

*Optimisez la Sécurité de vos environnements multi-cloud et hybrides
avec Microsoft Defender for Cloud*



Réda Benhameurlaine
Partner Sales Solution



Thibault Saint-Jean
Partner Sales Solution

Defender for Cloud

Security from code to cloud

- **Introduction**

- *Le contexte dans lequel évoluent les entreprises françaises*

- **Présentation de la CNAPP et de notre stratégie**

- *Présentation de la solution*
 - *Principaux facteurs de différenciation*
 - *Modèle de pricing de la solution*

- **Pour aller plus loin**

- *Quelques chiffres et arguments clés*
 - *Ressources pour approfondir le sujet*





Introduction

Contexte dans lequel évoluent les entreprises françaises

95%
des nouvelles
initiatives seront
cloud-native d'ici
2025¹



Technologies
cloud natives

89%
des organisations
adoptent le
multi-cloud²



Multicloud

500+
Nouvelles
applications
développées
dans une
entreprise en
moyenne³



Accélération du
rythme de
développement

**Le cloud
apporte
évolutivité et
agilité mais...**

**Il s'agit d'une
cible croissante
en matière de
cybersécurité**

**Augmentation
des attaques
dans le cloud**



82%

Des violations
concernaient des
données stockées
dans le cloud⁴



**Silos de
sécurité**

54%

Des organisations
n'incluent pas la
sécurité dans la
phase de
développement⁵



**4,88
millions**
Coût moyen d'une
violation de données⁶

1. Selon Gartner, quatre tendances façonnent l'avenir du cloud public – Gartner, août 2021

2. Rapport Flexera 2024 sur l'état du cloud

3. Rapport sur l'état de la nation des développeurs

4. Rapport DevOps d'entreprise Microsoft

5. Recherche sur les priorités et les pratiques de sécurité du cloud Microsoft

6. Rapport sur le coût d'une violation de données, 2024 - IBM



Que se passe-t-il dans vos environnements cloud ?

Où sont mes ressources ?

Où se trouvent mes données ?

Ces ressources devraient-elles être exposées à Internet ?

Qui peut accéder à mes données ?

Mes applications Gen AI exposent-elles des données sensibles ?

Mon code a-t-il des informations d'identification exposées ?

Où se trouvent les vulnérabilités critiques dans le contexte du risque commercial et de l'exploitabilité ?

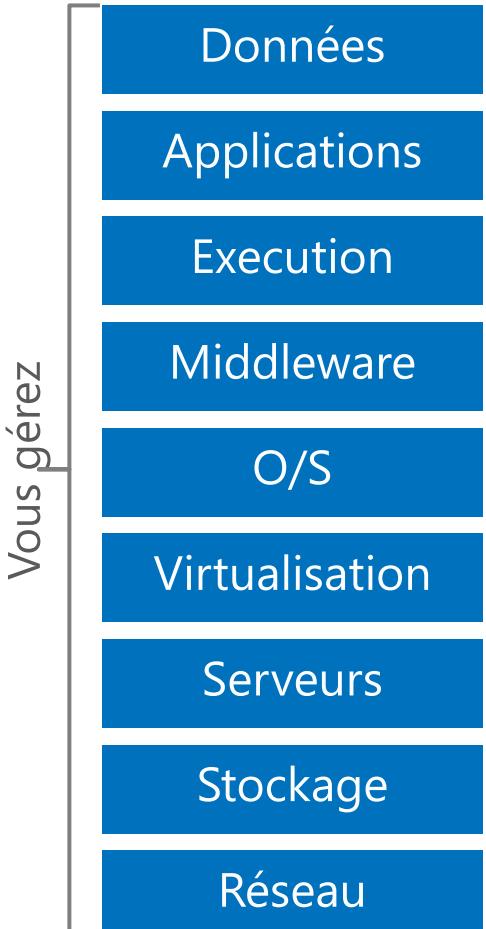
Y a-t-il des menaces **actives** dans mon environnement cloud ?

Comment puis-je réagir rapidement ?

Le client final est toujours responsable de ces sujets !

Les services Cloud

Sur site



Serveur Windows

Machines virtuelles Windows Azure
Windows Server Hyper-V

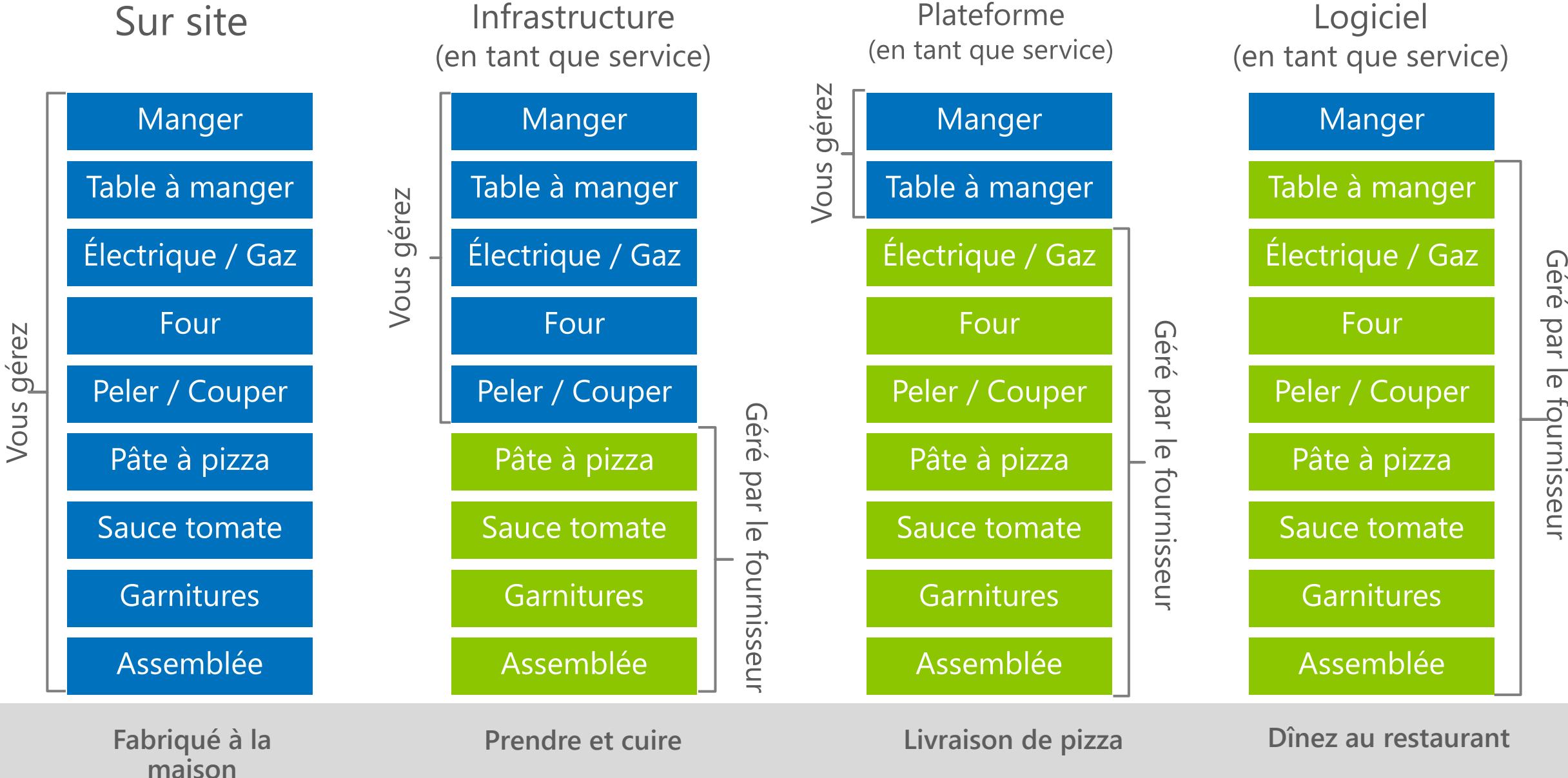
Windows Azure Cloud Services

Bureau 365
Dynamics CRM

Vous gérez

Microsoft gère

Pizza en tant que service





La plateforme CNAPP de Microsoft

Defender for Cloud

Lexique DevSecOps

Acronyme	Description	Typologie
DevSecOps	Approche intégrant la sécurité dès la conception et tout au long du cycle de développement logiciel et des opérations. Favorise l'automatisation, la collaboration et la réduction proactive des risques.	Culture/Méthodologie
Pipeline CI/CD	Processus d'intégration continue et de déploiement continu, automatisant tests, intégration et déploiement du code pour une mise en production rapide et fiable.	Méthodologie de développement
CNAPP	Cloud-Native Application Protection Platform. Plateforme intégrée protégeant les applications cloud dès leur conception, en combinant sécurité et surveillance.	Solution de cybersécurité
CSPM	Cloud Security Posture Management. Outil pour vérifier et corriger la configuration des environnements cloud afin de respecter les meilleures pratiques de sécurité.	Solution de cybersécurité
CIEM	Cloud Infrastructure Entitlement Management. Gère et surveille les accès, rôles et autorisations dans le cloud pour que chaque identité dispose uniquement des priviléges nécessaires. Attention : Ne confondez pas avec SIEM (Security Information and Event Management).	Solution de cybersécurité
CWP	Cloud Workload Protection. Sécurise les charges de travail (machines virtuelles, conteneurs, fonctions serverless) dans le cloud en surveillant leur configuration et leur comportement.	Solution de cybersécurité
CDR	Cloud Detection and Response. Permet de détecter en quasi temps réel des activités suspectes dans le cloud et d'y répondre rapidement pour contenir et neutraliser les incidents.	Solution de cybersécurité

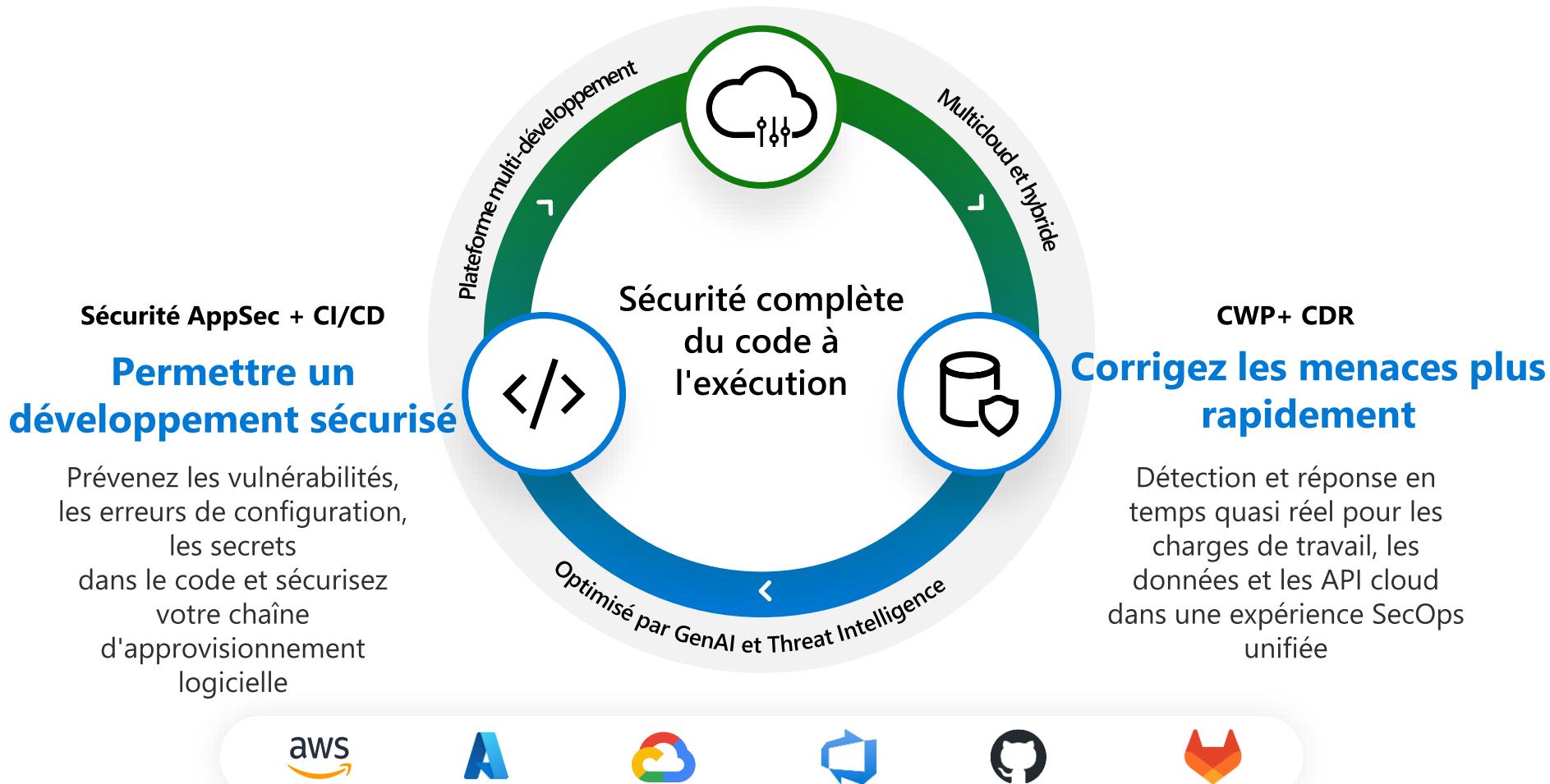
Sécurité multicouche Code to Cloud

Vue d'ensemble Defender for Cloud

CSPM + CIEM

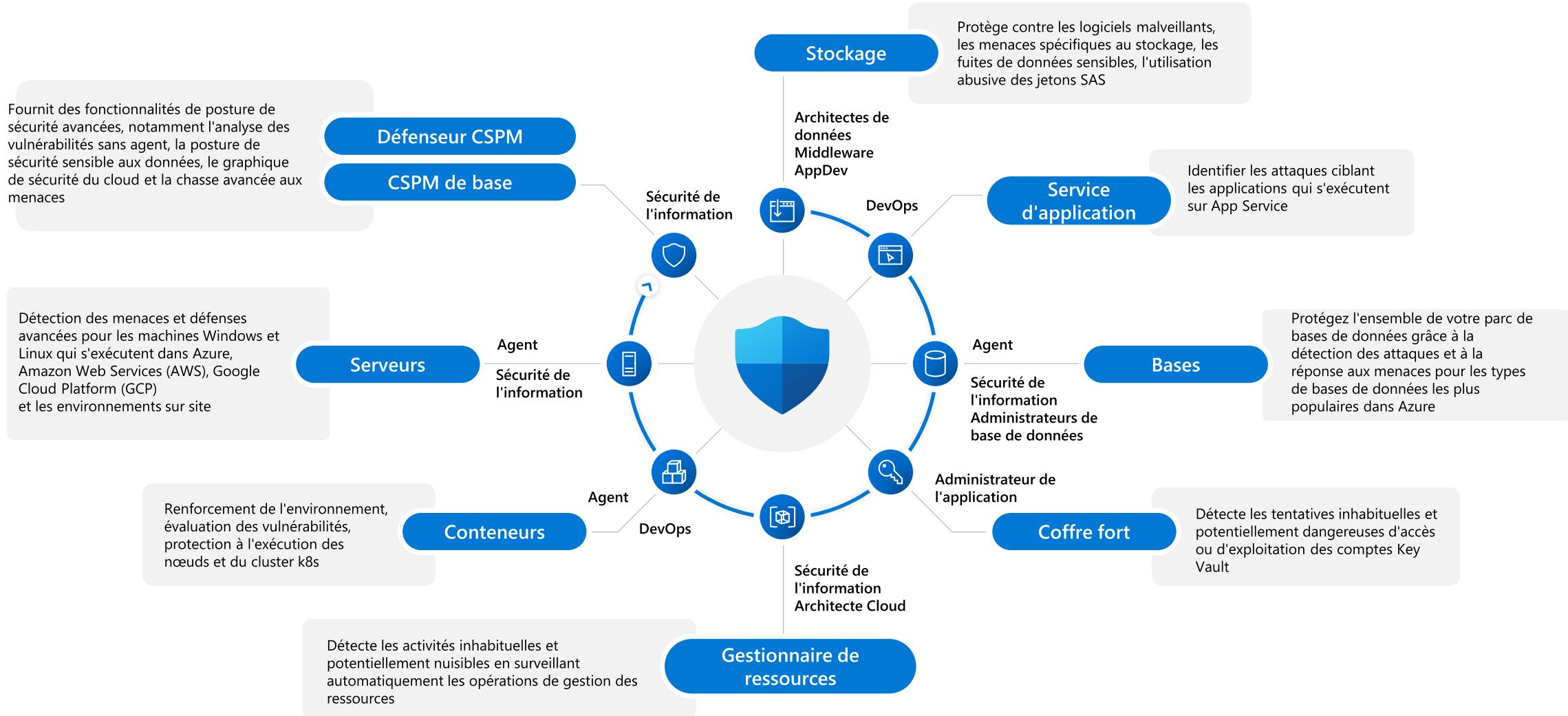
Réduire continuellement les risques

Gestion contextuelle et hiérarchisée de la posture de sécurité tout au long du cycle de vie des applications cloud



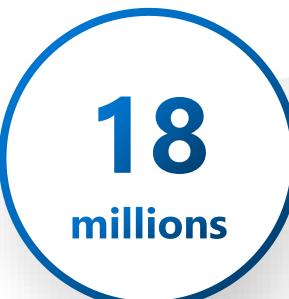
Sécurité multicouche Code to Cloud

Vue d'ensemble Defender for Cloud



En quoi nous sommes différents

Les développeurs utilisent GitHub et Azure DevOps



Résolution et prévention plus rapides des problèmes de sécurité dans le code pour les développeurs



Sécurité complète du code à l'exécution optimisée par Copilot



Les informations de sécurité les plus complètes éclairent notre hiérarchisation des risques



La protection la plus poussée contre les menaces pour les magasins de données et les charges de travail d'IA



Signaux synthétisés par jour



Experts en sécurité et en threat intelligence

Microsoft a plus d'informations que quiconque sur le développement d'applications

Microsoft a plus d'informations sur les comportements des attaquants que quiconque

Leadership dans trois rapports d'analystes

Rapports d'analystes et examens par les pairs

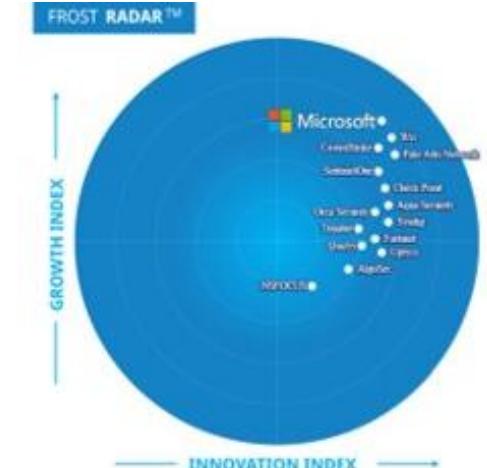
FORRESTER®

THE FORRESTER WAVE™
Infrastructure-As-A-Service Platform Native Security
Q2 2023



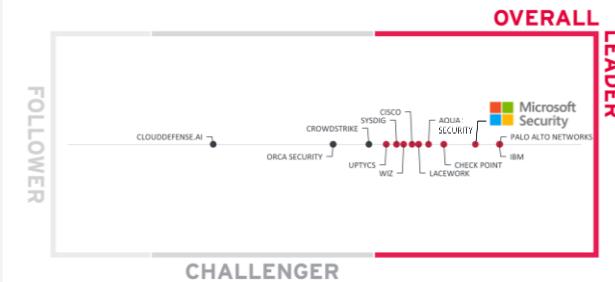
Microsoft est nommé leader dans le rapport The Forrester Wave™ : Infrastructure-As-A-Service Platform Native Security (IPNS)¹

FROST & SULLIVAN



Microsoft est nommé leader dans le rapport Frost Radar™ : Cloud Native Application Protection Platforms (CNAPP)²

KUPPINGERCOLE ANALYSTS



Microsoft est nommé leader dans le rapport KuppingerCole Leadership Compass for Cloud-Native Application Protection Platforms (CNAPP)³

¹ Forrester, Forrester Wave, Total Economic Impact et Forrester New Wave sont des marques commerciales de Forrester Research, Inc. The Forrester Wave™ : [Infrastructure-as-a-Service Platform Native Security, 2e trimestre 2023, Andras Cser avec Merritt Maxim, Caroline Provost et Christine Turley, avril 2023.](#)

² Frost Radar™ : [Plateformes de protection des applications cloud-natives, 2024](#)

³ KuppingerCole Leadership Compass : [Plateformes de protection des applications cloud-natives \(CNAPP\), 2024](#)

Defender for Cloud

Pricing Model

Microsoft Defender for Cloud Pricing Model														
Option	Price													
Foundational CSPM	Free													
Defender CSPM	\$0.007/Billable resource/hour*													
DevOps Security	Free													
Servers	<table><tr><td>Servers (Plan1)</td><td>\$0.007/Server/hour</td></tr><tr><td>Servers (Plan 2)</td><td>\$0.02/Server/hour</td></tr></table>	Servers (Plan1)	\$0.007/Server/hour	Servers (Plan 2)	\$0.02/Server/hour									
Servers (Plan1)	\$0.007/Server/hour													
Servers (Plan 2)	\$0.02/Server/hour													
Containers	<table><tr><td>Containers</td><td>\$0.0095/vCore/hour</td></tr><tr><td>SQL on Azure-connected databases</td><td>\$0.021/Instance/hour</td></tr><tr><td>SQL outside Azure</td><td>\$0.015/vCore/hour</td></tr></table>	Containers	\$0.0095/vCore/hour	SQL on Azure-connected databases	\$0.021/Instance/hour	SQL outside Azure	\$0.015/vCore/hour							
Containers	\$0.0095/vCore/hour													
SQL on Azure-connected databases	\$0.021/Instance/hour													
SQL outside Azure	\$0.015/vCore/hour													
Databases	<table><tr><td>MySQL</td><td>\$0.021/Instance/hour</td><td>* See the notes section (below) for additional information</td></tr><tr><td>PostgreSQL</td><td>\$0.021/Instance/hour</td><td></td></tr><tr><td>MariaDB</td><td>\$0.021/Instance/hour</td><td></td></tr><tr><td>Azure Cosmos DB</td><td>\$0.0012 per 100 RUs/hour</td><td></td></tr></table>	MySQL	\$0.021/Instance/hour	* See the notes section (below) for additional information	PostgreSQL	\$0.021/Instance/hour		MariaDB	\$0.021/Instance/hour		Azure Cosmos DB	\$0.0012 per 100 RUs/hour		
MySQL	\$0.021/Instance/hour	* See the notes section (below) for additional information												
PostgreSQL	\$0.021/Instance/hour													
MariaDB	\$0.021/Instance/hour													
Azure Cosmos DB	\$0.0012 per 100 RUs/hour													
Storage	<table><tr><td>Storage</td><td>\$0.0134 per storage account / hour*</td></tr><tr><td>Malware Scanning (add-on)</td><td>\$0.15/GB of data scanned</td></tr></table>	Storage	\$0.0134 per storage account / hour*	Malware Scanning (add-on)	\$0.15/GB of data scanned									
Storage	\$0.0134 per storage account / hour*													
Malware Scanning (add-on)	\$0.15/GB of data scanned													
APIs	APIs	Varies by plan. See notes section.												
Service Layer	<table><tr><td>App Service</td><td>\$0.02/Instance/hour</td></tr><tr><td>Key Vault</td><td>\$0.25/Vault/month</td></tr><tr><td>Resource Manager</td><td>\$5.04/Subscription/month</td></tr></table>	App Service	\$0.02/Instance/hour	Key Vault	\$0.25/Vault/month	Resource Manager	\$5.04/Subscription/month							
App Service	\$0.02/Instance/hour													
Key Vault	\$0.25/Vault/month													
Resource Manager	\$5.04/Subscription/month													

Avantages

- Pas de consommation minimum
- Pay as you Grow model
- Pas d'engagement minimum

Pour aller plus loin

Arguments et contenus complémentaires



Sécurisez tous vos clouds

Résultats et stratégies



Stratégie Multi Cloud et Hybride

Consolidation des différents outils/fournisseurs de sécurité + stratégie de migration pour sécuriser toutes les charges de travail

Équilibre entre le meilleur de sa catégorie (haute sécurité) et le meilleur de l'étendue (suffisamment bon et rentable) des solutions de sécurité

Renforcer l'environnement et la posture de sécurité pour réduire les violations et les atteintes à la réputation



Une infrastructure sûre, efficace et stable

Protégez l'environnement multicloud avec les outils de sécurité existants ou nouveaux

Améliorer les économies de coûts dans les opérations informatiques à allouer à de nouveaux projets d'IA



Développement d'applications sécurisé

Utiliser le processus de gestion sécurisée du cycle de vie pour développer des applications

Développez avec des mesures de sécurité avancées

Évaluez le code à l'aide de méthodes traditionnelles et basées sur l'IA

Réévaluez les applications et le code existants par rapport aux menaces potentielles des méthodes d'exploitation malveillantes de l'IA

Impact financier/KPI



Score de sécurité



Sécurité, licences et coûts opérationnels



Incidents de sécurité et gravité



Score de compétence et d'habilitation



Risque de violation de données



ROI



Temps consacré à la sécurité et à la conformité



Sécurité intégrée dans les nouvelles applications



applications avec évaluations du code de sécurité



Coût de la violation pour les données et l'application



Satisfaction des employés

Capacités

Surveillez la posture de sécurité et protégez toutes les ressources et charges de travail (cloud et sur site)

Simulez des scénarios d'attaque réels grâce à l'analyse contextuelle du chemin d'attaque

Identifiez les risques et hiérarchisez les actions de remédiation les plus efficaces

Réduire la lassitude des recommandations grâce à l'IA générative

Appliquez les meilleures pratiques de conformité en matière de sécurité multicloud avec des contrôles mappés aux principales références réglementaires du secteur

Sécurité cloud native intégrée du principal fournisseur de sécurité

Visibilité complète de l'inventaire DevOps, des pipelines et de la posture de sécurité du code d'application de pré-production

Modèles d'infrastructure en tant que code (IaC) sécurisés et images de conteneur

Hiérarchiser les correctifs de code critiques avec des annotations de demande de tirage ; Donnez aux développeurs des informations contextuelles complètes du code au cloud

L'impact™ économique total de Microsoft Defender pour le cloud Une protection meilleure et plus réactive



Fidélité accrue de la sécurité

50% de réduction des faux positifs



Temps moyen de réponse plus court

30% de réduction du temps de correction des menaces



Productivité accrue

5,6 millions de dollars

d'économies de productivité SecOps sur trois ans

« Microsoft Defender pour le cloud fait un très bon travail pour trouver le juste milieu en ne étant pas trop agressif avec la gestion de la posture de sécurité et en permettant aux opérations de s'exécuter efficacement.

– **Directeur principal des opérations informatiques**, Santé

Protégez les environnements multicloud, du développement à l'exécution

Ressources

- › [Blog Defender pour le cloud](#)
- › [Communauté technique Defender pour le cloud](#)
- › [Série de vidéos Defender pour le cloud sur le terrain](#)
- › [Documentation de Defender pour le cloud](#)

[Démarrer un
essai gratuit](#) »



Merci

