Progress® Chef®

Public Cloud Infrastructure Compliance Scanning at SAP with Chef

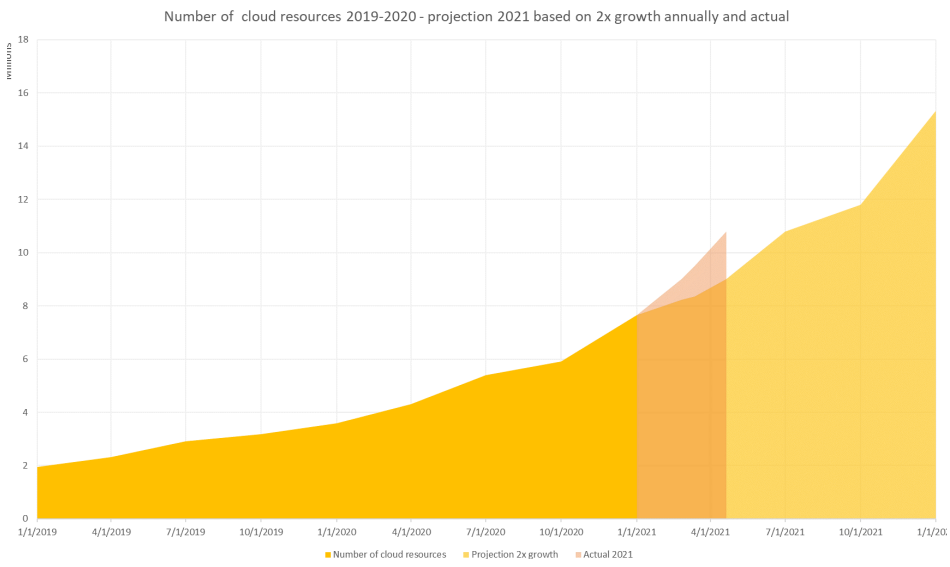
CASE STUDY

One of the essential security requirements for the public cloud is to ensure that misconfigurations in the landscape are avoided, and, if not, quickly remediated. Misconfigurations can leave landscapes inadvertently exposed and vulnerable without the operator being aware, and they are a growing problem. Well-known incidents like the Capital One data breach in 2019 have shown how damaging these misconfigurations can be.

Scanning for these misconfigurations impacting security is called Cloud Security Posture Management (CSPM) in the industry, tied to common security policies and frameworks (CIS benchmarks, NIST 800-53, etc.), and certification requirements like ISO, SOC and PCI. SAP has been conducting CSPM scanning centrally across the landscape for years through its Multi Cloud Security Operations team and has deployed two different tools on the market. Below is an overview of SAP's journey:

Scenario: SAP's Size & Growth Rate in Public Cloud

One of the biggest challenges SAP has is scale and growth rate. The company has over 9,500 active cloud accounts and over 11 million cloud resources across AWS, Azure, GCP, and AliCloud. SAP doubled its use of the public cloud each year for the past three years, and in 2021 that growth rate accelerated at a higher rate. The growth will only continue as a provider of solutions to customers operating on public cloud and through SAP's own internal public cloud use.



“The market for security tooling in public cloud is not very mature, and much that is available has trouble scaling to our volumes. The important question is, how do we solve the security problem as growth continues? Compliance scanning is a non-negotiable requirement, but at this scale there are not many options available, as we have to consider costs, that limits options even further.”

Jay Thoden van Velzen, Head of Security Operations, SAP Multi Cloud

Challenge: The Complexities of a Large Organization

SAP is a large organization of over 105,000 employees across multiple broad areas. The use of the public cloud naturally dominates in the development organizations for platforms, products and services. Still, it is spread across various broad areas, of all kinds of different teams of different sizes. There are customer-facing landscapes and many internal systems of various kinds – from development landscapes to training and demonstration environments.

The breadth of the SAP portfolio of solutions offered in the public cloud alone means there are many different organizations within the company involved, with a variety of development tooling and pipelines and different ways of operating. The company needed to accommodate and approach this in different ways and make it as easy to avoid security misconfigurations in the first place. Where they do occur, a quick resolution needs to be ensured.

The variety of use cases also means that teams may have valid business reasons for exceptions. Managing security exceptions (only granted after careful consideration and with appropriate controls in place to limit the risk) is a challenge in its own right, and SAP has developed its own solutions to manage this process.

Finally, when the team runs central compliance scans and calls other teams in the company to account based on them, it is crucial that the alerts generated are valid and correct. At this scale and across this wide variety of landscapes and cloud providers, running up against false positives is inevitable. Depending on a vendor to investigate and potentially correct alerts generating false positives can cause an inevitable time delay that will need

to be explained to the various teams involved and can take considerable time. Such false positives erode trust in the quality of the compliance scans and causes organizational reporting issues. It also makes teams less inclined to follow up on misconfiguration alerts with high priority.

Solution: Taking Control withCSPM and Chef InSpec for the Public Cloud

SAP first reviewed Chef InSpec in 2019. Then when SAP started working on "secure by default" public cloud infrastructure planning at the end of that year, InSpec was strongly recommended by an expert from one of SAP's hyperscaler partners, which confirmed SAP's thinking. At that point, the Multi Cloud SecOps team was confident that Chef InSpec could be containerized and run within a Kubernetes cluster as a result, scale as needed.

SAP Global Security defines policies and hardening procedures for public cloud that are abstractions from common public cloud baseline security requirements for common security frameworks, certification audits, regulatory reasons or contractual terms and conditions.

"These policies match, but don't necessarily fully align with the compliance checks included in CSPM tools on the market and we need to be able to adjust the ruleset to our policies. Chef InSpec, as compliance-as-code, allows us to do that in whatever way we might need."

Jay Thoden van Velzen, Head of Security Operations, SAP Multi Cloud

With the CIS Benchmark controls already available through the open source community, there was a good base to work from to modify them to SAP's needs and accelerate the team's development work.

“The code base being open source allows SAP to add new functionality and even cloud platforms to Chef InSpec’s capabilities, and therefore gives us the freedom and control to implement the detective controls we want, as long as the public cloud provider’s API supports it.”

Jay Thoden van Velzen, Head of Security Operations, SAP Multi Cloud

With the support of the Chef team, SAP deployed a first MVP, provided initial AliBaba Cloud coverage, and the company is ultimately moving public cloud infrastructure compliance scanning across all landscapes to the Chef solution.

Scale as Needed

The containerization was a success. SAP now runs a fully private Chef InSpec Kubernetes cluster of three nodes that scanned the entire landscape (around 8 million cloud resources) in three hours while taking over 900 exceptions (or waivers). During this test, SAP ran up to 280 containers, but during normal operations, this was 150. Depending on need as the number of cloud resources grows, SAP can both dial up the number of nodes and have room in the length of time the scan can run. With the most critical misconfigurations covered by SAP’s preventative controls, daily scans are considered timely enough for the organization to absorb, leaving us the opportunity to dial the knobs to keep operating costs under control as the cloud environment expands.

Shift-Left: Empower Teams and Solve Misconfigurations Early

Containerizing Chef InSpec has additional benefits. It gives SAP a highly flexible tool for teams throughout the company to use as they manage the compliance of their cloud accounts. SAP provides a consumer version of the container that can be run through a “docker run” command line and will run wherever Docker runs. Developer teams can run this interactively, integrate it into their development, testing and deployment pipeline, regardless of the toolset in use by the respective team. This allows teams using public

cloud to “shift-left” and adopt DevSecOps practices for public cloud infrastructure, as well as verify the status of their cloud accounts whenever they want. This also helps during any remediation exercise by developer teams, in being able to confirm instantly whether a configuration change brings the cloud account into compliance.

Control Coverage

SAP has controls implemented across AWS, Azure, GCP and AliBaba Cloud, with detective coverage – depending on hyperscaler capabilities – in the following areas:

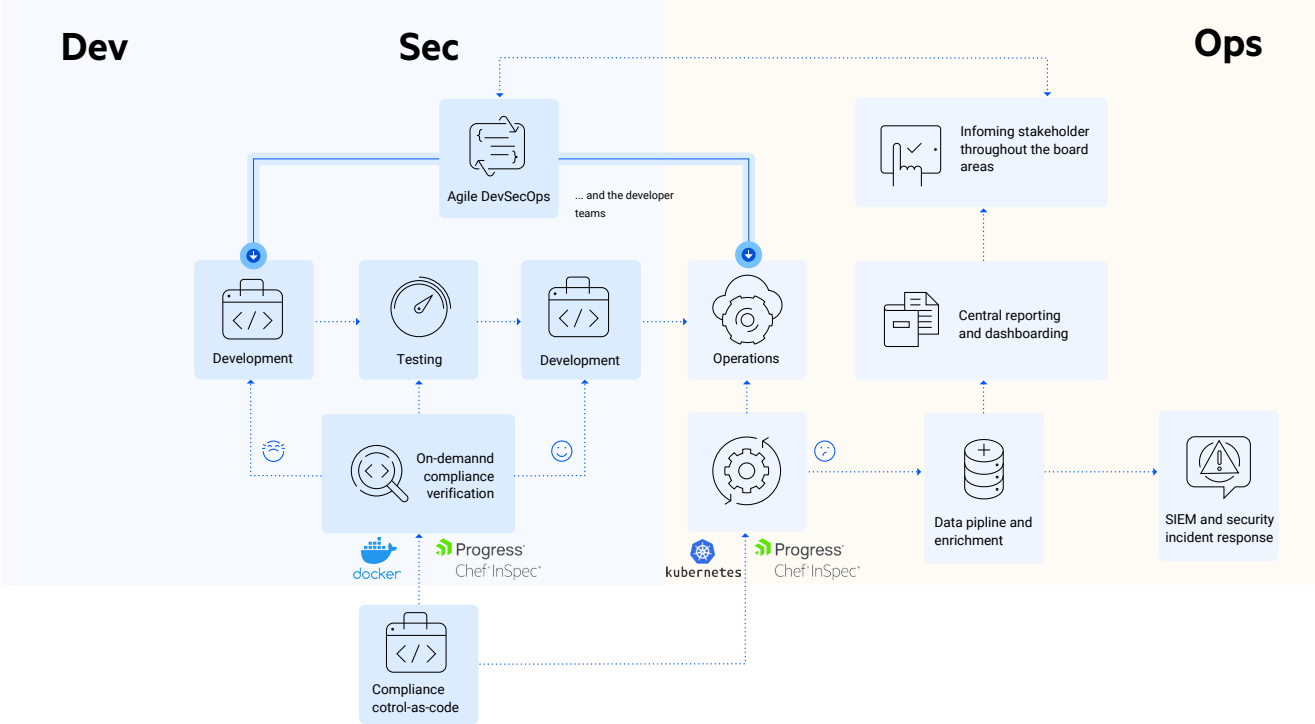
- Public storage buckets
- API logging centrally collected with appropriate log retention (minimum 6 months) and not publicly accessible
- Internet exposed admin ports and common database ports
- Disk volume and storage bucket encryption
- Encrypted communication for storage accounts
- TLS 1.2+ SSL policies
- Password policy, MFA and verified corporate identities for cloud admins
- Kubernetes master node logging
- KMS configuration and key rotation policies

In addition, control coverage is being extended to “medium” severity controls to match (and go beyond) the ruleset of the authoritative CSMP solution currently in place.

Tools Don’t Solve Problems, People Do: Organizational Support

Ultimately, tools don’t solve problems, but people do. Whether caught early during the development and testing pipeline, as part of a deployment, or during operational central scanning, teams need to follow up.

SAP has built up a support structure within SAP at multiple levels – from notifications to account owners, to direct interaction during weekly office hours with security experts and stakeholders within the business units, to executive reporting and weekly follow-up meetings with board area representatives to ensure any outstanding misconfigurations are responded to with the appropriate urgency. Scanning alerts are enriched with account metadata and organizational structure to facilitate security analytics and assignment of responsibility to the appropriate teams. This is already in place with SAP’s existing toolset and has proved very effective in ensuring accountability throughout the organization.



The integration becomes even tighter with the transition to Chef InSpec. There is a guarantee that the ruleset scanned for centrally in daily operations across the landscape is the same as the ruleset developer teams can scan for during the lifecycle of their cloud accounts.

This integration allows SAP to work efficiently with teams directly to deal with any suspected false positives. The control set compliance-as-code itself is available to inspect by developer teams and are very explicit in what they check. Teams can submit pull requests or reach out to the Multi Cloud team directly to test or correct the control. Since this is all an internal process, the turn-around time is much quicker. The transparency alone raises confidence and trust.

Open Source: Flexibility for SAP, Benefits Resonating Beyond

"Not only can SAP develop its own control set, but the company can also expand coverage where needed through the Chef InSpec Open Source process, both for the resource pack and for the back-end system," added Thoden van Velzen. There is support for new features and API changes for the different platform providers as SAP's policy controls require."

It provides SAP the flexibility in the future to potentially support additional cloud providers should business needs move in that direction and respond quickly to new and changing security requirements coming from SGS as changes in technology and cybersecurity require. It also provides other Chef InSpec users to benefit from those enhancements.

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 develop 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.

Rev 2022/01 RITM0140982

Progress

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA01803, USA
Tel: +1-800-477-6473

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