riverbed

LIVRE BLANC

Intégrez la résilience d'entreprise avec le portefeuille de solutions de gestion des performances réseau d'Alluvio

Les réseaux évoluent rapidement pour faire face à une succession sans fin de défis externes, tels que le passage au télétravail en réponse à la pandémie, ainsi qu'à des objectifs internes, tels que l'augmentation des performances et de la capacité avec des budgets stagnants. Pour y répondre, les équipes NetOps doivent s'adapter et innover, aujourd'hui plus que jamais. C'est le moteur de ce que l'on appelle la résilience d'entreprise. L'Organisation internationale de normalisation (ISO) définit la résilience organisationnelle ou d'entreprise comme suit : « La capacité d'une organisation à absorber et à s'adapter à un environnement changeant pour lui permettre d'atteindre ses objectifs, de survivre et de prospérer. »

Les réseaux hybrides modernes continuent d'évoluer rapidement en réponse aux défis internes et externes. Le rythme du changement a mis à l'épreuve les fondements de la résilience d'entreprise, et les exigences en matière de flexibilité n'ont fait que croître avec l'avènement des réseaux hybrides et l'adoption du SaaS. Les équipes IT font l'objet d'une attention constante pour mener à bien la transformation opérationnelle. Un échec à cet égard peut entraîner une perte de revenus, une désaffection de la clientèle, une perception négative de la marque et une perte de vitesse par rapport aux concurrents qui gèrent avec agilité les défis externes et internes. En outre, de plus en plus d'entreprises commencent à prendre conscience de l'importance de l'évolution de leurs activités : l'enquête de l'Enterprise Strategy Group (ESG) sur les intentions de dépenses technologiques pour 2023 a révélé que plus de 28 % des professionnels NetOps interrogés ont cité l'amélioration de la résilience opérationnelle contre les cyberattaques comme l'un de leurs principaux postes de dépenses pour 2023. L'amélioration de la résilience opérationnelle arrive juste après l'amélioration de l'expérience client (32 %), l'analyse des données (30 %) et l'automatisation (29 %).

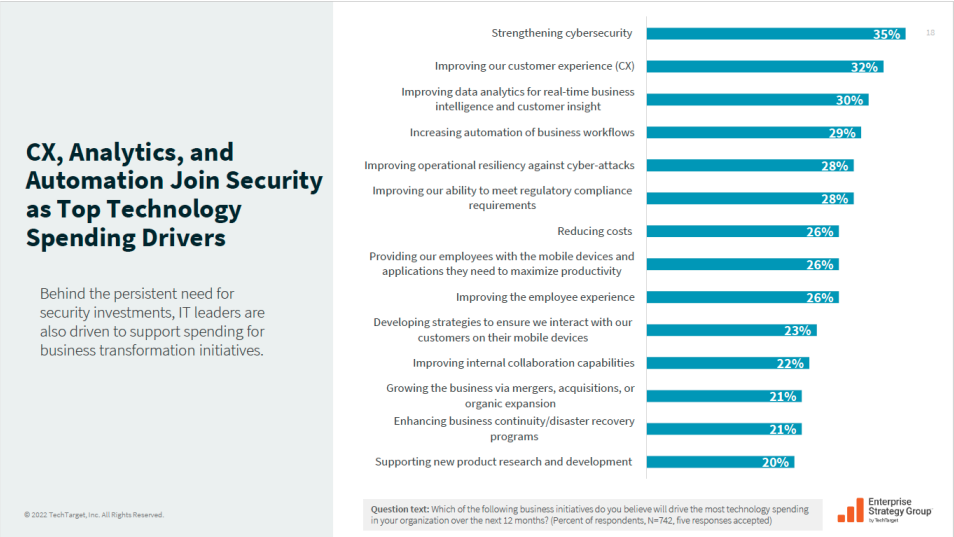

Figure 1 Enquête de l'ESG sur les intentions de dépenses technologiques pour 2023

Les changements opérationnels dans un environnement informatique hybride peuvent être très différents selon votre organisation, votre secteur et les besoins de votre équipe. Ce problème est accentué par le fait que les réseaux modernes ont évolué tout en continuant à s'appuyer sur une infrastructure IT ancienne. Toutefois, le processus de renforcement de la résilience d'entreprise, quelle que soit la forme ou la taille de votre organisation, est en grande partie le même. Tout d'abord, vous devez identifier les défis auxquels votre réseau hybride est confronté. Ensuite, vous devez aborder chaque aspect, en identifiant les solutions et les processus opérationnels que votre équipe peut adopter pour relever les défis tout en améliorant votre réseau hybride. Dans ce document, nous passerons en revue les défis les plus courants auxquels sont confrontés les réseaux modernes, ainsi que trois domaines que les organisations peuvent améliorer pour renforcer la résilience de leurs réseaux.

Le défi des réseaux hybrides

La plupart des réseaux hybrides sont le résultat d'une mise à niveau des technologies de réseau au coup par coup. Étant donné qu'il est trop coûteux et perturbant de tout mettre à niveau en même temps, les entreprises introduisent souvent de nouvelles technologies tout en abandonnant progressivement les anciennes. Si cette approche au coup par coup est courante (et compréhensible), elle s'accompagne souvent de difficultés qui introduisent de la fragilité plutôt que la résilience.

La transition vers le télétravail s'accompagne de lacunes en matière de visibilité

L'hybridation des réseaux n'est pas nouvelle, mais elle a connu un essor considérable pendant la pandémie, les équipes NetOps s'étant empressées de faire évoluer rapidement leurs réseaux pour prendre en charge le télétravail. Cela a souvent créé des lacunes en matière de visibilité, de conformité et de sécurité du réseau. Par exemple, les technologies patrimoniales sur site peuvent avoir des exigences de sécurité différentes de celles des systèmes basés sur le cloud. Si l'équipe NetOps ne le remarque pas, les cybercriminels peuvent plus facilement exploiter les failles de sécurité.

Préoccupations en matière de ressources

En raison du manque de main-d'œuvre, de temps ou d'argent, la mise en place d'un réseau performant, et a fortiori résilient, est difficile. La situation est devenue un problème dans tout le secteur. Dans le récent rapport de l'ESG sur les intentions de dépenses technologiques pour 2023, 54 % des professionnels de l'IT citent les inefficacités opérationnelles comme la principale motivation des initiatives de transformation digitale.

Non seulement ce manque de ressources est difficile à supporter pour les équipes NetOps, mais il rend également de nombreux réseaux hybrides vulnérables. En raison du manque de ressources appropriées, les équipes peinent à trouver les stratégies proactives nécessaires pour assurer le fonctionnement des réseaux hybrides complexes, et a fortiori leur résilience. En conséquence, de nombreuses équipes NetOps, confrontées à un réseau de plus en plus complexe et à des ressources limitées, passent tout leur temps à gérer des urgences.

Gestion des performances réseau : les bases de la résilience d'entreprise

La première mesure que toutes les organisations devraient prendre pour améliorer la résilience de leurs réseaux hybrides est de mettre en œuvre une solution NPM robuste. La gestion des performances réseau (NPM) est une approche proactive de la visualisation, de la surveillance, de l'optimisation, du diagnostic et du reporting sur la santé et la disponibilité de votre réseau. Elle recommande une combinaison d'outils et de processus opérationnels que les équipes peuvent adopter pour détecter rapidement les zones problématiques dans leur réseau hybride et les corriger, et pour positionner leur réseau de manière à traiter et à éviter ces problèmes à l'avenir. Une équipe qui utilise correctement la NPM dans son réseau hybride peut s'attendre à relever des défis internes et externes tout en atteignant ses objectifs de croissance et de performance. Mais les équipes NetOps font souvent l'erreur de privilégier la rapidité des informations par rapport à leur niveau de détail. Or, rapidité n'est pas synonyme d'exhaustivité et il arrive souvent que des détails importants susceptibles d'avoir un impact sur votre réseau soient omis.

La croissance des réseaux hybrides en chiffres :

- Les bureaux/sites distants se multiplient : 35 % des organisations disposent de 25 à 100 bureaux/sites distants dans le monde*
- L'utilisation du multicloud est en augmentation : 40 % des entreprises utilisent au moins trois fournisseurs de clouds publics**
- Complexité des réseaux après la pandémie : 33 % des professionnels de l'IT déclarent que leur environnement réseau est plus complexe qu'avant la pandémie***

Enterprise Strategy Group (ESG), End-to-end Network Visibility and Management Trends

* Combien de bureaux/sites distants votre entreprise exploite-t-elle dans le monde ? Combien de personnes votre organisation devrait-elle compter dans 24 mois ?
** Combien de fournisseurs de services d'infrastructure de cloud public votre organisation utilise-t-elle actuellement ?
*** D'une manière générale, quelle est la complexité de l'environnement réseau de bout en bout de votre organisation par rapport à il y a deux ans ?

Comment intégrer la résilience d'entreprise dans vos réseaux hybrides ?

Comme nous l'avons déjà évoqué, la résilience réseau ne se traduit pas de la même façon pour toutes les entreprises. Cependant, voici trois domaines de préoccupation communs pour les équipes NetOps qui gèrent des réseaux hybrides, et comment la NPM peut les aider à renforcer la résilience d'entreprise dans chacun d'entre eux.

Performances

Si tous les types de réseaux sont confrontés à des problèmes de performance courants liés au dysfonctionnement d'équipements, à l'utilisation intensive de la bande passante et aux problèmes de DNS, les réseaux hybrides présentent des caractéristiques uniques en matière de gestion et d'amélioration de la performance réseau. L'optimisation de votre réseau hybride pour améliorer les performances est un élément clé de la résilience d'entreprise. Après tout, la performance réseau est l'élément vital des organisations modernes. Si le réseau ne fonctionne pas, l'entreprise est à l'arrêt. En intégrant la résilience dans vos performances, votre entreprise peut continuer à fonctionner en toutes circonstances.

Examinons quelques problèmes qui affectent les performances des réseaux hybrides et où la NPM peut intervenir.

Manque de visibilité

Lorsqu'une équipe NetOps manque de visibilité sur ses applications, ses serveurs et ses environnements cloud-native, elle n'est pas en mesure de diagnostiquer correctement les problèmes de réseau tels que les menaces de sécurité non contrôlées, les ralentissements d'application et autres problèmes de performance. La rapidité et la clarté des informations fournies peuvent faire la différence pour éviter une panne importante. Pour les réseaux hybrides, le manque de visibilité est souvent dû à la latence. Cela se produit lorsque les informations sont trop sommaires et omettent des détails essentiels, lorsqu'elles sont trop lentes pour permettre aux équipes de réagir ou lorsqu'elles proviennent de sources ou d'outils cloisonnés qui fournissent des données contradictoires ou incomplètes. Dans le rapport EMA, Network Observability: Delivering Actionable Insights to Network Operations, 46 % des professionnels NetOps ont cité les conflits de données entre les différents outils comme l'un des principaux défis liés aux données dans leur ensemble d'outils NetOps.

Pourquoi la visibilité est importante :

- **68 %** des professionnels de l'IT déclarent que la visibilité unifiée est **très importante** dans leur environnement réseau. *

* Enterprise Strategy Group (ESG) - Tendances en matière de visibilité et de gestion du réseau

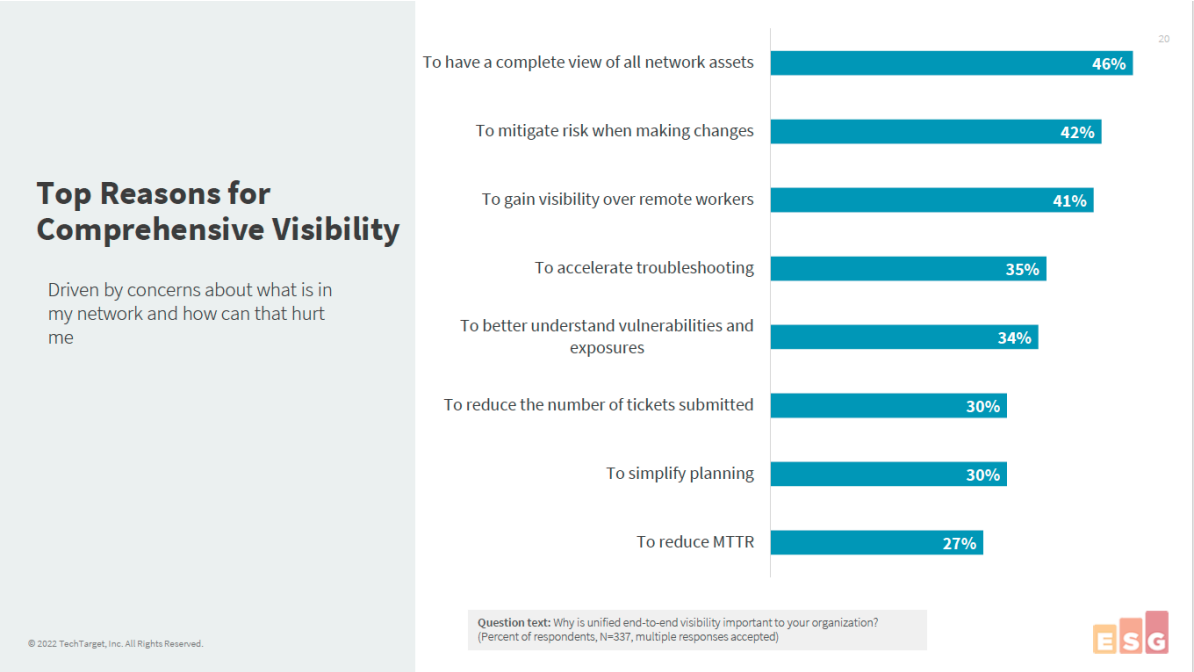

Figure 2 Enterprise Strategy Group (ESG) - Tendances en matière de visibilité et de gestion du réseau

- **42 %** pensent qu'une visibilité complète permet de réduire les risques lors des changements.
- **35 %** pensent qu'une visibilité complète accélère le diagnostic.
- **34 %** pensent qu'une visibilité complète aide les équipes IT à mieux comprendre les vulnérabilités et les risques.

Croissance exponentielle des données

Les réseaux hybrides génèrent et traitent plus de données que jamais. Selon un rapport publié par Statista, la quantité totale de données mondiales devrait doubler au cours des cinq prochaines années, passant de 64,2 à 180 zettaoctets. Des capacités de traitement inadéquates dans votre réseau hybride peuvent entraîner une congestion du réseau, une surcharge des nœuds du réseau et une perte de paquets. La perte de paquets peut se solder par une interruption du réseau, un ralentissement du service et même une perte de connectivité du réseau.

NPM et performance

L'optimisation de la performance des réseaux hybrides est essentielle pour améliorer la résilience d'entreprise. Les solutions NPM offrent aux équipes NetOps la possibilité d'accéder aux mesures cruciales des appareils, aux données de flux du réseau et aux données de paquets, éliminant ainsi toute confusion et mettant en lumière les zones d'ombre du réseau afin de diagnostiquer avec précision et résoudre les problèmes plus rapidement. Sans accès à une télémétrie NPM complète, il est impossible de voir les problèmes de performance ou de les résoudre à temps. Dans l'idéal, optez pour des outils NPM capables de s'adapter au volume croissant de données généré et absorbé par votre réseau hybride.

Conformité

La conformité de votre réseau hybride dépend de votre secteur d'activité : par exemple, les secteurs très réglementés tels que les services publics, médicaux et financiers ont généralement des exigences plus strictes. Le respect scrupuleux des normes de sécurité et d'exploitation est toutefois une nécessité dans une certaine mesure pour tous les réseaux hybrides.

Lorsque votre réseau ne répond pas aux exigences de conformité internes et externes, vous risquez de créer des failles de sécurité et d'encourir des amendes. Un réseau hybride géré activement selon des normes opérationnelles et de sécurité est toutefois capable de rester conforme, même en cas de perturbation du réseau, et de s'adapter en maintenant efficacement la résilience des applications/services plus anciens lors de l'introduction de nouvelles technologies.

Pourquoi les réseaux hybrides se heurtent-ils à des problèmes de conformité et quelles en sont les conséquences pour la résilience d'entreprise ?

Les entreprises sont souvent confrontées à des problèmes de conformité parce que les services cloud et sur site de leurs réseaux hybrides sont pris en charge par des fournisseurs tiers. La diversité des fournisseurs peut rendre difficiles la création de pistes d'audit, l'exécution de mises à jour en temps voulu, l'établissement de règles claires de gouvernance des données et l'accomplissement d'autres tâches faisant partie intégrante des exigences de conformité internes et externes. Les entreprises qui ne sont pas résilientes dans ce domaine s'exposent à des interruptions d'activité, à des pertes de productivité, à des pénalités et à des atteintes à leur réputation. Les entreprises, quel que soit leur secteur d'activité, dépensent des millions pour résoudre les problèmes de conformité.

NPM et conformité

Les organisations se contrôlent elles-mêmes en interne et suivent les réglementations gouvernementales en matière de conformité. Ces normes internes et externes fournissent une orientation, une supervision et une structure essentielles à leurs réseaux. Bien que les produits NPM offrent une visibilité sur le réseau, négliger la conformité de ces produits peut avoir un impact négatif sur cette visibilité et, en fin de compte, sur les performances réseau. Un manque de visibilité peut entraîner un certain nombre de problèmes, notamment des ralentissements et des arrêts.

Sécurité

Le concept de résilience d'entreprise est axé sur l'adaptation. Or, l'adaptation à l'évolution des besoins de sécurité de votre réseau hybride peut s'avérer difficile. Contrairement à un réseau standard, les workflows des réseaux hybrides combinent à la fois des data centers physiques et des environnements cloud, ainsi que des utilisateurs accédant à des applications à partir de différents équipements et emplacements. Tous ces éléments, ainsi que les données qui y transitent, doivent être protégés. En améliorant la sécurité de votre réseau et en le rendant plus adaptable, vous êtes mieux armés pour faire face aux menaces qui évoluent rapidement. Non seulement vous résisterez mieux aux attaques potentielles en vous rétablissant plus rapidement et en subissant moins de dommages, mais vous pourrez aussi en éviter d'autres.

Vulnérabilité des réseaux hybrides

La complexité des réseaux hybrides peut les rendre plus vulnérables aux attaques. Les services dans le cloud, une caractéristique commune des réseaux hybrides, posent des problèmes de sécurité supplémentaires, tels que des points de contrôle d'accès non sécurisés et une mauvaise configuration du système de sécurité. Les probabilités de violation des données augmentent avec la multiplication des menaces. En fait, 45 % des entreprises ont été victimes d'une violation de données dans le cloud au cours des 12 derniers mois. Les violations de données et les attaques de systèmes sont coûteuses. Aux États-Unis, ces violations coûtent environ 9,44 millions de dollars à une entreprise de taille intermédiaire. Ce chiffre augmente en moyenne de 1 million de dollars lorsque le télétravail est à l'origine de la violation, sans compter d'autres conséquences telles que la perte de revenus due à l'expérience négative des clients, ainsi que la responsabilité juridique.

NPM et sécurité

Les solutions NPM offrent des recommandations en matière de surveillance, de visualisation et de reporting, qui aident les équipes NetOps et SecOps à détecter les failles de sécurité et à y remédier plus rapidement. Ces recommandations permettent également aux équipes de disposer de données forensiques, ce qui leur donne la visibilité nécessaire pour être proactives dans un environnement extrêmement complexe et pour arrêter les menaces plus tôt.

Renforcer la résilience d'entreprise grâce au portefeuille de solutions de gestion des performances réseau (NPM) d'Alluvio

Les grandes entreprises travaillent souvent avec plusieurs outils NPM, ce qui est non seulement onéreux, mais aussi source de problèmes de communication (différentes équipes utilisant différents outils au sein de l'organisation). Cela peut avoir un impact sur la capacité d'une équipe à développer la résilience. Chaque équipe évalue des ensembles de données différents, identifie des problèmes et des solutions différents et travaille en vase clos.

Votre équipe a besoin d'une solution unique et interopérable qui fournira les performances, la conformité et la sécurité nécessaires pour offrir une expérience digitale cohérente sur l'ensemble du réseau hybride de votre organisation. Le portefeuille NPM d'Alluvio peut vous aider à éliminer les technologies superflues et à améliorer la communication entre vos équipes. Il contient les applications AppResponse, NetProfiler, NetIM et Portal. Ces produits fonctionnent ensemble pour aider votre équipe à créer un environnement IT agile, capable de répondre aux nouvelles exigences métier et d'évoluer rapidement, tout en accélérant l'information et en améliorant l'intégration pour de meilleures performances.

Alluvio AppResponse

- Analyse du réseau et des applications par paquets pour un diagnostic rapide
- Déploiement sur site et dans des environnements de clouds privés et publics
- Conception modulaire permettant d'accéder rapidement à des données et à des mesures de performance pertinentes
- Workflows de diagnostic rationalisés et analyse les données haute fidélité pour mieux diagnostiquer les causes profondes en quelques minutes

Alluvio NetProfiler

- Visibilité de bout en bout du trafic du réseau hybride
- Accès rapide aux données relatives au trafic : quantité de trafic, utilisateurs, flux et priorisation du trafic

Alluvio NetIM

- Automatisation des analyses et surveillance de l'infrastructure en temps réel
- Perspective globale du réseau éliminant les angles morts

Alluvio Portal

- Tableau de bord centralisé permettant aux équipes d'accéder facilement aux données de performance du réseau hybride
- Élimine la frustration liée à la production de données contradictoires par plusieurs outils et permet une meilleure communication/collaboration entre les équipes

Améliorer la visibilité et les performances de votre réseau

Les organisations font souvent état de problèmes pour connecter les travailleurs aux ressources de l'entreprise, que ce soit sur site, sur le campus, dans une succursale ou dans le cloud. La gestion des performances est essentielle pour que les travailleurs restent connectés dans un réseau hybride et pour améliorer l'expérience digitale de l'utilisateur final. La performance du réseau est intrinsèquement liée à celle du produit. Une visibilité complète en temps réel est essentielle pour identifier et prévenir les problèmes de performance réseau susceptibles d'affecter l'activité de l'entreprise. Le portefeuille Alluvio™ a évolué pour inclure les améliorations de performance des produits suivants :

Alluvio™ AppResponse :

- Augmentation de 50 % de l'écriture sur disque de la capture de paquets (WTD), qui passe de 20 Gbit/s à 30 Gbit/s pour l'appliance 8180
- Évolutivité, visibilité et capacité accrues du cloud
- Meilleures performances pour l'intégration de NetProfiler
- Prise en charge d'Oracle 19c

Alluvio™ NetProfiler :

- Augmentation de plus de 30 % de la capacité de flux, qui passe de 30 à 40 millions de flux par minute
- Prise en charge de Google VPC et SD-WAN

Alluvio™ NetIM :

- Télémétrie en continu, prise en charge de Cisco ACI et de ServiceNow

Ensemble, ces outils permettent à votre équipe de trouver et de résoudre plus rapidement les problèmes de trafic réseau, d'automatiser les workflows pour remédier rapidement aux incidents et d'accéder facilement à une analyse globale des données sur les éléments d'infrastructure dans le cloud et sur site. Le résultat est un réseau plus stable qui offre une meilleure expérience digitale à chaque utilisation.

En outre, la visibilité complète de NPM permet d'obtenir des modèles AIOps et des résultats d'automatisation plus précis. Les AIOps collectent et agrègent de grandes quantités de données interdomaines et exploitent généralement plusieurs techniques d'analyse pour obtenir les meilleurs résultats. Les sources de données d'Alluvio™ NPM fournissent des données riches et détaillées pour une identification précise des événements.

Alluvio IQ, le service SaaS d'observabilité unifiée de Riverbed, exploite les données NPM et DEM d'Alluvio, les AIOps et l'automatisation intelligente pour accélérer la réponse aux incidents et l'analyse en profondeur de la sécurité.

Assurer la gouvernance opérationnelle et la conformité

Les entreprises font aujourd'hui l'objet d'un examen minutieux en ce qui concerne les exigences de conformité, qu'elles soient imposées par l'organisation ou par le gouvernement. Trop souvent, les médias font état de fuites de données catastrophiques dans les entreprises dues à des applications ou des systèmes d'exploitation non conformes. Les cybercriminels ciblent ces vulnérabilités pour pénétrer dans le réseau et causer des dommages coûteux, voire irréparables. Comme évoqué plus haut, dans la récente enquête de l'ESG (figure 1), on a demandé à des professionnels de l'IT quelles étaient les initiatives commerciales qui entraîneraient le plus de dépenses technologiques dans leur organisation au cours des 12 prochains mois. Les initiatives de mise en conformité avec la réglementation ont été le plus souvent citées. Si votre équipe cherche à améliorer sa stratégie de sécurité ou son efficacité opérationnelle en répondant aux exigences de conformité, le portefeuille NPM d'Alluvio fournit des produits prêts pour la conformité, qui prennent en charge l'accessibilité, l'automatisation et la gestion des données.

Orchestration automatisée pour la conformité

Les entreprises des secteurs hautement réglementés, tels que les services financiers et la santé, mettent en œuvre des politiques réglementaires internes qui devancent les réglementations gouvernementales. Cette vigilance en matière de conformité s'étend également à leurs fournisseurs tiers. Les fournisseurs de produits de réseau sont censés intégrer dans leurs produits des normes de conformité organisationnelles ou gouvernementales. Avec l'orchestration automatisée, les équipes IT peuvent mettre en place, retirer et redéployer les produits NPM d'Alluvio dans un état de sécurité connu, de manière transparente. Cette fonctionnalité assure la surveillance et la gestion des données dont vous avez besoin pour atteindre et maintenir la conformité de votre réseau.

Prise en charge de la conformité gouvernementale

Le portefeuille NPM d'Alluvio évolue constamment pour prendre en charge les exigences de conformité en matière d'accessibilité, d'automatisation et de gestion des données, telles quela norme fédérale américaine de traitement de l'information [Federal Information Processing Standard (FIPS)] et laSection 508.

Utiliser des méthodes de sécurité intelligentes pour lutter contre les cybermenaces

Selon l'enquête sur les intentions de dépenses technologiques pour 2023 de l'ESG, 65 % des professionnels de l'IT prévoient de dépenser davantage pour la cybersécurité que pour tout autre domaine. De nombreuses équipes NetOps et SecOps consacrent leur budget à l'achat de solutions et d'outils de sécurité provenant de divers fournisseurs. Cela peut créer un système disparate qui empêche l'équipe IT de diagnostiquer et de résoudre rapidement les problèmes de sécurité.

Les produits NPM d'Alluvio offrent des processus automatisés de collecte, d'analyse et de détection des données afin que les équipes puissent rapidement identifier les risques potentiels que les outils de sécurité traditionnels et disparates pourraient manquer. Les outils de sécurité du portefeuille s'intègrent de manière transparente dans les processus automatisés existants de l'organisation, et favorisent la résilience d'entreprise en réduisant à la fois les risques sur le réseau et l'ampleur des événements lorsqu'ils se produisent.

Orchestration automatisée pour la sécurité

En cas de violation de la sécurité, votre réseau hybride doit rester opérationnel. Cependant, les équipes NetOps ont souvent du mal à maintenir sa disponibilité en cas d'attaque. Cela est dû à la multiplicité des équipements et des applications sur leur réseau, chacun étant géré par un fournisseur différent qui n'est pas toujours en mesure d'assurer le fonctionnement lorsque le réseau est compromis. Le portefeuille de produits NPM d'Alluvio peut être exploité et provisionné par l'orchestration automatisée, c'est-à-dire une pratique de mise à jour, d'installation, de réinitialisation, de configuration et de restauration de matériel ou d'appliances virtuelles sans intervention manuelle. Ainsi, quel que soit l'état de sécurité actuel de votre réseau, qu'il soit affecté par une attaque de ransomware externe ou compromis par des menaces internes, vous serez en mesure d'accéder à vos données NPM et de vous assurer que votre réseau est opérationnel pour les utilisateurs finaux.

Données forensiques

Les données forensiques fournies par les outils NPM établissent de meilleurs canaux de communication et de collaboration entre les équipes NetOps et SecOps. L'analyse en profondeur intelligente d'Alluvio NPM et d'Alluvio IQ permet aux équipes NetOps et SecOps d'automatiser l'identification des menaces et de réduire les risques.

Détection puissante des anomalies

La détection d'anomalies d'Alluvio NPM est soutenue par des outils d'intelligence artificielle et de machine learning (AI/ML) qui automatisent et accélèrent le processus d'analyse des données pour diagnostiquer les causes profondes, permettant ainsi à votre équipe de trouver (et de corriger) les problèmes de sécurité plus rapidement.

Données haute fidélité

Les données haute fidélité offertes par Alluvio NPM capturent chaque paquet, flux et mesure des équipements sans échantillonnage, ce qui signifie que vous pourrez détecter les problèmes de sécurité en temps réel, sans angle mort ni inconvénient lié à la multiplicité des outils tiers.

Alluvio NPM offre les éléments nécessaires à la résilience d'entreprise

Les équipes NetOps peuvent facilement être dépassées par la complexité de leurs réseaux hybrides. L'intégration de la résilience dans l'ADN de votre réseau permet de réduire la complexité et d'améliorer considérablement la capacité de votre équipe à s'adapter, à innover et même à évoluer face aux perturbations. Les organisations prennent conscience de l'importance d'une meilleure résilience d'entreprise et investissent en conséquence. En fait, lorsqu'ils sont interrogés sur la manière d'obtenir un financement pour des projets, les professionnels de l'IT citent l'amélioration de la résilience d'entreprise comme l'une des principales priorités.

Le portefeuille NPM d'Alluvio se concentre sur l'optimisation de votre réseau hybride dans trois domaines clés : la performance, la conformité et la sécurité. Chacun des trois piliers est essentiel à la construction d'un réseau plus résilient. L'optimisation des performances peut vous aider à offrir une expérience utilisateur cohérente, même en cas de perturbations. Une stratégie de sécurité plus solide et adaptable contribue à protéger votre système contre les cyberattaques et à remédier à leurs effets ; la capacité de rester en conformité évite à votre organisation de lourdes amendes. Un réseau hybride fragile est propice aux catastrophes. Le renforcement de la résilience dans chacun de ces domaines offre une meilleure visibilité de bout en bout, vous aide à exploiter des données significatives qui renforcent la collaboration transversale et aident votre équipe NetOps à être non plus réactive, mais proactive.

Prêt à renforcer la résilience d'entreprise de votre réseau hybride ?

Contactez-nous pour planifier une démonstration de gestion des performances réseau.

riverbed