

Chef Cloud Security

Easily Maintain Consistent, Compliant, and Secure Cloud Infrastructure

DATA SHEET



One-Stop Solution for all Your Cloud Security Needs

Shift Left with Infrastructure as Code Security

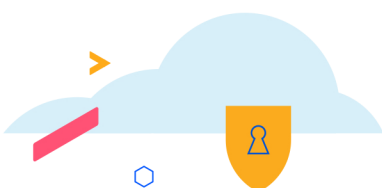
- Run security checks on your infrastructure as code (Terraform) during development and in CI/CD.
- Translate security compliance policies into code and help enterprises detect and correct potential security issues at scale before they reach production.

Ensure Continuous Cloud Compliance

- Gain real-time visibility and maintain security posture.
- Achieve compliance with CIS, STIG benchmarks, and other standard best practices.
- Monitor, detect, and audit misconfigurations across your public cloud services (AWS, Microsoft Azure, and Google Cloud) and Kubernetes clusters.
- Get total visibility of your cloud infrastructure and workloads through a “Single Pane of Glass” interface and quickly respond to vulnerabilities.

Scan and Analyze OS and Application Configurations

- Achieve unified security across your Software Systems – Operating Systems, Applications and Databases throughout your network.



Chef Cloud Security Powered By:

Progress® Chef® Automate™

Gain comprehensive security and compliance visibility across environments and allow DevSecOps teams to collaborate effortlessly.

Progress® Chef® Infra®

Automate infrastructure configuration to ensure consistent, repeatable, and fast software delivery to any data center or cloud environment.

Progress® Chef® InSpec®

Automate security tests to ensure compliance, security and other policy requirements are met in servers, Containers or Cloud Environments.

Progress® Chef® Premium Content™

Provides CIS regulatory and content compliance scanning across a range of enterprise assets out of the box.

Chef Cloud Security Benefits



Overcome Technical Skills Gaps

- Conversation based language
- 100s of out-of-box resources and helpers
- Built-in testing tools
- CIS/DISA STIG aligned profiles
- Automated waivers
- Visual UI for running scans, reporting, and dashboarding
- Free online learning, DevRel resources and Community



Increasing ROI with Adoption

- Same tooling and language for all systems and environments
- Fully extensible language
- End to coverage from dev to prod
- Hybrid and multi-cloud support
- Codified artifacts that can be integrated as part of automated workflows and pipelines
- Risk APIs and data feeds for integrating with corporate BI/AI systems
- Robust enterprise management platform for managing RBAC, DR, and Scaling



Limiting Risks and Increasing Speed

- Shift-left—policies and checks run at every stage of the pipeline
- Enterprise-wide control and visibility
- Harden systems, shut down non-necessary processes, limit risks
- Codified artifacts that feed automated pipelines
- Functional testing that ensures what you “fix” then still “works”



Key Features

Cloud Security Posture Management

- Continuously audit cloud accounts and services for security risks and misconfigurations.
- Scan infrastructure-as-code templates (Terraform) for security issues.
- Achieve consistent security across AWS, Azure, Google, and Oracle cloud.
- Remediate misconfigurations uncovered during audits without writing any code.
- Leverage a combination of in-node agents, network scans, and scans that use Cloud APIs to provide a 360-degree view of security and compliance posture across IP addressable AWS resources as well as non-IP Addressable AWS resources.

Container and Kubernetes Security

- Ensures ongoing secure configuration for your Kubernetes Clusters with built-in CIS benchmarks – Master and Worker node config files and RBAC.
- Achieve coverage from the build to the deployment stages – Docker based build and image files, Docker Host and Daemon configuration.
- Maintain history of scan results, policy changes and control failures.
- Create Custom Policies outside CIS standards based on your organization needs.

Cloud VM Security

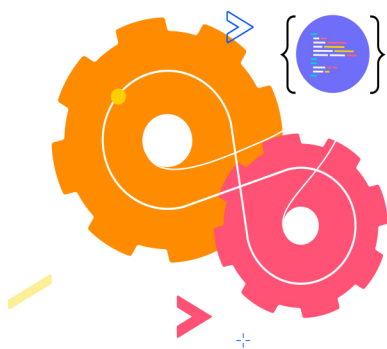
- Secure Linux and Windows based Cloud instances

Centralized Reporting for your Hybrid Cloud

- Multi Cloud Reporting: compliance- centric dashboard to gain deep insights into the state of the fleet.
- Continuously prove cloud compliance and spend less time on manual audits to stakeholders and auditors with one-click reports, and informative dashboards.

Regulatory Compliance

- Automate CIS benchmark tests for Audit and Remediation for Cloud, Kubernetes, and Docker.
- Maintain scheduled scans for internal organization policies and regulatory standards.
- Maintain history of scan results, policy changes and failures.



Policy as Code Approach

- Code is at the center of all our solutions and Chef is leading the evolution from “Infrastructure as Code” to “Policy as Code” which merges Infrastructure, Security, and Compliance Concerns into a Single Framework.

Platform and Integrations

- Manage users with LDAP/Active Directory and Single-Sign-On.
- Export Data into third party tools via REST API's.
- Send events into analytics and monitoring solutions (ServiceNow, Splunk, Kibana).

A Chef Cloud Security subscription provides access to an ever-growing list of profiles across your cloud native and hybrid environment—across all major public cloud providers, as well as container and Kubernetes deployments.

Environment	Audit
CIS for AWS Foundations Benchmarks Level 1 and 2	Yes
CIS Azure Foundations Benchmark - Level 1 & 2	Yes
CIS Docker Community Edition Benchmark - Level 1 & 2	Yes
CIS Kubernetes Benchmark 1.6.1- Level 1 & 2	Yes

Chef is the first CIS partner to achieve certification across AWS, Microsoft Azure, and Google Cloud Platform, giving its customers maximum flexibility when choosing and securing cloud platforms.



Learn More: www.chef.io