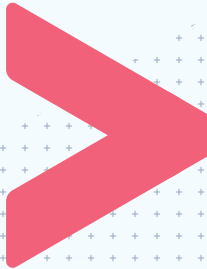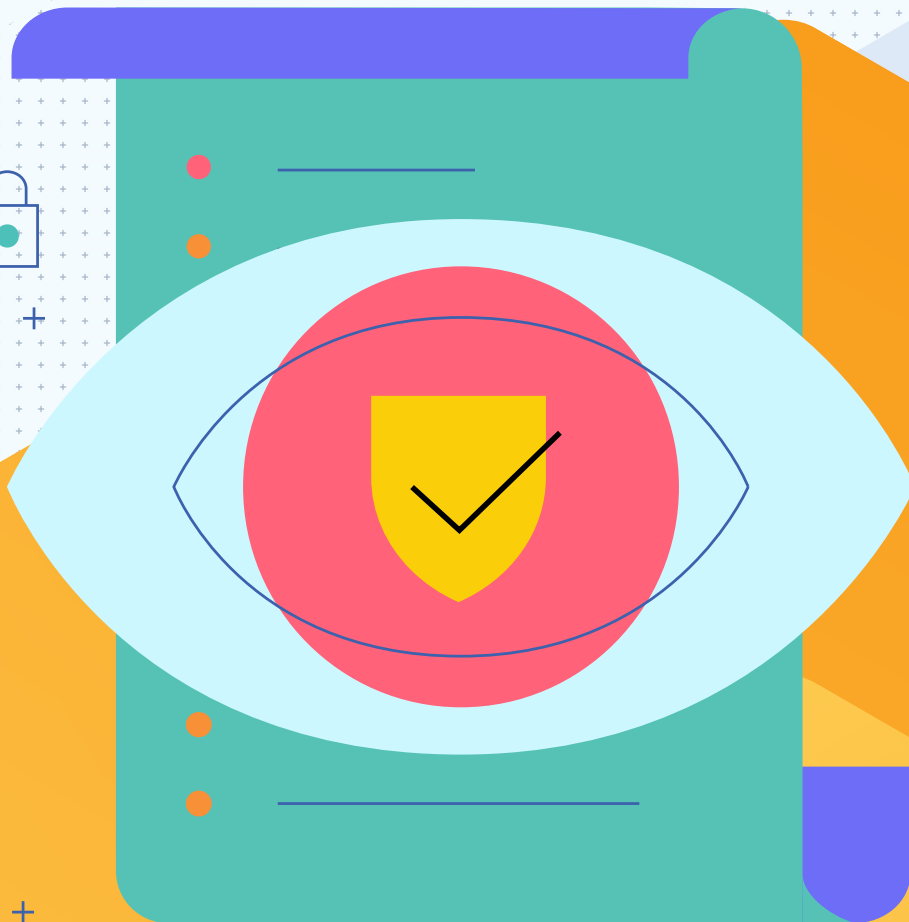# Progress® Chef

Chef Compliance Datasheet

Maintain compliance and prevent security incidents across heterogeneous environments
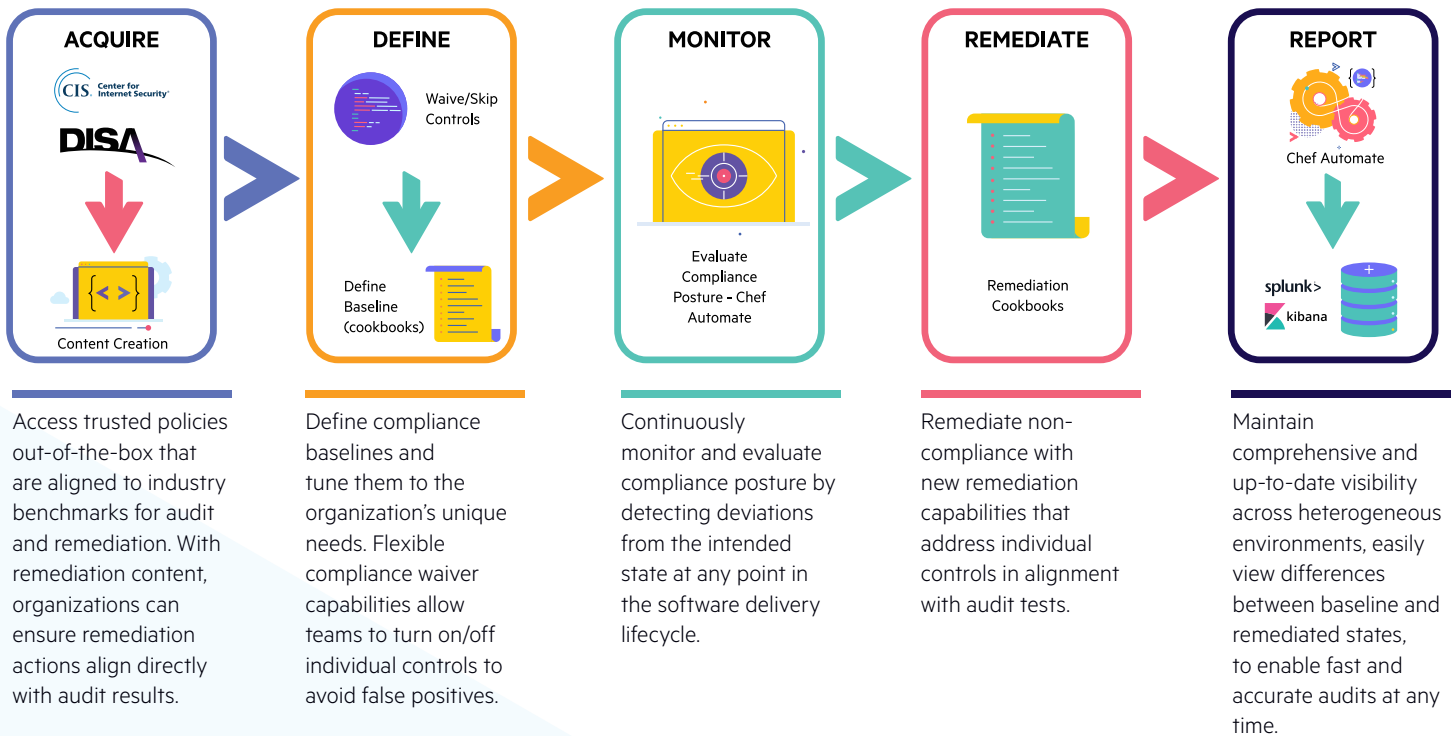
Chef Compliance Defined

Chef Compliance enables DevOps, InfoSec and compliance teams to collaborate and ensure that the software they ship or use is compliant and secure, turning InfoSec into an enabler rather than an inhibitor of velocity. Organizations can then reduce risk, increase speed, and improve efficiency in the DevOps process.

Chef Compliance makes it easier than ever to maintain and enforce IT compliance and security across the enterprise. With a standards-based audit and remediation policy content, easily tuned baselines to adapt to the organization's internal requirements, and visibility and control for security and compliance posture across heterogeneous environments, Chef Compliance ensures that your IT resources are always compliant and secure.

What does a Compliance workflow look like?

Chef Compliance helps across all stages of the compliance workflow:

ACQUIRE	DEFINE	MONITOR	REMEDIATE	REPORT
Content Creation	Waive/Skip Controls — Define Baseline (cookbooks)	Evaluate Compliance Posture – Chef Automate	Remediation Cookbooks	Chef Automate — splunk> kibana

Access trusted policies out-of-the-box that are aligned to industry benchmarks for audit and remediation. With remediation content, organizations can ensure remediation actions align directly with audit results.

Define compliance baselines and tune them to the organization's unique needs. Flexible compliance waiver capabilities allow teams to turn on/off individual controls to avoid false positives.

Continuously monitor and evaluate compliance posture by detecting deviations from the intended state at any point in the software delivery lifecycle.

Remediate non-compliance with new remediation capabilities that address individual controls in alignment with audit tests.

Maintain comprehensive and up-to-date visibility across heterogeneous environments, easily view differences between baseline and remediated states, to enable fast and accurate audits at any time.

Key Features

Premium Content

Chef Compliance delivers curated content for audits, remediation and desktop configuration based on CIS (Center for Internet Security) certified benchmarks or DISA Security Technical Implementation Guides (STIGs). Chef continuously maintains and updates the Premium Content library, and whenever an updated or new profile is identified, Chef quickly certifies the content and makes it available for content subscribers.

Policy as Code

Chef Compliance uses a policy-as-code approach where policies are managed with other application assets as part of your regular SDLC approach, including versioning, check-in, CI/CD, etc. 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 Compliance also allows customers to codify SCAP (Security Content Automation Protocol) content which helps strengthen the security posture when working in complex environments.

Custom Profiles

Chef Compliance can scan different types of operating systems, DBs, Web Servers and different applications via InSpec resources. With the help of more than 1000 InSpec resources, users can customize and write specific controls based on their needs. Chef resources can be used to write custom policies that perform checks on individual security settings of underlying systems, such as looking for a specific setting on an S3 bucket or a port.

Compliance Waivers

The Waivers feature's purpose is to indicate when a control is exempted, for how long, or when the exemption expires. Waivers help maintain operational continuity as you can easily track exceptions in the compliance posture and ensure these exceptions are removed as planned. This could be helpful for controls that are either not relevant to the customer's infrastructural architecture or are handled by another process within the customer's organization.

Support for regulations including PCI, GDPR, HIPAA

Chef's approach allows customers to support different regulatory requirements, including PCI-DSS, SOC 2, HIPAA and GDPR initiatives. Customers can use premium content as templates/generic rules to create their own security policies. The policy bundles are easily customizable by filtering out required rules through waivers and skipping certain rules. These rules can also be changed by editing the code that is applied through profiles as well.

Comprehensive Visibility

Compliance Remediation

Automated remediation helps close the loop between audit and remediation to enable continuous compliance in the enterprise. New remediation functionality and trusted, standards-based content makes it easy to remediate issues uncovered during audits without writing any code. Chef Compliance also has the extensibility and flexibility to allow for the customization of pre-packaged remediation content that can be modified to accommodate corporate-specific needs through code

Operating Systems	Applications	Cloud Environments
• Cent OS • RHEL • Ubuntu • SUSE • Debian • Oracle Linux • Amazon Linux • Windows	• NGINX • Apache Tomcat • OracleDB • MS SQL • MongoDB • PostgreSQL • MS Exchange • VMware ESXi	• AWS • Azure • GCP • Docker • Kubernetes

For details on the latest content **coverage**, please refer to our premium content page

The specially tailored compliance-centric dashboard allows organizations to gain deep and continuous insights into the state of their IT fleets. The Chef dashboard provides an end-to-end view across various systems managed both at an executive summary level as well as at a granular level, pointing to the code executing behind the scenes. Chef provides out-of-the-box integration with multiple platforms (ServiceNow, Splunk, ELK, Mino, AWS S3, to name a few), and, a webhook through data can be sent out to any platform of choice.
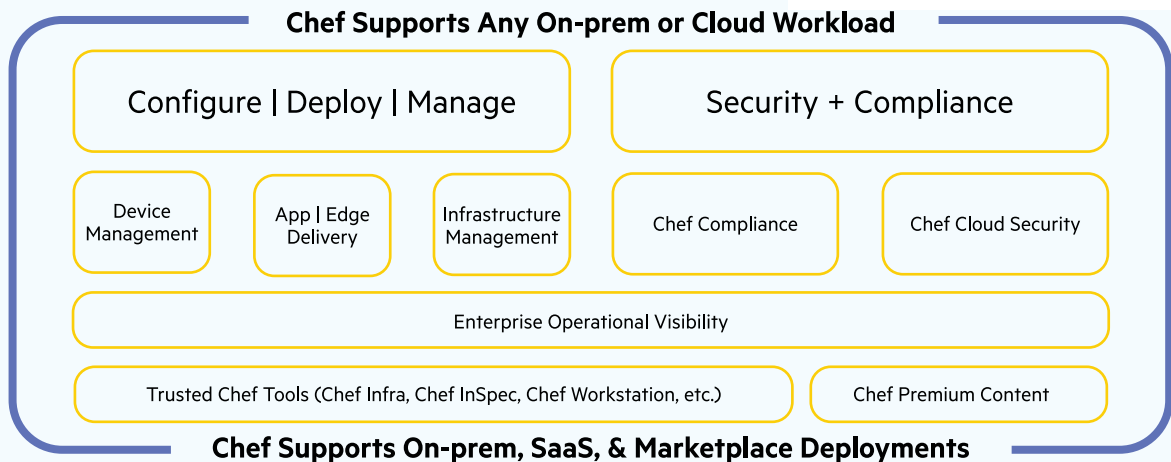
Tech Details

Chef Premium Content	Audit	Remediation
CIS Amazon Linux 2	✔	
CIS CentOS Linux 7	✔	✔
CIS CentOS Linux 8	✔	✔
CIS Debian Linux 9	✔	✔
CIS Docker Community Edition	✔	✔
CIS Kubernetes	✔	✔
CIS Microsoft 11$ 10	✔	✔
CIS Oracle Database 12c	✔	✔
CIS PostgreSQL 10	✔	✔
CIS RHEL 6	✔	✔
CIS RHEL 7	✔	
CIS RHEL 8	✔	✔
CIS Ubuntu Linux 18.04	✔	✔
CIS Windows Server 2016	✔	✔
DISA STIG RHEL 6	✔	
DISA STIG RHEL 7	✔	
DISA STIG Windows Server 2016	✔	
DISA STIG Windows Server 2019	✔	

Key Benefits

- **Faster audits:** Maintain up-to-date visibility into compliance state and easily report and share audit results.
- **Reduced risk:** Identify and eliminate risk with continuous compliance auditing and integrated remediation.
- **Ease of use:** No coding expertise is required, and dashboards help pinpoint imortant issues.
- **Faster time to value:** Leverage Chef Premium Content for audit and remediation and tune compliance profiles to address specific organizational requirements. Prioritize results through waivers and skip features to focus on important ones.
- **Increased Flexibility:** Write custom code based on your specific requirements and only check the environment needed.

Accelerate your DevOps Journey with Chef

Chef Supports Any On-prem or Cloud Workload

Configure | Deploy | Manage

| Device Management | App | Edge Delivery | Infrastructure Management |

Security + Compliance

| 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 Compliance visit:**
www.chef.io/products/chef-compliance

Progress®

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