Commandité par : Check Point Software Technologies Ltd.

Les solutions de centre de données hybrides répondent à de nombreux problèmes de sécurité rencontrés par les entreprises grâce à la visibilité, la portabilité et l'évolutivité des solutions de cloud privé et hybride sur site.

Guide de sécurisation du CloudDatacenter hybride à l'ère de la transformation numérique

janvier 2022

Écrit par : Philip Bues, directeur de recherche, sécurité du cloud

Introduction

Aujourd'hui, de nombreuses organisations non seulement transfèrent davantage de charges de travail vers le cloud, mais modernisent également leurs centres de données. Ils créent des environnements cloud hybrides avec des charges de travail distribuées qui doivent être sécurisées.

Le centre de données et le réseau modernes nécessitent la flexibilité d'une architecture de sécurité cloud hybride qui utilise l'automatisation et l'intelligence artificielle pour faire évoluer les performances de prévention des menaces à la demande, sur site et dans le cloud, avec un système de gestion simplifié et unifié. Le défi de la sécurité des centres de données hybrides est l'une des histoires méconnues du parcours de transformation numérique (DX) des entreprises.

Le parcours DX pour de nombreuses organisations a commencé avant la pandémie. À cette époque, les entreprises utilisaient le haut débit pour connecter le centre de données aux cloud publics. Ce fut également le début du « lift and shift » des charges de travail du centre de données vers le cloud. Le passage au cloud a été la partie la plus facile. Ce qui n'est pas facile, c'est la gestion de l'environnement cloud. DX en était encore à ses balbutiements, la confiance dans le cloud n'était pas encore bien établie, et beaucoup étaient encore en train de créer des tunnels ou de relier des bureaux et des utilisateurs distants au centre de données.

Une fois que le COVID-19 a frappé, les plans de transformation se sont accélérés, mais les complexités aussi. Lorsque le travail à domicile a commencé à l'échelle mondiale, les entreprises ont sécurisé le cloud en utilisant des services tels que l'infrastructure en tant que service (IaaS) et le logiciel en tant que service (SaaS). Dans le même temps, les cybercriminels ont augmenté la fréquence et la sophistication de leurs cyberattaques. Les services cloud n'étaient pas à l'abri des attaques. À mesure que les risques de sécurité augmentaient, les avantages et la complexité de l'exploitation des services cloud sont devenus évidents.

EN UN COUP D'OEIL

STATISTIQUES CLÉS

Au cours des cinq prochaines années, 59 % des organisations déplaceront davantage de charges de travail vers le cloud, tandis que 65 % moderniseront leurs centres de données.

PRINCIPAUX À RETENIR

» Une solution de centre de données hybride moderne peut étendre l'architecture, les règles et les politiques partagées d'un cloud privé sur site au cloud public. Cela permet aux organisations de maximiser leurs investissements institutionnels et réduit le recyclage ou le perfectionnement des compétences.

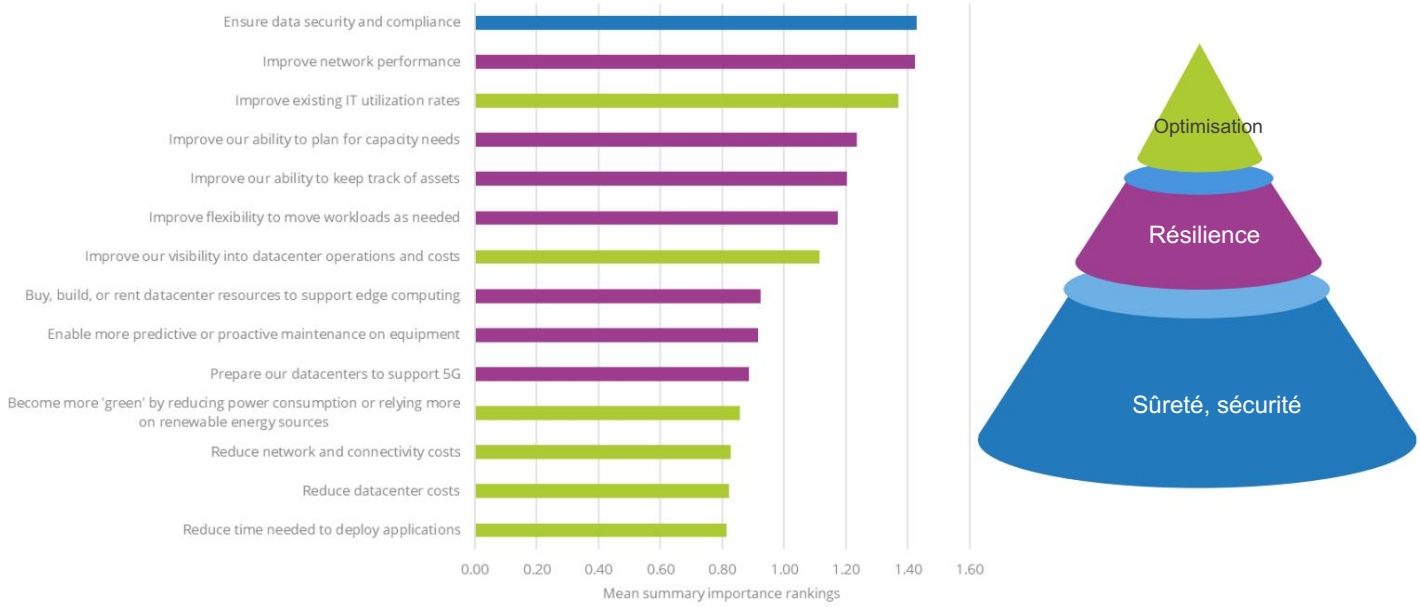
» Les centres de données hybrides modernes utilisent plateformes basées sur le cloud pour fournir l'intelligence artificielle et l'apprentissage automatique gestion et réponse automatisées aux menaces. Ces politiques de sécurité non seulement rationalisent et augmentent l'efficacité des équipes opérationnelles, mais réduisent également le besoin de contrôles manuels des modifications, réduisant ainsi le risque d'erreur humaine et de violations.

Toutes les organisations doivent garantir le contrôle de leurs données et de leurs opérations commerciales. Cependant, les acteurs des secteurs hautement réglementés tels que les services financiers, les soins de santé et la vente au détail doivent prendre des mesures supplémentaires, notamment en conservant des données et des charges de travail spécifiques sur site, pour être conformes. Un cloud privé sur site est la solution la plus efficace.

La modernisation du centre de données ne consiste plus seulement à éviter les temps d'arrêt ; il s'agit également de sûreté, de sécurité, de résilience et d'optimisation pour répondre aux exigences de la nouvelle économie numérique. Ne vous y trompez pas : ces initiatives ont un effet domino.

Les vieilles solutions « fragmentaires » qui conduisaient à des complexités ont fait leur temps. Dans l'enquête opérationnelle sur les centres de données 2021 d'IDC , les entreprises ont identifié l'importance des initiatives de centres de données modernes, notamment en faisant de la sécurité et de la conformité des données la priorité absolue (voir Figure 1). Vient ensuite la reconnaissance du fait que l'intégration d'une solution de cloud hybride dans le centre de données moderne nous rapproche de la garantie de la sécurité et de la conformité des données. , amélioration des performances du réseau, amélioration les taux d'utilisation informatique existants et de nombreux autres avantages révélés dans l'enquête. Les organisations qui cherchent à optimiser le calcul et le stockage tout en tirant parti de la gestion des changements via des API devraient considérer les avantages de la « cloudification » de leur centres de données sur site.

FIGURE 1 : Initiatives de centres de données



n = 400

Source : Enquête opérationnelle sur les centres de données d'IDC, 2021

Principaux défis des cloud privés et publics sur site

Les cloud privés des centres de données et les cloud hybrides sont désormais inextricablement liés, mais remplissent probablement des fonctions différentes.

Un cloud privé sur site peut être utilisé pour exécuter de grandes charges de travail de gestion de la relation client (CRM)/de planification des ressources d'entreprise (ERP) nécessitant une faible latence, tandis que les services de base tels que la messagerie électronique et le stockage de fichiers sont hébergés dans le cloud. Tout d'abord, nous devons situer dans leur contexte les défis liés à la sécurité des cloud publics et privés : des complexités existent toujours et les organisations continuent de subir des violations sur site et dans le cloud.

Dans le passé, de nombreux clients de services de sécurité attendaient qu'une urgence, telle qu'une violation, se produise avant de mettre en œuvre une stratégie cloud ou d'hygiène. Les raisons de l'attente pourraient être attribuées à un manque de personnel, compétences/formations et outils complexes. Cependant, le taux de violations s'est intensifié. Selon l'enquête EDR et XDR 2020 d'IDC , au cours des deux dernières années, la plupart des organisations ont connu entre une et six failles de sécurité majeures, voire plus, sur site, ce qui a nécessité des dépenses considérables. ressources supplémentaires pour y remédier. En conséquence, ces organisations ont alors entamé une transition vers le cloud. L'enquête 2020 d'IDC sur la sécurité du cloud a révélé que les environnements cloud IaaS de la plupart des organisations ont également a été violée avec le même résultat qui a nécessité la dépense de ressources supplémentaires importantes pour y remédier. Il convient de noter que moins de cas signalent « aucune violation » dans le cloud que sur site. Cela est dû en grande partie au modèle d'infrastructure partagée que l'on retrouve dans les cloud publics, dans lequel le fournisseur de services cloud devient un gardien de la sécurité pour différents niveaux de responsabilité, à commencer par l'IaaS avec le physique, l'infrastructure, le réseau et la virtualisation. Des services supplémentaires sont fournis par des fournisseurs tiers. .

Dans le cloud, la complexité pour l'organisation est réduite. Cependant, la réalité est que les entreprises adoptent une solution de centre de données hybride avec une présence à la fois dans un cloud privé sur site et dans un cloud public hors site :

- » Le parcours de transformation numérique conduit de nombreuses organisations à migrer vers plusieurs environnements cloud IaaS. Chaque cloud présente des configurations, des vulnérabilités de code et des problèmes de maintenance différents. Les nuages sont différents.
- » Gérer plusieurs cloud privés et publics disparates signifie apprendre à utiliser plusieurs outils pour orchestrer et sécuriser ces environnements sans plate-forme unifiée de visibilité, de gestion et de conformité.
- » Le modèle d'infrastructure partagée dans le cloud signifie que les contrôles des utilisateurs diminuent à mesure que le modèle de déploiement migre vers les services. Dans un cloud privé sur site, l'organisation conserve le contrôle total. Dans un cloud public, le fournisseur assume davantage de responsabilités et de risques à mesure que l'organisation évolue vers des niveaux de virtualisation plus élevés. Dans une offre SaaS typique, l'utilisateur conserve le contrôle uniquement sur son identité et ses données. La complexité augmente à mesure que de nouvelles instances SaaS sont ajoutées.
- » Un cloud privé et un cloud public sont optimisés pour différentes charges de travail et applications.

Les infrastructures changent. Modifications de la résidence des données Les menaces changent. Certains des principaux avantages qu'une solution de centre de données hybride peut offrir reposent sur la résilience. peu importe le changement apporté.

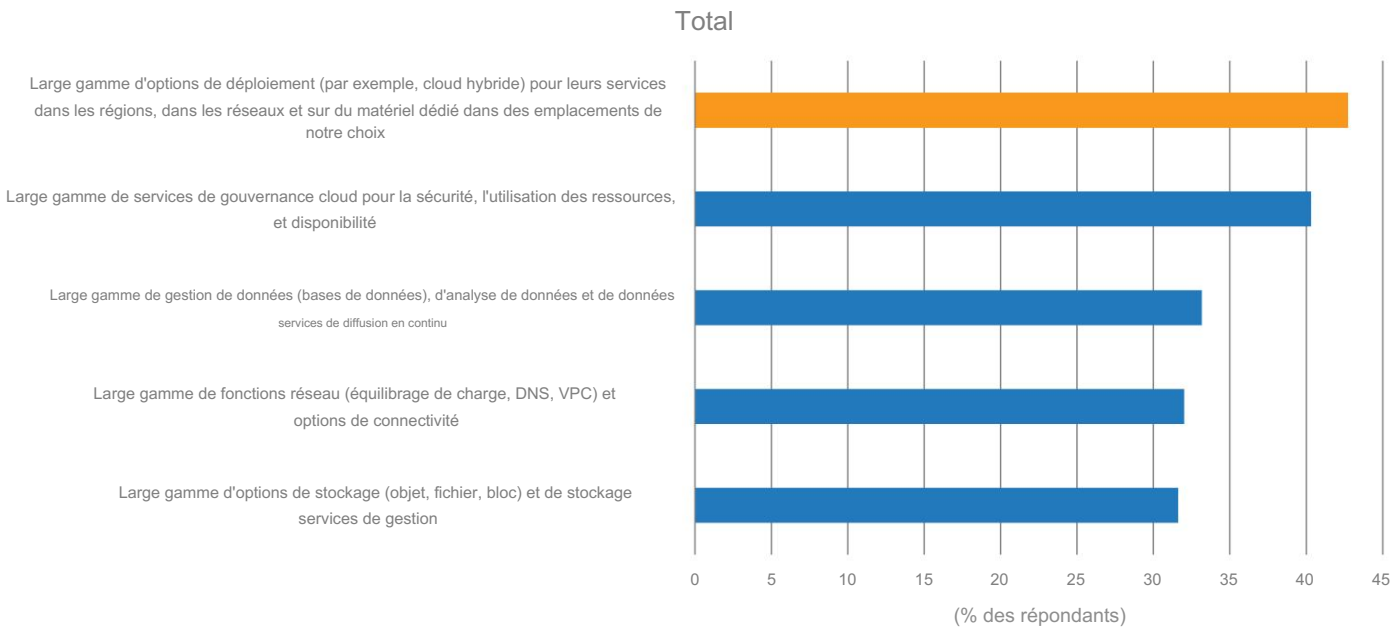
Avantages d'une solution de centre de données hybride

Une solution de centre de données hybride offre aux organisations une opportunité unique d'optimiser et de sécuriser leurs environnements sur le plan opérationnel. Cela commence par réduire la complexité de la gestion de plusieurs environnements cloud en transformant les processus commerciaux et de développement d'une organisation. Dans ce scénario, une solution de centre de données hybride peut étendre l'architecture, les règles et les politiques partagées du cloud privé au cloud public.

Les infrastructures changent. Modifications de la résidence des données. Les menaces changent. Certains des principaux avantages qu'une solution de centre de données hybride peut offrir reposent sur la résilience, quel que soit le changement apporté. Pour se préparer à de nouvelles perturbations de l'activité, les organisations ont besoin de plans, d'outils et des partenaires appropriés pour leur permettre de s'adapter rapidement plutôt que de réagir (voir Figure 2).

FIGURE 2 : Principaux services cloud

Q Parmi les portefeuilles de services/options suivants, lesquels sont les plus importants dans votre choix d'une plate-forme cloud principale pour soutenir vos plans de transformation numérique ? Ils proposent un…



n = 198

Source : Enquête d'IDC sur la résilience et les dépenses futures des entreprises, vague 7, juillet 2021.

» La portabilité et la résilience face à l'évolution des conditions commerciales mondiales sont aujourd'hui fondamentales dans les affaires. Les organisations doivent envisager le cloud de manière globale pour répondre à ces exigences d'élasticité. Solutions de datacenter hybrides Répondez à ce besoin en utilisant la virtualisation et en vous concentrant sur une sécurité flexible et évolutive.

» Une visibilité, des politiques et des contrôles centralisés unifiés sont nécessaires pour garantir la santé et la sécurité du système. les données clients du cloud privé du datacenter vers le cloud public IaaS, platform as a service (PaaS)(conteneurs), fonctionner en tant que service (FaaS) (sans serveur) ou SaaS. Ce besoin s'est accru compte tenu de la nature distribuée des environnements SaaS et de l'environnement de travail depuis n'importe où.

» Les centres de données hybrides modernes utilisent des plates-formes basées sur le cloud pour fournir une gestion et une réponse automatisées aux menaces grâce à l'intelligence artificielle et à l'apprentissage automatique. Ces politiques de sécurité non seulement rationalisent et augmentent l'efficacité des équipes opérationnelles, mais réduisent également le besoin de contrôles manuels des modifications, réduisant ainsi le risque d'erreur humaine et de violations.

» La redondance et le contrôle des catastrophes font partie de la structure du centre de données hybride.

La pénurie de talents en cybersécurité a été encore aggravée par la pandémie. Les équipes informatiques ont été mises à rude épreuve et IDC a observé que les rôles traditionnels (par exemple, les administrateurs du service d'assistance) consacrent désormais du temps à des tâches informatiques non traditionnelles telles que la cybersécurité. Tirer parti du cloud signifie que les professionnels de la sécurité auront le temps de faire le tri alertes et violations tout en laissant les autres fonctions de niveau 1 au fournisseur de services cloud. Chaque fois que les organisations parviennent à réduire les risques et la complexité, c'est une victoire.

Pour maintenir le rythme de l'innovation afin de protéger les charges de travail contre les menaces et les vulnérabilités, la facilité d'utilisation, la compatibilité avec les outils de gestion des cyber-risques existants et la facilité de mise en œuvre de la sécurité à mesure que de nouvelles charges de travail sont instanciées en développement et en production sont essentielles.

Principales tendances

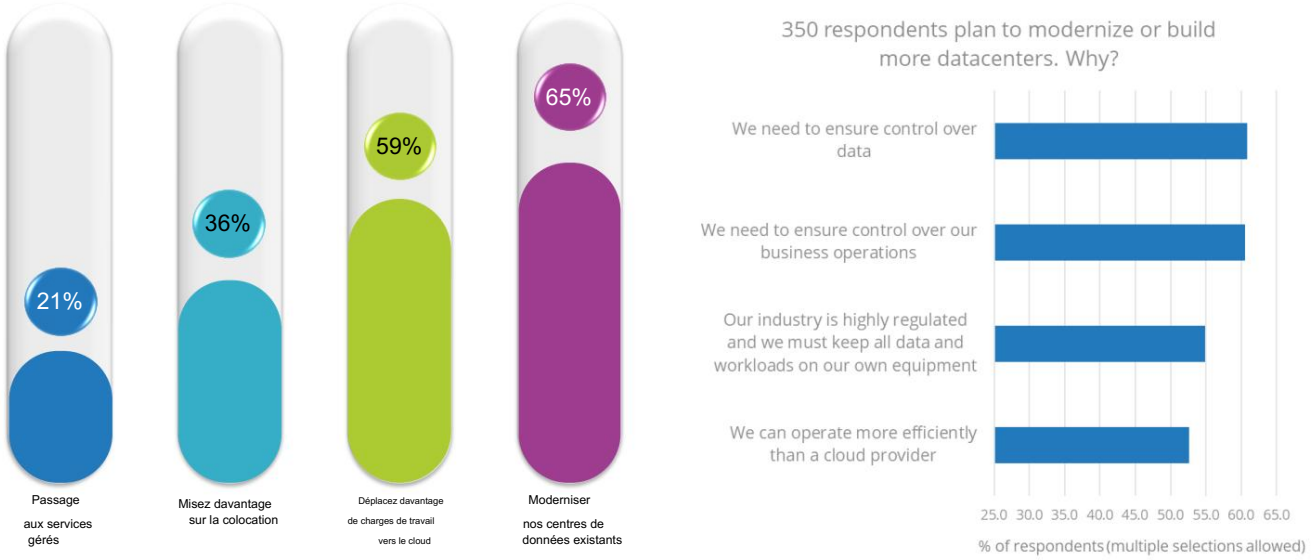
Les investissements dans la transformation numérique suivent le rythme des dépenses pré-pandémiques, voire les dépassent dans certains cas. Mais qui sont les décideurs, et quelles sont les activités d'investissement et d'optimisation des coûts ?

La transformation numérique a ouvert la voie à un nouvel ensemble d'acheteurs de technologies. Selon le guide mondial des dépenses informatiques d'IDC, 50 % des dépenses technologiques proviennent de l'extérieur du service informatique et sont pilotées par les acheteurs du secteur d'activité (LOB). En général, ils donnent la priorité à la création de revenus, à une bonne expérience client et à la réduction des coûts. Dans le futur d'août 2021 d'IDC Enquête sur la résilience et les dépenses des entreprises, vague 8 : 774 personnes interrogées ont répondu à la question suivante : à la suite des développements survenus pendant la pandémie de COVID-19, comment évalueriez-vous où se situe votre organisation en ce qui concerne sa transformation numérique par rapport à ses pairs ? La majorité des personnes interrogées (29,5 %) ont indiqué que leurs initiatives DX sont lancées au niveau de la fonction ou du secteur d'activité, avec un certain lien avec la stratégie de l'entreprise. IDC a également constaté que les responsables de la sécurité de l'information (RSSI) sont rarement inclus dans les discussions sur le DX. Cela semble être une tendance que les organisations devraient explorer.

Les activités cloud et datacenter sont liées. Comme le montre la figure 3, les ressources sont allouées sur la base d'un plan quinquennal pour la plupart des organisations qui élaborent leurs stratégies de plate-forme cloud et de centre de données. Dans l'enquête opérationnelle sur les centres de données 2021 d'IDC menée auprès de 400 personnes interrogées, 59 % des entreprises déplaceront davantage de charges de travail vers le cloud, tandis que 65 % moderniseront leurs centres de données existants. Les organisations savent qu'elles sont aussi fortes que leur maillon le plus faible. Ces actions démontrent la valeur et la confiance accordées au modèle de centre de données hybride.

FIGURE 3 : Le plan quinquennal concerne le cloud et le centre de données

Q Au cours des cinq prochaines années, votre organisation fera-t-elle l'une des choses suivantes ?



n = 400

Source : Enquête opérationnelle sur les centres de données d'IDC, 2021

La dernière tendance, celle sur laquelle nous nous concentrons le plus, est l'augmentation des violations dans les organisations disposant de plusieurs environnements cloud IaaS et la manière dont ces violations de sécurité sont en corrélation positive avec le temps écoulé dans les alertes triées. Moins il y a de violations, plus le temps de réponse augmente en une heure et vice versa. Cela est logique étant donné la pénurie de talents et l'augmentation des violations dues aux logiciels malveillants avancés, qui incluent les ransomwares en tant que service.

Considérant Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. est un fournisseur majeur de solutions de cybersécurité auprès de plus de 100 000 gouvernements et entreprises dans le monde. Ses solutions protègent les entreprises clientes contre les cyberattaques multivecteurs sophistiquées de cinquième génération avec un taux de capture substantiel sur les logiciels malveillants, les ransomwares et d'autres types d'attaques.

Le portefeuille Check Point Hybrid Datacenter permet aux clients de bénéficier des avantages de la consolidation en sécurisant leurs environnements cloud et datacenter sous un seul fournisseur en utilisant une approche DevSecOps dès la première étape, orchestrée à partir de la plateforme de gestion unifiée de la sécurité Infinity-Vision. Cette plateforme offre une approche plus conviviale et gère de manière centralisée l'architecture du centre de données hybride à partir d'un seul panneau de verre. Ce système unifié est également extensible à l'aide des API RESTful, qui fournissent un cadre pour automatiser la sécurité et les réponses aux menaces.

L'innovation clé pour cloudifier le centre de données est l'architecture de sécurité réseau hyperscale Quantum Maestro.
Check Point Maestro apporte l'évolutivité, l'agilité et l'élasticité du cloud sur site en maximisant la capacité de sécurité des passerelles de sécurité avec un clustering N+1 efficace basé sur la technologie brevetée HyperSync. Cela permet aux entreprises de créer leur propre cloud privé virtualisé sur site en connectant plusieurs passerelles de sécurité Check Point.
Les passerelles de sécurité peuvent être regroupées par ensemble de fonctionnalités de sécurité, par politique ou par actifs qu'elles protègent et les virtualiser davantage grâce à la technologie des systèmes virtuels.

L'architecture de sécurité réseau Quantum MaestroHyperscale évolue à mesure que les exigences commerciales et techniques évoluent.
Qu'une entreprise soit connectée au cloud public via le haut débit ou qu'elle commence tout juste le processus de migration vers le cloud DX, Quantum Maestro est conçu pour fournir une protection avancée contre les menaces, une redondance améliorée, un provisionnement automatique des pare-feu et une sécurité intégrée, le tout dans un souci de consolidation, conduisant à une plus petite empreinte du centre de données.

Alors que les utilisateurs ont besoin de davantage d'applications SaaS dans le cloud, telles que la messagerie électronique, la productivité au bureau et la vidéoconférence, Check Point Harmony Connect est conçu pour insérer la sécurité dans cette communication. Harmony Connect est le canal permettant de rendre l'architecture et les applications sur site disponibles dans le cloud avec le même regarder et sentir.
Les protections supplémentaires disponibles par Harmony incluent des solutions de sécurité pour les points finaux et mobiles qui s'étendent à l'environnement de travail depuis n'importe où. Une fois qu'une organisation migre vers le cloud et utilise une approche DevOps, Check Point CloudGuard est introduit pour offrir :

- » Sécurité des réseaux privés et publics
- » Gestion de la posture de sécurité du cloud
- » Protection des charges de travail (conteneurs et sans serveur)
- » Protection des applications Web et des API
- » Intelligence cloud et chasse aux menaces

Les organisations peuvent également exploiter Check Point Infinity SOC pour une détection et une réponse avancées aux incidents, ainsi que la base de données mondiale des menaces ThreatCloud de Check Point, qui consolide les menaces locales sur le réseau et mondiales. Grâce à ThreatCloud, Check Point exploite les données anonymisées sur les menaces provenant de ses propres appliances et de ressources externes telles que les forces de l'ordre pour collecter et améliorer les renseignements sur les menaces. Les tableaux de bord et les mesures de sécurité proposés dans Infinity SOC sont également utilisés par l'équipe de recherche de Check Point en interne. Les avantages de ces plateformes incluent l'élimination des faux positifs et des alertes redondantes et, surtout, la libération d'un personnel précieux.

Check Point se différencie du reste du marché en continuant à innover, en ajoutant des partenaires dans l'écosystème et en comblant les lacunes en matière de cybersécurité grâce à des acquisitions stratégiques, plus récemment Avanan. L'intégration d'Avanan dans le portefeuille Check Point fournit une offre de sécurité de messagerie sécurisée conçue pour protéger le personnel distant.

Défis

Check Point a réussi sur le marché de la sécurité des centres de données et des réseaux sur site avec la famille d'appliances de sécurité Quantum, MaestroHyperscale Security Orchestrator et Infinity-Vision Unified Security Management. À mesure que de plus en plus d'entreprises adoptent l'architecture de centre de données hybride, Check Point bénéficierait de la poursuite du développement de ses produits et services de sécurité cloud. Check Point a récemment élargi ses offres de sécurité CloudGuard avec des acquisitions telles que Dome9 pour la gestion de la posture, Protego pour le sans serveur et Avanan pour la sécurité de la messagerie. Check Point est récemment entré sur le marché de la sécurité des conteneurs cloud, mais sa première version manquait de contrôle des applications. La sécurité des conteneurs Check Point offre un filtrage d'URL, une prévention des menaces et une politique d'accès autonome. Check Point devrait continuer à étendre les fonctionnalités de sécurité du cloud pour les applications, les API et les microservices, y compris les conteneurs et les fonctions sans serveur.

Conclusion

IDC estime que le centre de données hybride constitue le « meilleur des deux mondes », tirant parti des services et innovations modernes des centres de données et du cloud hybride. Alors que les entreprises entament leur transition vers la modernisation et le cloud, elles feraient bien de travailler avec un fournisseur qui contribuera à faciliter un plan pluriannuel et qui valorise une approche DevSecOps et reconnaît que les mesures de performance doivent inclure la confiance comme élément clé. Le marché des centres de données hybrides continuera de croître avec le cloud hybride. Étant donné que le portefeuille de sécurité des centres de données hybrides de Check Point permet aux entreprises de sécuriser en toute confiance En intégrant leurs environnements cloud et de centre de données sous un seul système de gestion de sécurité unifié, l'entreprise dispose d'une opportunité significative de réussite continue.

À propos de l'analyste

Philippe Bues, Gestionnaire de recherche, sécurité cloud

Phil Bues est le responsable de recherche pour la pratique Cloud Security d'IDC. Dans ce rôle, Phil dirige la recherche, assure un leadership éclairé et conseille les clients sur des questions complexes, notamment la cybersécurité du cloud et dans le cloud. Son commentaire aborde les avantages et les défis de ce qu'on appelle le modèle de responsabilité partagée et la manière dont cette ligne pourrait changer à l'avenir.

MESSAGE DU COMMANDITAIRE

À propos du logiciel Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) est l'un des principaux fournisseurs de solutions de cybersécurité qui protège plus de 100 000 organisations de toutes tailles. Ses solutions protègent les entreprises contre les cyberattaques de 5e génération avec un taux de capture parmi les meilleurs du secteur contre les logiciels malveillants, les ransomwares et d'autres types d'attaques. Check Point propose son architecture de sécurité multiniveau Infinity Total Protection avec prévention des menaces contre les cyberattaques avancées de génération V. La sécurité de Check Point défend les centres de données d'entreprise, le cloud, les réseaux, les appareils mobiles, les points finaux et l'IoT. Check Point fournit le système de gestion de sécurité unifié à point de contrôle le plus complet et le plus intuitif.

Déterminez dès aujourd'hui les risques de sécurité de votre centre de données, de votre réseau et du cloud grâce à une évaluation gratuite de la sécurité de votre centre de données hybride sur https://www.checkpoint.com/solutions/data-center-security/

IDC Custom Solutions

Le contenu de cet article a été adapté de recherches existantes d'IDC publiées sur www.idc.com.

IDC Recherche, Inc.

140, rue Kendrick

Bâtiment B

Needham, MA 02494, États-Unis

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com