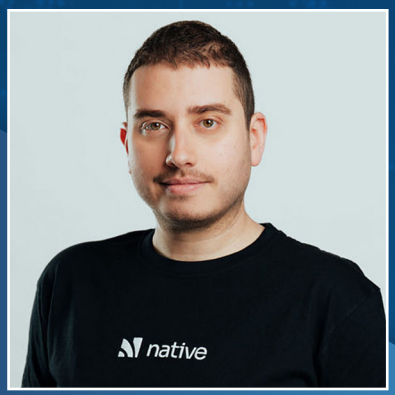
FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

Building Security Instead of Detecting Risk: The Future of Secure-by-design Cloud Security



Gal Ordo
Co-founder &
Chief Product Officer,
Native Security
in conversation with
Jarad Carleton
Global Vice President of Research,
Cybersecurity, Frost & Sullivan

Building Security into the Cloud from the Start

Cloud computing has fundamentally transformed how organizations build, deploy, and scale applications. At the same time, cloud environments have become increasingly dynamic, with infrastructure changing continuously across multiple providers, development teams, and deployment pipelines. While security technologies have become more sophisticated, many organizations still struggle to answer a basic question: **Is the environment actually secure by design, or are they simply identifying risks after they appear?**

As cloud adoption accelerates and artificial intelligence (AI) introduces new operational complexity, traditional approaches that focus primarily on detecting misconfigurations and vulnerabilities are beginning to show their limitations. According to Gal Ordo, organizations need to move beyond finding security issues after deployment and instead ensure that security principles are embedded into cloud architecture from the very beginning.

In this Transformational Growth Leadership conversation, Gal Ordo, **Co-founder & Chief Product Officer** of Native Security, explains why the future of cloud security lies in translating architectural intent into preventative controls. He discusses how secure-by-design principles, cloud-native governance, and AI-enabled development are reshaping enterprise security, allowing organizations to reduce risk while maintaining the speed and flexibility that modern cloud environments demand.

> "The industry has become very good at detecting risk. Now it's time to build security."
>
> — Gal Ordo, Co-founder & Chief Product Officer, Native Security

Why Detection Alone Is No Longer Enough

Jarad Carleton: *Cloud security has evolved significantly over the past decade, yet many organizations continue to struggle with governance and risk despite investing in multiple security tools. What gaps do you see in today's approach to cloud security, and why do you believe the industry needs to rethink the way security is built into cloud environments?*

Gal Ordo: Over the last several years, organizations have invested heavily in technologies that identify misconfigurations, vulnerabilities, and compliance issues across cloud environments. Those capabilities are important, but they primarily focus on discovering problems after infrastructure has already been deployed.

The challenge is that most organizations already know how they want their cloud environments to be built. Security teams define architectural standards, development teams follow reference architectures, and organizations establish policies for identity, networking, encryption, and infrastructure. Yet there is often a disconnect between those intended designs and what is actually deployed.

As a result, security teams spend significant time identifying issues that ideally should never have been introduced in the first place. The industry has become very effective at detecting risk, but much less effective at ensuring that cloud environments are built securely from the outset.

For us, that raises a more fundamental question. Instead of continuously searching for security findings after deployment, why not ensure that cloud environments are built according to approved architectural principles from the very beginning? That shift, from detecting problems to preventing them, is where we believe cloud security needs to evolve.

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.

From Detection to Secure by Design

Jarad Carleton: *You have spoken about moving beyond detection toward a secure-by-design approach. What does secure by design actually mean in practice, and why is it becoming so important for modern cloud environments?*

Gal Ordo: Secure by design begins with the recognition that security should not be treated as a final validation step after applications and infrastructure have already been deployed. It should become part of the design process itself.

Most organizations already know how they want their cloud environments to be built. They define architectural standards, approved services, identity models, networking requirements, and governance policies that reflect both business and security needs.

The challenge is ensuring that those architectural decisions are consistently translated into deployed infrastructure. Rather than relying primarily on tools that detect misconfigurations after the fact, organizations should be able to express their intended security architecture in a way that can be enforced throughout the deployment lifecycle. When infrastructure is built according to those predefined principles, security becomes proactive rather than reactive.

This approach also changes how security teams work with developers and cloud engineers. Instead of reviewing environments after deployment and asking teams to remediate issues, security becomes part of the engineering process itself. Developers receive clear architectural guidance upfront, enabling them to build secure environments while maintaining the speed and agility that modern cloud development requires.

At its core, secure by design is about creating confidence that cloud environments are being built correctly from the start, rather than relying on continuous detection to identify what has already gone wrong.

Turning Security Architecture into Operational Reality

Jarad Carleton: ***Moving from a secure-by-design philosophy to day-to-day operations is often where organizations struggle. How can security teams ensure that architectural principles are consistently reflected in the cloud environments they actually deploy?***

Gal Ordo: One of the biggest challenges organizations face today is translating architectural intent into operational reality. Most enterprises already have well-defined security architectures. They know how identities should be managed, how networks should be segmented, which encryption standards should be used, and how cloud resources should be configured. The problem is not a lack of architectural guidance. The problem is ensuring that every cloud deployment consistently follows those principles.

As **cloud infrastructure** becomes larger and more dynamic, manual governance simply doesn't scale. Development teams are deploying infrastructure continuously, and security teams cannot realistically review every change after it has already been made. That's why we believe architecture itself should become executable. Instead of documenting security requirements and hoping they are followed, organizations should be able to translate those requirements into preventative controls that guide deployments from the outset.

In practice, that means compiling those requirements into the security controls the cloud providers already ship, and doing it consistently across AWS, Azure, Google Cloud, and OCI. You define the architecture once, and it's enforced everywhere through each provider's own primitives, instead of being rebuilt by hand for every cloud. That's what turns an intended architecture into something you can actually operate, not just document.[1.1]

When security policies become part of the deployment process, organizations no longer need to depend entirely on identifying violations after infrastructure reaches production. They create an environment where secure configurations become the default rather than the exception.

The goal is to ensure that the cloud environment organizations intended to build is the one they actually deploy.

Reducing Risk While Increasing Agility

Jarad Carleton: *Many organizations worry that stronger security controls will slow development. How do you balance secure-by-design principles with the speed and agility that modern cloud teams expect?*

Gal Ordo: That's a common assumption, but in practice we have seen the opposite. When security is introduced only after infrastructure has been deployed, development teams often have to stop what they're doing, investigate findings, redesign configurations, and redeploy workloads. That creates delays, frustration, and unnecessary operational overhead.

By providing clear architectural guardrails from the beginning, developers know what "good" looks like before they start building. Rather than receiving long lists of findings later, they can deploy infrastructure with greater confidence that it already aligns with organizational security requirements.

It also helps that teams can see the impact of a control before it's ever enforced. We replay real activity from the environment against a proposed guardrail, so everyone can see exactly which workloads and identities it would affect before anything ships. If something unexpected shows up, rolling it back is as simple as rolling it out. That's usually what turns "this might break production" into "let's turn it on."[2.1]

This approach doesn't reduce agility; it actually improves it. Security teams also benefit because they spend less time reviewing repetitive configuration issues and more time focusing on strategic risks, governance, and emerging threats.

Perhaps more importantly, secure by design changes the relationship between developers and security teams. Instead of becoming a checkpoint at the end of the process, security becomes an enabler that helps engineering teams move faster while reducing overall risk.

AI Increases the Need for Secure by Design

Jarad Carleton: *Artificial intelligence is transforming software development and cloud operations. How do you see AI influencing the future of cloud security?*

Gal Ordo: AI is accelerating software development in remarkable ways. Developers can now generate code, automate infrastructure creation, and build applications much faster than before. That's incredibly powerful, but it also means mistakes can be created and replicated, much more quickly.

AI agents raise the stakes further. They're non-deterministic by nature, so you can't count on guardrails living inside them. The architecture has to define what an agent can reach and act on from the outside, regardless of the permissions it inherits. And because every engineering team is becoming an AI team, decisions about what a model can access aren't just application choices anymore. They're architectural ones.[3.1]

If organizations continue relying primarily on detecting security issues after deployment, the number of findings will only continue to grow as development speeds increase. That's why I don't see AI changing the fundamental principles of cloud security. If anything, it reinforces the importance of secure by design.

Organizations need security architectures that can guide automated development in exactly the same way they guide human developers today. Security shouldn't become a separate process that tries to keep up with AI-generated infrastructure. It needs to become part of the engineering framework itself. AI can certainly help improve security operations, but it should be used to strengthen good architectural practices rather than compensate for weak ones. As organizations increasingly adopt AI across software development, embedding security into the design process becomes even more critical.

Redefining the Future of Cloud Security

Jarad Carleton: *As organizations continue investing in cloud security, where do you believe the industry is heading over the next few years? How do you see cloud security evolving beyond today's approaches?*

Gal Ordo: I believe we are approaching a fundamental shift in how organizations think about cloud security. For many years, success has largely been measured by how effectively organizations can identify vulnerabilities, misconfigurations, or compliance gaps after infrastructure has been deployed. Those capabilities will continue to be important, but they shouldn't be the primary objective.

The real objective is ensuring that cloud architectures are built correctly from the beginning. As organizations become increasingly cloud-native, security needs to evolve from identifying exceptions to establishing secure foundations that guide every deployment. I think we will also see much closer alignment between security, platform engineering, and development teams.

Cloud security can no longer operate as an isolated function that reviews infrastructure after it has been created. It needs to become part of how organizations design, build, and operate cloud environments every day. That shift will allow organizations to spend less time reacting to security findings and more time building resilient, scalable cloud platforms that support long-term innovation.

Leading Change Across the Organization

Jarad Carleton: *Technology is only one part of the equation. As organizations adopt a secure-by-design approach, what leadership and cultural changes are equally important for making that transition successful?*

Gal Ordo: Technology alone doesn't change security outcomes. Organizations also need to change the way different teams work together. Security teams, developers, platform engineers, and cloud architects all have different responsibilities, but they ultimately share the same objective: building secure systems that enable the business. That requires trust, collaboration, and shared ownership.

Instead of security becoming a gatekeeper that reviews infrastructure after deployment, it should become a partner that provides developers with clear guidance from the beginning. When security requirements are transparent and easy to apply, developers don't see them as barriers. They become part of the engineering process itself.

Leadership also plays an important role. Organizations need leaders who recognize that security isn't simply about reducing risk. It's about creating confidence that the business can innovate safely, move quickly, and adopt new technologies without compromising governance. Secure by design is as much an organizational transformation as it is a technical one.

Listening to Customers While Challenging Convention

Jarad Carleton: *Native Security is introducing a different way of thinking about cloud security. How do you balance challenging long-established practices while continuing to listen to customer needs?*

Gal Ordo: Innovation has to begin with listening. Our customers are dealing with increasingly complex cloud environments, and many of the challenges they describe are remarkably consistent. They aren't asking for more findings or additional dashboards. They are asking for greater confidence that their cloud environments are being built correctly from the outset. That feedback has reinforced our belief that the industry needs to move beyond simply identifying problems after deployment.

The way we think about it, the cloud needs a control plane for security: one place to define the architecture you want and turn it into active, operational defenses that hold as the environment keeps changing. The foundation of that is architecture itself, the perimeters, segmentation, and baselines that decide what's even possible in your cloud, all enforced through the controls your providers already built.[4.1]

At the same time, introducing a different approach requires patience. Organizations don't change established security practices overnight. They need to understand why a different model creates better outcomes and how it fits within the way they already build and operate cloud environments. For us, innovation isn't about replacing everything organizations already do. It's about helping them evolve toward a model where security becomes part of cloud architecture itself rather than something that's applied after the fact.

Looking Ahead: Making Secure by Design the Industry Standard

Jarad Carleton: *Looking ahead five to ten years, how would you like organizations to think differently about cloud security because of the work Native Security is doing?*

Gal Ordo: My hope is that secure by design becomes the default way organizations approach cloud security. Today, many organizations begin by deploying tools that identify misconfigurations and security findings after infrastructure has already been built. Those technologies provide important visibility, but I believe the industry should gradually move beyond relying primarily on reactive detection.

Instead, organizations should begin by defining how secure cloud environments are meant to be built and then ensure those architectural principles are consistently enforced throughout the deployment lifecycle. When that becomes the norm, security teams will spend less time investigating repetitive findings and more time helping the business innovate securely.

Ultimately, I would like to see cloud security evolve from asking, "*What went wrong?*" to asking, "*How do we ensure it is built correctly from the beginning?*"

If the industry embraces that shift, organizations will become both more secure and more agile.

Changing the Way Organizations Think About Cloud Security

Jarad Carleton: ***Finally, when people look back a decade from now, what do you hope Native Security will have contributed to the evolution of cloud security?***

Gal Ordo: I don't think success is measured simply by building another security platform. Success is changing the way cloud security is approached. If organizations begin treating secure architecture as the starting point rather than relying primarily on finding problems after deployment, then we'll know we have helped move the industry forward.

Cloud environments will only continue to grow in complexity. Development will become faster, AI will automate more of the engineering process, and organizations will need security models that can scale alongside that change.

My hope is that secure by design becomes an accepted foundation for cloud security, not something organizations add later, but something they build into every cloud environment from the beginning.

My vision is for cloud security to become far more proactive. Rather than sitting back and waiting for security findings, organizations should plan, build securely from the outset, and then operate confidently within those architectural guardrails.

Closing Reflections: Building Security Before Risk Emerges

Throughout the conversation, Gal Ordo consistently challenged one of the cloud security industry's longest-standing assumptions: that stronger security comes from detecting more problems. Instead, he argues that lasting resilience begins much earlier, with building security into cloud architecture from the outset.

Secure by design, as Gal describes it, is about translating architectural intent into operational reality. Rather than relying primarily on identifying misconfigurations after deployment, organizations should establish preventative guardrails that guide development from the very beginning. In doing so, security becomes an integral part of engineering instead of a separate validation exercise.

As cloud adoption accelerates and AI enables organizations to build and deploy infrastructure at unprecedented speed, this shift becomes even more important. The future of cloud security, Gal believes, lies in embedding governance, security, and architectural consistency directly into the development lifecycle, allowing organizations to innovate faster while reducing risk.

Secure by design is about moving cloud security from reactive observation to proactive engineering, enabling organizations to build resilient cloud environments with confidence from day one.

As Gal concluded:

> "I want the way cloud security is being done to change. You don't sit idly and wait. You go and plan, and you build, then you run your business within that."
>
> — Gal Ordo, Co-founder & Chief Product Officer, Native Security

Gal Ordo | Co-founder & Chief Product Officer, Native Security

Gal Ordo is the Co-founder and CPO of Native. He previously led product management for AWS Security Hub, AWS's native CSPM (Cloud Security Posture Management) product, driving features that helped customers achieve better security outcomes faster. Earlier, Gal served in the Intelligence Technology Unit of the Israeli Defense Forces, where he began as a vulnerability researcher and rose to become one of the youngest Majors in Israeli Intelligence, leading all cybersecurity and IT training for his unit.

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: Secure-by-design Cloud Security

Cloud security is entering a new phase as AI-driven development, cloud-native architectures, and increasingly dynamic deployment environments reshape enterprise operations. Organizations are moving beyond reactive risk detection toward secure-by-design strategies that embed security into cloud architecture, automate preventative controls, strengthen governance, and enable resilient cloud environments from the outset.

To support organizations navigating this transformation, Frost & Sullivan provides forward-looking intelligence across cloud security, cloud-native application protection, AI-driven cybersecurity, and cyber resilience, including:

- Cloud-native Application Protection Platform (CNAPP) Market, Global, 2025–2029
- Frost Radar™: Cloud-native Application Protection Platforms, 2026
- Cloud/Application Runtime Security (CARS) Market, Global, 2025–2029
- Zero-trust Browser Security Market, Global, 2025–2030
- Automated Security Validation (ASV) Market, Global, 2025–2030

Together, these perspectives reinforce the central themes of this Transformational Growth Leadership discussion: embedding security into cloud architecture from the outset, shifting from detection to prevention, translating architectural intent into operational reality, and enabling AI-ready, resilient cloud environments through secure-by-design principles.

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