

**TAG**

# USING DETERMINISTIC AI TO SECURE CLOUD INFRASTRUCTURE

DR. EDWARD AMOROSO,  
FOUNDER & CEO, TAG



# USING DETERMINISTIC AI TO SECURE CLOUD INFRASTRUCTURE

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG

---

This TAG analyst report offers insight into how Gomboc uses artificial intelligence to address weaknesses in cloud infrastructure-as-code (IaC) deployment. The goal here is to introduce the value of Gomboc's approach, while also demonstrating the promise of using AI for cyber.

## INTRODUCTION

Gomboc is one of the more interesting startups we've reviewed at TAG who are integrating artificial intelligence (AI) to enhance cybersecurity across cloud infrastructures, applications, and software. By employing deterministic AI in their platform, Gomboc delivers precise and consistent remediation of security vulnerabilities. This appears especially promising for security teams that demand predictable responses to security-related inquiries.

Unlike generative AI models that produce varied outputs, deterministic AI involves algorithms and models that ensure consistent and accurate remediation of security issues. This approach guarantees that identical inputs yield the same outputs, providing predictability and reliability in addressing vulnerabilities. Such consistency is crucial in cloud security, where uniformity in remediation actions is essential to maintain a secure environment.

## INTEGRATION WITH INFRASTRUCTURE AS CODE (IAC) TOOLS

Gomboc's AI platform integrates with major IaC tools like Terraform, CloudFormation, Pulumi, and Puppet. This integration allows Gomboc to manage and secure cloud infrastructures throughout their lifecycle. By leveraging these tools, Gomboc's AI can configure and manage various components, including compute resources, storage, DNS entries, and SaaS applications, ensuring that security best practices are consistently applied across the infrastructure.

Our assessment of using deterministic AI for the protection of these types of resources is still preliminary (this type of approach is new), but we like the idea that in environments where different workloads are instantiated across a hybrid, multi-cloud infrastructure, the last thing a security team would want is to have varying responses to the use of AI in dealing with threats and vulnerabilities.

We also like the idea that deterministic AI will help with compliance processes. In addition to mapping IaC policies to applicable compliance frameworks for cyber, the use of deterministic AI algorithms should improve the testing and review process so common for cyber compliance, especially in regulatory environments. Test output predictability is essential to demonstrate compliance, and non-deterministic AI will introduce uncertainties into the verification process.

## POLICY-DRIVEN SECURITY ENFORCEMENT

As hinted above, Gomboc's use of AI enables organizations to create and manage security policies in plain English, eliminating the need to learn platform-specific frameworks. These policies can be organization-wide or specific to certain stages or projects, providing flexibility and control over security enforcement. Time will tell how effective this approach will be with security operations center (SOC) teams, but the concept looks promising.

What happens specifically is that the Gomboc AI engine translates organizational security policies into actionable remediation steps, pushing fixes directly to CI/CD pipelines as pull requests. This process streamlines the remediation workflow, allowing DevOps teams to approve or deny suggested fixes efficiently. We expect to see TAG enterprise customers begin to demand this type of capability, so Gomboc's timing appears excellent.

## REAL-TIME UNDERSTANDING AND COMPLIANCE

Another aspect of the platform we believe to be powerful is that Gomboc's AI is continuously updated with real-time understanding of cloud service providers and the organization's specific environment. This continuous learning ensures that the AI remains contextually aware, producing code that aligns with security best practices and compliance frameworks. And obviously, this must be done in a manner consistent with the deterministic AI approach.

It is also true that by maintaining compliance standards during and after remediation, Gomboc will help organizations adhere to regulatory requirements and industry standards, reducing the risk of non-compliance penalties. Time will tell whether AI-specific regulations emerge, but we can envision the power of deterministic results when an organization's AI application is subjected to auditors demanding predictable test results.<sup>1</sup>

---

<sup>1</sup> The confluence of compliance requirements and AI usage in enterprise is only now coming into some focus. We expect AI security compliance to be one of the key components of most security programs in 2025, even though frameworks such as NIST SP 500.53 were not designed with AI usage in mind.

## DEMONSTRATING THE POWER AND PROMISE OF AI IN CYBERSECURITY

By automating the remediation of security vulnerabilities with precision and consistency, Gomboc's approach to AI security should reduce the manual effort required from security and DevOps teams. This automation not only accelerates the remediation process but also minimizes the risk of human error. (No security practitioner should have to be persuaded to the power of automation.)

At TAG, we are pleased to see Gomboc leveraging deterministic AI to provide consistent, precise, and automated remediation of security vulnerabilities in cloud infrastructures, applications, and software. Through integration with IaC tools, policy-driven enforcement, real-time understanding, and compliance adherence, Gomboc showcases the power and promise of AI in reducing cyber risks and enhancing organizational security.

Readers who require more guidance on the Gomboc commercial offering, the use of deterministic AI, or any other aspect of enterprise security protection can either contact a TAG analyst through their TAG Research as a Service (RaaS) portal – or can contact TAG via the contact information listed above. Readers are also encouraged to reach out to Gomboc directly for more details on their platform and how it might be deployed.

## ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.

Copyright © 2025 TAG Infosphere, Inc. This report may not be reproduced, distributed, or shared without TAG Infosphere's written permission. The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.

