< GOUVERNANCE DES CONFIGURATIONS DANS LE CLOUD >

CAMPUS CYBER 2026

< SOMMAIRE >

< 1. DÉFINITIONS >

1.1 PÉRIMÈTRE DU DOCUMENT

Dans l'écosystème Cloud, les entreprises peuvent choisir de développer leurs propres applications ou d'utiliser des solutions SaaS prêtes à l'emploi. Quelle que soit l'approche, ces applications s'exécutent dans des workloads - des environnements d'exécution tels que des machines virtuelles ou des conteneurs pour les microservices - configurés pour assurer leur bon fonctionnement.

Ces workloads reposent sur une infrastructure Cloud complète, incluant le réseau, les services PaaS, le stockage, la gestion des identités et des accès (IAM), etc., conçue pour offrir élasticité, sécurité et efficacité. C'est dans ce cadre que nous identifions quatre niveaux de gestion, illustrés dans la figure 1.

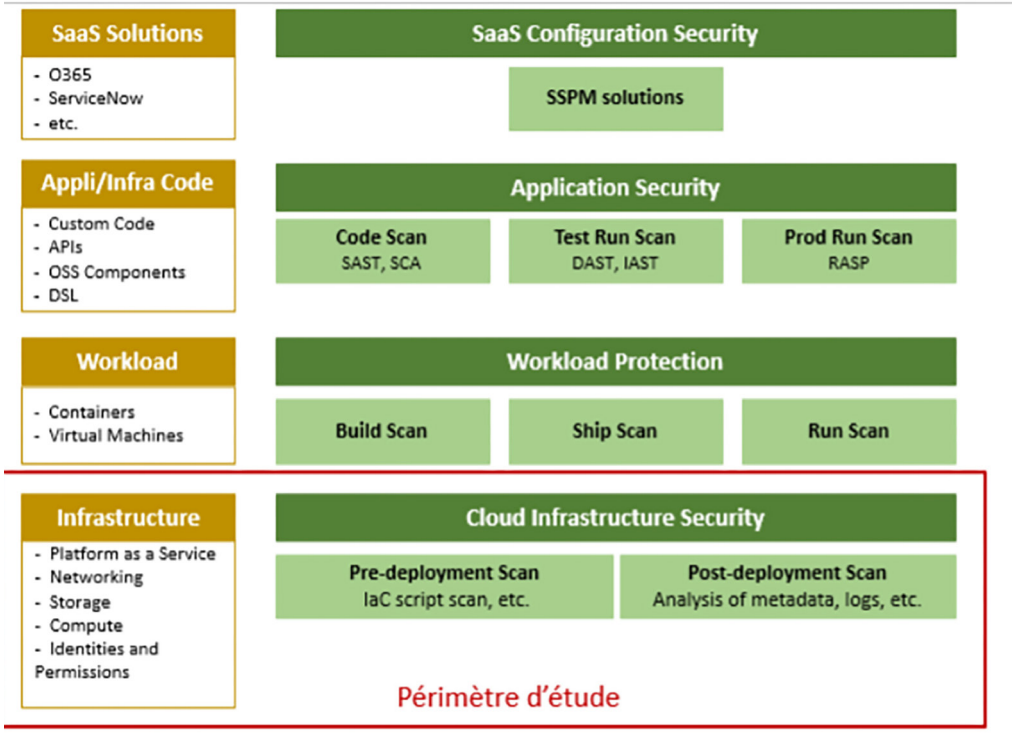


Figure 1 : Gestion de vulnérabilité sur les différents niveaux et périmètres cloud

Lorsque qu'on aborde la gestion des configurations et vulnérabilités, en particulier dans le Cloud, il est important de comprendre que cela couvre un large spectre de risques affectant les différents niveaux illustrés dans la figure 1. Chaque niveau nécessite des solutions spécifiques, basées sur des mécanismes de détection adaptés à la nature des failles. Ces vulnérabilités ne se limitent pas aux failles applicatives ou aux workloads deployés, mais concernent également la configuration de l'infrastructure Cloud.

Ce document se concentrera sur la couche infrastructure Cloud.

1.2 GOUVERNANCE DES CONFIGURATIONS DANS LE CLOUD

Les mauvaises configurations dans le Cloud représentent une source majeure d'exploitation pour les attaquants. Des erreurs telles que des stockages exposés à Internet ou des permissions excessives peuvent entraîner des fuites de données ou d'autres types d'attaques.
En 2025, on estime que 68% des incidents de sécurité Cloud sont liés à des configurations incorrectes [1] et 23% des incidents sont directement déclenchés par cela.[2] Gartner prédisait déjà qu'à horizon 2025, 99% des failles seraient dues à des erreurs humaines plutôt qu'à des vulnérabilités logicielles.[3] La mauvaise configuration est devenue un risque systémique du cloud moderne, avec un impact financier direct.

La gestion des mauvaises configurations dans le Cloud suit cinq étapes clés :

1. Préparation
- Définition des assets concernés et mise en place des outils avec les règles adéquates

2. Détection, classification et priorisation
- Inventaire des ressources Cloud
- Identification des configurations incorrectes
- Évaluation de la conformité selon les benchmarks et normes
- Visualisation via tableaux de bord et rapports

3. Analyse
- Étude des configurations détectées pour définir les actions correctives

4. Remédiation
- Application des corrections nécessaires

5. Contrôle
- Vérification continue de l'efficacité des remédiations mises en œuvre avec rétroaction pour ajuster les règles et leur priorisation

La configuration est bien un défi majeur du cloud :

- **Complexité croissante :** les environnements multi-cloud (Azure, AWS, GCP, OVH…) sont foisonnants, chaque plateforme ayant ses outils et ses règles. La gestion manuelle devient vite impossible à échelle.
- **Erreur humaine** : La majorité des mauvaises configurations sont causées par une mauvaise manipulation ou une méconnaissance des bonnes pratiques, et non par des défauts logiciels.
- **Impact économique et réglementaire** : Les conséquences vont de la perte de données, aux sanctions juridiques (non-respect RGPD, PCI-DSS, etc.) et coût de réputation.

1. Cloudpso. (2025). Cloud Security is Failing in 2025 Due to Misconfigurations.
2. Exabeam. (2025). 61 Cloud Security Statistics You Must Know in 2025.
3. Crowdstrike. (2022). Risques, Menaces Et Défis Liés À La Sécurité Du Cloud

1.3 OUTILS DE GESTION DE LA POSTURE DE SÉCURITÉ

Face à cette réalité, les entreprises doivent adopter une approche proactive pour détecter, corriger et prévenir ces mauvaises configurations. Les solutions permettant d'assurer la gouvernance sécurisée des configurations à ce niveau sont appelées, selon Gartner, Cloud Security Posture Management (CSPM).[4]
Elles jouent un rôle clé : elles permettent de surveiller en continu la posture de sécurité du Cloud, d'identifier les écarts par rapport aux bonnes pratiques, et de garantir la conformité aux standards de sécurité.

La détection des mauvaises configurations peut s'effectuer :

- **Avant le déploiement**, via l'analyse des scripts d'Infrastructure as Code par exemple
- **Pendant l'exécution,** à partir des logs, des métadonnées des instances, etc.

Les outils CSPM permettent d'automatiser la détection, l'analyse et la remédiation des risques liés à la sécurité dans les infrastructures Cloud. Ils offrent une visibilité continue sur la posture de sécurité, analysent les configurations des ressources, et identifient les écarts par rapport aux bonnes pratiques, aux politiques de conformité et aux standards (CIS, ISO, GDPR, HIPAA…).

Bien que non couvertes en détail ici, il est utile de mentionner les solutions utilisées pour la détection de vulnérabilité pour les autres couches :

- **Application :** Static Application Security Testing (SAST), Software Composition Analysis (SCA), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), Runtime Application Self-Protection (RASP) – analysent le code, les dépendances et le comportement de l'application déployée
- **SaaS** : SaaS Security Posture Management (SSPM) – permet d'identifier et de corriger les erreurs de configuration, de contrôler les accès, et de surveiller les intégrations de solutions SaaS
- **Workloads (OS et middleware)** : Cloud Workload Platform Protection (CWPP) — détecte les vulnérabilités tout au long du cycle de vie (Build, Ship Run).

Le marché des solutions CSPM a évolué pour inclure des fonctionnalités plus larges, désormais regroupées sous le terme CNAPP (Cloud-Native Application Protection Platform). Le CNAPP intègre, au-delà du CSPM, d'autres capacités clés telles que la protection des workloads (CWPP), la gestion des identités et des permissions (CIEM – Cloud Infrastructure Entitlement Management), ainsi que la sécurité applicative (SAST, DAST, SCA, etc.). Cette approche unifiée permet de couvrir l'ensemble du cycle de vie des applications — du développement à l'exécution — sur plusieurs couches techniques (infrastructure, identités, workloads) tout en offrant une analyse contextuelle des risques.
Ce document vise à présenter, au-delà des options techniques, quelle est la gouvernance à mettre en place pour assurer une bonne gouvernance des configurations dans le Cloud.

4. Gartner. (2026). Definition of Cloud Security Posture Management.

< 2. RISQUES >

L'utilisation du Cloud transforme profondément les modèles opérationnels des entreprises, en leur offrant agilité, scalabilité et réduction des coûts d'infrastructure. Toutefois, cette transformation s'accompagne de nouveaux risques en matière de cybersécurité, qu'il est essentiel d'identifier, de hiérarchiser et de maîtriser.

Ces risques sont multiples et de nature variée :

- **Risques financiers** : lié à l'usage non maîtrisé ou involontaire de ressources Cloud, pouvant entrainer une facturation excessive. Ces risques sont traditionnellement couverts par une fonction dite « FinOps » ;
- **Risques juridiques** : découlant d'un manque de clarté contractuelle ou d'un non-respect des réglementations (RGPD, HIPAA, etc.). Ces risques sont couverts par un encadrement contractuel rigoureux des prestations de Cloud computing et par un suivi régulier du niveau de sécurité des fournisseurs de cloud computing ;
- **Risques de disponibilité** : dus à des interruptions de service, des défaillances réseau ou des dépendances critiques vis-à-vis du fournisseur. Ils sont couverts par des plans de continuité et de réversibilité de la prestation de cloud computing et par une surveillance renforcée des liaisons réseau entre l'entreprise et le fournisseur de cloud.
- **Risques de sécurité technique** : incluant les intrusions, les fuites de données, les prises de contrôle de ressources, ou encore les mauvaises configurations exploitables par des attaquants.

Comme précisé dans le chapitre précédent, ce document se concentre sur les risques techniques liés à la gouvernance des configurations Cloud.
Ces risques peuvent être traduits en scénarios d'attaque concrets, que nous chercherons à détecter, contrôler et bloquer à l'aide d'une tour de contrôle de la posture de sécurité, reposant notamment sur les solutions CSPM.

ID	Scénario global	Description
R0	Accès illégitime à une ressource cloud	Tout accès illégitime à une ressource Cloud de l'entreprise par un utilisateur ou un service, en dehors des conditions de sécurité attendue. Cela inclut les accès provenant de réseaux non fiables (Internet, tiers), les ressources exposées sans filtrage adéquat, ainsi que les accès permis par une mauvaise configuration des droits (RBAC mal appliqué, absence de principe du moindre privilège, MFA non activé, secrets exposés ou mal gérés).
R1	Élévation de privilège	Obtention ou usage abusif de privilèges excessifs par des utilisateurs ou services, en dehors du cadre défini par la politique d'identité de l'entreprise.

ID	Scénario global	Description
R2	Partage de donnée illégitime / vol de donnée	Tout transfert illégitime de données internes en dehors des canaux autorisés. Cela inclut les flux sortants non filtrés, les partages mal contrôlés, ou les ressources configurées pour permettre des copies de données vers l'extérieur.
R3	Stockage de données non chiffrées	Présence de données stockées en clair sur des ressources Cloud, ou utilisation de mécanismes de chiffrement obsolètes ou non conformes aux politiques de sécurité de l'entreprise.
R4	Flux de donnée non chiffré	Transmission de données via des canaux non sécurisés ou utilisant des protocoles de communication obsolètes, exposant les données à des risques d'interception.
R5	Non-conformité	Non-respect des exigences légales ou normatives en vigueur et applicables à la gestion des données dans le Cloud, notamment en matière de localisation, de confidentialité, de traçabilité ou de sécurité.
R6	Manque de traçabilité	Absence ou insuffisance de journalisation des actions réalisées dans l'environnement Cloud, rendant difficile la détection d'incidents ou l'analyse post-incident.

Pour atténuer ces risques, il est crucial de mettre en place des mesures de sécurité robustes, telles que le chiffrement des données, des contrôles d'accès stricts, des audits réguliers de sécurité, et de choisir des fournisseurs de services cloud réputés et conformes aux normes de sécurité.

Pour bien identifier les mesures à mettre en place, il est nécessaire de décrire précisément les besoins fonctionnels de sécurité pour couvrir ces risques, ces besoins sont listés dans le tableau ci-dessous :

ID	Scénario global	Besoin de contrôle
R0	Accès illégitime à une ressource cloud	R0.1 : Aucune exposition de ressource de stockage sur internet. R0.2 : Aucune adresse IP publique configurée sur les ressources (VM, Base de données). R0.3 : Implémentation de l'authentification forte pour toutes les ressources devant être exposées sur internet. R0.4 : Usage du modèle de contrôle d'accès de l'entreprise pour accéder à la ressource. R0.5 : Revue régulière des configurations de contrôle d'accès aux ressources (usage d'un bastion, gestion des accès d'administration, etc.). R0.6 : Tests réguliers des API pour prévenir des attaques par injection. R0.7 : Eliminer les permissions non exploitées
R1	Elévation de privilège	R1.1 : S'assurer qu'une identité dispose des seuls privilèges nécessaires pour réaliser ses opérations. R1.2 : S'assurer qu'une identité dispose des seuls privilèges requis pour accéder aux informations dont elle a besoin. R1.3 : S'assurer que le service du cloud provider utilise un modèle de droit RBAC. R1.4 : S'assurer que le service du cloud provider respecte la politique IAM de l'entreprise (gestion des mots de passe, comptes locaux, adossement à un annuaire, etc.).
R2	Partage de donnée illégitime / vol de donnée	R2.1 : S'assurer que toutes les ressources réseaux sont configurées pour que les flux transitent au travers des firewall implémenté dans l'environnement cloud. R2.2 : S'assurer que les politiques de filtrage réseaux possèdent par défaut une règle de blocage « deny » configurée. R2.3 : S'assurer que la ressource cloud ne permet pas de réaliser de copie de donnée en dehors du cadre autorisé par l'entreprise. R2.4 : S'assurer que les ports sensibles sont restreints, et que les protocoles non-sécurisés ou non conformes aux normes de sécurité sont interdits.

ID	Scénario global	Besoin de contrôle
R3	Stockage de données non chiffrées	R3.1 : S'assurer que le service du cloud provider est configuré pour chiffrer l'intégralité des données stockées (disque, base de données, etc.) respectant la politique de gestion des clés de l'entreprise. R3.2 : Contrôler les ressources qui utilisent une version d'algorithme cryptographique / protocole de chiffrement déprécié (ex : SSLv3, TLS 1.0).
R4	Flux de donnée non chiffré	R4.1 : Interdiction d'instancier une ressource si cette dernière n'est pas configurée pour n'accepter que du trafic chiffré (ex : TLS). R4.2 : Contrôler les ressources qui utilisent une version d'algorithme cryptographique / protocole de chiffrement déprécié (ex : SSLv3, TLS 1.0).
R5	Non-conformité	R5.1 : Détecter toute non-conformité à une réglementation applicable dans le pays ou est déployée la ressource.
R6	Manque de traçabilité	R6.1 : S'assurer que les capacités de détection et de collecte de traces sont actives sur les ressources.

< 3. OPTIONS TECHNIQUES >

Comme vu précédemment, la sécurité dans le cloud public repose sur un principe fondamental : la bonne configuration des ressources.

Les entreprises disposent d'un outil pour gérer et assurer la sécurité des configurations dans le cloud : les outils de Cloud Security Posture Management (CSPM).

3.1 TROIS PRINCIPALES OPTIONS TECHNIQUES

1. Les outils natifs des fournisseurs de cloud
Ces solutions sont souvent activées par défaut et proposent des alertes, et un bon niveau de personnalisation. Par leur nature, leur intégration au sein de la plateforme qui les propose est optimale. Cependant, hors de leur environnement d'origine, elles peuvent faire face à des limites techniques. Des exemples d'outils : AWS Config, AWS Trusted Advisor, Azure Policy, Microsoft Defender for Cloud, Google Cloud IAM, Google Cloud Security Command Center ou encore IBM SCC Security and Compliance Center. Les offres européennes comme OVH ou Bleu intègrent quant à elles des outils spécifiques aux technologies utilisées.

2. Les solutions CSPM spécialisées du marché
Des acteurs du marché proposent des solutions clés en main, comme Prisma Cloud, CloudGuard, Wiz, Orca, Lacework, SentinelOne, etc. Le Gartner en fait la liste exhaustive chaque année.[5] Ces solutions sont multi-cloud, permettant une vision unifiée et une intégration avec d'autres briques de sécurité comme le SIEM ou SOAR. Ces solutions intègrent généralement le CSPM dans une solution plus large : le CNAPP.

3. Les outils open-source
Des alternatives gratuites et transparentes, qui permettent un contrôle et un hébergement directement dans le SI, sans dépendance à un tier : Cloud Custodian, ScoutSuite, Kube-bench, KICS, Open Policy Agent, etc. Cependant, comme tout ce qui est open-source, ces solutions requièrent une expertise technique et une maintenance interne à prévoir.

Ces options permettent aux organisations de choisir la méthode la plus adaptée à leurs besoins spécifiques, qu'il s'agisse de sécurité, de conformité ou d'optimisation des ressources. Bien que ces outils poursuivent un même objectif, ils présentent de nombreuses différences dont l'analyse d'impacts est essentielle pour identifier la solution la mieux adaptée au contexte local.
En fonction de ce qui est recherché dans la gestion des configurations, plusieurs équipes pourront consommer les informations remontées (SOC, Compliance, Gouvernance...). Cela sera vu dans une prochaine partie.

5. Gartner. (2025). Peer Insights - Best Cloud Security Posture Management Tools Reviews.

3.2 AIDE À LA COMPARAISON

1. Les outils natifs des fournisseurs de cloud

Ces outils natifs incluent des politiques de sécurité, des contrôles d'accès et des fonctionnalités de surveillance qui aident à maintenir une posture de sécurité robuste. Facile d'utilisation, et intégré par défaut dans l'environnement, ils permettent un bon premier niveau de sécurité et sont peu coûteux car généralement inclus dans l'offre cloud. Cependant, sans personnalisation, ces outils sont rapidement limités par leur offre générique

Ces solutions natives sont directement intégrées aux plateforme, facilitant ainsi leur adoption et leur utilisation. Elles bénéficient en plus d'un support officiel, de mise à jour automatique, sont conformes aux normes du fournisseur et peuvent tirer parti des mécanismes de contrôle d'accès, de journalisation ou de gouvernance propres à chaque cloud.

Bien que profitant d'une intégration profonde dans l'environnement Cloud propriétaire, ces solutions présentent des limitations en multi-cloud et pour les environnements hybrides complexes.

De plus, leurs fonctionnalités avancées de corrélation ou de priorisation de risque sont souvent limitées, nécessitant des développements complémentaires pour atteindre le niveau de maturité des outils spécialisés.

2. Les solutions CSPM spécialisées du marché

Le marché des solutions CSPM (Cloud Security Posture Management) a évolué pour inclure des fonctionnalités plus larges regroupées sous le terme CNAPP (Cloud-Native Application Protection Platform).

Les CSPM offrent des capacités avancées pour auditer et corriger les configurations erronées, détecter les vulnérabilités, et gérer les droits d'accès dans les environnements cloud multifournisseurs. Ces solutions sont particulièrement utiles pour les entreprises qui utilisent plusieurs fournisseurs de cloud, car elles fournissent une visibilité unifiée et des outils pour sécuriser l'ensemble de leur infrastructure cloud.

Les CSPM du marché se distinguent par leur moteur d'analyse contextuelle avancée : ils peuvent, par exemple, identifier qu'un excès de privilèges IAM combiné à une vulnérabilité sur une machine exposée représente un risque critique. Leur force réside dans leur capacité à prioriser les risques, à fournir des recommandations précises, et souvent à s'intégrer avec d'autres briques de sécurité (SIEM, SOAR, CI/CD). Une personnalisation des règles est aussi possible.

Cependant, ces solutions représentent un coût élevé et nécessitent souvent des déploiements plus complexes. Malgré leur offre clé en main, les compétences internes nécessaires pour assurer une exploitation optimale sont à prendre en compte.

De plus, ces solutions posent des questions de souveraineté et de confiance – car nécessitant l'accès à des métadonnées sensibles via des autorisations cloud, avec parfois une nécessité d'avoir des accès en écriture pour tirer parti de toutes les fonctionnalités.
Il existe encore peu d'acteurs CSPM véritablement européens, et ces solutions restent généralement moins matures que celles des grands éditeurs internationaux. Toutefois, elles répondent aux exigences spécifiques du marché européen, en mettant l'accent sur la souveraineté des données et la conformité au RGPD qui sont des critères essentiels pour les organisations soumises à des réglementations strictes. On peut citer par exemple l'acteur européen Secucloud (Allemagne).
A noter qu'en général, différents modèles de déploiement sont proposés par ces solutions : en SaaS ou on-premise.

3. Les outils open-source

Les outils CSPM open source offrent une alternative flexible et souvent gratuite pour surveiller les configurations cloud.
Des outils comme Cloud Custodian permettent de définir des politiques sous forme de code pour identifier et corriger les mauvaises pratiques, tandis que ScoutSuite ou Prowler fournissent des audits de sécurité en ligne de commande. Ces outils offrent de la transparence et une bonne adaptabilité à des workflows DevSecOps. Ils permettent aux entreprises un contrôle de leur outil CSPM, offrant une liberté vis-à-vis des éditeurs. Ils sont bien adaptés aux petites équipes techniques ou aux environnements à contraintes spécifiques (ex. : souveraineté).
Néanmoins, ils demandent plus d'expertise technique, sont difficiles à maintenir dans le temps, ne couvrent pas toujours les environnements multi-cloud de façon homogène, et n'intègrent pas nativement de priorisation des risques, ce qui peut limiter leur efficacité dans des environnements complexes ou très dynamiques.

3.3 STRATÉGIE DE DEPLOIEMENT

Les stratégies de déploiement varient selon le contexte de l'entreprise et ses moyens. Le déploiement peut reposer sur des approches multi-solutions ou sur une montée en maturité progressive, d'une solution native, nécessitant peu de compétences spécifiques, et peu chères, vers une solution open source ou éditeur, avec une personnalisation plus poussée et une vue unifiée des différents environnements Cloud.

Tableau récapitulatif de comparaison des outils

Critères	Outils natifs	Outils du marché	Outils open source
Coût	+++ Inclus dans les coûts du CSP (parfois payant à l'usage)	+ Coût élévé (licences)	++ Gratuit mais coûts d'infrastructure, de maintenance et de développement sont à prévoir
Couverture multi-cloud	+++ Spécialisé dans leur environnement d'origine, les capacités multi-cloud demeurent limitées comparées à celles des solutions spécialisées disponibles sur le marché	+++ Forte capacité à superviser et sécuriser des environnements multi-cloud de manière homogène et centralisée	++ Variable, souvent plus restreinte que celle des outils du marché, en raison de ressources et d'intégrations plus limitées
Facilité de déploiement	+++ Simple et rapide, grâce à leur intégration directe dans l'environnement du CSP	++ Demandent un déploiement plus élaboré, nécessitant souvent une configuration initiale et une intégration avec plusieurs environnements	+ Complexes à déployer en raison d'une installation manuelle (scripts, lignes de commandes…)
Fonctionnalités avancées	++ Limitées, avec des capacités de corrélation de risques, d'analyse et de contextualisation souvent restreintes à l'écosystème du CSP	+++ Très avancées, incluant une corrélation fine des risques, une analyse approfondie des configurations et une contextualisation étendue des alertes	+ Variables, généralement moins développées sur la corrélation de risques et la contextualisation, mais pouvant évoluer selon la contribution de la communauté

Critères	Outils natifs	Outils du marché	Outils open source
Priorisation des risques	++ Basique, essentiellement basée sur la gravité technique des alertes sans prise en compte approfondie du contexte ou de l'exposition réelle	+++ Contextuelle et intelligente, intégrant des facteurs tels que l'exposition, l'impact potentiel et les dépendances entre ressources	+ Simple, reposant sur des règles statiques ou sur la gravité technique des vulnérabilités détectées
Remédiation automatisée	++ Simple mais souvent limitées aux actions disponibles dans leur propre environnement cloud et peu configurables	+++ Complète et flexible, permettant d'orchestrer des actions correctives sur plusieurs environnements et de personnaliser les workflows selon les besoins	+ Limitée en fonction des scripts fournis par la communauté ou nécessite un effort manuel important de développement
Référentiel de règles par défaut	+++ Complètes et adaptées à l'environnement cloud, permettant une protection rapide et standardisée dès le déploiement	+++ Large éventail de règles couvrant de nombreux scénarios multi-cloud et bonnes pratiques de sécurité	++ Variable, parfois limitées et nécessitant des ajustements ou compléments manuels
Personnalisation des règles	++ Possible mais les règles sont préconfigurées pour les services du CSP et la personnalisation n'est pas toujours simple à réaliser en fonction du cloud provider	+++ Avancée : possibilité d'adapter les contrôles aux besoins de l'entreprise et à des environnements multi-cloud avec des compétences techniques sur l'outil	+++ Variable, souvent puissante mais nécessitant des connaissances techniques et un effort de configuration plus important
Intégration dans la chaîne DevSecOps	++ Simple pour les pipelines DevSecOps propres à leur cloud, peu de flexibilité pour des environnements DevOps hybrides ou multi-cloud	+++ Flexible et simple, dans des pipelines DevSecOps variés, facilitant l'automatisation de la sécurité sur plusieurs clouds et outils	+ Possible mais nécessite souvent des développements et configurations manuels importants

Critères	Outils natifs	Outils du marché	Outils open source
Maintenance / Support	+++ Support officiel du CSP	+++ Support éditeur (SLA, support pro)	+ Pas de support officiel (communauté open source)
Souveraineté / Contrôle des données	Dépend de la solution choisie : des permissions en écriture peuvent s'ajouter aux permissions de lecture du CSP	Dépend de la solution choisie : données envoyées à un tiers, la plupart du temps américain	Dépend de la solution choisie : contrôle total, à condition de disposer des ressources pour la gestion et l'hébergement

Légende :
+ Maturité limité ++ Maturité intermédiaire +++ Maturité avancé

3.4 COMMENT CES OUTILS AIDENT À LA GESTION DES RISQUES

Ces exemples concrets illustres comment les outils type CSPM couvrent les scénarios R0-R6 identifiés ci-dessus :

- **Détection et prévention d'une exposition involontaire** : Les outils CSPM permettent d'identifier rapidement toute exposition involontaire — comme des ressources accessibles publiquement, des ports mal sécurisés ou des instances non chiffrées — et de les corriger. Ils automatisent la surveillance des configurations réseau et la prévention d'accès non autorisé grâce à des politiques et des contrôles continus. Ces approches permettent aux entreprises de réduire les risques liés à l'accès illégitime à des ressources cloud.
- **Conformité avec les normes de sécurité (ISO 27001, PCI-DSS, GDPR, etc.)** : Le CSPM vérifie en temps réel que les ressources cloud répondent aux normes de sécurité (ISO 27001, PCI-DSS, RGPD…). Par exemple, une entreprise traitant des données de carte bancaire peut utiliser un CSPM pour vérifier en continu que les volumes ou les services de stockage contenant des données sensibles soient chiffrés. Il génère des alertes et facilite les audits en cas d'écarts, réduisant significativement les risques de non-conformité et de sanctions.
- **Correction** : Au-delà de la détection, le CSPM accélère la correction des failles : des remédiations sont proposées, souvent clé en main, et peuvent être automatisées (ex : fermeture d'un port ouvert, réinitialisation d'un accès) pour réduire la fenêtre d'exposition et alléger la charge sur les équipes sécurité. Les outils CSPM permettent la remédiation automatisée à travers des scripts ou des fonctions serverless. Il est tout de fois nécessaire d'être prudent avec cette possibilité, car elle demande souvent des droits importants dans les environnements et peut impacter directement la production : une analyse d'impact est nécessaire.

- **Visibilité** : Le CSPM regroupe toutes les informations de sécurité (ressources exposées, statuts IAM, compliance) dans une console unique, ce qui est essentiel pour les environnements multi-cloud. Cela permet de visualiser rapidement les risques et incohérences sur l'ensemble des environnements, évitant la fragmentation des configurations entre clouds. Il offre de plus une vision rapport, utile pour le management des entreprises. De plus, certains outils proposent la fonctionnalité d'inventaire des ressources, ce qui améliore la cartographie des risques.
- **Priorisation** : Enfin, le CSPM classe les mauvaises configurations et vulnérabilité selon leur gravité et leur contexte : il détecte les combinaisons les plus critiques (ex : excès de privilèges sur une instance accessible publiquement sans MFA) et guide les équipes sur ce qui nécessite une action immédiate, ce qui limite le bruit des alertes et concentre l'effort sur les failles dangereuses.

Avec ces cinq piliers, les outils de type CSPM permettent aux organisations de prévenir, corriger et optimiser en continu la sécurité de leur infrastructure cloud, tout en restant conformes et efficaces face à la complexité croissante du cloud moderne.

< 4. PROCESSUS OPÉRATIONNELS >

Pour assurer une bonne mise en place de ces outils et une gestion optimale de la posture de sécurité dans le cloud, il est nécessaire de structurer les processus opérationnels.Cela passe par l'articulation des alertes, des exceptions et des remédiations. Ces processus devront s'inscrire dans un cadre de gouvernance plus large, détaillé dans la section suivante.

4.1 GESTION DES ALERTES

Dans le contexte de gestion des mauvaises configurations dans le Cloud, les alertes doivent permettre de réduire les risques de déviation dans la posture de sécurité tout en réduisant le bruit. En effet, comme tout outil de sécurité, l'activation des alertes par défaut va générer un grand nombre d'alertes, avec des criticités élevées qui les rendraient inexploitables par les équipes en charge.

- **Priorisation et cas d'usage**
  Il est nécessaire de distinguer les alertes de conformité des alertes de sécurité. Les scénarios à fort impact doivent être définis, en lien avec les usages métiers et les enjeux de sécurité, afin de permettre la mise en place des alertes adaptées. Exemple : ressource critique rendue publique, désactivation d'un paramètre de sécurité, chiffrement non mis sur un service critique ou changement de configuration de comptes à haut privilège.
  Une fois ces scénarios établis, une mise en service progressive, organisée par vagues de contrôles, permettra aux équipes d'ajuster le niveau d'alerte et d'absorber la charge opérationnelle. Les premières vagues pourront couvrir les fondamentaux de la sécurité dans l'environnement de l'entreprise, avant de s'étendre aux services Tiers 1, puis aux autres périmètres.

- **Utiliser l'existant**
  Si un SOC et un SIEM central sont en place, il est intéressant d'y raccorder les alertes générées afin de profiter des processus et des outils déjà en place. L'enjeu est d'éviter la multiplication des consoles et permettre aux équipes de corréler les alertes avec d'autres signaux pour identifier les scénarios de compromission. Cela ne sera cependant possible que si les scénarios ont été définis en amont, pour ne pas surcharger ces équipes.

4.2 GESTION DES EXCEPTIONS

A chaque règle ses exceptions : elles conditionnent la crédibilité des indicateurs, et reflètent une réalité terrain car liées à de l'existant, des contraintes techniques ou à des architectures spécifiques.
Toute exception doit être rattachée à un scénario de risque spécifique, tels que ceux décrits dans la section « Risques ». Comme les alertes, celles-ci doivent être intégrées au processus global de gestion des dérogations de l'entreprise, afin d'éviter la création de silos et de garantir une traçabilité et une gouvernance cohérentes. Ces processus permettront d'identifier l'auteur de chaque demande d'exception, d'en préciser le périmètre, de formaliser les acteurs de la validation, et de définir une durée de validité limitée assortie de revues périodiques afin d'en réévaluer la pertinence.
Si elles existent déjà, les exceptions doivent être suivies dans les comités de sécurité et les outils de gestion des risques, et non seulement dans l'outil CSPM, pour assurer la visibilité globale et la correcte évaluation du risque résiduel.

4.3 REMÉDIATION

Dans la plupart des outils proposés sur le marché, la remédiation repose sur différents modes d'actions :

- **Blocage préventif** : lorsqu'une mauvaise configuration est détectée, la mise en production est bloquée. Par exemple, le déploiement d'un compte de stockage exposé sur internet sera refusé, avec un message d'erreur ou non. D'un point de vue sécurité, cela permet d'éviter d'exposer un environnement à un risque critique et permet à l'équipe ou à la personne concernée de chercher et apprendre de son erreur. Cependant cela peut aussi perturber les équipes si les règles sont trop strictes ou mal comprises.
- **Correction manuelle et guidée** : certains outils proposent des instructions pas à pas, voire des bouts de code déjà écrit, clé en main (Terraform, ARM, CloudFormation, etc.) mais sans bloquer les déploiements. Cette méthode permet aux équipes d'appliquer elles-mêmes les correctifs, renforçant ainsi leur compréhension des enjeux de configuration et de sécurité. Cependant, la ressource ou environnement rendu vulnérable, en l'absence de suivi des remédiations, peut le rester.
- **Correction automatique :** des outils, avec droit en écriture, propose des correctifs déclenchés sur la base de règles et de playbooks, et donc automatiques. Par exemple : le déploiement d'un compte de stockage en public sera corrigé directement au niveau de la ressource. Cette méthode, bien que très efficace, peut avoir des effets de bords, par exemple en corrigeant un cas d'usage légitime et validé. De plus, elle nécessite de donner des droits en écriture étendus aux solutions, ce qui peut engendrer des dérives, et ne permet pas aux équipes d'apprendre de leurs erreurs de configuration. Cette méthode a un intérêt pour les cas fréquents et peu risqués mais cela doit être pour des scénarios bien cadrés et testés en amont.

Dans tous les cas, il est essentiel que les actions de remédiation soient réalisées par les bonnes personnes (comme les propriétaires de ressources) et, pour les corrections critiques en production, qu'elles passent par un workflow d'approbation dans un outil de ticketing ou de gestion des incidents, afin d'assurer traçabilité, transparence et responsabilisation des acteurs.

Un plan d'action standardisé doit définir :

- La manière dont les alertes sont triées (priorisation, contexte métier) ;
- Le responsable de l'analyse et le responsable de la correction ;
- Le délai de remédiation selon la criticité.

En fonction de ce plan d'action, il est possible de distinguer différents modes de remédiation avec par exemple de la remédiation manuelle pour les cas sensibles, un blocage préventif pour les écarts simples et de la remédiation automatique encadrée pour des scénarios maîtrisés.

Une fois les outils choisis et les processus mis en place, la question n'est plus seulement de savoir « quoi corriger » mais qui ? La définition d'une gouvernance autour de la gestion des configurations dans le cloud devient centrale : définition du cycle de vie des règles, plan d'actions pour la remédiation, définition d'indicateurs simples mais parlants.

< 5. GOUVERNANCE >

Une gouvernance adéquate permet de transformer ces informations techniques en plans d'action et décisions stratégiques pour la sécurité des environnements Cloud, tout en restant alignés avec les enjeux métiers.

Le cadre de gouvernance doit préciser :
- Le périmètre couvert (comptes, souscriptions, environnements, ressources) ;
- Les objectifs de conformité (règlementations, politiques internes) et leur suivi (KPIs, comités) ;
- Les parties prenantes impliquées (équipes cloud, sécurité, dédiées).

Ce cadre doit permettre d'apporter de la visibilité à ces différents acteurs et de formaliser les principes de bases : critères de criticité, scénarios de compromissions, règles, etc.

5.1 RÔLES ET RESPONSABILITÉS

A titre d'exemple, voici des rôles types dans la gestion des conformités dans le cloud, dont la dénomination est dépendante de l'entreprise :
- La cybersécurité (définition des politiques, supervision, arbitrage des risques)
- Les équipes Cloud et plateforme/infrastructure (mise en œuvre des contrôles et des règles, intégration dans les environnements)
- Les équipes de développement ou projets (remédiation des ressources dont elles sont propriétaires)
- Les responsables métiers ou cyber (validation d'exceptions)
- Ou encore les équipes SOC pour la gestion des alertes et des incidents.

Les accès à l'outil doivent correspondre à cette répartition, suivant le modèle de Role-Based Access Control : certains profils peuvent accéder en lecture seule aux rapports, alors que d'autres auront besoin d'accès en écriture pour modifier les règles. Seuls les rôles identifiés peuvent déclencher des remédiations sur les environnements de production.
Les matrices de RACI, bien connues de tous, peuvent être utilisées. Elles doivent être maintenues à jour, les services Cloud évoluant rapidement, et donc les domaines de responsabilités avec eux.

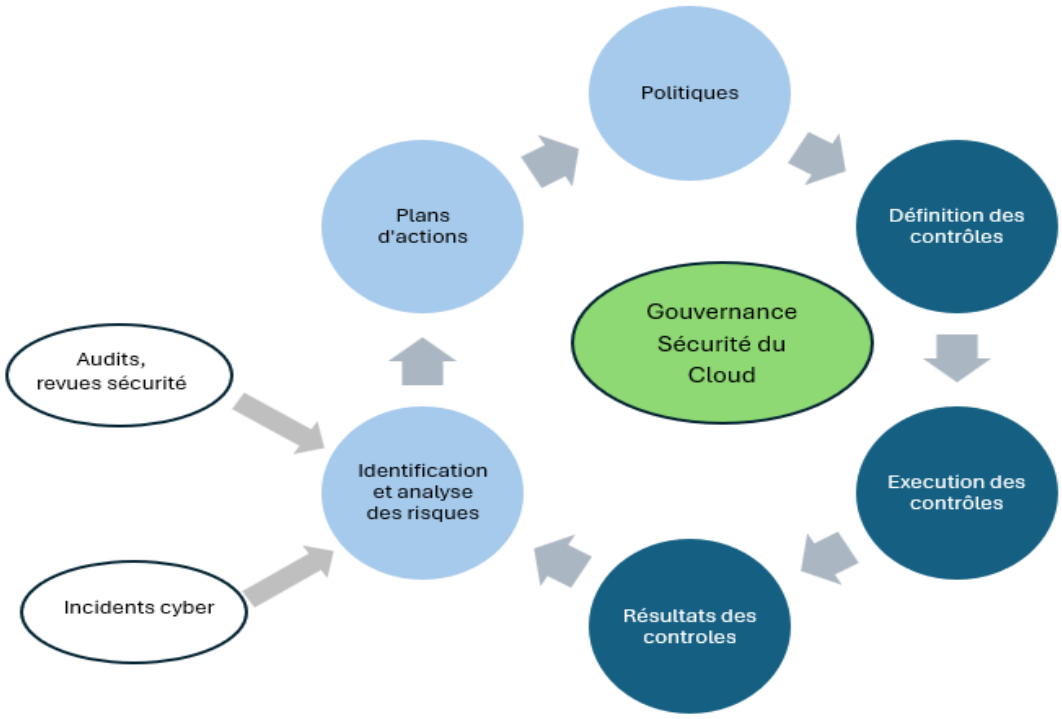
5.2 INDICATEURS ET PILOTAGE

Des métriques et indicateurs peuvent être définis pour rendre la posture de sécurité lisible et favoriser l'arbitrage entre les contraintes opérationnelles et exigences de sécurité. Ci-dessous, des exemples :
- Pourcentage de ressources conformes aux politiques définies
- Délai de remédiation par criticité

- Tendance des non-conformités ouvertes
- Exceptions en cours

5.3 INTÉGRATION DANS LA GOUVERNANCE SÉCURITÉ DU CLOUD

La gouvernance associée à la gestion des configurations est une des briques sur lesquelles la gouvernance sécurité du Cloud s'appuie. Les contrôles s'appuient sur les politiques, les outils de CSPM/CNAPP permettent de s'assurer que les politiques sont respectées ou lorsque des écarts sont constatés, d'identifier de nouveaux risques et plans d'actions au même titre que les risques et plans d'action identifiés à partir d'éventuels incidents cyber reportés par le CERT/CSIRT ou d'audits (voir schéma ci-dessous).



Il s'agit d'un processus itératif permettant l'amelioration continue (Plan-Do-Check-Act), il est formalisé au travers de comités avec une représentation de la direction adaptée. Les décisions de traitement des potentiels nouveaux risques identifiés pourront être validées et plans d'actions identifiés pourront donc être mis en place/lancés. Les politiques pourront nécessiter d'être modifiées/enrichies en conséquence.

5.4 INTÉGRATION DANS LA DÉMARCHE DEVSECOPS

Finalement, si l'entreprise a déjà entrepris une démarche DevSecOps, la gestion des configurations dans le cloud doit être alignée avec celle-ci. Cela signifie l'intégration des contrôles de sécurité dès la conception et le développement, pour réduire le volume des alertes après une mise en production.

Le scan Infrastructure-as-Code (IAC) fait partie des outils CNAPP, et permettent de détecter les mauvaises configurations avant le déploiement de l'infrastructure. Cela permet de renforcer la conformité des configurations et de faire du « shift-left ».

Dans ce modèle, les outils CSPM/CNAPP deviennent un outil partagé, soutenant la culture de la sécurité by design.

< 6. CONCLUSION >

La gestion des mauvaises configurations dans le cloud constitue aujourd'hui un enjeu majeur de sécurité. La majorité des incidents sont imputables à des erreurs de configuration, bien davantage qu'à des vulnérabilités logicielles. Les solutions du marché (CSPM ou CNAPP) offrent une visibilité continue et des capacités de remédiation automatisée, mais leur efficacité dépend d'un cadre de gouvernance structuré et d'une articulation claire entre les équipes techniques, la cybersécurité, le métier et la direction.

Seule une démarche alignée sur les enjeux métiers, les exigences réglementaires et les bonnes pratiques du secteur permet d'assurer une posture de sécurité pérenne et de transformer la gestion des configurations en levier de résilience et de conformité.

Le Campus Cyber tient à remercier chaleuresement l'ensemble des contributeurs du GT « Gouverance des configurations dans le Cloud » rattaché à la Communauté d'Intérêt « Sécurisation du Cloud », notamment Jeanne GRENIER (Bouygues SA), Grégory TERRIEN (Société Générale), Mayssa JEMEL (BNP Paribas), Gilles GHATTAS (BNP Paribas), Elise JOUSSELIN (Wavestone), Julien BERNARD (Amadeus) et Ronan LE NOZACH (BNP Paribas).

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX

CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT
DANS LE CADRE DU PROGRAMME D'INVESTISSEMENTS D'AVENIR