

riverbed®

La NPM unifiée
pour les
opérations des
services financiers
post-COVID



Sommaire

- 3 2020 : une année de changement
- 4 Le travail à distance stimule la transformation digitale
- 5 La visibilité haute fidélité au service de la transformation digitale
- 6 Exemples de cas d'utilisation
- 8 Témoignage client dans le monde réel
- 9 Comment identifier VOTRE solution NPM
- 10 Améliorer la résilience et la sécurité du réseau avec Riverbed

2020 : une année de changement

La pandémie ayant mis en exergue les risques liés à la technologie et à l'infrastructure des entreprises...



46 %

investissent en priorité dans la mise à niveau des opérations de base et les mesures de résilience, contre 43 % en juin 2020¹



46 %

ont davantage recours à l'adoption des services gérés et du cloud¹

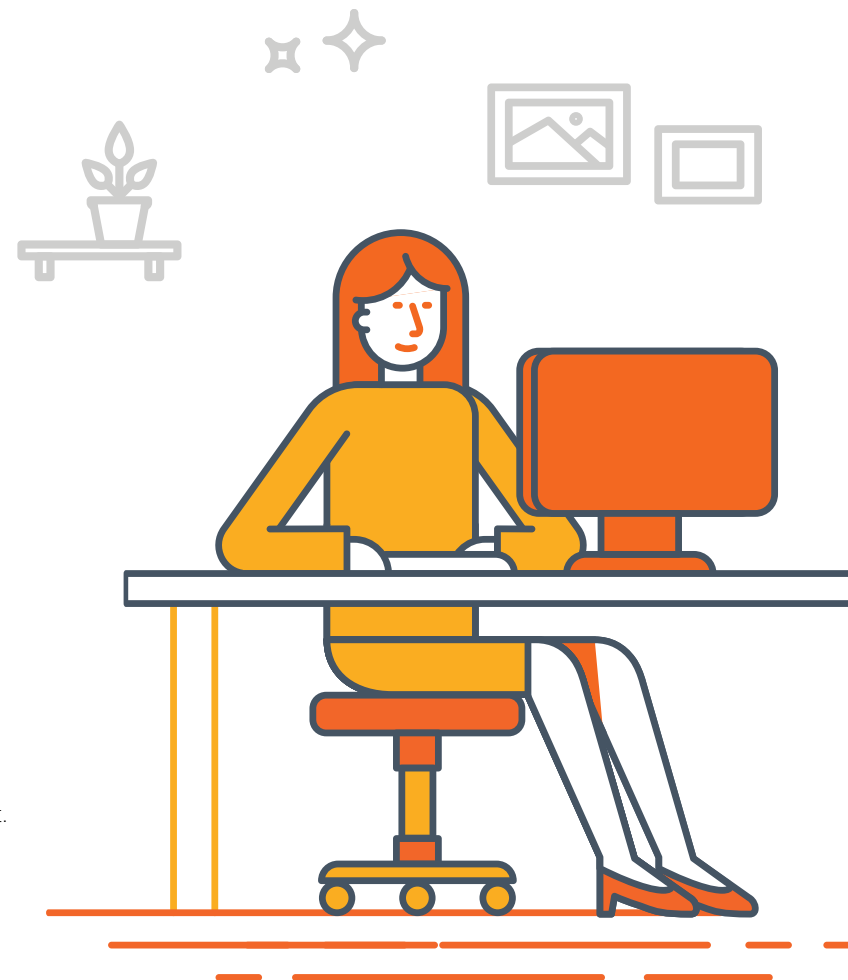


66 %

portent une attention particulière aux outils de cybersécurité, contre 49 % en juin 2020¹

La montée en flèche du travail à distance a touché des centaines de millions de personnes à travers le monde, plus de la moitié de la main-d'œuvre ayant été contrainte de rester à la maison et d'y travailler. Les équipes IT se sont démenées (d'une manière quasi héroïque) afin de permettre au personnel d'être opérationnel et de travailler en toute sécurité dans leur environnement de travail à domicile, quel qu'il soit. Pourtant, la collaboration avec certains clients en a souffert et ce changement a exposé les institutions financières à des menaces supplémentaires en matière de cybersécurité.

Seules 21 % des entreprises de services financiers déclarent souhaiter le retour de leurs employés au bureau dès que possible. Quant aux autres, il semblerait que la plupart d'entre elles aient développé une nouvelle tolérance pour le travail à distance et sont davantage susceptibles d'en tirer parti à l'avenir afin de réduire leur empreinte physique et leur structure de coûts globale.¹



Le travail à distance stimule la transformation digitale

La COVID-19 présente une opportunité d'encourager une plus grande utilisation des capacités digitales et stimule la transformation digitale. Chaque investissement en transformation digitale nécessite une surveillance renforcée afin d'assurer un bon fonctionnement tout au long de la transition et de démontrer objectivement que le ROI et les résultats commerciaux escomptés sont obtenus, et ce sur la durée.

Les clients veulent une expérience sans ruptures. Le secteur bancaire ne fait pas exception. Les plateformes omni-canaux permettent aux banques de proposer des expériences bancaires fluides de bout en bout et de capturer une vue à 360 degrés du comportement des clients sur plusieurs canaux.

L'intégration digitale des clients permet d'élargir rapidement et harmonieusement votre base de clients, et elle est essentielle pour créer une expérience qui corresponde aux générations X et Y. Elle est également stratégique pour rester à la pointe des technologies financières.

De plus, 78 % des entreprises du secteur des services financiers prévoient d'investir dans l'IA au cours des 12 prochains mois afin d'accélérer la prise de décisions dans les domaines qui dépendent de l'intervention humaine, notamment les prêts aux particuliers, le financement automobile, les cartes de crédit, etc. Cela permettra de préserver la satisfaction et la fidélité des clients.¹

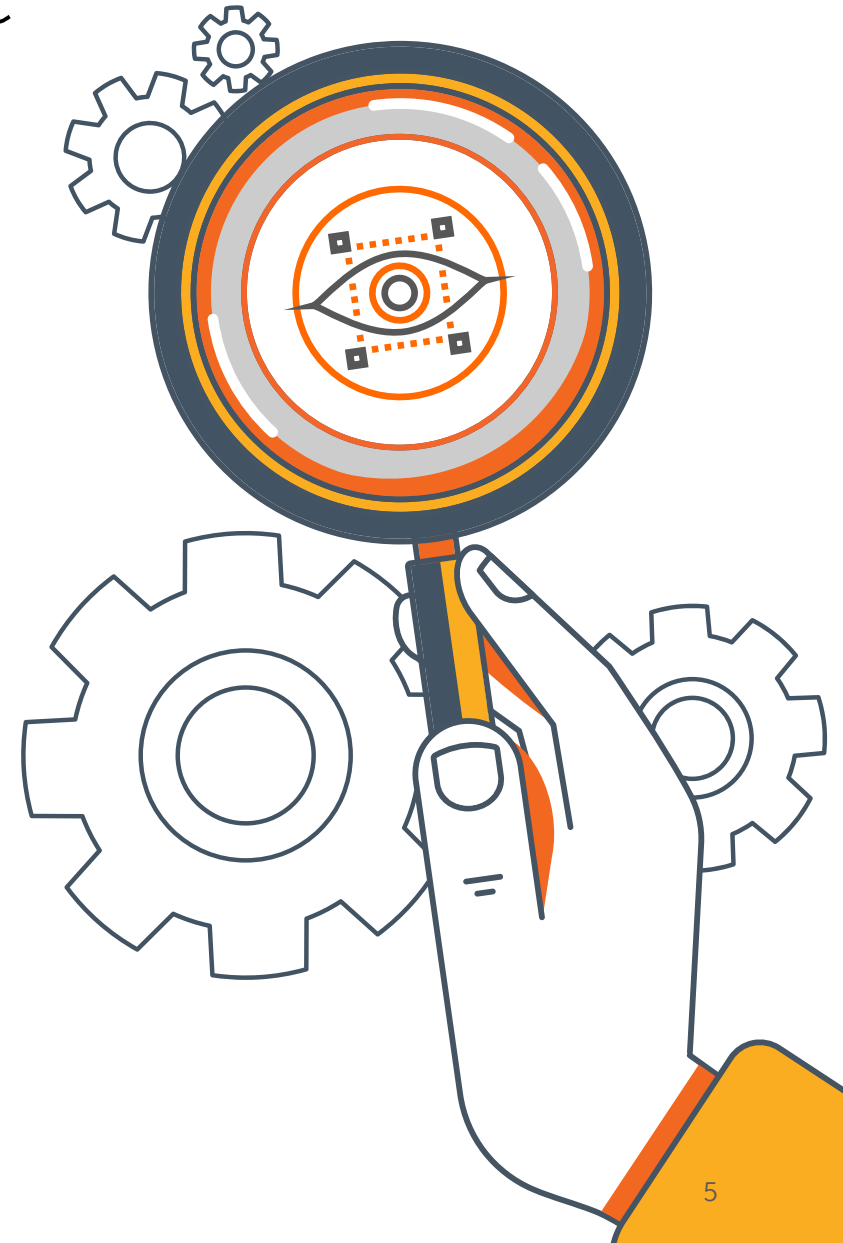
Les banques doivent améliorer l'efficacité de leurs opérations grâce à la digitalisation, et l'une des méthodes éprouvées pour y parvenir consiste à tirer parti du cloud pour augmenter la résilience et l'efficacité de l'infrastructure.



La visibilité haute fidélité au service de la transformation digitale

L'innovation digitale est une priorité pour les entreprises financières, mais 70 % des transformations digitales, un chiffre stupéfiant, échouent.² Même si vous effectuez des mises à niveau globales pour améliorer l'agilité, la flexibilité, la vitesse et l'évolutivité, une faille peut compromettre l'intégralité de vos investissements : le manque de visibilité sur les applications et le réseau. Comment parvenir à une visibilité de bout en bout, et pourquoi est-ce important ?

Un manque de visibilité hybride peut ralentir ou compromettre votre réussite, et les angles morts en particulier peuvent entraver les migrations vers le cloud et votre infrastructure hybride. À mesure que vous transformez votre capacité à prendre en charge l'intégration digitale, l'adoption du cloud, etc., vous avez besoin d'une visibilité haute fidélité et d'une analytique offrant des informations globales à l'échelle de l'entreprise, afin de comprendre comment les applications fonctionnent et d'identifier les points d'achoppement. Sans cela, vous avancez à l'aveuglette.



Exemples de cas d'utilisation

Une solution offrant la visibilité adéquate peut résoudre de nombreux problèmes. Voici quelques exemples :

Migration vers le cloud

Les entreprises financières doivent adopter le cloud, et l'étape suivante logique consiste donc à migrer leurs applications du data center existant vers le cloud. Une solution NPM adéquate les aidera à :

- établir des références de base pour le réseau ;
- prévoir les modèles de trafic et déterminer la latence des applications stratégiques avant la migration ;
- mapper les dépendances applicatives ;
- utiliser des analyses quantitatives pour estimer les performances post-migration ;
- surveiller en permanence le comportement post-migration des applications sur le réseau et signaler les valeurs hors normes.

Diagnostic des applications bancaires digitales

Une solution NPM unifiée peut déchiffrer le trafic Web pour fournir une visibilité sur les services sous-jacents et contribuer à comprendre les performances des applications bancaires digitales.

- Les graphiques de composition des temps de réponse indiquent immédiatement si un problème est lié au réseau ou à une application.
- Les diagrammes en cascade illustrent les performances, en isolant celles de chaque objet individuel sur la page et l'expérience utilisateur générale pour la page.
- Les visualisations TruePlot analysent chaque transaction à la recherche de performances hors norme et de modèles.
- L'analyse TLS permet de déterminer où les certificats SSL/TLS sont valides et leur date d'expiration afin de protéger les données.

« Dans 50 % des cas, le problème ne vient pas du réseau. La solution NPM unifiée de Riverbed nous aide à avoir une communication plus productive avec les autres personnes en charge des serveurs, du stockage ou des applications afin d'identifier l'origine exacte du problème. »

Architecte principal des outils réseau dans une société de participation financière privée



Exemples de cas d'utilisation

Surveillance de segments du réseau mondial

Les grandes entreprises financières disposent habituellement de réseaux qui sont véritablement mondiaux par nature. Ils couvrent plusieurs sites et data centers, et sont très complexes. Le segment Internet, communément appelé « DMZ », s'étend généralement sur plusieurs régions et data centers et héberge plusieurs dispositifs d'équilibreurs de charge, de pare-feux, de réseaux VPN, etc. Il est très difficile de diagnostiquer tout cela efficacement, particulièrement sans une vue de bout en bout du réseau.

Grâce à la visibilité des paquets et à des groupes d'interfaces virtuelles (VIFG) aux points d'entrée/sortie Internet, vous pouvez comprendre les performances à différents stades sur le parcours. Cela est primordial pour vous aider à surveiller le trafic avant et après un pare-feu, un dispositif d'équilibreur de charge, etc., et pour identifier l'origine des problèmes réels ou potentiels.

« Durant la pandémie, nous avons pu fournir à notre équipe de direction, rapidement, facilement et quotidiennement un tableau de bord montrant la capacité VPN et Internet ainsi que les sessions VPN concurrentes. Sans Riverbed, nous aurions dû trouver un moyen pour élaborer ces rapports manuellement et les envoyer par e-mail à tous les intéressés. »

Ingénieur principal dans une grande compagnie aérienne basée aux États-Unis

Analyse de la sécurité

La solution NPM unifiée de Riverbed recueille et analyse les flux et les données des paquets en toute fidélité afin de résoudre le problème en l'absence d'un périmètre de sécurité fixe. Elle fournit des renseignements essentiels pour détecter et investiguer les menaces avancées qui contournent les mesures préventives standards, ainsi que celles qui trouvent leur origine au sein du réseau.

Les équipes en charge de la sécurité tirent parti de la visibilité de bout en bout des solutions NPM unifiées de Riverbed pour identifier, détecter et gérer de manière proactive les menaces de sécurité telles que les programmes malveillants, les sites sur liste noire, l'exfiltration de données, les activités par force brute, les attaques DDoS, etc.

« Hier encore, nous avons découvert que quelqu'un s'attaquait à un serveur Skype. Sans la solution NPM unifiée de Riverbed, nous n'aurions pas été en mesure d'identifier le coupable. Nous avons pu identifier l'adresse IP exacte qui nous attaquait de l'extérieur. Sans cette solution, notre équipe de sécurité allait simplement commencer à bloquer des adresses IP. »

Architecte principal des outils de réseau dans une société de portefeuille de services financiers privée

Témoignage client dans le monde réel

OneMain Financial

Une prise de décision rapide est un avantage concurrentiel pour les prêteurs. L'objectif d'OneMain Financial est de faire une offre 20 secondes seulement après qu'un client ait fait sa demande en ligne. La lenteur des vérifications de solvabilité ou les retards de signature électronique ne sont pas acceptables.

Le diagnostic est difficile dans l'environnement complexe de OneMain. « Lorsque les performances applicatives ralentissent, on cherche les responsables à montrer du doigt », déclare Richard Hurst, superviseur des services réseau pour OneMain Financial. « Le fournisseur de services Internet, l'agence de crédit et les autres acteurs ont tendance à croire que le problème incombe à quelqu'un d'autre. »

OneMain Financial a trouvé la réponse avec Riverbed® AppResponse, une solution de gestion des performances réseau (NPM). **Voici quelques-unes des façons dont la solution NPM de Riverbed a permis à OneMain d'assurer le bon fonctionnement de ses activités :**

- Elle a permis de convaincre une agence de crédit que son processus de demande était lent.
- Elle a permis de diagnostiquer la cause de la lenteur des performances applicatives des signatures électroniques.
- Elle a permis d'analyser par microrafales de problèmes de bande passante.
- Elle a permis d'isoler l'origine des problèmes de qualité de la voix.



Comment identifier votre solution NPM

La bonne solution de visibilité peut garantir la résilience et la sécurité du réseau pour vos utilisateurs, qu'ils travaillent au bureau, en déplacement ou à domicile. Quatre exigences sont fondamentales :

- 1. Une visibilité complète**
Nous ne parlons pas de visibilité *éparse* ou d'échantillonnage de seulement certaines données. Le but est de fournir une transparence *totale* sur chaque metric de paquet, de flux et d'équipement dans les environnements physiques, cloud, multi-cloud et en périphérie, en tirant parti des appliances physiques, virtuelles ou cloud pour permettre aux équipes de travailler depuis n'importe où. En outre, la solution doit pouvoir exploiter des flux de données provenant d'outils divers, tout en étant capable de reconnaître et de comprendre les chemins applicatifs et les dépendances.
- 2. Une analyse scientifique de la sécurité**
Analysez les données de flux et de paquets afin de détecter les menaces de sécurité, notamment les programmes malveillants, les sites sur liste noire et les attaques DDoS. C'est d'autant plus important que le nombre de terminaux augmente en raison du travail à distance, tout comme le nombre de cyberattaques.
- 3. L'intelligence artificielle (IA) et le machine learning**
Effectuez des analyses dans tous les domaines pour détecter les anomalies et les modèles qui signalent des problèmes de performances et des menaces de sécurité, mais aussi pour réduire le temps de diagnostic et de résolution des problèmes et réduire davantage le « bruit » des événements.
- 4. Une intégration profonde**
Dans un environnement hautement complexe et distribué, les solutions modernes doivent être étroitement intégrées dans leurs portefeuilles ou familles de produits. Elles doivent également se connecter tout aussi efficacement à des services cloud multiples, à des logiciels tiers au moyen d'API ouvertes et à des outils existants (p. ex. : gestion des performances applicatives, journalisation et workflow).

NPM autonome vs unifiée

Les plateformes intégrées sont plus efficaces pour la surveillance des performances que des outils autonomes haut de gamme.³



Améliorer la résilience et la sécurité du réseau avec Riverbed

La plateforme NPM unifiée de Riverbed aide les organisations financières à améliorer la résilience et la sécurité du réseau. Contrairement aux outils disparates, Riverbed combine les données interdomaines, notamment tous les metrics des paquets, flux et équipements, grâce au machine learning et aux analyses avancées pour vous fournir une visibilité et des renseignements détaillés sur votre environnement hybride.

Pour en savoir plus sur la façon dont la plateforme NPM unifiée de Riverbed peut offrir une visibilité sur les réseaux cloud, virtuels et sur site pour soutenir vos travailleurs et vos clients, visitez notre site à l'adresse riverbed.com/npm

¹The 2020 FIS Readiness Report, novembre 2020

²<https://www.mckinsey.com/industries/retail/our-insights/the-how-of-transformation>

³EMA, NETWORK PERFORMANCE MANAGEMENT FOR TODAY'S DIGITAL ENTERPRISE, mai 2019