FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

Reimagining Application Security: How Program Behavior Intelligence Is Advancing Security from Detection to Assurance

Stanislaw Lewak

CEO, praedictio.ai

in conversation with

Jarad Carleton

Global Vice President of Research, Cybersecurity, Frost & Sullivan

For nearly three decades, application security has largely been built around identifying vulnerabilities, detecting threats, and responding to an ever-expanding list of things that could go wrong. But as the number and complexity of vulnerabilities continue to grow, that approach is becoming increasingly difficult to sustain.

For Stanislaw Lewak, **CEO of praedictio.ai,** the answer is not to build a better scanner or create a larger threat database. It is to rethink the problem itself.

praedictio.ai is developing what Lewak calls **Program Behavior Intelligence**, an approach that starts with a different question: *What is the software supposed to do?* Rather than attempting to enumerate an effectively infinite set of malicious behaviors, praedictio.ai models the finite set of expected software behavior and enforces that boundary.

That philosophy is at the heart of the company's approach to application security. It is also shaping how Lewak thinks about AI, customer adoption, partnerships, product development, and the challenge of creating an entirely new security category.

> "Stop trying to list everything that could go wrong. Define what your software is supposed to do and prevent everything else." — Stanislaw Lewak, CEO of praedictio.ai

Rethinking the Application Security Model

Jarad Carleton: *For nearly three decades, application security has focused heavily on identifying vulnerabilities. Why do you believe that model has reached its limits?*

Stanislaw Lewak: I think that model initially made sense when the threats were very small. You had a list of everything that was bad, and the list of bad was relatively small compared to the list of good, and everything worked fine.

But the list of threats is becoming larger and larger. If we think about it in terms of set theory, the number of flaws is essentially infinite, and it's not fully knowable. That's why we still have zero days. Even with something like the vulnerability in JFrog's Artifactory, you would have thought they had tested it and knew what could happen, but they couldn't know. By the time they realized it, it was already too late.

With AI being used to find more vulnerabilities at machine speed, we were going to run into a wall, so the best way of solving it was to have a different approach. We do know what our software is supposed to be doing. That's what QA is all about, and that's what we expect our software to do.

So we focus on that finite, albeit large, set and make sure that bad stuff doesn't happen.

AI Is Changing the Security Equation

Jarad Carleton: *AI is changing both how software is written and how attackers operate. Which shift do you think security leaders are currently underestimating?*

Stanislaw Lewak: My heart goes out to security leaders because there are so many things happening. One is that AI is finding flaws much faster than people can fix them, so that's a problem. But the other problem is AI-generated code. We now have AI writing what you want, but potentially also putting vulnerabilities into the code. We have AI finding flaws, and then we're trying to use AI agents that are using our systems in ways that were never expected.

I think all of that is an issue and a problem. We're looking at a whole new world, essentially, with all new rules.

Jarad Carleton: *With the speed of technology evolution today, is there something security leaders should be asking themselves that they aren't asking today?*

Stanislaw Lewak: I think they should be asking themselves: **"What do we expect our software to do and then, make sure that that's all it does."** Jarad, we have anecdotal evidence that not everyone's approach to DevSecOpps and AppSec is as robust as it should be. We've heard stories of code being updated directly into production, bypassing the rigorous QA test processes that originally underpinned the industry. The causes of these shortcuts (lapses in judgement?) are perhaps a topic worth exploring on its own.

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

Inverting the Security Problem

Jarad Carleton: *You have taken a very different approach to application security. What was the assumption you felt the industry needed to rethink?*

Stanislaw Lewak: We rejected the whole idea that you cannot enumerate infinity, so there has to be a way of solving that problem. We are not trying to model an infinite number of bad things. *We're trying to model the finite set of good.* So, we are saying, let's look at it from a different point. Let's invert the traditional way of looking at the challenge, which is difficult for a lot of people to get their heads around initially.

Jarad Carleton: *Was there an inflection point that convinced you this behavior-based model could work?*

Stanislaw Lewak: Seeing all the different AI exploits made us realize that there had to be a different approach.

The real proof came with our ActiveMQ demo. We took a 2022 release of ActiveMQ and demonstrated that a 2023 flaw that had been found would compromise it. We trained the model on the expected behavior to make sure that nothing bad was supposed to be happening. Then we forced that behavior again, trying to hit it with that 2023 flaw, and we managed to stop it.

Then Horizon3.ai, using Anthropic's Claude, identified a new flaw this year in that same codebase that had been there for 13 years, and we still prevented that because the model existed before the threat did. That's when we had proof that this was going to work.

Building a New Layer, Not Another Security Tool

Jarad Carleton: *Was there a direction you deliberately decided not to go in because you believed the industry was solving the wrong problem?*

Stanislaw Lewak: Absolutely. We are not a scanner, we are not a detector, we are not a threat feed. Other people have made great attempts at doing that, but we feel that's a losing battle.

We have also refused probability scoring or taxonomy of attacks. The moment you're guessing, you're again back in the noisy game of infinite potential vulnerabilities.

We deliberately chose not to build our own pane of glass, either. Everyone is used to the different panes of glass. We just want to be able to integrate into them and not duplicate or try to fight that same battle. We want to be a nice complement to add into what security professionals already use.

Making Program Behavior Intelligence Understandable

Jarad Carleton: *Program Behavior Intelligence represents a fundamentally different approach to application security. How do you explain that shift to prospective customers?*

Stanislaw Lewak: We have been trying to find the right way, and I think we have finally settled on one that resonates with our target demographic. It's like a club with a vetted guest list. You have got your bouncer at the door, and he knows that this is a vetted member, and he's letting them come in. We don't keep a list of all the potentially bad people or make judgment calls regarding if someone appears to be a person you don't want in.

We are modeling a finite set of variables that define what a program is supposed to do, from the tests an organization already runs, and we prevent everything outside of those parameters. It's deterministic, with no signatures and no source access, and it's auditable.

Jarad Carleton: ***What's the biggest misconception customers have before they experience your approach?***

Stanislaw Lewak: The biggest problem is that people are looking through the lens of what they know. Every other system out there is based on threat vectors or a function of threat vectors. They are looking at detection of those threats or anomalies after the fact.

We do the opposite. We don't make a judgment that something is a threat. We are saying that something is happening that you've not told us you expected. It could be a lack of test cases, in which case we can help you build up your test cases. Or it could be a flaw in the program. If it's a flaw, it could be a vulnerability. You decide what you want to do. The problem is that people are looking at security solutions through the lens of threat vectors, and it can be difficult to get them to view the business challenge differently.

From Detection to Prevention

Jarad Carleton: ***If security teams begin focusing on application behavior instead of an infinite number of vulnerabilities, what changes inside the organization?***

Stanislaw Lewak: Work starts shifting left. We have got a design partner helping us, and they see that the work is shifting left because we're helping them understand the set of test cases that are underway and whether that is adequate.

It also stops the question of which of the ten million CVEs we have to start worrying about, prioritize, or adjudicate. Instead, we say: let's focus on the behavior so we know we'll be safe. It simplifies life. It's a different approach to the whole problem.

Turning Security Into an Engineering Quality Assurance Win

Jarad Carleton: ***Beyond improving security, what types of business outcomes can this approach deliver?***

Stanislaw Lewak: You have hardened test coverage as a byproduct. We are going to show you the missing test cases, and that's an engineering quality assurance win. If you are in a regulated GRC environment, that's much better because you can show it. Not just this is what we think is happening, we guarantee it's happening.

There's no false-positive tax. Teams should stop drowning in all these probabilistic alerts because when we come up with an alert, it's either a flaw in the software that must be resolved, or it's a test case. If it's a missing test case, that's good to know and document.

Protection that doesn't exist doesn't depend on a patch cycle. We are not saying patches are over and done with, but suddenly you have got security even though you haven't patched an application.

You also have supply-chain confidence when you're doing a patch. We can compare the behavior of the software before and after the patch and see the differences. If something changes that shouldn't, you can identify a potential software supply-chain vulnerability. It hardens your software, removes alert noise, and security is no longer a tax on engineering.

AI Should Advise, Not Decide

Jarad Carleton: *How do you determine where AI should make decisions and where human judgment should remain essential?*

Stanislaw Lewak: Currently, our model is deterministic and auditable, and it's built with machine learning, which is a limited AI. There's no randomness. It's always the same. It's clearly explainable and auditable, and our enforcement is deterministic.

AI should be assisting the human. We have people playing with something we call ADA, our Advanced Defensive Agent. After we build the model, our PBI Explainer can explain it, and ADA can look at that explanation and help determine whether something seems good, whether there's a missing test case, or whether there is a software supply-chain problem.

During enforcement, if something happens, ADA can help evaluate whether it is a flaw, an attack, or a missing test case.

It should always advise and it doesn't decide. AI belongs on the human side of the decision, not in the control path.

Knowing Where AI Should Not Be Used

Jarad Carleton: *Do you think the cybersecurity industry is overestimating AI today?*

Stanislaw Lewak: It seems that everybody would like AI to be able to decide what is malicious and get rid of probability and noise. But in fact, in some cases, it can increase probability and noise. If AI is looking at things after the fact, you still have a problem that you must remediate or repair that security incident. I think the industry is betting that AI will reliably tell good from bad. A safer bet is a deterministic boundary where you don't really need AI's judgment at all.

Building a New Security Category

Jarad Carleton: *What milestones would tell you that the industry is beginning to embrace this behavior-based approach to application security?*

Stanislaw Lewak: I think when buyers start asking, **"What does my software do?"** Not just what's in it. SBOMs are a great first step, but they don't tell you really what the software is doing. Another milestone will be analysts trying to name a new category based on what we're calling Program Behavior Intelligence. The whole point is to do software behavioral assurance.

When the CISO starts asking what the software is allowed to do, we'll see more RFPs asking for enforcement of intended behaviors, and then incumbents will start adopting behavioral enforcement language, that's going to be validation. And that shift is starting to happen now.

Earning Trust Without Replacing What Already Works

Jarad Carleton: *What role do technology partners, and the broader ecosystem play in accelerating this vision?*

Stanislaw Lewak: The process of selling security, especially something that requires a lot of trust, has changed a great deal. That trust can come from a company that's been around for a long time, or from a partner they have been working with, such as an MSSP or security solutions provider.

We have found that to be very important. Our goal is to find the appropriate partners so they can help us gain that trust and educate people that we're not trying to do a rip and replace.

The other technology has value, but we're a new layer that can complete the QA at build time, secure the software supply chain at change time, and enforce at run time. We want to complement, not compete with, technology already being used.

The Hardest Part of Transformational Growth: Changing Minds

Jarad Carleton: *What's been one of the hardest things about bringing a new security philosophy to market?*

Stanislaw Lewak: I absolutely was not expecting the resistance to change or the inability to set aside a perception. Everyone has been living in a lifetime of threat vectors and how to respond to them, and this is so different and so challenging. We spend a lot more time trying to help people understand that we're not detection. We are focused on enforcing their expectations.

Inverting the business challenge as we have as praedictio.ai, is sometimes much harder than I thought it would be for people to understand.

Learning That Education Is Part of the Product

Jarad Carleton: *Looking back over the journey, is there anything you wish you had understood at the beginning that you know today?*

Stanislaw Lewak: Absolutely. I did not realize that people were so stuck in their status quo and that it was difficult for them to see the challenge from a different perspective. Some people see this and think it was still focused on threat vectors or some new threat-vector system.

When more people understand it, it will be far easier for it to take off. And I think one of the other important issues is that people really want those established relationships when considering a new type of security solution.

This is where you must have good partners pushing into organizations with our solution for the first time. Maybe in one to two years, when people understand Program Behavior Intelligence as a new category, our growth trajectory will be easier.

The biggest challenge is educating the market about why our technology is a game changer, and that was a blind spot for me. I was so focused on the technology and making sure it was safe, and that it could execute and deliver, that I missed the importance of market education for a new security concept.

Adapting Technology to People

Jarad Carleton: *In London we spoke about the innovative impact of Steve Jobs on the world. How does that type of innovative thinking influence the way you balance your own vision with what customers are asking for?*

Stanislaw Lewak: My first company was the one of the first hardware Macintosh

peripherals companies, and I met Steve Jobs. I realized that the biggest thing he was doing was adapting technology to people, not people to technology. He was trying to make it just work and show them the benefit of using this great tool. I think that's always been a driver for me.

I also believe that if people don't understand that something is going to make their life better, then they won't use it. We need to communicate so customers can understand the benefits. On the engineering, we hold a firm line. A lot of companies today operate in a fake-it-till-you-make-it mode, shipping something that doesn't really work and promising to fix it later. We don't build that way. Our CTO spent fourteen years building payment systems at ING, where software that isn't solid simply is not an option. Software is never finished, you improve it continuously, but what goes out to your first customers has to be stable and dependable, not something half-working that you then spend eternity repairing.

Jarad Carleton: ***So how do you balance listening to customers with a vision they may not fully understand yet?***

Stanislaw Lewak: If they don't understand, then the problem is mine because I'm not communicating it properly.

It's critical to listen to customers and to talk to them. We've realized that we need to reinforce what we're doing and not make assumptions that they've come to the table understanding what we're doing and why we're doing it this way.

It's an educational issue. Our role is to educate the customer, help them understand what we have, how it can help them solve their problems, why it's unique, and why it's so easy to implement.

The idea of using your existing test cases is important because it's as simple as rerunning your QA. You get a model of what your program is doing, you can explain that model, verify that you don't have software supply-chain risks, and then enforce that model.

That is to me the big deal: seamlessly and frictionlessly delivering a solution.

Closing Reflection: Defining What Software Is Allowed to Do

The central idea behind praedictio.ai is a fundamental inversion of traditional application security. Instead of attempting to identify every possible vulnerability or malicious behavior, Stanislaw Lewak argues that organizations should define what their software is supposed to do and enforce that intended behavior. In doing so, the approach shifts the focus from an effectively infinite set of "bad" behaviors to a finite set of expected behavior.

That philosophy extends beyond technology. praedictio.ai is working to establish Program Behavior Intelligence as a new category, while recognizing that education, trusted partnerships, and helping customers understand a fundamentally different approach to application security are critical to adoption.

As Lewak puts it:

> "Stop trying to list everything that could go wrong. Define what your software is supposed to do and prevent everything else."

That is the transformation at the heart of praedictio.ai: moving application security from chasing what might go wrong to enforcing what software is actually supposed to do.

Stanislaw Lewak | CEO, praedictio.ai

Stanislaw Lewak is the founder and CEO of praedictio.ai, a software behavioural assurance company redefining application protection and software supply chain security. A seasoned technology entrepreneur, he has built businesses across hardware and software for more than three decades. His first company, Levco, became an award-winning leader in Macintosh hardware expansion before being acquired in 1987. In 1992, he founded The Polished Group, which delivered pioneering internet solutions for organisations including Sun Microsystems, Microsoft, Netscape and Reuters, before its acquisition in 1999.

Stanislaw is the lead inventor named on the patents underpinning praedictio.ai's Program Behavior Intelligence. The technology builds a deterministic model of how software is expected to behave, explains that behaviour so it can be verified, and enforces the approved model at runtime. This Build, Explain, Enforce approach strengthens applications and secures the software supply chain by revealing what changed, updated and AI-generated components actually do. Through praedictio.ai, Stanislaw is pioneering a deterministic, prevention-based approach to application security.

Jarad Carleton | Global VP of Research, Cybersecurity, Frost & Sullivan

Jarad Carleton brings 26+ years of experience in the USA and Europe to his role. He works with organizations in Israel, North America, Europe, and Asia, focusing on various security domains such as Active Directory, zero-trust enterprise browsers, managed security services, digital risk protection, digital trust, Internet of Things (IoT) security and privacy, encrypted voice and text messaging, automated security validation, vulnerability management, IT/OT security convergence, fraud detection and prevention, and cloud service provider (CSP) security services. His quantitative research on security trends, maturity, services, and products informs legislators, regulatory bodies, and CXOs, helping them make data-driven decisions that enhance growth.

Ready to Lead the Transformation?

- **Schedule a Growth Strategy Dialog:** Align your growth roadmap with Frost & Sullivan's Visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts:** Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Showcase Your Transformational Leadership:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council:** Collaborate with industry leaders shaping the future of your ecosystem.
- **Explore Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Benchmark Your Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Tell Your Story:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Appendix: Behavioral Assurance for Application Security

Application security is evolving as AI-generated code, software supply chain risks, and increasingly complex applications challenge traditional threat- and vulnerability-centric approaches. Organizations are moving toward prevention-based strategies that define intended software behavior and enforce it across the development and runtime lifecycle.

To support this transformation, Frost & Sullivan provides forward-looking intelligence across:

- Cloud/Application Runtime Security (CARS) Market, Global, 2025–2029
- Frost Radar™: Cloud/Application Runtime Security, 2026
- Global Cyber Threat Intelligence and Threat Intelligence Platform Growth Opportunities

Together, these perspectives reinforce the key themes of this Transformational Growth Leadership discussion: defining intended software behavior, strengthening software assurance, securing the software supply chain, and moving application security from detection toward deterministic prevention.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN