now like Disneyland for developers. We do not want anyone falling off, and that is where Endor Labs comes in.