Cloud misconfigurations are the primary way hackers gain access and exploit your systems. Common, and dangerous, misconfigurations can put cloud services like object storage, virtual networks and firewalls, and Identity and Access Management (IAM) at risk.

Detecting problems in Infrastructure as Code (IaC) helps teams move faster and avoid making dangerous mistakes. The IaC Pack lets you catch configuration issues early in your Terraform files, so that these misconfigurations — AKA potential hacker entry points — never make it into production.

Are your applications — and the servers they are running on — safe and compliant?

In addition to choosing and configuring the right open source components, as a developer you now own the process of writing code to provision and configure your cloud infrastructure.

Combined with Nexus Lifecycle, the Infrastructure as Code (IaC) Pack gives you all of the information you need to choose the best open source components AND keep your cloud infrastructure secure.

Cloud and open source security together in one place.

**Developer-Centric IaC Security**
Catch issues in Terraform before deploying to production with early developer feedback for configuring secure IaC.

**Cloud Misconfiguration Elimination**
Misconfigurations are the #1 reason for cloud data breaches. Give your developers tools they need to ensure your cloud infrastructure is secure.

**Cloud Security Best Practices**
The most complete set of rules and compliance mappings to reduce cloud risk and ensure your applications meet the highest standards.

---

**Common Cloud Misconfigurations by Type**

- **44% SECURITY GROUP RULES**
- **40% INSECURE IDENTITY ACCESS MANAGEMENT POLICIES**
- **36% ENCRYPTION AT REST DISABLED**
- **33% ENCRYPTION IN TRANSIT DISABLED**
- **33% OBJECT STORAGE ACCESS POLICIES**
- **31%**

**Misconfigurations are the #1 reason for cloud data breaches.**

Cloud misconfigurations are the primary way hackers gain access and exploit your systems. Common, and dangerous, misconfigurations can put cloud services like object storage, virtual networks and firewalls, and Identity and Access Management (IAM) at risk.

Detecting problems in Infrastructure as Code (IaC) helps teams move faster and avoid making dangerous mistakes. The IaC Pack lets you catch configuration issues early in your Terraform files, so that these misconfigurations — AKA potential hacker entry points — never make it into production.
Using the highest standards for cloud compliance is no longer optional.

Compliance standards for every major industry include controls for how cloud infrastructure should be used and configured. If your organization is operating under any regulations, it’s critical that your cloud infrastructure meets those standards.

The IaC Pack leverages the most complete set of rules and compliance mappings, with out-of-the-box support for Center for Internet Security (CIS) Foundations Benchmarks, CIS Docker Benchmarks, CIS Controls, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, CSA Cloud Controls Matrix, and SOC 2.

“Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes.”

— NEIL MACDONALD, GARTNER

Cloud and open source security and compliance, together in one place.

Ensure that both your applications and the servers they are running on are compliant and secure with Nexus Lifecycle and the Infrastructure as Code Pack.

Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype’s Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit [Sonatype.com](http://Sonatype.com) or connect with us on [Facebook](http://Facebook), [Twitter](http://Twitter), or [LinkedIn](http://LinkedIn).