PROTÉGEZ VOTRE DATACENTER CONTRE LE CRYPTOJACKING ET LES MENACES AVANCÉES

OLIVIER BOUZEREAU – FONDATEUR DE DCLOUD NEWS
VINCENT MEYSONNET – RESPONSABLE TECHNIQUE AVANT-VENTE

Bitdefender

OLIVIER BOUZEREAU

- **Journaliste et concepteur informatique**
  - Services métiers, contenus riches, interactions multimédias
  - Secteurs : presse, distribution, finance, e-santé
- **Coordinateur de projets de R&D collaboratifs**
  - Communauté internationale OW2 middleware open source
- **Fondateur et Rédacteur en chef DCloud News (dcloudnews.eu)**
  - Responsable de conférences et modérateur
  - Solutions Datacenter Management, Cloud World Expo, Roomn

Bitdefender

VINCENT MEYSONNET

Responsable Technique Avant-Vente Bitdefender

- 10 ans d'expérience dans le domaine de la sécurité des systèmes d'information
  - Ingénieur Système & Réseau puis Chef de Projet Intégration

- Rejoint Bitdefender en 2014
  - Responsable Technique Avant-Vente

Bitdefender

SOMMAIRE

- À propos de Bitdefender
- Tendances et transformations du datacenter
- Évolution des cybermenaces
- La protection traditionnelle du datacenter
- La protection Next-Gen du datacenter
- Questions/réponses

À PROPOS DE BITDEFENDER

Bitdefender

UN EXPERT EN CYBERSÉCURITÉ

- Société Européenne, disposant de plus de 20 ans d'expérience dans le domaine de la sécurité des données
- +1 500 collaborateurs, +700 ingénieurs en R&D
- Des technologies antimalwares 100% développées en interne
- Des solutions classées N°1 en Protection et Performance

MEMBRE DU GIP ACYMA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention du risque numérique

Bitdefender

500 millions

d'endpoints protégés

LA PLUS GRANDE INFRASTRUCTURE DE CYBERSÉCURITÉ AU MONDE

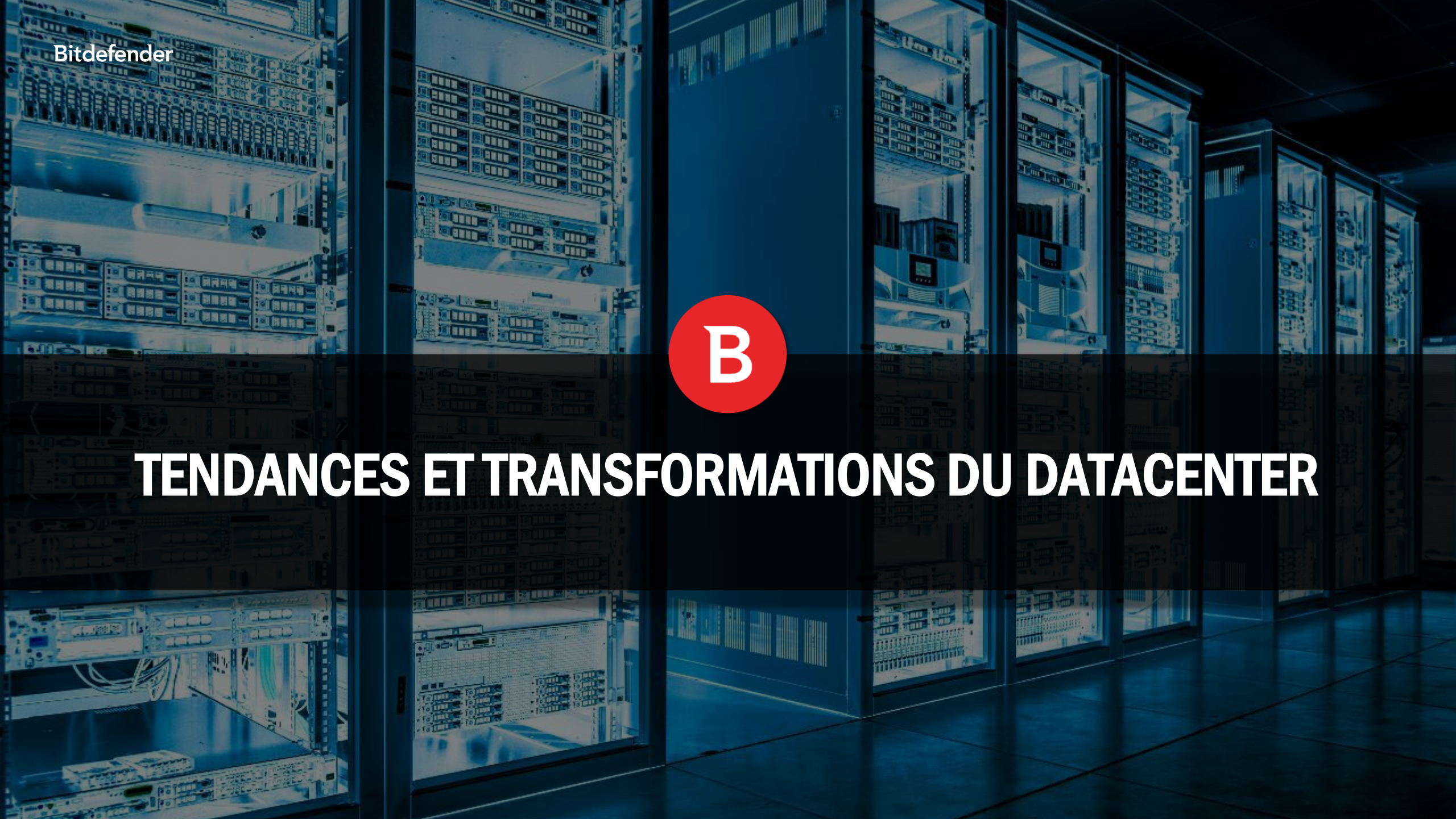
150

pays

132

partenaires OEM

© 2018 Bitdefender


Bitdefender
TENDANCES ET TRANSFORMATIONS DU DATACENTER

Bitdefender

DONNÉES NUMÉRIQUES A PROTÉGER

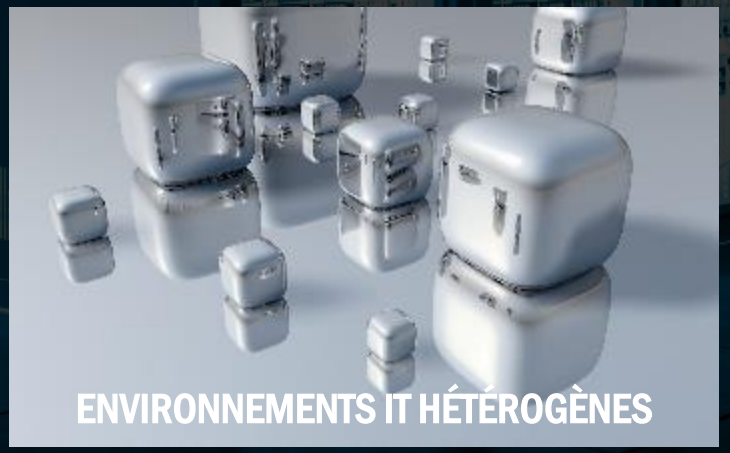
Cambridge Analytica

Bitdefender

SERVICES NUMÉRIQUES A PROTÉGER

Bitdefender

LE BUSINESS TRANSFORME L'IT



Bitdefender

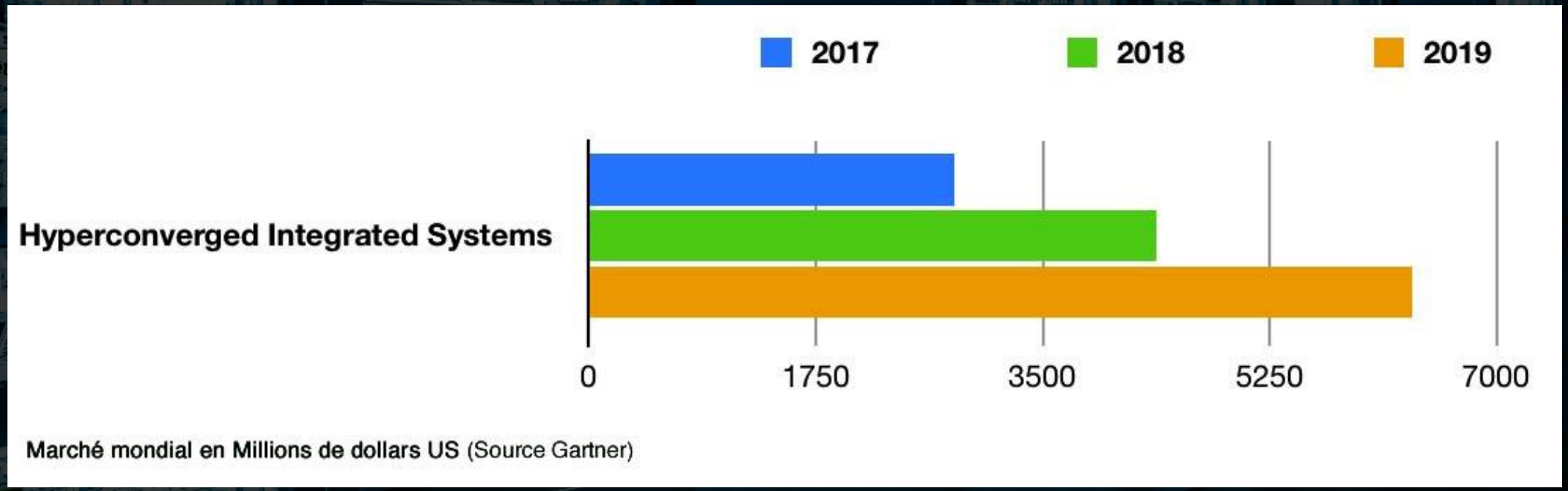
LA TRANSFORMATION DU DATACENTER

SOFTWARE-DEFINED DATACENTER

HYPERCONVERGENCE

CLOUD HYBRIDE

- *8,5 milliards d'e*



Bitdefender

LE SOFTWARE-DEFINED DATACENTER

Applications d'entreprise

Virtualisation et administration

Calcul (SDC)

Stockage (SDS)

Réseau (SDN)

+26.5%

par an
d'ici à 2021

83.2 Md$

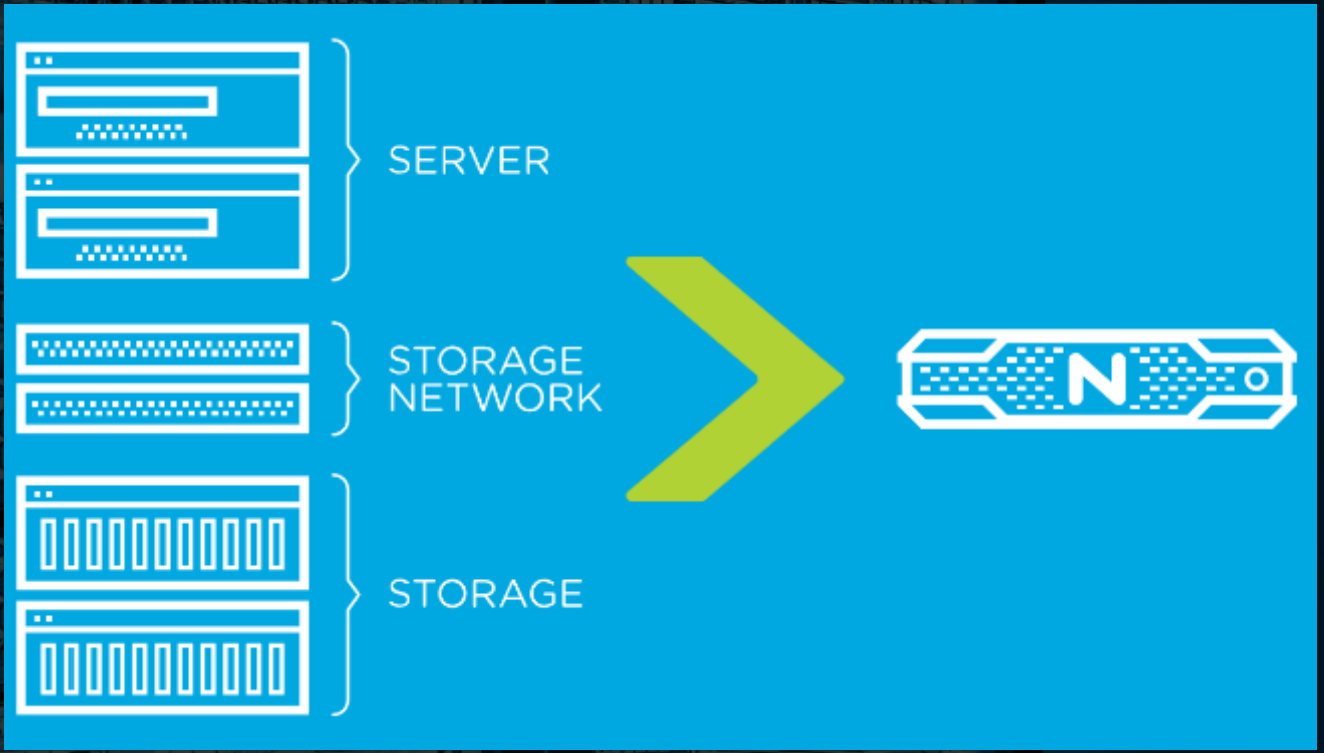
(source Markets&Markets)

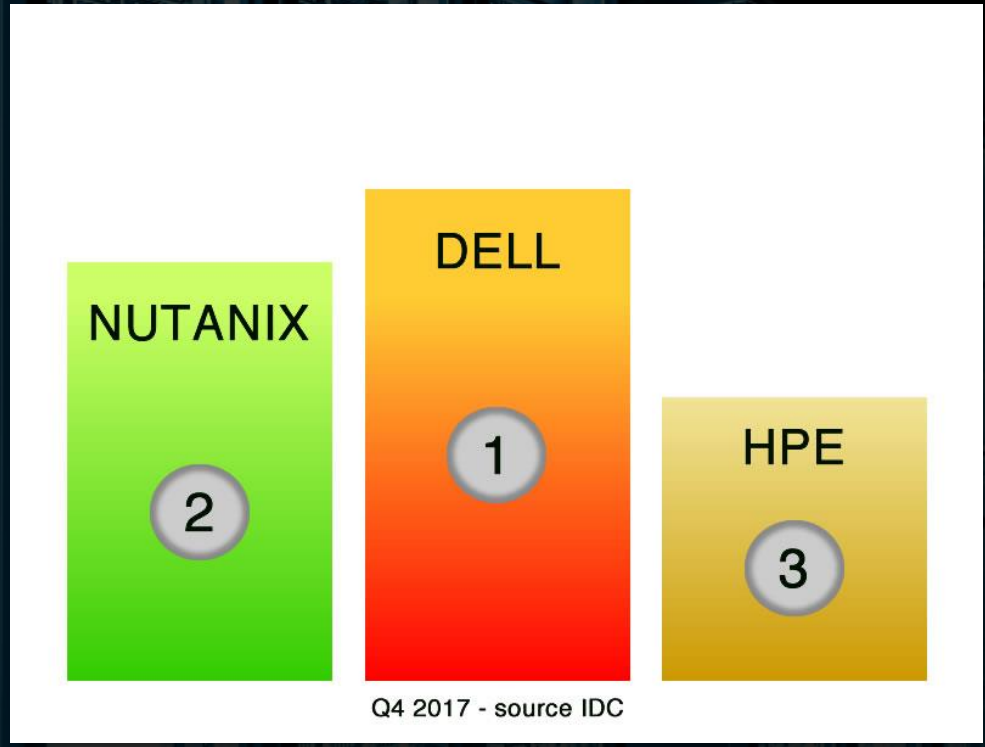
Infrastructure dans laquelle les ressources IT sont définies au niveau du logiciel.

L'objectif est d'accélérer les prestations de services, de réduire les coûts et de rendre l'environnement plus flexible et agile.

Bitdefender

L'INFRASTRUCTURE HYPERCONVERGÉE



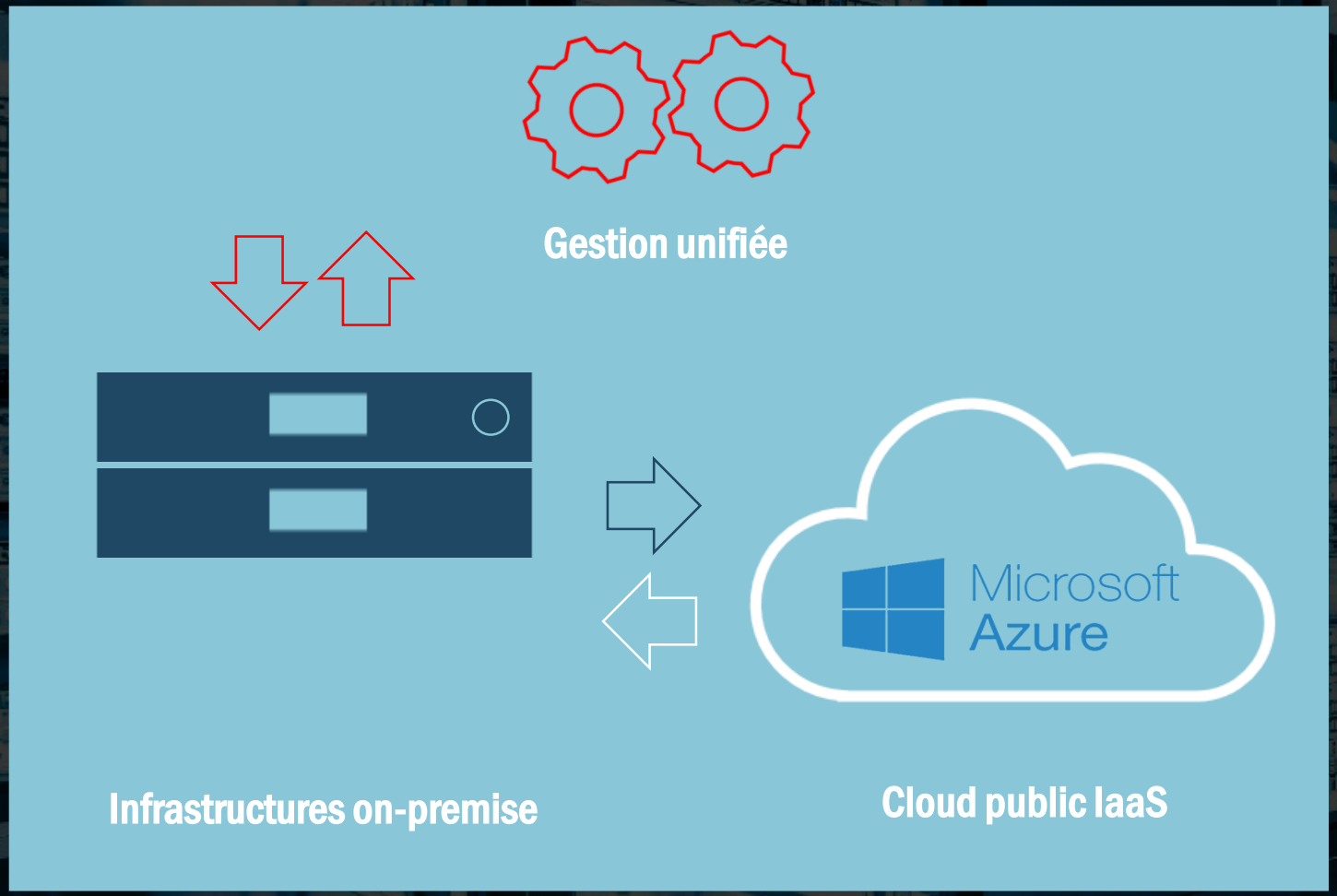


Infrastructure qui intègre les composants de traitement, de stockage de réseau et de virtualisation

Consolidation sur une seule pile logicielle tous les composants, dans une démarche « software defined »

Bitdefender

LE CLOUD HYBRIDE



Environnement IT cloud combinant des services de cloud privés on-premise, des services de cloud publics, et offrant des outils de gestion unifiée

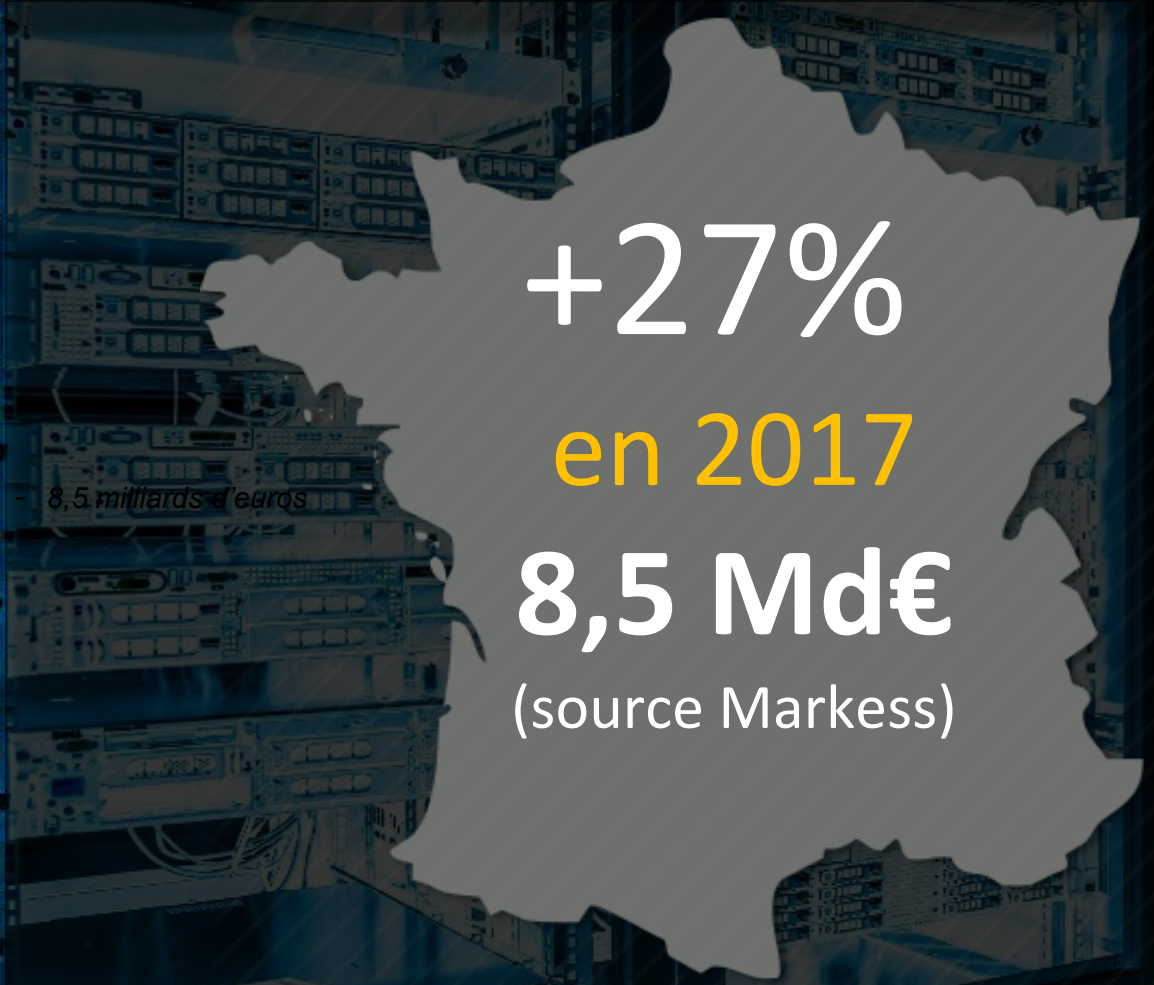
Cas d'usages :

1. Débordement
2. PRA/PCA
3. Archivage
4. DevOps

Bitdefender

LE CLOUD

EN FRANCE & DANS LE MONDE



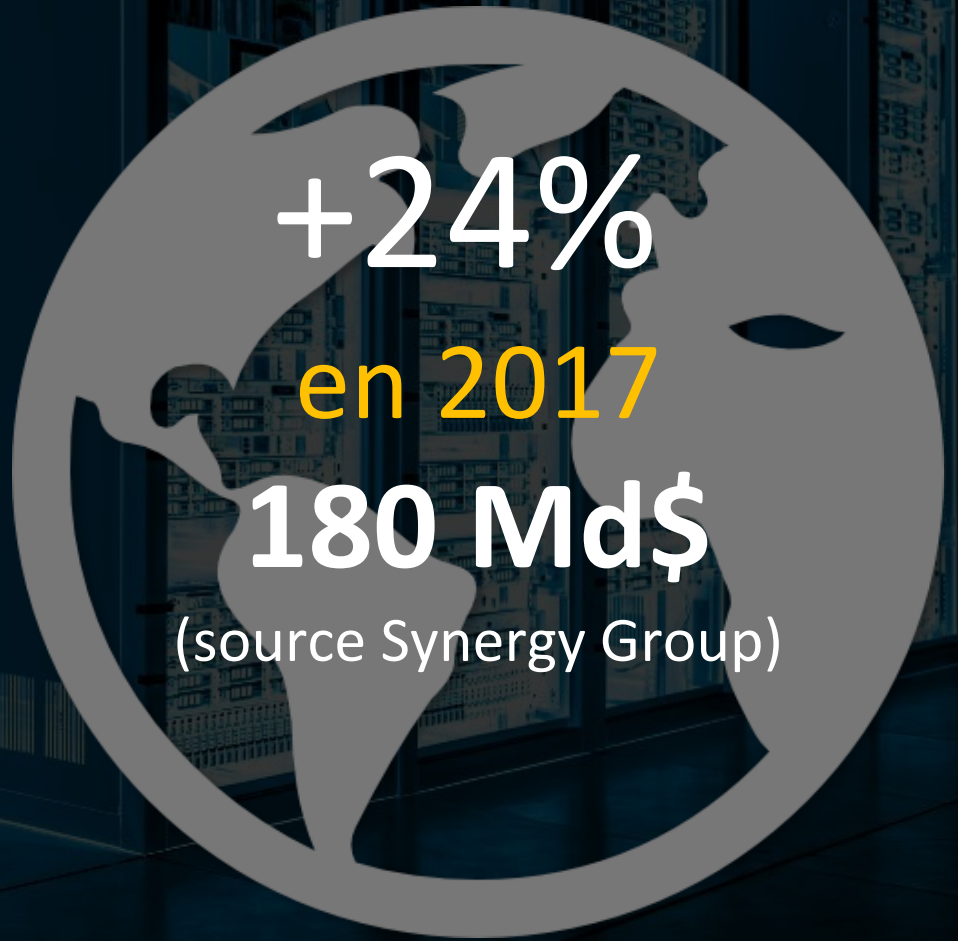
+27%

en 2017

8,5 Md€

(source Markess)

- *8,5 milliards d'euros*



+24%

en 2017

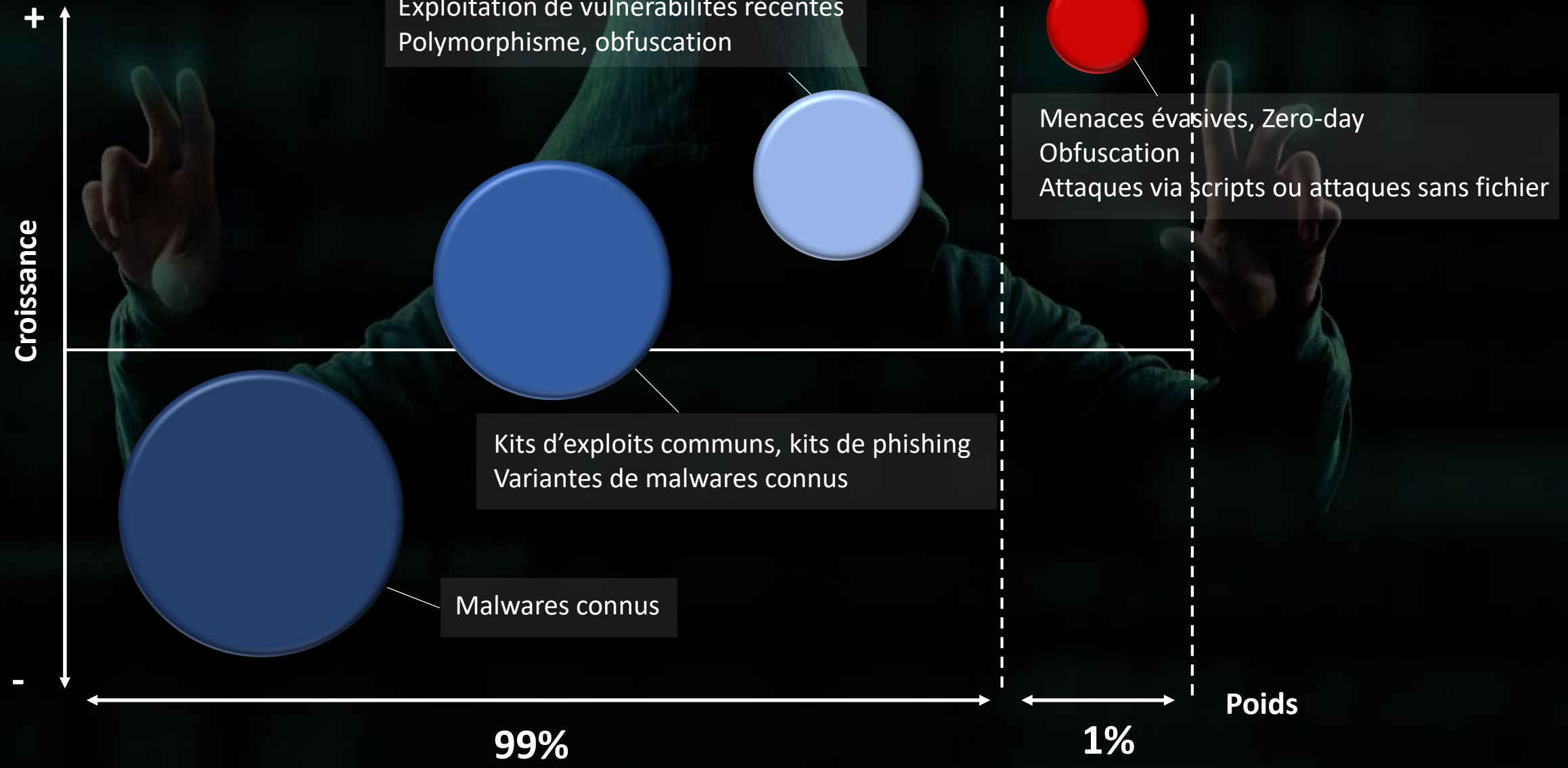
180 Md$

(source Synergy Group)


Bitdefender
ÉVOLUTION DES CYBERMENACES

Bitdefender

UN PAYSAGE DES MENACES EN CONSTANTE ÉVOLUTION



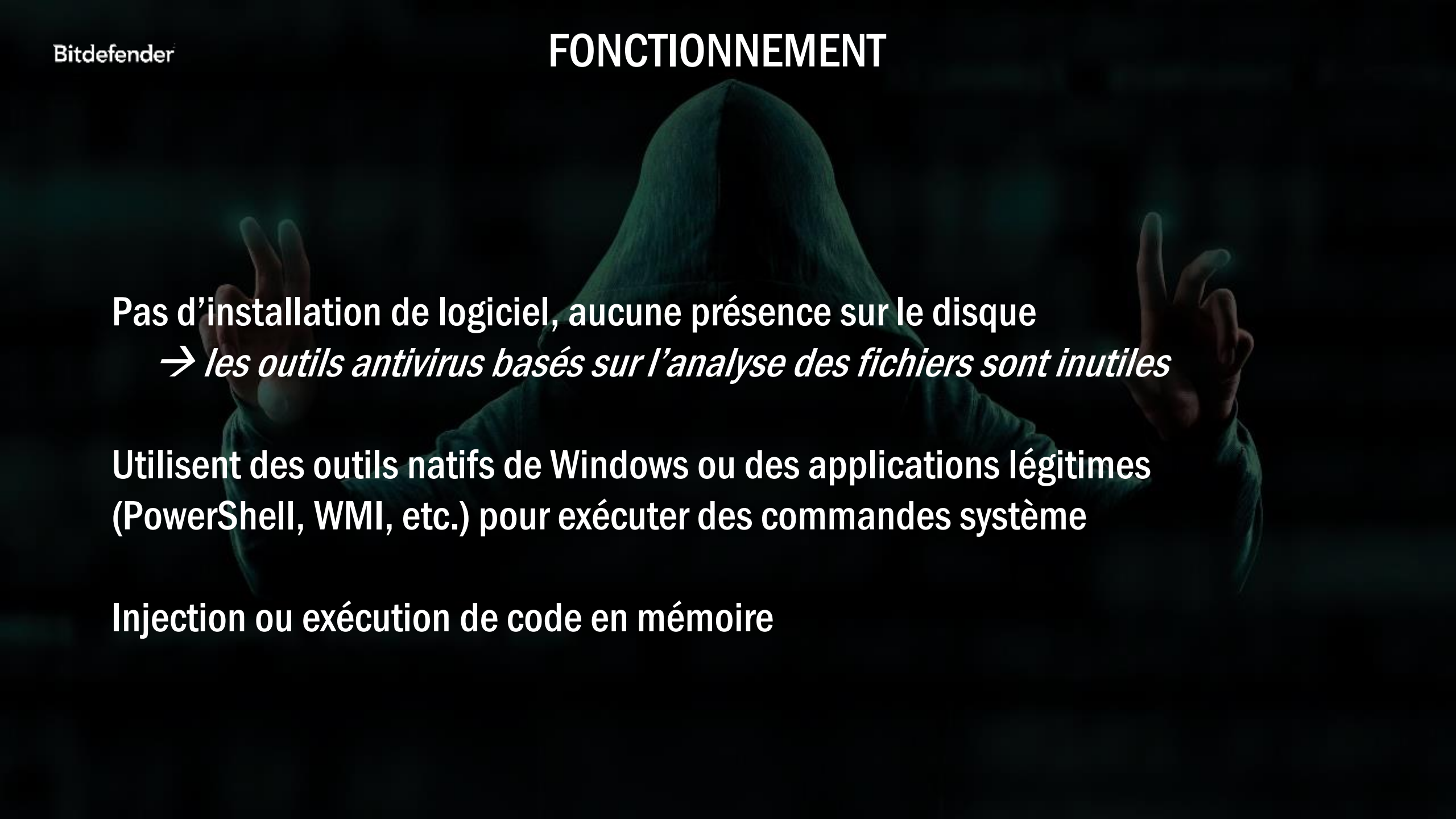
FOCUS SUR...

LES ATTAQUES SANS FICHIER

Bitdefender

Bitdefender

FONCTIONNEMENT



Pas d'installation de logiciel, aucune présence sur le disque

→ *les outils antivirus basés sur l'analyse des fichiers sont inutiles*

Utilisent des outils natifs de Windows ou des applications légitimes (PowerShell, WMI, etc.) pour exécuter des commandes système

Injection ou exécution de code en mémoire

Bitdefender

ANATOMIE DE 2 TYPES D'ATTAQUES SOPHISTIQUÉES

Canaux de diffusion	Techniques d'infection/ d'exploitation	Techniques de diffusion de charge utile	Objectifs

Attaque sans fichier – Basée sur un exploit


PowerShell
WMI


Code

Vol de données
Vol d'identifiants
Espionnage

Attaques « obfusquées »


PowerShell
WMI

Chiffrement
Packers
Polymorphisme

Vol de données
Vol d'identifiants
Espionnage

FOCUS SUR...

LE CRYPTOJACKING

Bitdefender

LES CRYPTO-MONNAIES

Monnaies virtuelles basées sur un système logiciel appelé « blockchain »

Produites grâce aux ressources matérielles des membres du réseau blockchain et visant à résoudre des problèmes mathématiques complexes. Rémunération en crypto-monnaies

Plus 1 300 crypto-monnaies existent

Bitcoin la plus populaire – valeur ayant atteint 20 000$ en 2017

DES GAINS FINANCIERS COLOSSAUX
POUR LES CYBERCRIMINELS EXPLOITANT LE CRYPTOMINING

0,25$ Monero par jour

X 2 000 victimes

500$ par jour

182 500$ par an

RANSOMWARE VS. CRYPTOJACKING

UN RAPPORT DE 1 À 100 – LA CYBERMENACE N°1 EN 2018

Un attaquant gagne de l'argent uniquement des victimes qui paient la rançon	Un attaquant gagne de l'argent de toutes ses victimes
Attaque est visible	Attaque invisible
Un seul versement d'argent	Un gain d'argent pendant plusieurs mois, voire plus

DES DOMMAGES IMPORTANTS DANS LES DATACENTERS

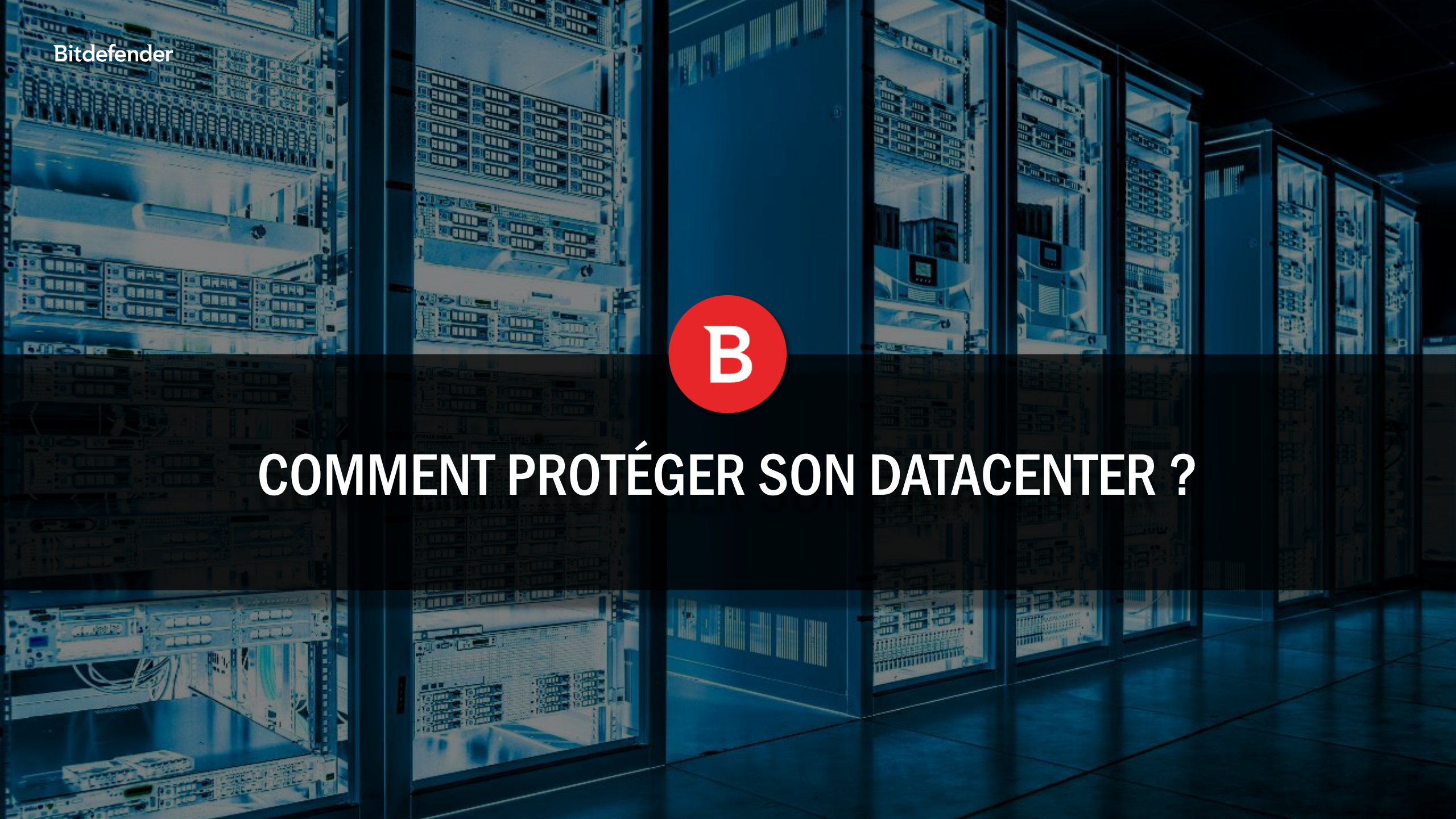
Impacte l'expérience utilisateur, les ratios de consolidation et la densité de virtualisation

Augmente les coûts de provisionnement, sans cause apparente

- En particulier pour les entreprises qui provisionnement automatiquement de nouvelles ressources

Infiltre et déstabilise les infrastructures critiques

Persistance importante


Bitdefender
COMMENT PROTÉGER SON DATACENTER ?

Bitdefender

SÉCURITÉ DES DATACENTERS : DEUX FAITS MARQUANTS

+30% de ressources CPU utilisées par la sécurité

20% de temps de réponse des applications supplémentaire à cause de la sécurité

Bitdefender

INCONVÉNIENTS DE LA SÉCURITÉ TRADITIONNELLE

PERFORMANCE DE L'INFRASTRUCTURE, UTILISATION ET EXPÉRIENCE UTILISATEUR

- **X** La sécurité traditionnelle est basée sur la sécurité des environnements physiques, ce qui ne permet pas de tirer avantage de la virtualisation et du Cloud
- **X** Des agents antimalwares lourds sont installés sur chaque VM, réalisant des analyses et stockant en local des bases de données complètes de signatures
  - **X** Forte consommation des ressources des VM, avec des impacts négatifs sur le CPU, la mémoire, les IOPS et la densité de virtualisation
  - **X** Conflits de ressources lorsque les agents sont en concurrence avec les charges de travail primaires
  - **X** Chutes de performance des applications causées par les AV-storms et qui entravent l'expérience utilisateur
- **X** Des manquements de sécurité au démarrage des VM rendent les systèmes vulnérables aux attaques

Bitdefender

INCONVÉNIENTS DE LA SÉCURITÉ TRADITIONNELLE

ADMINISTRATION

x Des agents multiples et/ou plusieurs consoles pour gérer la sécurité , ce qui complexifie les déploiements et l'administration

Agent 1

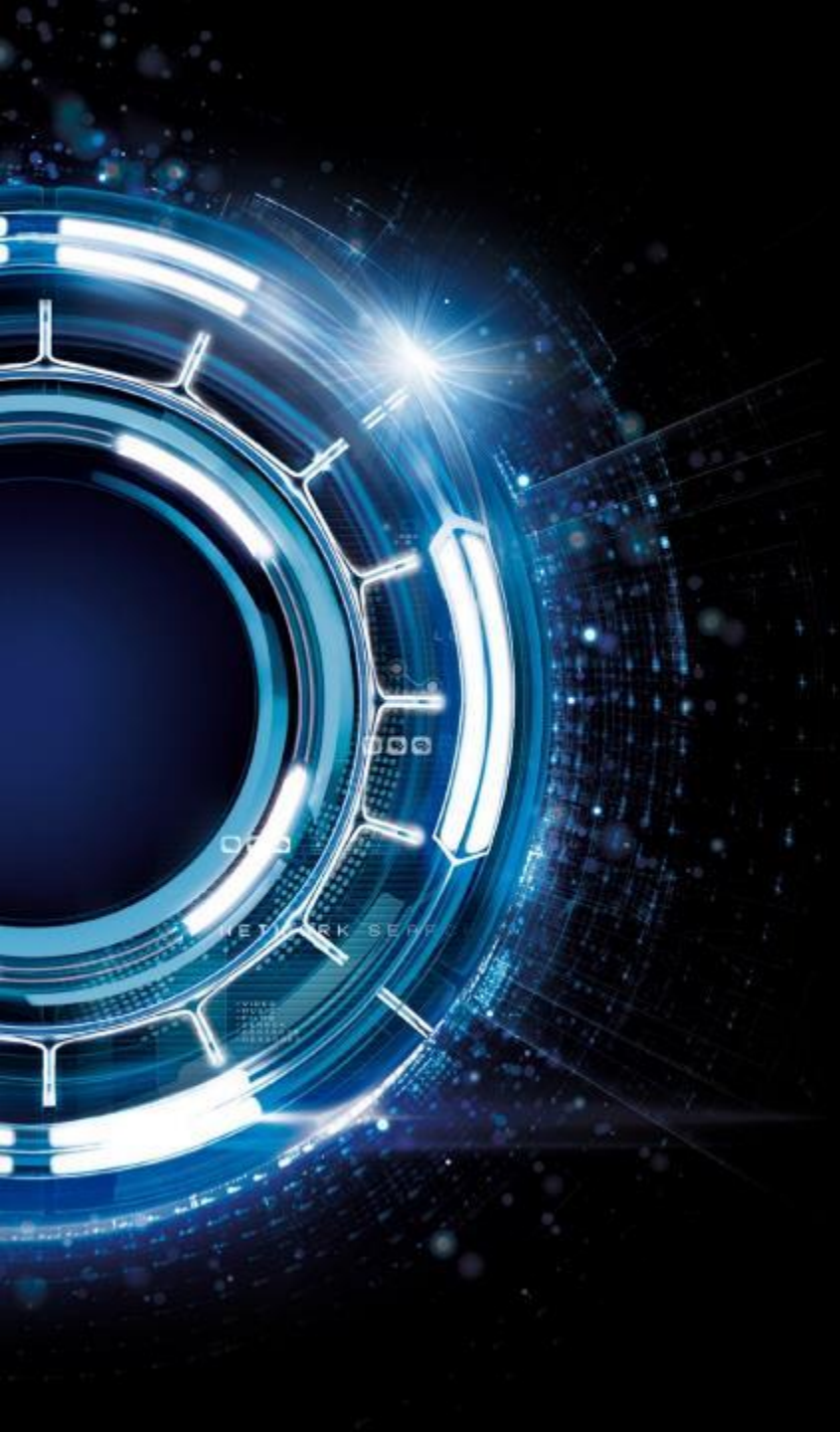
Agent 2

Agent 3

Console 1

Console 2

Console 3



“...DÉPLOYEZ DES SOLUTIONS SPÉCIFIQUEMENT DÉVELOPPÉES POUR LA PROTECTION DES CHARGES DE TRAVAIL DU CLOUD HYBRIDE”

Gartner, “Market Guide for Cloud Workload Protection Platforms,” 2017

Bitdefender

Bitdefender

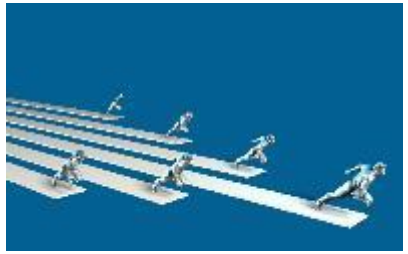
COMMENT OPTIMISER LA SÉCURITÉ, L'EFFICACITÉ OPÉRATIONNELLE ET LES PERFORMANCES DE VOTRE INFRASTRUCTURE ?

Bitdefender

LES AVANTAGES DE GRAVITYZONE

PROTECTION MAXIMIMALE

AGILITÉ ET EFFICACITÉ OPÉRATIONNELLES



MEILLEURE UTILISATION DE L'INFRASTRUCTURE

MEILLEURES PERFORMANCES ET EXPÉRIENCE UTILISATEUR

COMPATIBILITÉ UNIVERSELLLE

CITRIX ready

vmware READY

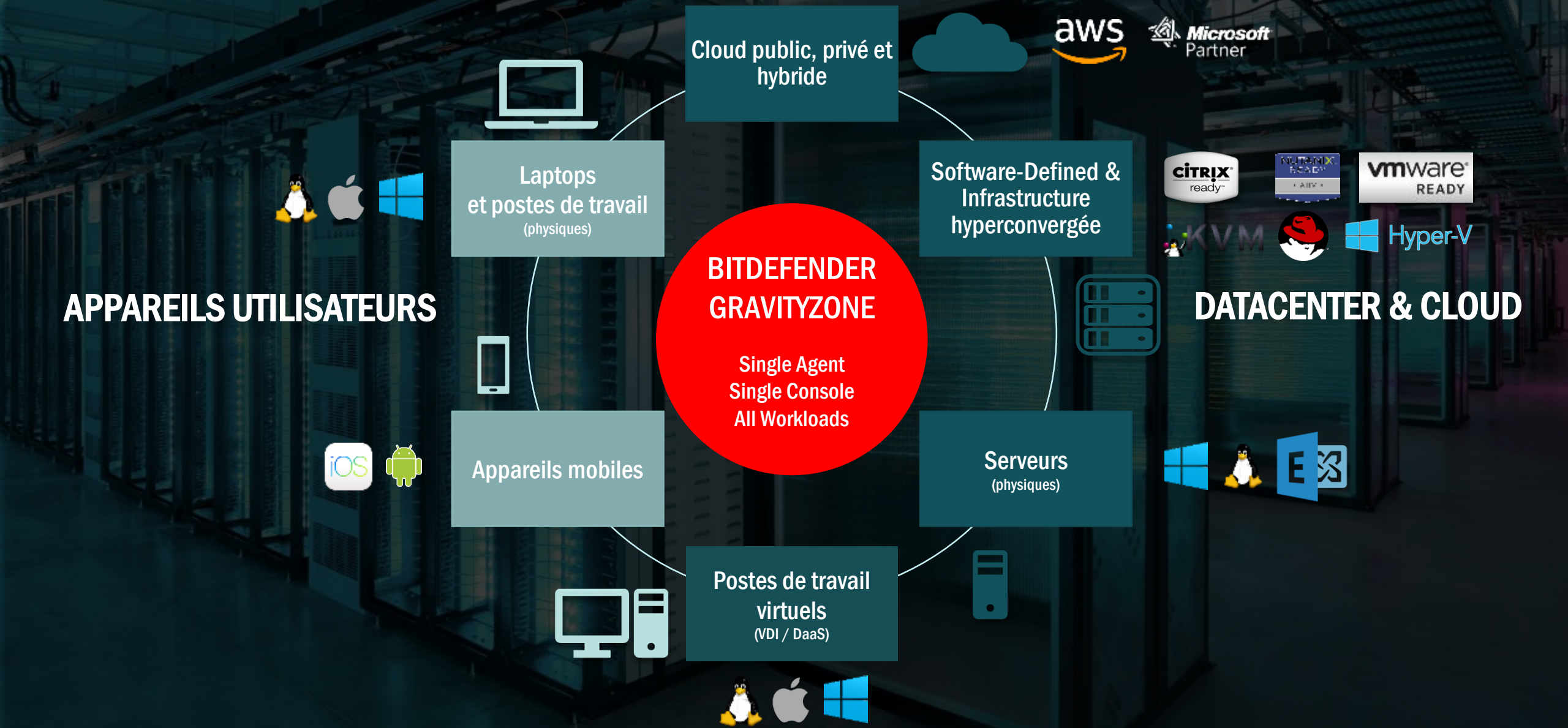
NUTANIX READY AHV

amazon web services

ÉVOLUTIVITÉ ILLIMITÉE

Bitdefender

UNE PLATEFORME DE SÉCURITÉ COMPLÈTE

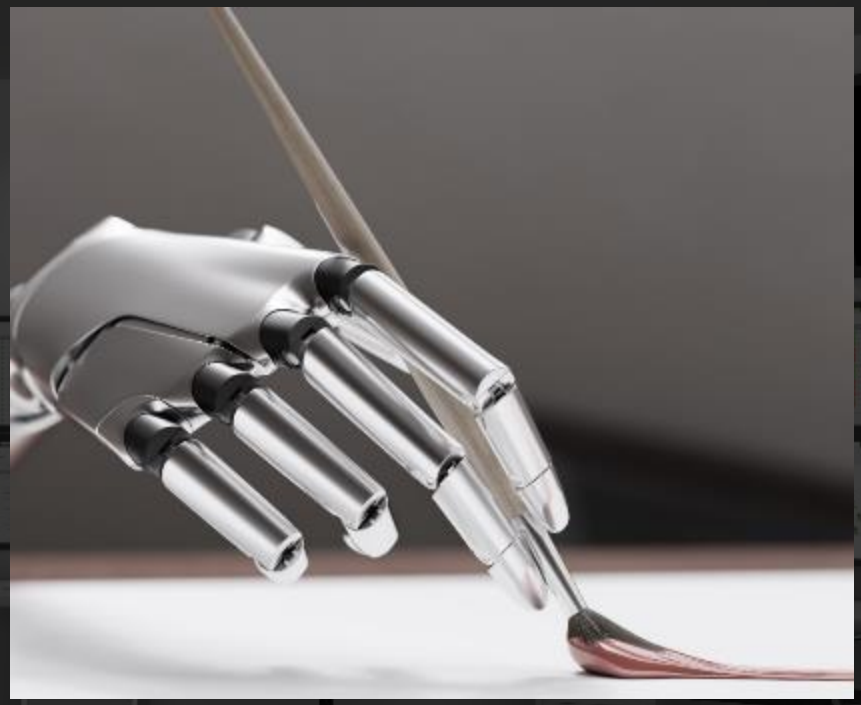


MEILLEURE AGILITÉ ET EFFICACITÉ OPÉRATIONNELLES VIA UNE GESTION UNIFIÉE

GESTION CENTRALISÉE DE LA SÉCURITÉ

- Console de gestion centralisée et agent modulaire unique pour tous les endpoints physiques et virtuels, sur site ou dans le Cloud
- Visibilité depuis un point unique sur l'inventaire des endpoints de l'entreprise et sur l'état de la sécurité et de la conformité

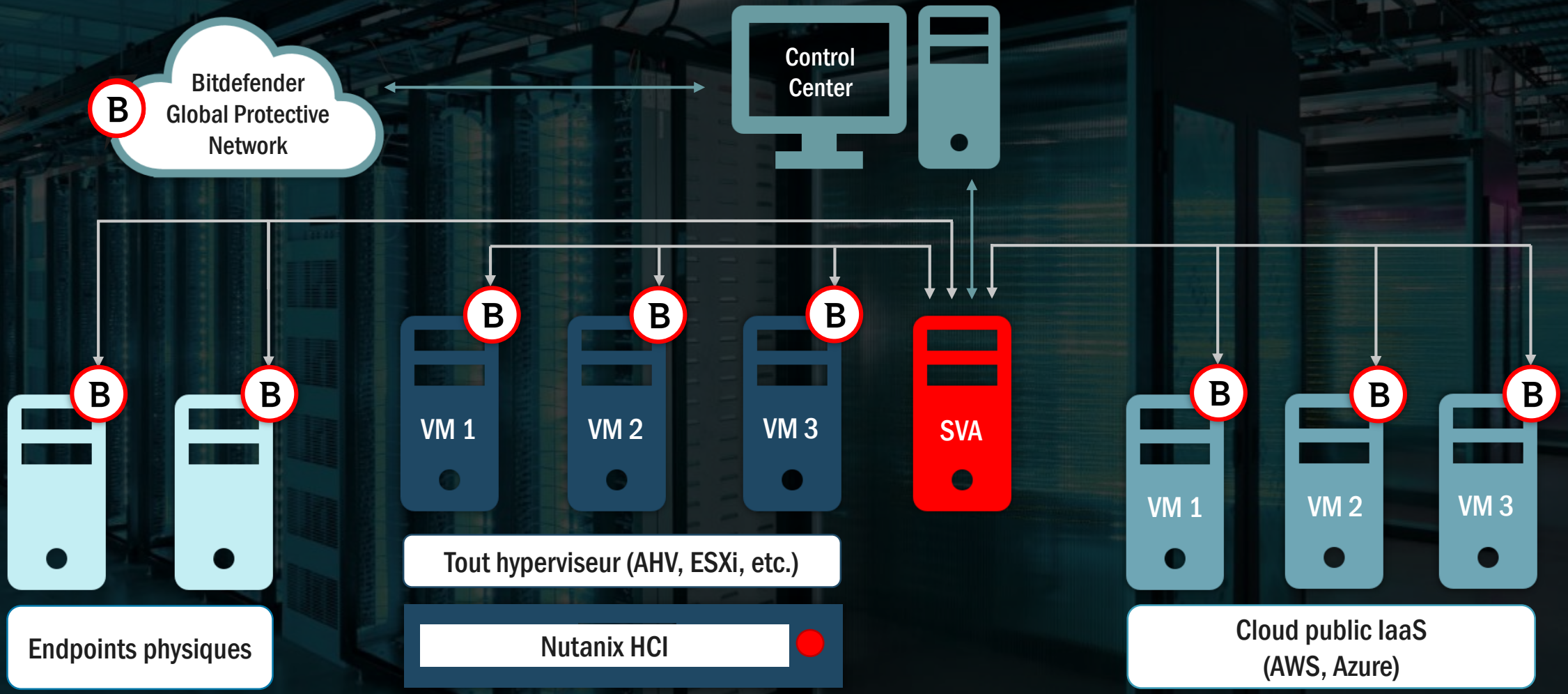
AUTOMATISATION DE LA SÉCURITÉ



- Déploiement, configuration et mises à jour automatiques
- Découverte automatique des endpoints
- Provisionnement et activation des agents automatiques
- Remédiation et annulation des modifications malveillantes
- Récupération automatique de licence lors de la mise hors service des VM

Bitdefender

GRAVITYZONE : EFFICACE ET ÉVOLUTIF, VIA UNE ARCHITECTURE AGILE



Bitdefender

PLATEFORME DE SÉCURITÉ MULTI-COUCHES NEXT-GEN

RENFORCEMENT & CONTRÔLE


Contrôle des applications


Contrôle de contenu


Antiphishing


Pare-feu


Contrôle des périphériques


Full-Disk Encryption

DÉTECTION MULTI-NIVEAUX

PRÉ-EXÉCUTION


Recherche par signature et dans le cloud


Machine Learning (Local & Cloud)


HyperDetect


Sandbox Analyzer

À L'EXÉCUTION


Anti-Exploit


Process Inspector

ACTION AUTOMATIQUE


Blocage des accès


Quarantaine


Désinfection / Suppression


Arrêt des processus


Annulation des modifications

VISIBILTÉ & RAPPORTS


Rapports et tableau de bord personnalisables


Indicateurs de compromission


Activités suspectes


Contexte sur les menaces


Alertes et notifications

Bitdefender

FOCUS SUR LES FONCTIONNALITÉS NEXT-GEN

Contrôle de contenu

Contrôle des périphériques

Machine Learning (Local et Cloud)

Anti-Exploit

Process Inspector

Contrôle de contenu

- Analyse du trafic entrant et des e-mails
- Blocage des URL via analyse comportementale et ML
- Filtrage par catégories Web

Contrôle des périphériques

Permet aux administrateurs de gérer les autorisations pour les périphériques externes, tels que les clés USB, les périphériques Bluetooth, etc.

Machine Learning dynamique

Des algorithmes entraînés sur plus de 500M d'endpoints et 3 trillions d'échantillons pour une efficacité maximale avec peu de faux positifs

Protection contre les exploits

Détecte les techniques d'exploits et protège la mémoire des navigateurs, des visionneuses, des lecteurs et des applications bureautiques

Process Inspector

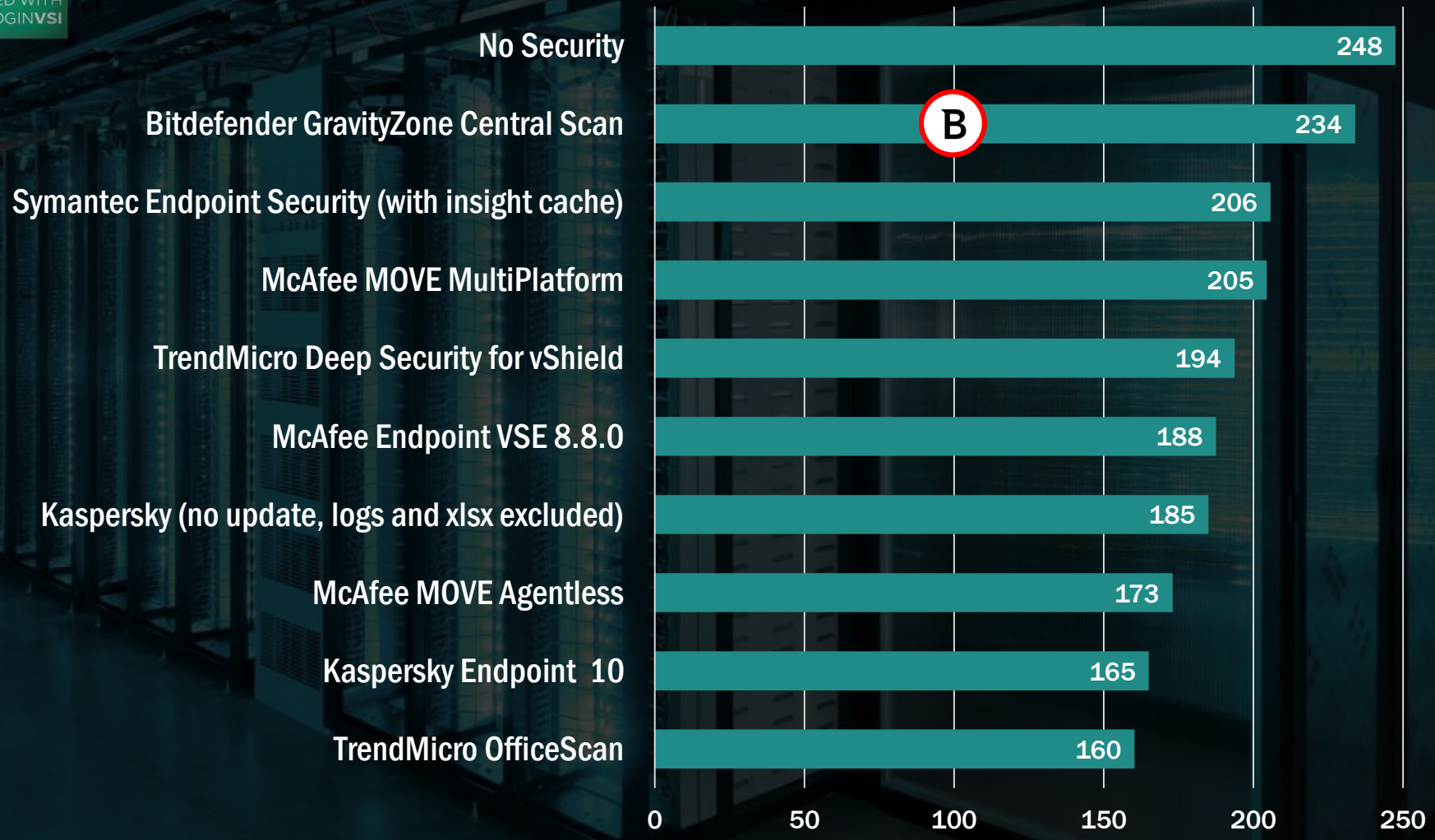
Détection proactive et dynamique des menaces inconnues basée sur la surveillance en continu des processus et des événements système, et le marquage des activités suspectes

Bitdefender

RÉDUCTION DES COÛTS DE L'INFRASTRUCTURE GRÂCE À UNE MEILLEURE UTILISATION

TESTED WITH LOGINVSI

Nombre maximum de sessions VDI simultanées par hôte



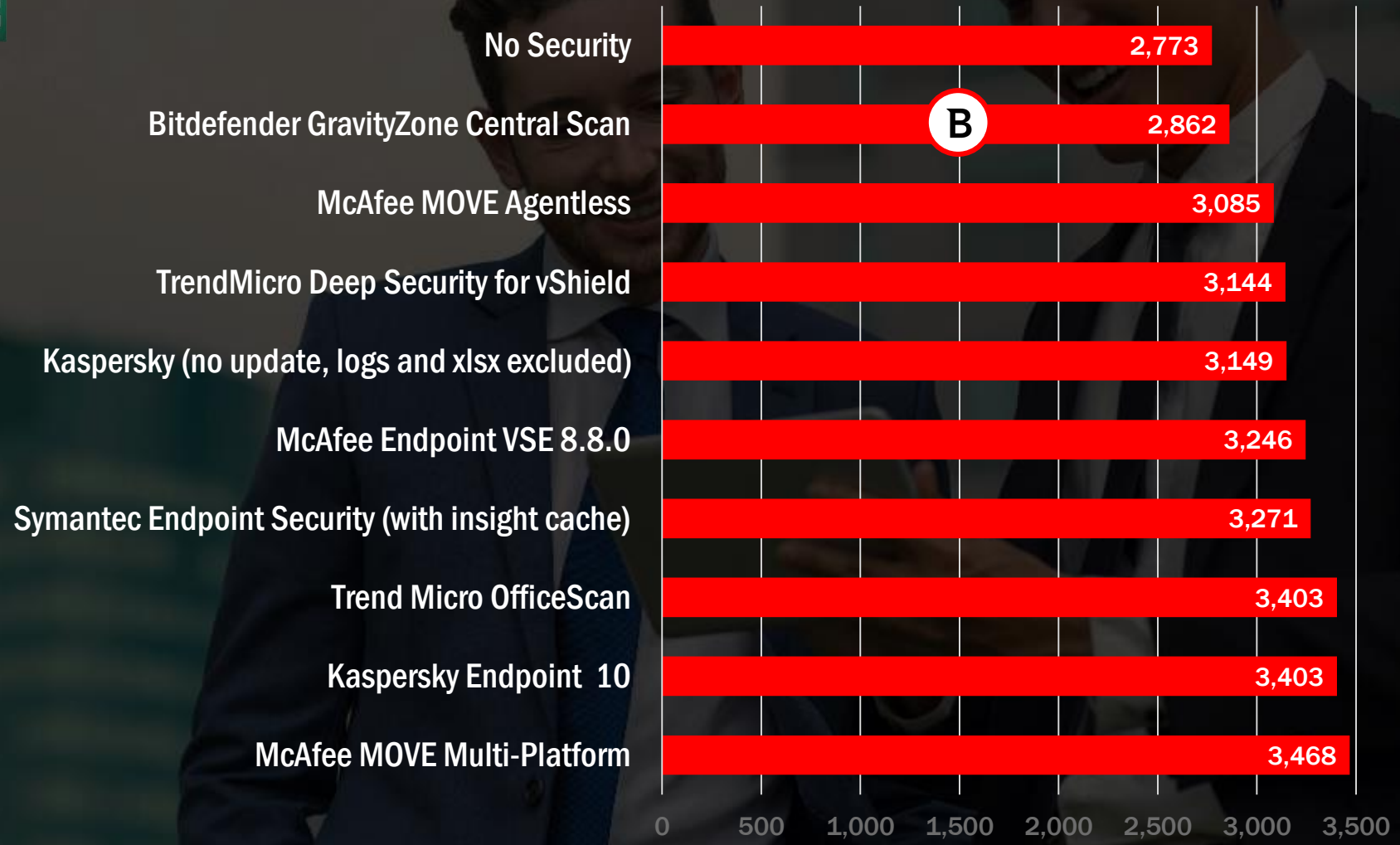
AMÉLIORATION DE 35% DE LA DENSITÉ DE VIRTUALISATION

Bitdefender

MEILLEURE EXPÉRIENCE UTILISATEUR GRÂCE À L'AMÉLIORATION DES PERFORMANCES DES APPLICATIONS

TESTED WITH LOGINVSI

Temps de réponse des systèmes (en millisecondes)



17% DE MOINS DE LATENCE AU NIVEAU DE LA RÉPONSE DES APPLICATIONS

MERCI ! QUESTIONS/RÉPONSES

Olivier Bouzereau – Fondateur de DCloud News
Vincent Meysonnet – Responsable Technique Avant-Vente

www.bitdefender.fr/business

Bitdefender