

Chef Cloud Security

Continuous Cloud Compliance
at Multi-dimensional Scale
with Unified Visibility





Chef Cloud Security empowers IT Teams to continuously monitor cloud accounts and container platforms for security misconfigurations. Align internal/external regulation at scale to achieve consistent, unified multi-cloud security using a coded approach and with extensive community support.

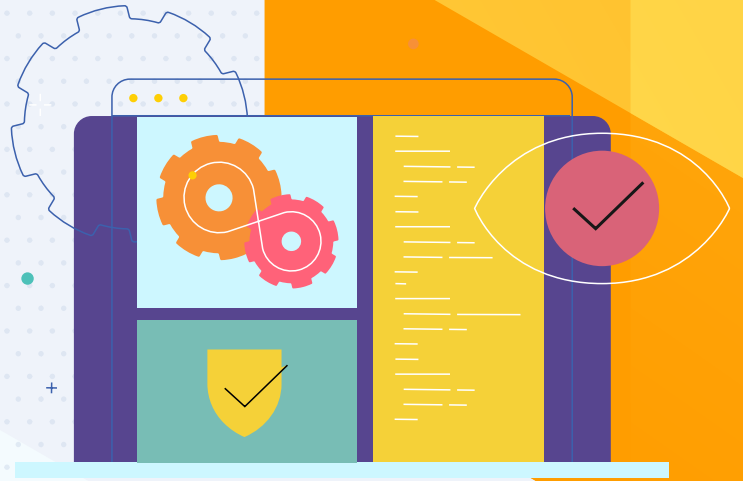
Key Features

Cloud Security Posture Management

Optimize CSPM strategy with continuous audits for security risks and misconfigurations.

Scan systems across environments (dev, pre-prod, prod), systems (cloud, Kubernetes, VMs, containers, Windows, Linux), and cloud providers (AWS, Azure, Google, and many others).

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.



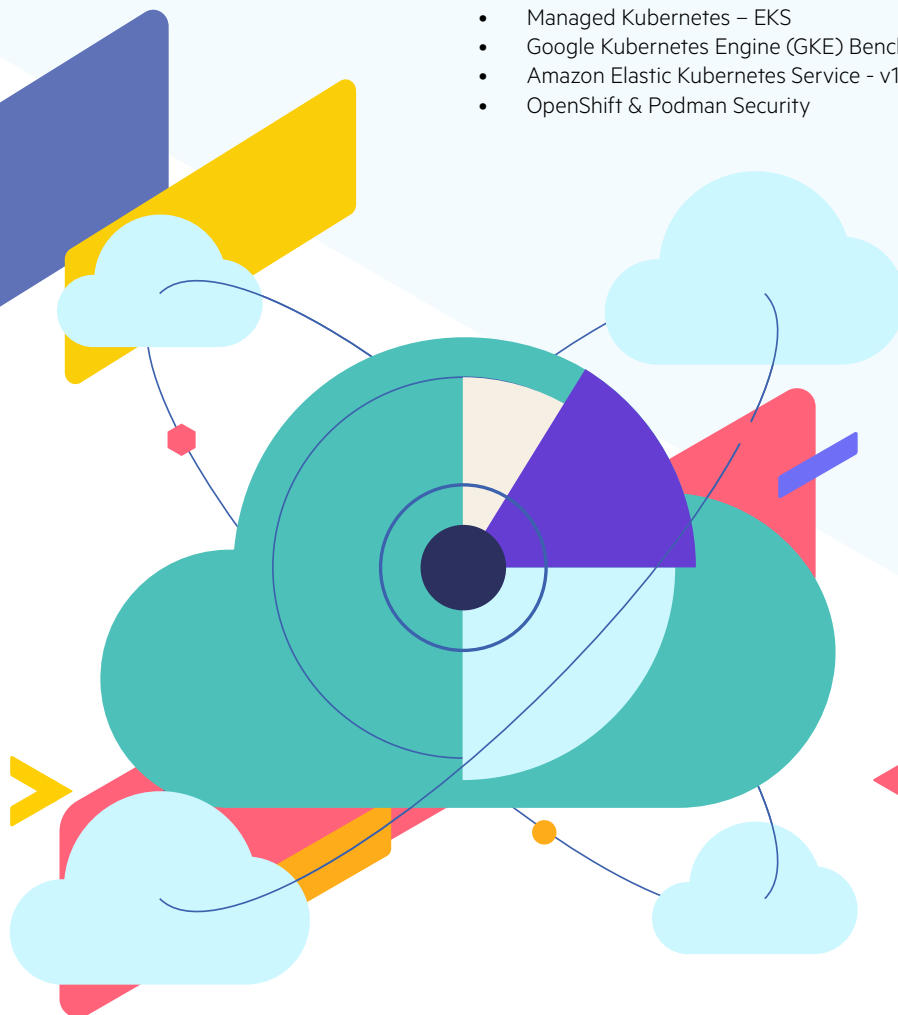
Container and Kubernetes Security

Automate compliance audits with curated benchmark profiles to manage container and Kubernetes security. Verify access privileges and secure configuration of Kubernetes clusters - scan container images including Docker based build and image files, Docker Host and Daemon configuration.

Secure OpenShift environments through integrated security and compliance checks that can validate container configuration and ensure your cloud infrastructure is compliant.

Validate Docker and Kubernetes infrastructure with best practices from CIS Benchmarks:

- Benchmarks for Docker and Kubernetes
- Managed Kubernetes – EKS
- Google Kubernetes Engine (GKE) Benchmark v1.1.0 (Beta)
- Amazon Elastic Kubernetes Service - v1.0.1 (Beta)
- OpenShift & Podman Security



Policy as Code

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. The policies are codified and human-readable, which facilitates collaboration and eliminates spreadsheets or other manual ways of tracking policy. In this way, collaboration is optimized across all these key disciplines- app dev, IT Ops, security and compliance.

Chef also allows customers to codify SCAP (Security Content Automation Protocol) content which helps strengthen the security posture when working in complex environments comprising many tools from multiple vendors.

Regulatory Compliance

Chef Cloud Security offers new premium cloud content to enable scanning cloud resources across all major public cloud providers, as well as container and Kubernetes deployments. Automate CIS benchmark tests for cloud, Kubernetes, and Docker.

Maintain scheduled scans for internal organization policies and regulatory standards and view history of scan results, policy changes and failures.

Centralized Reporting for Cloud Infrastructure

Compliance- centric dashboard to gain deep insights into the state of the fleet. Chef provides out-of-the-box integration with multiple platforms (ServiceNow, Splunk, Kibana, Mino, AWS S3, to name a few), and, a webhook through which data can be sent out to any platform of choice.

Maintain comprehensive and up-to-date visibility across multi-cloud and cloud native environments. View differences between baseline and remediated states. Track waiver status to enable fast and accurate audits at any time.

Continuously prove cloud compliance and spend less time on manual audits to stakeholders and auditors with one-click reports, and informative dashboards.

Visibility

Visibility into Compliance Posture across Cloud and Container Environments

Remediate

Remediation Guidance for correction policy violations



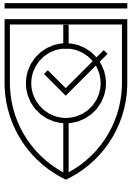
Audit

Scan Cloud Resources Compliance & Security Posture Against Industry Benchmarks and Best Practices

Detect

Misconfigurations and failed controls according to rules and profiles.

Chef Cloud Security Benefits



Secure hybrid cloud and maintain multi-cloud/cloud native governance

Maintain security and compliance across different environments – cloud, multi-cloud or cloud native.



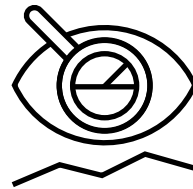
Detect misconfiguration on cloud resources

Detect misconfigurations on virtual machines, containers, and other cloud resources to prevent security breaches and maintain compliance posture.



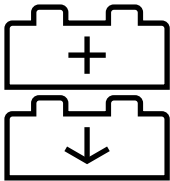
Achieve Continuous security and compliance on the cloud

Perform audits based on industry standards and benchmarks like CIS, PCI, HIPAA and DISA or customize compliance profiles to organization specific policies, to achieve continuous compliance.



Gain comprehensive visibility into cloud security and compliance posture

View the state of your cloud resources on a dashboard and gain visibility into audit run history, errors and compliance status.



Applying code-driven automation to scale cloud security and compliance

Perform audits based on industry standards and benchmarks like CIS, PCI, HIPAA and DISA or customize compliance profiles to organization specific policies, to achieve continuous compliance.



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.

CLOUD

Audit

CIS Amazon Web Services Foundation Benchmark - Level 1 & 2
CIS CentOS Linux 7
CIS Azure Foundations Benchmark - Level 1 & 2
CIS Google Cloud Platform Foundation Benchmark - Level 1 & 2



CONTAINER

Audit

CIS Docker Community Edition Benchmark - Level 1 & 2
CIS Kubernetes Benchmark 1.6.1 - Level 1 & 2
CIS Google Kubernetes Engine
CIS Redhat OpenShift Container Platform
CIS Amazon Elastic Kubernetes Service (EKS)



Accelerate your DevOps Journey with Chef Products

Chef Supports Any On-prem or Cloud Workload

Configure | Deploy | Manage

Security + Compliance

Device Management

App | Edge Delivery

Infrastructure Management

Chef Compliance

Chef Cloud Security

Enterprise Operational Visibility

Trusted Chef Tools (Chef Infra, Chef InSpec, Chef Workstation, etc.)

Chef Premium Content

Chef Supports On-prem, SaaS, & Marketplace Deployments



For more information on Chef Cloud Security visit:
www.chef.io/products/chef-cloud-security

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

2023 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.



- facebook.com/getchefdotcom
- twitter.com/chef
- youtube.com/getchef
- linkedin.com/company/chef-software
- learn.chef.io
- github.com/chef
- twitch.tv/chefsoftware