Stordata

Plateformisation du système d'information : des premiers pas à l'industrialisation de la conteneurisation

Plateformisation : le terrain d'entente entre la DSI et ses utilisateurs

La technologie conteneurs permet de construire une plateforme polyvalente et évolutive qui assure :

- Pérennité de l'investissement initial
- Collaboration inter-équipes *via* des primitives standardisées (packaging, configuration, déploiement)
- Déploiement accéléré de services pré-conteneurisés
- Modèles de consommation self-service sur étagère
- Risque minimisé pour les services expérimentaux
- Autonomie préservée des utilisateurs pour créer leurs propres services conformes

Depuis plusieurs décennies, les entreprises cherchent à trouver la martingale entre 2 grands enjeux :

- autonomie, souplesse et instantanéité pour les utilisateurs, afin qu'ils disposent de l'outil adéquat pour porter le business ;
- rationalisation des technologies et des processus proposés par la DSI, pour des raisons de maîtrise des technologies et des coûts, et de conformité à certaines contraintes (d'entreprise ou externes) de l'ensemble de la chaîne.

ITIL, mouvement Agile, pratiques DevOps ont été autant d'initiatives en ce sens. Avec les facilités du cloud public (provisioning instantané, self-service, élasticité, variété technologique), certains utilisateurs se sont détournés de la DSI, et ont adopté ces solutions de façon autonome. Mais ce shadow IT pose, dans l'entreprise, un problème de gouvernance, de sécurité et de coûts. La DSI rattrape ce mouvement avec des initiatives move-to-cloud, réintroduisant ses contraintes, tout en n'offrant guère de valeur ajoutée pour les utilisateurs déjà autonomisés.

En popularisant la notion de conteneur informatique, **Docker** a matérialisé explicitement la **surface de collaboration entre la DSI et ses utilisateurs** : ce qui se passe dans la boîte est du ressort des utilisateurs, ce qui manipule cette boîte, et en assure le *run*, est du ressort de la DSI.

Aboutissement de ces initiatives passées, ce modèle opérationnel s'est imposé comme un standard. Et ce d'autant plus que les éditeurs eux-mêmes standardisent de plus en plus leurs solutions sous format conteneurisé, parfois exclusivement. Ce qui était une simple option technologique devient un véritable prérequis, y compris pour les solutions sur « étagère ».

L'euphorie de trouver (enfin !) cette technologie et son modèle opérationnel, entrant en adéquation avec les attentes des utilisateurs et les exigences de la DSI, n'évacue pas les enjeux historiques : **le conteneur n'est rien seul**. Pour qu'il soit efficace, il faut la grue qui le manipule, et le navire porte-conteneur qui le transporte. La performance, la résilience, et globalement la sécurité des systèmes demeurent des enjeux centraux et nécessitent une approche renouvelée, d'autant plus essentielle que la consommation de la plateforme se réalise directement, sans l'intervention des administrateurs.

Un écosystème en perpétuel mouvement, des maturités hétérogènes

Les niveaux de maturité varient considérablement selon les organisations : certaines entreprises testent prudemment quelques projets pilotes, d'autres multiplient expérimentations et déploiements de technologies diverses (orchestrateurs, registres, outils de monitoring). À l'autre bout du spectre, les « *early adopters* » optimisent leurs plateformes existantes en imaginant déjà les étapes suivantes : l'industrialisation et la gouvernance optimisée.

Chaque étape soulève des enjeux spécifiques. Les choix technologiques demeurent délicats, complexifiés par l'effervescence du secteur (Kubernetes évolue tous les quatre mois environ) et la multiplicité d'acteurs proposant solutions et services associés : la Cloud

Native Computing Foundation, qui pilote l'écosystème Kubernetes, maintient un référentiel de plus de 900 solutions, en croissance de 10 % chaque année ! Cette complexité technique défie particulièrement les équipes DSI traditionnelles, habituées à des cycles de renouvellement plus longs.

Débuter aujourd'hui : profiter d'un marché déjà mature

Si les primo adoptants ont « essuyé les plâtres » il y a près d'une décennie (qui se souvient de BlablaCar choisissant CoreOS Rocket plutôt que Docker, ou des batailles entre CoreOS Fleet, Nomad, CloudFoundry ou Docker Swarm face à Kubernetes ?), les nouveaux utilisateurs d'aujourd'hui bénéficient d'un écosystème mature et structuré.

Le paysage s'est stabilisé autour de Kubernetes comme standard, même si l'effervescence technologique perdure dans l'écosystème satellite. Cette maturation permet aux organisations de s'appuyer sur des principes d'architecture éprouvés et des retours d'expérience documentés, et de se concentrer sur l'adoption plutôt que l'expérimentation.

BON À SAVOIR

Conteneurs *vs* machines virtuelles ?

› Une VM constitue un ordinateur complet avec son propre système d'exploitation, ses pilotes et des ressources allouées sur une portion virtualisée du matériel sous-jacent (CPU, RAM, stockage). Chaque VM fonctionne de manière indépendante, impliquant une isolation quasi-totale.
Un conteneur crée une isolation logique de l'environnement d'exécution d'une application. Le noyau du système d'exploitation hôte reste commun, mais les processus, les fichiers et les ressources réseau de l'application sont isolés.

› Conséquence : légers et rapides à déployer, leur volatilité exige une stratégie de cyber-résilience adaptée. Leur isolation logique limitée nécessite quant à elle une stratégie de cybersécurité spécifique.

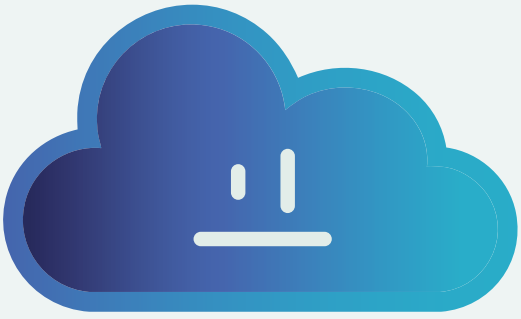
Comprendre les nouveaux périmètres de responsabilité

La conteneurisation transforme l'organisation DSI traditionnelle structurée autour des silos infrastructure, middleware et applicatif. Cette évolution redéfinit les périmètres de responsabilité historiques, et introduit une dimension *self-service* qui modifie fondamentalement les modalités de consommation IT.

Par exemple, l'administrateur de stockage traditionnel n'est plus l'unique point de passage de son domaine d'expertise puisque l'infrastructure sous-jacente (stockage SAN, NAS, etc.) est destinée à être directement « consommée » par l'utilisateur *via* une interface logicielle unifiée.

Dans cette configuration, les équipes historiques d'infrastructure et de stockage doivent adapter leurs méthodes de travail et élargir leurs compétences pour répondre aux nouveaux modèles de consommation, et ainsi ne plus penser seulement « service » mais « product as a service ». Bien que cette évolution représente un changement significatif dans leurs pratiques, **leur expertise technique fondamentale conserve toute sa valeur dans ce nouveau contexte** : « le cloud est juste le serveur de quelqu'un d'autre ! »

De leur côté, les équipes parties consommer du cloud public en indépendance ont acquis une approche déjà alignée sur ces nouveaux paradigmes. Leur familiarité avec les modèles API-first ou autre « Infrastructure as Code » facilite leur adaptation et leur adoption, car leur indépendance se fait au prix du maintien de leur niveau d'expertise dans un écosystème technologique particulièrement évolutif, et de modérer leur trajectoire, divergente des pratiques de l'entreprise…



There is no Cloud

It's just someone else's computer

Dans tous les cas, **la conteneurisation reste accessible à toutes les organisations**. Pour les équipes traditionnelles, le pas à franchir peut sembler important mais reste atteignable avec un accompagnement combinant acculturation, formation et réassurance sur la continuité de leur expertise.

La standardisation Kubernetes, l'écosystème d'outils étoffé et les approches graduelles facilitent cette adoption. L'enjeu principal : bien identifier les besoins métiers qui motivent cette transformation majeure. Sans oublier également les mécanismes de collaboration entre consommateurs et fournisseurs de la plateforme à mettre en place : consommation de la plateforme, détection des nouveaux besoins émergents, gouvernance de l'évolution de la plateforme pour la conserver en adéquation avec les attentes de ses utilisateurs, etc.

Quelles stratégies de mise en œuvre initiale adopter ?

La mise en œuvre d'une plateforme de conteneurs reste un projet IT comme un autre. À une échelle tactique, des projets pilotes sont menés pour démontrer rapidement la valeur ajoutée business ou technologique. Lors de cette phase exploratoire, les porteurs de projets ont toute latitude pour faire des choix technologiques rapides et peu concertés, sur des plateformes dédiées, limitant l'adhérence et les frictions liées aux processus de la DSI.

À l'échelle stratégique toutefois, la gouvernance doit se montrer particulièrement vigilante. Tout d'abord au risque de dispersion technologique, liée aux innombrables solutions existant dans l'écosystème des conteneurs. Ensuite, au risque de déplacement non maîtrisé du modèle organisationnel au moment du passage à l'échelle de l'entreprise.

L'expérience montre que certaines organisations se retrouvent rapidement avec plusieurs dizaines de clusters Kubernetes montés de façon empirique, poussés par les projets successifs. Cette croissance organique génère des problèmes majeurs contrariant l'industrialisation, pourtant nécessaire : rationalisation des coûts, harmonisation des licences ou encore optimisation des efforts d'administration.

Pour éviter cet écueil, il convient tout d'abord d'avoir conscience de ce risque « d'anarchie » et de difficile gouvernance future, et de définir dès l'origine une stratégie d'accostage pour les choix technologiques par défaut, contraints ou opportunistes : éditeur déjà présent dans l'organisation, prix cassés, etc. Concrètement, il s'agit d'anticiper :

- d'éventuelles évolutions technologiques à 2-3 ans (évolutions des besoins, nouveautés du marché, etc.), tout en conservant une trajectoire cohérente ;
- l'effort de convergence à produire à l'avenir, *via* une collaboration renforcée dans la co-construction de la plateforme (fonctionnalités natives et/ou catalogue de services), la mise en place d'initiatives organisationnelles transverses telles que le mode « chapter lead » comme Spotify, une dynamique d'open source interne, ou encore en veillant à la bonne mise en œuvre du rôle « d'enabler » de la *system team* dans une organisation SAFe.

POINT D'ATTENTION

Deux courbes d'apprentissage distinctes

La montée en compétences sur les technologies conteneurisées suit deux trajectoires parallèles aux enjeux différenciés.

Les consommateurs (équipes développement et métiers) doivent acquérir les principes de conception d'applications *cloud native* tels que décrits dans 12-factor app manifesto.

Les «platformers» (équipes infrastructure et plateforme) gèrent des enjeux plus complexes : mise à disposition d'une plateforme robuste, maintien en condition opérationnelle, gestion des montées de version et de la sécurité. Ils peuvent **accélérer leur adoption** *via* des **services managés, prestations spécialisées** ou **distributions d'éditeurs**, et ainsi bénéficier de leurs efforts de veille technologique et de leurs conseils en termes de choix architecturaux. Des stratégies de réassurance externe permettent de développer progressivement les compétences internes en parallèle.

Choix technologiques : entre pragmatisme et vision

Aucune solution technologique ne répond parfaitement à tous les besoins. Les choix sont guidés par l'existant, les compétences disponibles et les besoins identifiés.

L'arbitrage fondamental oppose stratégie full open source et accompagnement éditeur. La première économise le coût des licences mais nécessite à la fois de s'assurer de la pertinence et de la qualité des solutions open source retenues, et d'investir massivement en ressources humaines pour suivre le rythme d'évolution des technologies mises en œuvre sur la plateforme conteneurs. L'alternative s'appuie sur des éditeurs qui absorbent cet effort de veille technologique et d'intégration de composants multiples dans une solution cohérente et complète. Attention toutefois à bien se préserver du risque de « verrouillage client ».

Les critères de choix dépassent la dimension purement technique : contraintes économiques, considérations de politiques internes, affinités éditeur, niveau d'intégration… Cette réalité impose d'accepter les compromis tout en préservant une vision de long terme cohérente, apte à anticiper la phase suivante : l'industrialisation de la conteneurisation, ou plus exactement la véritable plateformisation.

BON À SAVOIR

Le stockage dans l'écosystème conteneurs : entre continuité et innovation

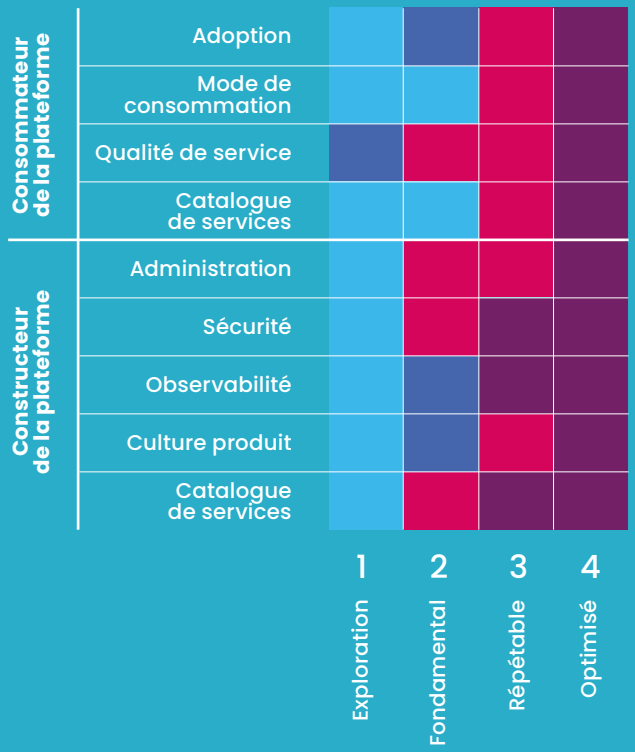
L'écosystème conteneurisé transforme l'approche du stockage sans pour autant évacuer ses exigences fondamentales. Des solutions comme Portworx créent une couche d'abstraction destinée à banaliser l'effort de consommation et de mise à disposition des solutions de stockage sous-jacentes : baies SAN, NAS, infrastructure hyperconvergée, mode block, mode file, mode objet, etc.

Cette approche permet aux utilisateurs de consommer des ressources de stockage avec provisioning automatique. Le stockage devient un service à la demande, que les équipes infrastructure auront à cœur de décliner selon différentes classes de stockage (qualité, performance, résilience, disponibilité et fonctionnalités en fonction des besoins utilisateurs), et représentant les différentes infrastructures sous-jacentes selon un catalogue unifié.

L'avis de l'expert

En phase d'audit et de cadrage, Stordata explore la transformation sur des axes complémentaires : technologique bien sûr, mais aussi organisationnel (périmètres de responsabilité, adhésion des utilisateurs… et des administrateurs), opérationnel (sécurité, conformité). Cette analyse permet d'évaluer le degré de transformation envisageable et les attentes court et long terme.

La maturité se mesure ensuite sur une matrice dédiée, déclinant les enjeux selon quatre niveaux : exploration initiale, premières applications en production, modèle opérationnel nominal, puis cible finale la platform-as-a-service. Cette cartographie, positionnant l'existant et les priorités du client, constitue le socle du plan d'action pour l'implémentation et l'accompagnement des équipes.



Industrialiser la conteneurisation : de la fédération à l'unification

Paradoxalement, en matière de conteneurs, la multiplicité des projets réussis engendre sa propre complexité : différentes distributions, canaux d'acquisition variés, modalités de support distinctes, etc. Si l'ensemble peut « vivre » un temps de manière fédérée, dans une logique de rationalisation, une approche d'unification de la plateforme est inévitable.

Homogénéiser les technologies et processus

L'industrialisation commence par la consolidation des choix éditeurs. Plutôt que de maintenir un écosystème disparate où coexistent OpenShift sur hôtes bare metal, Tanzu sur infrastructure VMware et services managés dans le cloud public, l'organisation doit converger vers un nombre restreint de solutions maîtrisées. Cette consolidation facilite la rationalisation des canaux d'achat, et évite la multiplication des contrats et des interlocuteurs commerciaux. En complément, la standardisation du support et du maintien en condition opérationnelle n'en est qu'optimisée.

À noter que l'enjeu dépasse la simple uniformisation technique : la plateforme doit désormais séduire non seulement les *early adopters*, mais aussi les populations *late adopters*, moins engagées dans ces nouvelles technologies. Pour convaincre ces utilisateurs, une expérience simplifiée et des processus d'accompagnement adaptés à leur niveau de familiarité constituent généralement les clés du succès.

Maîtriser la volatilité et la vélocité

L'environnement conteneurisé impose un rythme radicalement différent des habitudes construites depuis de nombreuses années. Monitorer des workloads éphémères (parfois de seulement quelques minutes) exige des approches distinctes de celles appliquées aux serveurs traditionnels. L'alerting doit s'adapter à cette volatilité, et se concentrer sur le monitoring du service rendu (avant la santé des ressources).

Autre défi majeur : la vélocité technologique. Les évolutions permanentes de Kubernetes imposent un suivi constant des mises à jour et de leurs impacts. Cette cadence soutenue nécessite des processus automatisés de test et de déploiement, ainsi qu'une veille technologique permanente pour anticiper les évolutions.

Standardiser et autonomiser

L'évolution naturelle mène de la Platform-as-a-Service à une offre Kubernetes-as-a-Service, où les utilisateurs commandent directement leur cluster dédié avec le niveau de service souhaité, en sélectionnant les services managés dans le catalogue DSI, ce qui a aussi pour effet d'augmenter le niveau d'autonomie offert et la valeur ajoutée globale de la plateforme.

BON À SAVOIR

Sauvegarde et PRA : des enjeux qui demeurent

En environnement conteneurisé, sauvegarde, continuité multi-sites et résilience, associées ou non à des PRA ou PCA, restent essentiels. Car si les équipes pilotes auront été sélectionnées pour leurs affinités DevOps et leur adhésion à ce modèle opérationnel, des utilisateurs moins favorables exigeront toujours que sauvegardes, reprise ou continuité d'activité de leur application soient garanties par la plateforme, sans relever de leur propre responsabilité.

Dans ce contexte, la volatilité des workloads exige des stratégies de cohérence des données repensées. Les mécanismes de réplication synchrone et asynchrone doivent s'adapter à cette dynamique accélérée sans compromettre l'intégrité des sauvegardes : la technologie de sauvegarde doit pouvoir travailler de concert avec Kubernetes pour savoir quelles données restaurer et associer à quel moteur de base de données créé ou supprimé à la demande (lors des campagnes de qualification fonctionnelle applicative, par exemple).

L'écosystème conteneurs facilite cette transition *via* des standards matures comme ClusterAPI et ses implémentations (k0rdent), permettant de générer à la volée des clusters pré-configurés selon différents *templates*. La DSI peut ainsi proposer du multi-cloud, multi-hébergeurs et des plateformes spécialisées par usage, tout en limitant l'effort de construction et de maintenance.

L'industrialisation ne consiste plus à automatiser une plateforme unique, mais à orchestrer des composants standardisés et réutilisables : conteneurs, services au catalogue, cluster Kubernetes dédié, et plus globalement standards Kubernetes utilisés sur la plateforme, etc.

Le self-service constitue dès lors le marqueur de la maturité : provisioning automatique, scaling à la demande, monitoring intégré. La DSI se repositionne alors sur l'innovation et l'optimisation continue de la plateforme, automatisant les tâches opérationnelles répétitives, et reprenant le leadership sur le rôle d'architecte et de facilitateur de la transformation digitale, grâce à son catalogue de services IT à la demande.

BON À SAVOIR

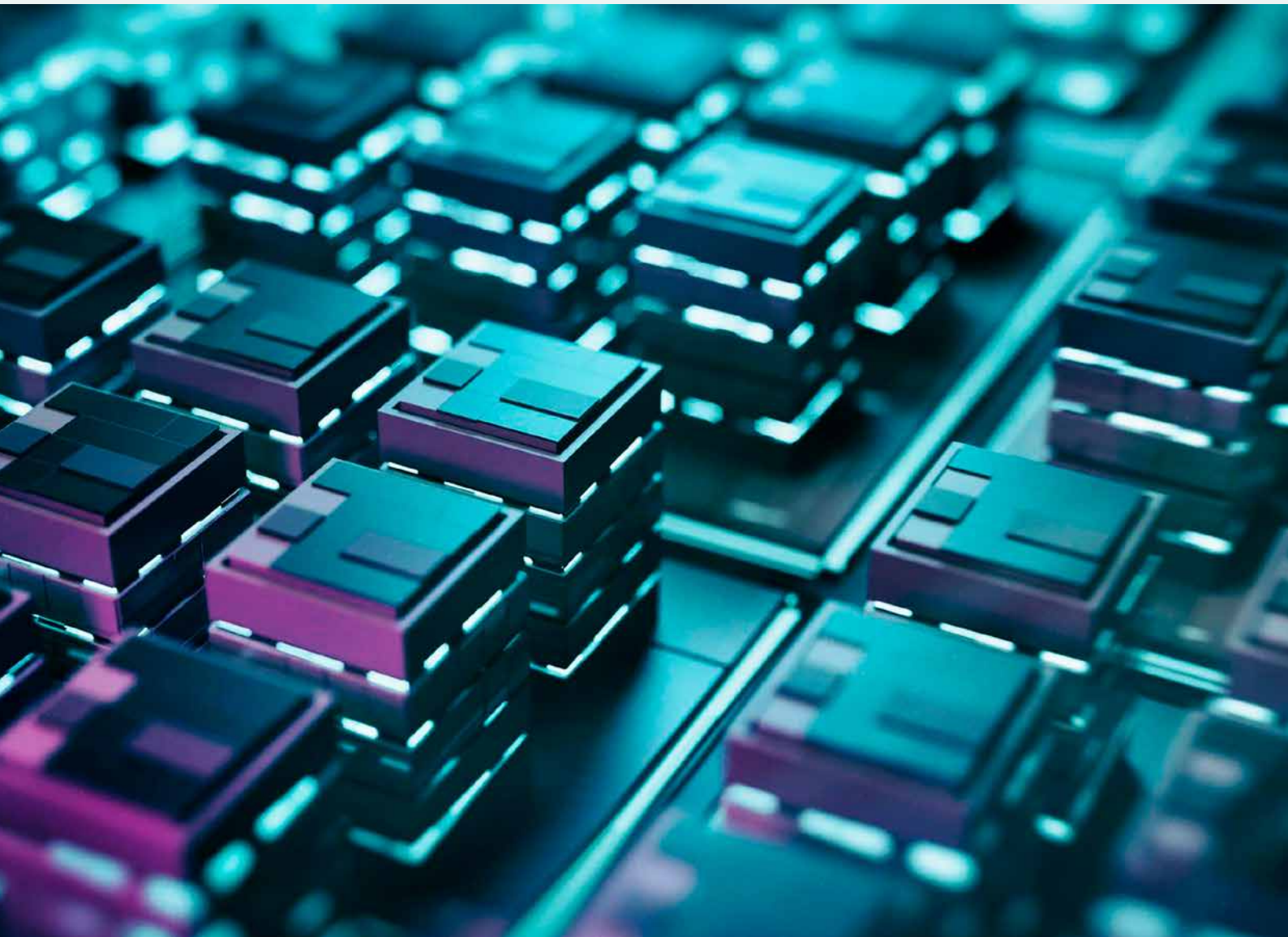
La sécurité des plateformes conteneurisées : la complexité d'une protection dynamique en temps réel

Avec des workloads conteneurisées volatiles, le modèle self-service et l'effet «boîte noire» sur les usages :

› la gestion des vulnérabilités devient critique avec les fréquentes montées de version ;

› l'outillage de sécurité doit être rapidement opérationnel et s'inscrire dans le temps réel ;

› les questions de traçabilité et d'audit se complexifient, et la politique de logs doit être adaptée à des preuves qui peuvent disparaître aussi vite qu'elles apparaissent.



Stordata

Siège - Versailles
28, rue Saint-Honoré
78000 Versailles
Tél. : +33 1 30 21 42 42

Agence Paris
24, rue Fabert
75007 Paris
Tél. : +33 1 44 18 30 01

Agence Sud-Est
11, Chemin des Anciennes Vignes
69410 Champagne-au-Mont-d'Or
Tél. : +33 4 78 48 09 47

Agence Sud-Ouest
6, rue Maurice Caunes
31200 Toulouse
Tél. : +33 5 34 50 49 00

Agence Méditerranée
Parc de Bellegarde
1 chemin de Borie
34170 Castelnau le Lez
Tél. : +33 5 34 50 49 00

Agence Ouest
34, quai Magellan
44000 Nantes
Tél : +33 2 28 08 09 93

Agence Est
9, rue Icare
67960 Entzheim
Tél. : +33 3 88 76 47 64

www.stordata.fr