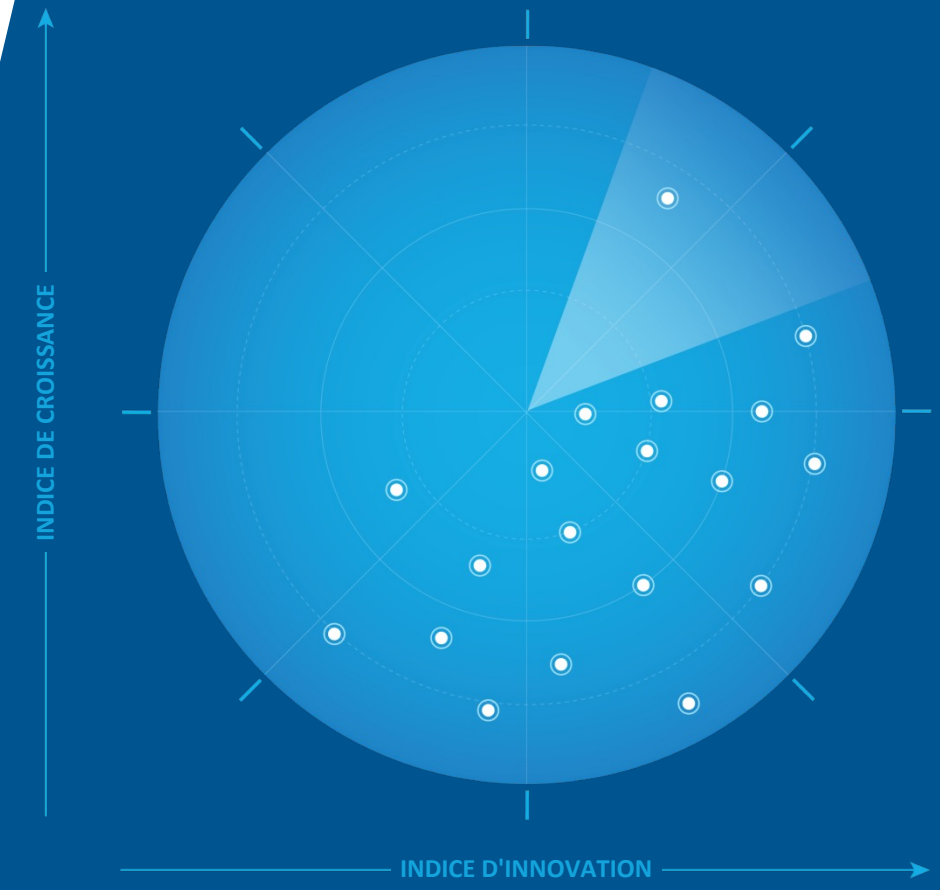
FROST & SULLIVAN

# Frost Radar™ : plateformes de protection des applications cloud native 2022

Système d'analyse comparative visant à inciter les entreprises à agir – L'innovation au service des nouvelles transactions et des pipelines de croissance




Auteur : Anh Tien Vu
Responsable secteur, cybersécurité internationale

**PD8C-74**
**Novembre 2022**

FROST & SULLIVAN

# Impératifs stratégiques et environnement de croissance

# Impératifs stratégiques

Avec toute une gamme de modèles et de services cloud disponibles, le cloud computing est en passe de devenir la norme dans l'environnement d'entreprise. La migration accélérée vers le cloud a permis aux entreprises d'amorcer leur transformation numérique, ainsi que de simplifier leur infrastructure et leurs opérations informatiques.

L'utilisation du cloud computing transforme le cycle de développement des applications, les opérations de sécurité, ainsi que la manière dont les entreprises conçoivent, exploitent et gèrent l'infrastructure back-end et les applications front-end destinées à leur clientèle, comme les conteneurs/Kubernetes, les solutions sans serveur, l'IaC (Infrastructure-as-Code, ou infrastructure sous forme de code) et autres plateformes d'intégration/de livraison continue (CI/CD), utiles pour la gestion, les applications, le développement et le déploiement cloud. Tandis que l'accent est mis sur les technologies de développement d'applications cloud native, les entreprises passent d'un modèle traditionnel de développement d'applications monolithiques à une architecture en microservices et à une approche conteneurisée avec davantage de dépendances et de bibliothèques open source.

Les technologies de conteneurs/Kubernetes et l'informatique sans serveur transforment les stratégies de développement des applications, dans le sens où elles permettent aux entreprises de concevoir, de développer, de tester et de lancer leurs applications de façon flexible, améliorant ainsi l'expérience client. L'enquête annuelle 2021 de la Cloud Native Computing Foundation (CNCF) a révélé que 96 % des entreprises utilisent ou envisagent d'utiliser Kubernetes, et que 93 % intègrent déjà ou prévoient d'intégrer des conteneurs dans leur processus de production. L'utilisation de logiciels, de bibliothèques/dépendances et de registres open source accroît toutefois les menaces et les préoccupations en matière de sécurité, dans la mesure où ces artefacts d'application restent exposés à la vulnérabilité des images de conteneur, aux failles de sécurité des hôtes, à l'injection de code (pour les applications sans serveur) et aux problèmes de conformité.

Source : Frost & Sullivan

# Impératifs stratégiques (suite)

La complexité croissante de l'environnement hybride et multicloud, ainsi que l'expansion de la surface d'attaque et la multiplication des défis liés aux opérations de sécurité requièrent une plateforme cloud native intégrée pour fournir aux entreprises la visibilité, le contrôle et la protection nécessaires pour sécuriser les architectures cloud modernes (notamment les machines virtuelles [VM], les conteneurs, Kubernetes et les solutions sans serveur), ainsi que pour intégrer la sécurité au cycle de développement logiciel, et les aider à gérer efficacement les questions de conformité. L'approche traditionnelle de la sécurité devient ainsi dépassée, dans la mesure où elle n'est pas conçue pour prendre en charge la micro-segmentation ni pour être suffisamment robuste face aux changements applicatifs, en particulier dans les environnements conteneurisés et sans serveur.

Face à ce constat, la CNCF a appelé à un changement de paradigme et à l'adoption d'un modèle de sécurité « Shift Left et Shield Right » pour protéger les applications cloud native en rapprochant la sécurité des workloads dynamiques identifiés sur la base d'attributs et de métadonnées telles que les balises et les étiquettes. Ce modèle exige d'intégrer la sécurité à un stade précoce et tout au long du cycle de développement des applications, plutôt que de se limiter aux étapes ultérieures, mais aussi de gérer la sécurité de l'environnement cloud dans lequel les applications sont déployées et exécutées, ce qui fait naître la nécessité de disposer d'une plateforme de protection des applications cloud native (CNAPP).

Contrairement aux solutions de sécurité cloisonnées telles que les solutions CSPM (gestion du niveau de sécurité du cloud), CWPP (plateforme de protection des workloads cloud) et de gestion des vulnérabilités, une plateforme CNAPP de sécurité intégrée permet aux entreprises de répondre aux menaces et aux défis de sécurité. Les solutions CNAPP renforcent en outre la collaboration entre les équipes en charge de la sécurité, des processus informatiques/plateformes et du développement, ce qui améliore la productivité et la gestion des risques auxquels les environnements cloud sont exposés.

Source : Frost & Sullivan

# Environnement de croissance

En 2021, le marché mondial des solutions CNAPP a enregistré un chiffre d'affaires de 1 720,6 millions de dollars, soit une croissance de 48,8 % par rapport à l'année précédente. Frost & Sullivan prévoit la poursuite de cette dynamique à un taux de croissance annuel composé de 25,7 % entre 2021 et 2026, avec un chiffre d'affaires qui devrait atteindre 5 406,8 millions de dollars en 2026. Ces estimations s'appuient sur la nécessité croissante de disposer d'une plateforme de sécurité cloud unifiée capable de renforcer la sécurité de l'infrastructure cloud et de protéger les applications et les données tout au long de leur cycle de vie.

Depuis un certain temps, les entreprises tendent à adopter des composants CNAPP de façon individuelle, avec en tête les solutions CSPM (pour assurer la visibilité et le contrôle de la sécurité du cloud) et CWPP (pour la protection à l'exécution et la conformité). Les investissements dans la sécurité DevOps ont récemment augmenté avec l'apparition du modèle Shift Left nécessaire à l'intégration de la sécurité dès les premiers stades du développement logiciel. De même, les solutions CIEM (gestion des droits sur l'infrastructure cloud) et de sécurité des réseaux cloud sont largement utilisées parmi les adopteurs précoces du cloud, qui exploitent les solutions cloud native de leurs fournisseurs de services cloud.

Ceci étant, les entreprises du monde entier consacrent d'importants moyens financiers aux différentes formes de solutions CNAPP, principalement dans le but d'acquérir des produits individuels destinés à répondre à des cas d'usage et à des défis spécifiques. À l'image de l'acronyme qui lui est associé, le concept de CNAPP, qui consiste à regrouper tous ces outils, reste nouveau et suscite par conséquent une certaine confusion chez ses utilisateurs potentiels, qui se montrent frileux à l'heure d'investir. Néanmoins, l'adoption accélérée des services cloud et des technologies de développement d'applications cloud native, ainsi que l'expansion de la surface d'attaque des environnements cloud devraient encourager les dépenses dans les technologies de sécurité du cloud, et en particulier dans les plateformes CNAPP.

Source : Frost & Sullivan

# Environnement de croissance (suite)

De nombreuses entreprises, en particulier celles qui sont parvenues à maturité, savent que le risque lié au cloisonnement des applications, au caractère open source et à l'incapacité de réagir rapidement face aux menaces qui pèsent sur l'infrastructure et les workloads peut créer des failles de sécurité et compliquer le travail des équipes. La nécessité d'identifier, de prioriser et de corriger les risques de façon centralisée va conduire à une augmentation de la demande de solutions CNAPP.

Disposer d'une plateforme qui allie sécurité renforcée, visibilité granulaire et gestion efficace des risques est indispensable pour gérer à la fois les risques de sécurité et de conformité. Cela s'explique par l'adoption croissante de la stratégie multicloud, le besoin permanent de protéger les workloads contre les attaques et les pressions en faveur d'une application cohérente des règles au sein des différents environnements, qu'il s'agisse d'infrastructures cloud, de conteneurs/Kubernetes, d'IaC ou de pipelines CI/CD.

La nécessité d'améliorer l'intégration des solutions CNAPP au cycle DevOps et aux plateformes CI/CD se fait de plus en plus ressentir, le but étant de favoriser la prise en compte de la sécurité dès la conception (sécurité Shift Left) et à chaque étape du flux de création des logiciels (développement, test et lancement). L'intégration des solutions CNAPP au modèle DevOps vise à répondre aux principales préoccupations liées à l'analyse des artefacts des applications (tests de sécurité statiques et dynamiques des applications [SAST/DAST], analyse des API (interfaces de programmation d'applications), SCA [analyse de la composition du logiciel] et gestion des vulnérabilités), aux risques du cloud associés à la configuration, à l'analyse des comportements d'exécution et aux exigences de conformité. Ce changement fait naître le besoin de disposer de solutions cloud native pour protéger les plateformes de même nature, notamment les conteneurs/Kubernetes, les hôtes, les dépendances applicatives, les applications/codes sans serveur, les outils CI/CD, mais également les autres plateformes d'orchestration.

Source : Frost & Sullivan

# Environnement de croissance (suite)

Si, en termes de consommation, les solutions CSPM et CWPP et la sécurité DevOps sont vouées à rester des éléments clés des plateformes CNAPP, les solutions CIEM et les services de sécurité des réseaux cloud connaîtront eux aussi un essor au cours des cinq prochaines années. Pour améliorer leur gestion et disposer d'une protection plus efficace, nombreuses sont les entreprises qui utilisent au moins deux composants d'un même fournisseur simultanément.

Cette consolidation des fonctionnalités de sécurité du cloud se poursuivra au cours des prochaines années. Par ailleurs, d'autres fournisseurs rejoindront l'univers des CNAPP, que ce soit par le biais de leurs propres technologies propriétaires ou d'acquisitions. Les entreprises qui disposent d'une offre solide de solutions CWPP, à l'image de Kaspersky, Fortinet et VMware, feront très probablement leur entrée sur le marché au travers d'une expansion technologique ou d'une acquisition. Néanmoins, l'essentiel des innovations et de la concurrence pourrait venir de start-ups proposant leurs propres solutions de sécurité cloud native orientées CSPM, CWPP et sécurité DevOps.

Études Frost & Sullivan en lien avec cette analyse indépendante :

- Global Cloud Workload Protection (CWP) Growth Opportunities
- Global Cloud-native Application Protection Platform Growth Opportunities, 2022

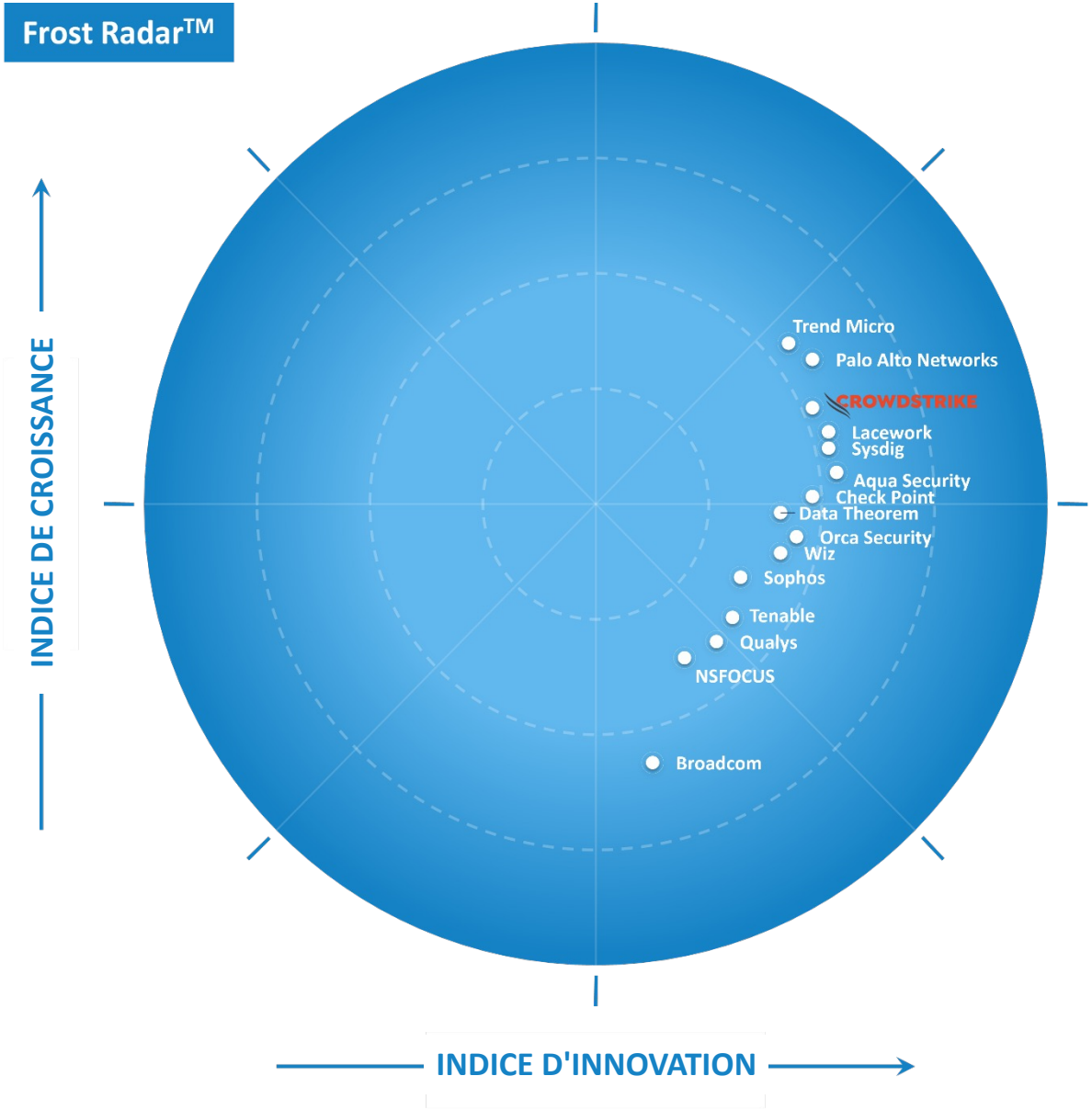
Source : Frost & Sullivan

FROST & SULLIVAN

# Frost Radar™

# Plateformes de protection des applications cloud native

# Frost Radar™ : Plateformes de protection des applications cloud native




Source : Frost & Sullivan

# Frost Radar™

## Environnement concurrentiel

Relativement jeune et fragmenté, le marché des solutions CNAPP regroupe les fournisseurs traditionnels de solutions de sécurité des endpoints et des réseaux, ainsi que d'évaluation des vulnérabilités, et les start-ups spécialisées dans la sécurité du cloud. À partir d'un groupe de plus de 20 participants issus du secteur et basés partout dans le monde, Frost & Sullivan a identifié dans son analyse Frost Radar™ les 15 meilleures entreprises. Les fournisseurs inclus dans le rapport remplissaient les critères suivants :

- Présence dans au moins deux régions (Amérique du Nord ; Europe, Moyen-Orient et Afrique [EMEA] ; Asie-Pacifique [APAC] ou Amérique latine) en 2021 et au cours du premier semestre 2022
- Chiffre d'affaires annuel d'au moins 20 millions de dollars en 2021 et part de marché d'au moins 1 %
- Plateforme CNAPP reconnue comme telle au plus tard en septembre 2022 (autrement dit, une plateforme qui comprend au moins des fonctionnalités CSPM et CWPP)

Cette étude Frost Radar™ met en vedette les entreprises suivantes : Aqua Security, Broadcom, Check Point Software Technologies, CrowdStrike, Data Theorem, Lacework, NSFOCUS, Orca Security, Palo Alto Networks, Qualys, Sophos, Sysdig, Tenable, Trend Micro et Wiz. Si d'autres entreprises explorent le marché des solutions CNAPP, ou l'ont récemment intégré, ces noms ont été retenus par Frost & Sullivan comme étant ceux qui le dominent et le façonnent.

À mesure que le marché évolue, davantage de grandes entreprises de cybersécurité et de start-ups spécialisées dans la sécurité du cloud y feront leur entrée. Frost & Sullivan prévoit d'ailleurs une intensification de la concurrence et une modification significative du paysage au cours des deux prochaines années, que ce soit sur le plan des stratégies de commercialisation ou de l'innovation technologique.

Source : Frost & Sullivan

# Frost Radar™

## Environnement concurrentiel (suite)

La capacité des fournisseurs à proposer une plateforme intégrée qui consolide et unifie les fonctionnalités de sécurité afin d'aider les entreprises à gérer leur niveau de sécurité, à détecter les risques et les menaces et à y répondre tout au long du cycle de développement des applications en environnement cloud native est un facteur clé du processus décisionnel des clients, au même titre qu'une assistance de qualité, le coût et la flexibilité et la transparence du modèle de tarification.

Les clients sont à la recherche d'un ensemble plus large de fonctionnalités qui leur offre visibilité et sécurité depuis la conception jusqu'à la production, en passant par les étapes DevOps, DevSecOps et l'infrastructure cloud. Ils veulent des solutions CNAPP qui couvrent l'ensemble de leur architecture (code, applications, workloads et infrastructures). En réalité, ces solutions peuvent les aider à mettre en place une stratégie de sécurité globale et à parvenir à une approche Zero Trust de la sécurité dans leurs différents environnements cloud.

De plus en plus, les entreprises exploitent les capacités de l'intelligence artificielle/du Machine Learning (IA/ML) pour améliorer leur gestion des risques dans l'environnement cloud. Par conséquent, les solutions CNAPP devront s'inscrire dans un modèle Shift Left dès les premières étapes de la conception et du développement du code, et s'appuyer sur l'intelligence artificielle et le Machine Learning pour fournir des renseignements plus pertinents sur le comportement des workloads/applications et sur la manière dont ils interagissent au sein de l'infrastructure cloud afin de renforcer les fonctionnalités de détection et de réponse automatisées aux menaces.

La demande d'une intégration plus poussée avec la protection des applications web s'intensifie en raison de la nécessité de faire converger cette protection avec celle des workloads cloud sous-jacents qui les alimentent.

Source : Frost & Sullivan

# Frost Radar™

## Environnement concurrentiel (suite)

Bien que les plateformes CNAPP soient disponibles sous forme de solutions autohébergées gérées par le biais d'un partenariat avec un fournisseur de services de sécurité managés ou en tant que SaaS (Software-as-a-Service), les clients ont tendance à opter pour un modèle cloud, qui leur permet de réduire leurs frais généraux, de réaffecter leurs ressources à d'autres tâches et de gagner en fiabilité. C'est particulièrement vrai pour les petites et moyennes entreprises. Du fait des exigences en matière de confidentialité et de conformité, le modèle autohébergé reste en revanche pertinent pour les grandes entreprises et celles qui appartiennent à des secteurs très réglementés.

CrowdStrike a été choisi par Frost & Sullivan dans son Indice de croissance en raison de sa croissance forte et constante au cours des trois dernières années, malgré le fait qu'il ne se classe que septième en termes de part de marché. Frost & Sullivan salue sa solide base de clients et sa perception supérieure de la marque, ainsi que l'importance que CrowdStrike accorde à la sécurité du cloud, qui lui permettra certainement de maintenir une forte dynamique de croissance autour de sa solution CNAPP durant les deux à trois prochaines années.

Source : Frost & Sullivan

FROST & SULLIVAN

# Entreprises à suivre :

## Entreprises à considérer en priorité en vue d'un investissement, d'un partenariat ou d'une évaluation comparative

# CrowdStrike

## INNOVATION

- *L'offre CNAPP de CrowdStrike comprend Falcon Cloud Workload Protection avec agent, Falcon Horizon* ***(CSPM) sans agent, une solution CIEM*** et une fonction de sécurité des conteneurs prolongée par un modèle de sécurité Shift Left dans le cadre de la plateforme globale CrowdStrike Falcon.
- La plateforme utilise des technologies d'analyse comportementale pour détecter les menaces sans logiciels malveillants et les attaques sans fichiers afin d'aider les entreprises à identifier et à prévenir les erreurs de configuration du cloud, à garantir la conformité, mais aussi à gérer et à protéger les hôtes, les machines virtuelles, les applications et les conteneurs/Kubernetes grâce à l'identification précoce des vulnérabilités, à la détection et à la réponse aux menaces, à la protection à l'exécution et au respect des exigences de conformité. Bien qu'elles soient proposées sous la forme de deux modules distincts, ces fonctionnalités peuvent être fournies par CrowdStrike Falcon moyennant une optimisation reposant sur une base de données propriétaire regroupant Threat Graph, Asset Graph et Intel Graph et compilée à partir des endpoints, des workloads cloud, des conteneurs et d'autres sources de télémétrie.

## CROISSANCE

- CrowdStrike est l'un des fournisseurs de sécurité cloud qui connaît la plus forte croissance, principalement grâce à ses solutions XDR/EDR et MDR. Son intérêt marqué pour le marché de la sécurité cloud a permis à sa solution CNAPP de gagner en popularité au niveau mondial.
- D'après les estimations de Frost & Sullivan, le chiffre d'affaires dégagé par CrowdStrike pour sa solution CNAPP a enregistré une croissance annuelle de 71,7 % en 2021, lui permettant de devenir l'un des principaux fournisseurs du marché avec une part de 5 %.
- Bien que la majorité de ses activités se déroulent en Amérique du Nord, l'entreprise a connu une croissance de 92,6 % et de 82,3 % dans les régions EMEA et APAC, respectivement.
- CrowdStrike, qui est l'un des fournisseurs les plus dynamiques de solutions cloud native de sécurité des endpoints, et qui dispose d'un solide écosystème de partenaires de distribution, peut proposer ses modules de sécurité du cloud aux grandes entreprises de plusieurs secteurs verticaux sous la forme d'extensions ou solutions additionnelles, ce qui l'aidera à maintenir une forte dynamique de croissance.

## ANALYSE DE FROST

- CrowdStrike a gagné en popularité grâce à son offre CNAPP, qui a connu une croissance rapide au niveau mondial au cours des deux dernières années.
- Frost & Sullivan reconnaît la dynamique de croissance de CrowdStrike, qui repose sur son pipeline durable, sa solide base de clients acquis grâce à son offre XDR/EDR, et son écosystème robuste de partenaires de distribution, qui contribueront à faire progresser ses activités autour de sa solution CNAPP.
- Sa capacité à fournir des services MDR et de Threat Hunting spécialisés cloud, en particulier, est considérée comme un argument de vente qui le distingue de ses concurrents, étant donné qu'elle peut contribuer à renforcer la confiance des clients et à améliorer l'expérience d'utilisation des solutions.
- En outre, CrowdStrike devrait étendre son offre CNAPP en y ajoutant des fonctionnalités d'analyse des vulnérabilités du code afin de rendre sa plateforme plus complète.

Source : Frost & Sullivan

FROST & SULLIVAN

# Réflexions stratégiques

# Réflexions stratégiques

1

Bien qu'encore tout jeune, le marché des solutions CNAPP est de plus en plus concurrentiel, avec de nouveaux fournisseurs qui y feront leur entrée au cours des deux ou trois prochaines années. Les fournisseurs existants seront dès lors soumis à une pression énorme pour maintenir leurs avantages concurrentiels en matière d'innovations technologiques et de modèles de tarification. La forte concurrence exigera des acteurs du marché qu'ils déploient davantage d'efforts en matière de recherche et développement ainsi que de fusions et acquisitions pour renforcer les capacités de leurs plateformes s'ils veulent s'imposer et trouver des solutions pour réduire le coût total de possession, tout en offrant une assistance supérieure et une expérience de meilleure qualité à leurs clients.

2

L'éducation du marché est essentielle au succès des solutions CNAPP en devenir. Les fournisseurs doivent impérativement travailler en étroite collaboration avec les parties prenantes de leur secteur pour renforcer la sensibilisation des entreprises mondiales à la sécurité du cloud et à l'importance du concept de CNAPP dans le cadre de leur migration vers le cloud.

La croissance des fournisseurs repose en grande partie sur leurs programmes de partenariats de distribution. Il est donc essentiel qu'ils disposent des partenaires adéquats, capables d'éduquer le marché, de promouvoir leurs solutions, de s'impliquer auprès des clients et de fournir une assistance locale pour gagner la confiance et l'adhésion des clients.

3

Le choix et l'achat d'une solution CNAPP ne sont pas des décisions qu'un RSSI peut prendre seul. Une telle solution exige une collaboration plus étroite à tous les niveaux, dans la mesure où elle implique diverses équipes en charge du développement, de la sécurité et des opérations, qui ont chacune leurs propres stratégies, préférences et indicateurs clés de performance. La décision doit reposer sur la contribution des directeurs des systèmes d'information, des développeurs principaux et des chefs d'entreprise, dans la mesure où ils sont tous animés par un objectif commun.

Source : Frost & Sullivan

FROST & SULLIVAN

# Étapes suivantes : utiliser le rapport Frost Radar™ pour autonomiser les principales parties prenantes

# Importance de figurer dans le rapport Frost Radar™

Les entreprises qui figurent au Frost Radar™ sont les leaders de leur secteur en ce qui concerne la croissance ou l'innovation, voire les deux, et contribuent à l'évolution de leur secteur.

**POTENTIEL DE CROISSANCE**

Votre entreprise affiche un potentiel considérable de croissance, ce qui fait d'elle une entreprise à suivre.

**BONNES PRATIQUES**

Votre entreprise est bien placée pour orienter les bonnes pratiques Growth Pipeline™ de votre secteur.

**INTENSITÉ**

Votre entreprise est l'un des principaux contributeurs à la concurrence de l'environnement de croissance.

**VALEUR POUR LES CLIENTS**

Votre entreprise a démontré sa capacité à améliorer de manière significative sa proposition de valeur pour les clients.

**POTENTIEL DE PARTENARIAT**

Votre entreprise est perçue par les clients, les investisseurs, les partenaires de la chaîne de valeur et les futurs talents comme un fournisseur de grande valeur.

Source : Frost & Sullivan

# Frost Radar™ : un outil précieux pour l'équipe dirigeante chargée de la croissance

## IMPÉRATIFS STRATÉGIQUES

- Croissance de plus en plus difficile à atteindre
- Niveau de concurrence élevé
- Nécessité de renforcer la collaboration, le travail d'équipe et la mobilisation
- Complexité de l'environnement de croissance

## FINALITÉ DU FROST RADAR™

- Promouvoir un environnement de collaboration propice à l'application des bonnes pratiques au sein de l'ensemble de l'équipe dirigeante grâce aux outils à disposition
- Évaluer le potentiel d'évolution grâce à la plateforme de mesure à disposition
- Soutenir le PDG en s'appuyant sur la puissance de l'outil Growth Pipeline™

## ÉTAPES À SUIVRE

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline Dialog™ avec l'équipe Frost**

Source : Frost & Sullivan

# Frost Radar™ : un outil précieux pour les investisseurs

## IMPÉRATIFS STRATÉGIQUES

- Faible flux de transactions et forte concurrence
- Devoir de diligence entravé par la complexité du secteur
- Gestion inefficace du portefeuille

## FINALITÉ DU FROST RADAR™

- Se concentrer sur le potentiel de croissance en créant un puissant pipeline d'entreprises à suivre en vue de réaliser des investissements prometteurs
- Effectuer des vérifications préalables pour améliorer la précision et accélérer le processus de transaction
- Atteindre le taux de rendement interne maximal et assurer le succès à long terme des actionnaires
- Comparer régulièrement les performances aux bonnes pratiques au profit d'une gestion optimale du portefeuille

## ÉTAPES À SUIVRE

- **Growth Pipeline Dialog™**
- **Atelier sur les diverses opportunités**
- **Growth Pipeline Audit™ à titre de devoir de diligence obligatoire**

Source : Frost & Sullivan

# Frost Radar™ : un outil précieux pour les clients

## IMPÉRATIFS STRATÉGIQUES

- Complexité croissante des solutions, pouvant avoir des répercussions à long terme
- Confusion engendrée par les solutions proposées par les fournisseurs
- Confusion accentuée par la volatilité des fournisseurs

## FINALITÉ DU FROST RADAR™

- Évaluer les fournisseurs potentiels et identifier les partenaires qui fourniront des solutions performantes à long terme grâce au cadre analytique à disposition
- Évaluer les solutions les plus innovantes et comprendre comment les différentes solutions peuvent répondre à leurs besoins
- Bénéficier d'une perspective à long terme concernant les partenariats avec les fournisseurs

## ÉTAPES À SUIVRE

- **Growth Pipeline Dialog™**
- **Growth Pipeline Diagnostic™**
- **Système d'analyse comparative Frost Radar™**

Source : Frost & Sullivan

# Frost Radar™ : un outil précieux pour les conseils d'administration

| IMPÉRATIFS STRATÉGIQUES | FINALITÉ DU FROST RADAR™ | ÉTAPES À SUIVRE |
|---|---|---|
| • Croissance de plus en plus difficile à atteindre ; PDG en quête de conseils<br>• Nécessité de disposer de compétences spécifiques pour appréhender l'environnement de croissance<br>• Évolution de la chaîne de valeur du client | • Superviser le succès à long terme de l'entreprise grâce à un système de mesure unique<br>• Protéger les investissements des actionnaires grâce à une plateforme de discussion qui se concentre sur les problématiques de base, les critères de référence et les bonnes pratiques<br>• Garantir la qualité de l'encadrement, du soutien et de la gouvernance des PDG afin de maximiser le potentiel de croissance | • **Growth Pipeline Audit™**<br>• **Growth Pipeline as a Service™** |

Source : Frost & Sullivan

FROST & SULLIVAN

# Analyses Frost Radar™

# Frost Radar™ : analyse comparative du potentiel de croissance

## 2 indices principaux, 10 composantes analytiques, 1 plateforme

**AXE VERTICAL**

L'**indice de croissance (IC)** mesure la performance et les antécédents d'une entreprise en matière de croissance, ainsi que sa capacité à élaborer et à mettre en œuvre une stratégie et une vision de croissance parfaitement alignées, un système de pipeline de croissance solide, ainsi que des stratégies de vente et de marketing efficaces axées sur le marché, la concurrence et les utilisateurs finaux.

## COMPOSANTES DE L'INDICE DE CROISSANCE

- **IC1 : PART DE MARCHÉ (SUR LES 3 DERNIÈRES ANNÉES)**
  Comparaison de la part de marché d'une entreprise par rapport à celle de ses concurrents dans un espace de marché donné et pour les 3 dernières années.
- **IC2 : CROISSANCE DES REVENUS (SUR LES 3 DERNIÈRES ANNÉES)**
  Observation du taux de croissance des revenus d'une entreprise sur les 3 dernières années au sein du marché, du secteur ou de la catégorie étudié(e) dans le cadre du rapport Frost Radar™ en question.
- **IC3 : PIPELINE DE CROISSANCE**
  Évaluation de l'efficacité et de l'effet de levier du système de pipeline de croissance d'une entreprise, en vue de capturer, d'analyser et de prioriser en continu ses opportunités de croissance.
- **IC4 : VISION ET STRATÉGIE**
  Évaluation de l'alignement de la stratégie de croissance d'une entreprise sur sa vision. Les investissements dans de nouveaux produits et marchés sont-ils cohérents avec la vision revendiquée ?
- **IC5 : VENTES ET MARKETING**
- Mesure de l'efficacité des efforts de vente et de marketing mis en place par une entreprise afin de stimuler la demande et d'atteindre ses objectifs de croissance.

# Frost Radar™ : analyse comparative du potentiel de croissance

## 2 indices principaux, 10 composantes analytiques, 1 plateforme

**AXE HORIZONTAL**

L'**indice d'innovation (II)** mesure la capacité d'une entreprise à développer des produits/services/solutions (tout en disposant d'une compréhension claire des mégatendances déstabilisatrices), qui sont à la fois exploitables à l'échelle mondiale, susceptibles d'évoluer et d'être étendus à de multiples marchés et alignés sur les besoins changeants des clients.

## COMPOSANTES DE L'INDICE D'INNOVATION

- **II1 : ÉVOLUTION DE L'INNOVATION**
  Détermine si les innovations d'une entreprise peuvent évoluer et être exploitées à l'échelle mondiale, aussi bien sur les marchés en développement que sur les marchés matures, mais aussi dans les secteurs verticaux, qu'ils soient adjacents ou non.
- **II2 : RECHERCHE ET DÉVELOPPEMENT**
  Mesure l'efficacité de la stratégie de recherche et développement d'une entreprise, telle que déterminée par l'importance de ses investissements R&D et leur impact sur le pipeline d'innovation.
- **II3 : PORTEFEUILLE DE PRODUITS**
  Analyse le portefeuille de produits d'une entreprise en se concentrant sur la contribution relative des nouveaux produits à ses revenus annuels.
- **II4 : INFLUENCE DES MÉGATENDANCES**
  Évalue la capacité d'une entreprise à tirer proactivement parti des opportunités à long terme en constante évolution et des nouveaux modèles commerciaux, en tant que fondement de son pipeline d'innovation. Pour en savoir plus sur les mégatendances, cliquez ici.
- **II5 : ALIGNEMENT SUR LES BESOINS DES CLIENTS**
  Évalue l'applicabilité des produits/services/solutions d'une entreprise aux clients actuels et potentiels, ainsi que l'influence de l'évolution des besoins des clients sur sa stratégie d'innovation.

# Annexe

# Liste des abréviations

CNAPP : Cloud-native Application Protection Platform (plateforme de protection des applications cloud native)
DAST : Dynamic Application Security Testing (test dynamique de sécurité des applications)
IAST : Interactive Application Security Testing (test interactif de sécurité des applications)
SAST : Static Application Security Testing (test statique de sécurité des applications)
CSPM : Cloud Security Posture Management (gestion du niveau de sécurité du cloud)
CWPP : Cloud Workload Protection Platform (plateforme de protection des workloads cloud)
IaC : Infrastructure as Code (infrastructure sous forme de code)
CIEM : Cloud Infrastructure Entitlement Management (gestion des droits sur l'infrastructure cloud)
CI/CD : Continuous Integration / Continuous Delivery (intégration continue / distribution continue)
API : Application Program Interface (interface de programmation d'application)
SCA : Software Composition Analysis (analyse de la composition du logiciel)
SBOM : Software Bill of Materials (nomenclature des logiciels)
CNWS : Cloud Networks Security (sécurité des réseaux cloud)
WAAP : Web Application and API Protection (protection des API et applications web)

Source : Frost & Sullivan

# Avis de non-responsabilité

Frost & Sullivan ne peut être tenu responsable des informations incorrectes fournies par les entreprises ou les utilisateurs. Les informations quantitatives relatives au marché ont essentiellement été collectées lors d'entretiens et sont par conséquent sujettes à des variations. Les services de recherche de Frost & Sullivan prennent la forme de publications limitées contenant de précieuses informations sur le marché, qui sont fournies à un groupe sélectionné de clients. Lorsqu'ils commandent ou téléchargent ces publications, les clients reconnaissent qu'elles sont destinées à un usage interne et non à une publication générale ni à une divulgation à des tiers. Ces publications ne peuvent en aucun cas être données, prêtées, revendues ou divulguées à des personnes autres que des clients sans autorisation écrite. En outre, aucune partie ne peut être reproduite, stockée dans un système de recherche ni transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, par photocopie, enregistrement ou autre) sans l'autorisation de l'éditeur.

Pour toute question concernant cette autorisation, veuillez envoyer un e-mail à l'adresse suivante : permission@frost.com