Dawnguard

Cloud Security Design and Automation in the Age of AI

Overcoming Challenges to Ship Faster and Safer

Introduction

As organizations continue to navigate the complexities of secure cloud delivery, it is essential to examine the everyday challenges faced by both development and security teams. Developers often find themselves overwhelmed by the need to interpret and gather non-functional requirements from a patchwork of security policies—policies that may be difficult to understand, inconsistently documented, or rapidly evolving. This struggle is compounded by the diverse technologies and frameworks present in modern cloud architectures, forcing development teams to translate broad compliance mandates into actionable, code-level controls with little guidance or standardization. The result is frequent confusion, wasted effort, and friction across the delivery pipeline.

On the other side, security teams are pressured to keep pace with an ever-expanding landscape of cloud services and applications. As organizations embrace AI-enabled automation, the speed of software delivery accelerates dramatically, leaving security professionals perpetually in a reactive stance. The mounting demand for security reviews, policy enforcement, and compliance checks often stretches teams to their limits, creating bottlenecks that slow innovation and erode trust between departments. The challenge is not just about having enough resources; it is about building automated workflows and tools that can scale as quickly as the technology they are designed to protect.

By acknowledging these struggles — from developers wrestling with ambiguous requirements to security teams fighting to keep up with the pace of change—we underscore the urgent need for solutions that foster collaboration, clarity, and continuous protection. At the conclusion of this whitepaper, we will highlight how Dawnguard is uniquely positioned to address these challenges, offering tangible ways to empower teams to ship faster and safer without compromising security or compliance.

Executive Summary

Cloud computing has revolutionized how organizations innovate and scale, but with this flexibility comes the constant challenge of maintaining control, visibility, and robust security. For CISOs and CIOs, the promise of the cloud is often tempered by the everyday reality: security is bolted on late, development and security teams are stretched thin, and the friction of protracted security reviews delays projects, drives up costs, and creates frustration throughout the organization. Industry studies estimate that over 60% of cloud breaches could have been mitigated by earlier security intervention (Gartner, 2023). Addressing these issues demands a new approach—one where automation empowers teams to embed security from the start and validate it throughout the lifecycle.

The Cloud Control Conundrum

Despite the cloud's many advantages, companies often struggle to maintain consistent control over sprawling architectures. The pace of innovation, rapid adoption of new services, and distributed responsibility models leave security gaps and expose organizations to risk (McKinsey & Company, 2022). When CISOs and CIOs attempt to impose control after the fact, they encounter resistance, delays, and mounting costs.

Lack of visibility

Dynamic cloud environments are notoriously difficult to monitor for compliance and security posture.

Fragmented responsibility

Cloud security is a shared responsibility, but accountability often becomes blurred among teams and vendors.

Missed opportunities

Security is often seen as a blocker, rather than an enabler of innovation, due to late-stage integration.

The Cost of Late Security

Most organizations still review security requirements only at design sign-off or deployment, leading to a familiar cycle of frustration. Developers feel pressure to deliver quickly, while security teams are tasked with catching issues, often with limited context or resources. According to a Ponemon Institute survey (2023), 73% of security professionals cite “late involvement in the development lifecycle” as a primary source of inter-team conflict and delay.

Extra effort, extra cost

Security retrofits require costly remediation and rework.

Project delays

Back-and-forth reviews between development and security slow progress.

Burnout risk

Back-and-forth reviews between development and security slow progress.

> "Dawnguard isn’t just building tech — they’re rewriting the DNA of cybersecurity. In a world addicted to patching symptoms, they’ve chosen to re-engineer the root. That’s not just bold — it’s necessary.”
>
> Dimitri van Zantvliet
>
> DUTCH RAILWAYS CISO & AI GOVERNANCE LEADER

Beyond a Binary Approach

One of the most persistent misconceptions in cloud security is the idea that risk is a simple binary—assets are either secure or insecure. In reality, risk exists on a spectrum, shaped by each organization's unique context, business priorities, budget constraints, and appetite for risk. What may be an unacceptable vulnerability for one company might be an acceptable trade-off for another, depending on factors such as regulatory obligations, customer expectations, or the criticality of the workload involved.

Today's teams often face a deluge of identified risks, but the challenge lies in determining which ones truly matter and how—or even if—they should be addressed. Without a clear framework for contextualizing risk, organizations can become paralyzed by indecision or waste resources chasing low-impact issues. This ambiguity is compounded by the rapid pace of change in the cloud, where new threats and vulnerabilities emerge constantly, and yesterday's priorities may no longer apply.

To move forward, it is essential to adopt a holistic, business-aligned perspective on risk. This means integrating risk management into decision-making processes, aligning security actions with organizational goals, and fostering open communication between technical and business stakeholders. By moving beyond a binary view, organizations can prioritize what truly matters, allocate resources effectively, and ensure that security investments deliver meaningful value in the broader context of enterprise objectives.

> "Most security architecture is still stuck in the dark ages, with manual reviews, scattered docs, and nothing that actually enforces design intent. Dawnguard flips that on its head. It validates your architecture up front, generates production-ready IaC, and keeps your posture aligned long after deployment. It's real security by design — not a paper exercise, not an afterthought, and definitely not business as usual."
>
> Terry O'Daniel
>
> SECURITY LEADER AMPLITUDE, SALESFORCE & NETFLIX

The Path to Faster, More Secure Cloud Delivery

The solution lies in automating non-functional requirements (NFRs), design, and deployment validation. By making security an automated, continuous part of the process, organizations can reduce manual work, eliminate bottlenecks, and improve outcomes.

Automated NFRs

Security policies, compliance checks, and operational controls are codified and integrated into CI/CD pipelines (NIST, 2021).

Design automation

Infrastructure-as-code and automated threat modeling ensure secure architectures from the outset (OWASP, 2022).

Validated deployment

Deployments are continuously checked against approved designs, reducing drift and catching misconfigurations before production (CSA, 2023).

Contextualized risk treatment

Automation helps organizations manage risk dynamically by using real-time data and business context in security decisions. High-risk changes can be flagged for review, while low-risk updates move forward automatically, balancing speed and security. This makes risk an ongoing, adaptive process rather than a static checklist.

Business Impact: Shipping Faster, Reducing Costs, and Enhancing Security

Organizations that automate security integration throughout the development and deployment lifecycle experience measurable benefits:

Accelerated delivery

Teams ship new features and products faster, with fewer security bottlenecks.

Lower costs

Early detection and prevention of issues reduces expensive late-stage remediation.

Stronger collaboration

Development and security teams work together more effectively, with less friction.

Robust security posture

Automated validation and continuous compliance dramatically lower the risk of breaches.

According to Forrester [2023]

Organizations that automate security in the cloud:

Time-to-market	Average security cost reduction
-38%	25%

Conclusion

CISOs and CIOs face intense pressure to innovate and protect their organizations in the cloud. The old model—where security is tacked on at the finish line—no longer works. By embracing automation for non-functional requirements, design, and deployment validation, organizations can regain control, ship faster, reduce costs, and dramatically improve security. The future belongs to those who integrate security early, continuously, and automatically [Gartner 2025].

References

- Cloud Security Alliance. (2023). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0.
- Forrester Research. (2023). The State of Cloud Security Automation.
- Gartner. (2023). Cloud Security Best Practices.
- McKinsey & Company. (2022). Managing Cloud Risk: New Approaches for Security Leaders.
- NIST. (2021). Framework for Improving Critical Infrastructure Cybersecurity.
- OWASP. (2022). Automated Threat Modeling in Cloud Architectures.
- Ponemon Institute. (2023). The Cost of Cloud Security Failures.
- Gartner. [2025] Top Strategic Technology Trends for 2026: Preemptive Cybersecurity.

Dawnguard