Boostez votre supervision IT grâce aux trois piliers de l'observabilité

Tirez le meilleur parti de vos données avec les métriques, les traces et les logs

splunk> turn data into doing™

Pour toute organisation informatique, l'un des plus grands défis consiste à garder une longueur d'avance sur les changements qui perturbent le paysage de la supervision. Vous devez vous munir des meilleurs outils et tactiques pour protéger votre infrastructure et vos applications. Vous devez évaluer les nouvelles technologies et séparer l'utile de l'engouement médiatique. Les analystes et les fournisseurs introduisent constamment de nouveaux termes qui mobilisent parfois inutilement votre attention.

Aujourd'hui, vous connaissez peut-être le concept d'observabilité. Vous avez peut-être entendu dire qu'elle peut vous aider à obtenir des informations sur vos applications et votre infrastructure en temps réel. Vous utilisez peut-être déjà des outils d'observabilité ou étudiez actuellement la meilleure façon de les adopter. Nous allons aborder trois principes fondamentaux de l'observabilité (métriques, traces et logs) et voir comment ils fonctionnent ensemble et peuvent vous aider à prendre le chemin de l'observabilité complète.

Les métriques, les traces et les logs peuvent vous aider à résoudre trois problèmes cruciaux des organisations numériques axées sur les données :

- la complexité ;
- les coûts ;
- l'expérience client.

Complexité

L'adoption du cloud, la sécurité du cloud et l'expansion des infrastructures génèrent des quantités massives de données impossibles à gérer et à analyser pour des opérateurs humains. La détection des problèmes sous-jacents et l'identification des causes profondes sont complexes et demandent beaucoup de temps.

Les services IT modernes utilisent une grande variété d'outils, souvent achetés auprès de fournisseurs et à des moments différents, et ces outils suivent les événements et génèrent des données dans des formats hétérogènes. Dans un tel contexte, la corrélation de toutes ces données et l'extraction d'informations utiles devient un véritable défi.

Des ensembles d'outils complexes peuvent également contraindre l'IT à superviser avec un outil et dépanner avec un autre. Certains outils se limitent à une supervision basée sur des métriques, d'autres à la journalisation. Les équipes sont contraintes d'utiliser des outils différents qui s'intègrent rarement les uns avec les autres. Il arrive même qu'elles emploient des langages entièrement différents, ce qui crée inévitablement des silos et décourage la collaboration.

Coûts

Naturellement, de nombreuses organisations se tournent vers le cloud pour la flexibilité qu'il offre. L'augmentation des dépenses en cloud peut toutefois poser problème en multipliant les demandes de budget et d'acquisition. Pire encore, une grande partie de ces dépenses est inutile. Si vous n'avez pas une visibilité complète sur l'ensemble de votre pile cloud, vous risquez de gaspiller de la capacité sur des projets abandonnés et des usages inefficaces, et ainsi de recevoir des factures que vous ne devriez pas avoir à payer.

Expérience client

Quelle que soit l'évolution des organisations, la définition de l'expérience client repose toujours sur des fondamentaux. Les interruptions et les dégradations de performances sont à proscrire, surtout lorsqu'elles provoquent des ruptures dans la continuité des activités. Les solutions de supervision obsolètes et insuffisantes sont souvent à blâmer. Vous ne pouvez pas vous permettre d'attendre des heures pour identifier, dépanner et résoudre un problème si vous tenez à la survie de votre entreprise. En bref, les équipes IT doivent travailler en temps réel, résoudre les problèmes rapidement et passer à la suite.

Les services IT ont besoin d'une solution unique

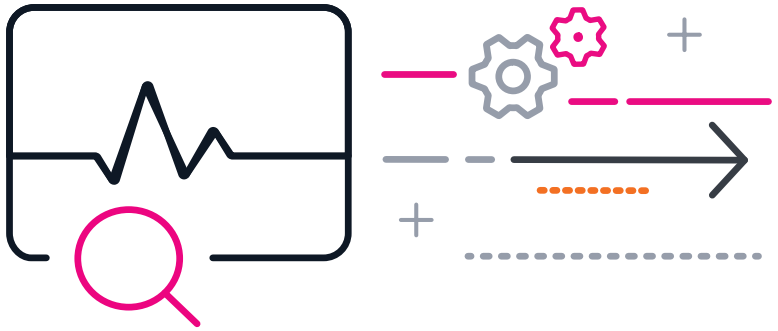
Et cette solution doit effectuer une supervision holistique des environnements locaux, hybrides et multicloud, exploitant l'intégralité des données de toutes les sources, à n'importe quelle échelle. C'est un concept simple, mais source de frustration pour les équipes informatiques aux prises avec leurs systèmes hérités.

Tous les fournisseurs de solution de supervision informatique vantent leur capacité à analyser les données, mais il faut se pencher sur les détails pour faire la différence. Il ne s'agit pas seulement d'analyser des données. Il s'agit de savoir de quelles données il s'agit et d'où elles viennent.

Il est temps de prendre l'observabilité au sérieux

On a dit tout et son contraire sur l'observabilité, que c'était un mot à la mode de plus, ou bien une technique indispensable de « supervision sous stéroïdes ». La réalité est plus sérieuse, en particulier face à la complexité croissante des infrastructures modernes et l'indubitable nécessité de renforcer la supervision du haut de la pile et des profondeurs du système.

La visibilité opérationnelle n'est plus réservée aux administrateurs système et aux analystes des opérations IT : même les développeurs cherchent à mieux comprendre ce qui se passe pour offrir une meilleure expérience client. Pour y parvenir efficacement, tous les rôles ont besoin de visibilité sur l'intégralité de l'architecture, des applications tierces aux développements internes, pour résoudre et à terme prévenir les problèmes. L'intégration de cette capacité, qui est à la base de l'observabilité, facilite la visibilité, permet une meilleure compréhension de la situation et laisse plus de temps pour des initiatives plus stratégiques.



Les systèmes distribués sont source de problèmes pour les services IT chargés d'avoir une vision globale de la situation, car chaque nœud d'un système peut avoir un responsable spécifique ayant ses propres exigences et priorités. Les solutions d'observabilité permettent au service IT d'obtenir toutes les données pertinentes dont il a besoin sans avoir à s'adresser à d'autres équipes.

Les équipes d'une organisation utilisent les informations d'application de différentes manières :

Les **équipes de développement** veulent connaître les performances de leurs applications en fonction de la façon dont les utilisateurs interagissent avec eux en temps réel.

Les **équipes DevOps** besoin de déployer le code rapidement, de le maintenir à jour et d'en suivre les modifications.

En mettant en œuvre les principes d'observabilité dans vos solutions de supervision informatique, vous pouvez adapter les résultats aux besoins de chaque utilisateur.

Exploiter la puissance des métriques, des traces et des logs

L'observabilité est basée sur trois types de données de télémétrie : les métriques, les traces et les logs, souvent appelés les « trois piliers de l'observabilité ». Individuellement, ils peuvent vous fournir des informations pour identifier les problèmes et leurs causes profondes, mais pris ensemble, leur puissance s'amplifie considérablement.

Si vous remontez assez loin dans l'histoire de l'informatique, vous constaterez qu'il n'y avait ni logs, ni traces, ni métriques. L'« application » prenait plus ou moins le contrôle du système et s'exécutait jusqu'à son terme… ou non.

Mais même à l'époque, il existait un concept pour détecter les problèmes au sein des systèmes, appelé « wolf fencing » et formalisé vers 1982. Ce nom provient d'une méthode pour trouver un loup en Alaska. On commence par construire une clôture au milieu de l'état, puis on écoute le loup hurler pour savoir dans quelle moitié il se trouve. On divise à nouveau cette partie en deux, et ainsi de suite jusqu'à ce que le loup ait été isolé.

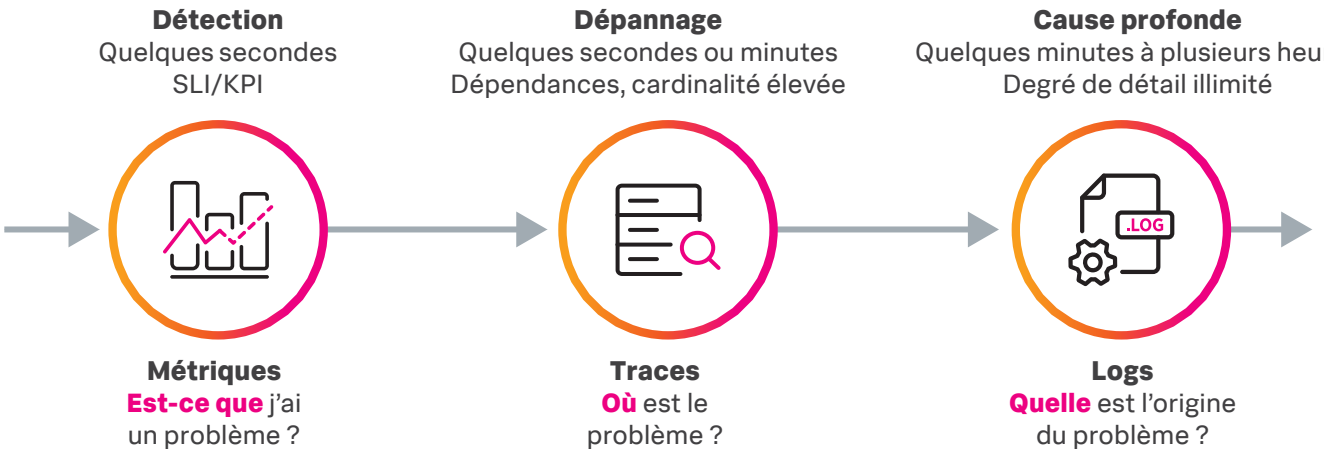
Pour identifier un problème dans une application, un utilitaire de résolution des problèmes basé sur ce concept de circonscription progressive pourrait, par exemple, ajouter une déclaration indiquant : « Je suis arrivé à la ligne 148 ». Une fois imprimé, cela signifiait : « Nous ne savons pas encore où se trouve le problème, mais nous savons que ce n'est pas avant la ligne 148 ».

C'est en formalisant cette approche en tant que méthode opérationnelle standard qu'est né le concept de logs, qui révèlent la cause du problème, et ainsi de nouvelles méthodes de débogage.

Alors que nos environnements et nos applications sont devenus de plus en plus complexes, les métriques et les traces se sont ajoutées aux logs pour former une image plus complète.

Les données sont au cœur de tout

Les trois piliers de l'observabilité



Le débogage des systèmes complexes est un processus itératif

- Tout d'abord, commencez par une métrique de haut niveau.
- Ensuite, approfondissez et démêlez les nœuds en vous appuyant sur des données et des observations à granularité fine.
- Enfin, faites les bonnes déductions sur la base des preuves obtenues.

Tout est un événement, mais l'événement n'est pas tout

Nous devons d'abord comprendre que tout ce qui se passe peut être considéré comme un événement. Si c'est enregistré, c'est un événement. Si ça n'a pas été enregistré, ça ne s'est pas produit. Les métriques, les traces et les logs sont autant d'événements qui se chevauchent, mais ils fournissent des types d'informations différents qui, pris ensemble, dressent un tableau complet.

Les applications modernes fournissent un ensemble d'informations si complexe qu'il peut être difficile de savoir quoi observer. Les composants sont trop nombreux et interconnectés. Ce n'est qu'en rassemblant les métriques, les traces et les logs que vous pourrez savoir où chercher pour identifier un problème.

Métriques

Les métriques aident à répondre à certaines des questions les plus fondamentales du service IT. Est-ce qu'un ralentissement des performances du système affecte les clients ? Les employés ont-ils des difficultés à se connecter ? Le volume de trafic est-il anormalement élevé ? Notre taux de désabonnement est-il en hausse ?

Les métriques sont des points de données numériques capturés au fil du temps qui peuvent être compressés, stockés, traités et récupérés plus efficacement que les logs. Vous pouvez facilement corréler les données de métriques avec d'autres données d'événement pour recevoir des alertes sur la nature du problème (métriques) et sa cause (logs). Les métriques peuvent être considérées comme le plus précieux des trois piliers, si on les prend individuellement, car elles sont générées plus fréquemment et sont omniprésentes, des systèmes d'exploitation aux applications. Comme les métriques proviennent de nombreuses sources différentes, leur corrélation peut produire une vue plus complète d'un problème.

Les métriques peuvent provenir de serveurs, d'applications, de capteurs IoT ou de tout autre objet qui génère des données machine contenant des données numériques en séries chronologiques. Pour citer quelques exemples courants de métriques que vous connaissez peut-être, il y a les mesures du système telles que l'utilisation du processeur, de la mémoire ou de l'espace disque, les mesures d'infrastructure d'AWS CloudWatch et les mesures des appareils IoT comme les relevés de température ou la localisation GPS (paires latitude-longitude au fil du temps notamment).

Les métriques diffèrent des données de log en ce qu'elles peuvent être stockées et optimisées plus efficacement pour les requêtes. Elles ne contiennent pas les informations riches d'un log, mais permettent de suivre l'évolution d'une mesure spécifique d'un système au fil du temps.

On recense plusieurs métriques courantes :

- les métriques système (utilisation du CPU, mémoire, E/S disque) ;
- les métriques d'applications (taux, erreurs, durées) ;
- les métriques métier (revenus, inscriptions de clients, taux de rebond, abandons de paniers).

Traces

Les traces font exactement ce que leur nom suggère : elles tracent le parcours d'un événement à travers le réseau. Une trace peut vous aider à identifier à quel endroit un événement se produit à répétition ou à localiser un goulot d'étranglement. Si les clients ont des difficultés à se connecter, par exemple, une trace peut trouver la base de données qui leur interdit l'accès.

Les traces aident à réunir les données fournies par les métriques et les logs pour produire une image plus complète des performances d'un système au fil du temps. Dans un environnement informatique distribué moderne, qui comprend des applications et des microservices conteneurisés, une requête ou une action peut transiter par tout un éventail de systèmes. Une trace intègre toutes les informations pour cartographier ce trajet et ce qui s'est passé le long du chemin.

Une trace unique capture généralement des données sur :

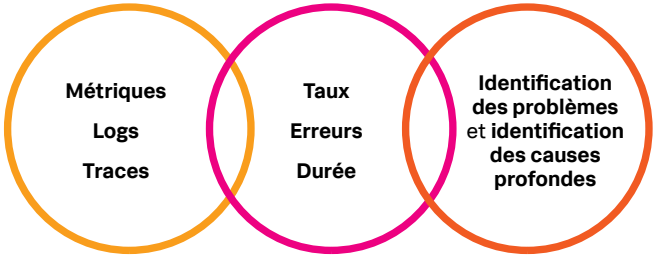
- les unités logiques (nom du service, nom de l'opération, durée et autres métadonnées) ;
- les erreurs ;
- la durée des opérations importantes au sein de chaque service ;
- les attributs personnalisés.

Ils se recoupent les uns les autres

Les logs peuvent fournir des métriques

Les traces peuvent fournir des métriques

Mais il faut avoir les trois



Bien que les trois types de données soient traités séparément, ils se recoupent tous en réalité. Les logs peuvent fournir des métriques. Les traces peuvent fournir des métriques. Les métriques peuvent vous indiquer la bonne trace ou le bon log.

Avec les métriques, les traces et les logs, vous pouvez identifier les problèmes plus rapidement pour en trouver la cause sous-jacente.

Logs

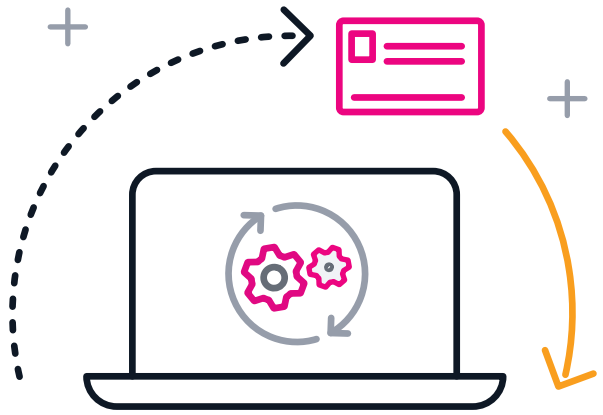
Les logs sont des enregistrements, générés par le système, des événements qui se produisent dans une application. Les systèmes informatiques modernes génèrent des quantités considérables de fichiers de log pour suivre tous les événements. Les systèmes de supervision IT tels que Splunk reposent sur la capacité à analyser les données des logs et à les utiliser pour identifier et résoudre les problèmes du système, voire les prévenir avant qu'ils ne surviennent. Ils offrent davantage d'informations et de contexte sur les causes d'un problème, en plus des simples données qui identifient l'événement.

Tout le défi de l'utilisation des logs pour identifier et résoudre les problèmes réside dans leur volume : tous ces systèmes génèrent tellement d'informations de log qu'il peut être difficile de trouver les indices les plus importants. Les différents systèmes du réseau d'une organisation emploient différents formats de log, obscurcissant potentiellement le chemin vers la résolution du problème.

Les données de log peuvent inclure :

- les logs système et serveurs (syslog, journald) ;
- les logs des pare-feu et des systèmes de détection des intrusions ;
- les flux de réseaux sociaux (Twitter, etc.) ;
- les logs d'application, de plateforme et de serveurs (log4j, log4net, Apache, MySQL, AWS).

Travailler pour différents groupes	
Une alerte concernant un service (métrique)	SRE, Opérations
Conduit à une erreur d'expiration de délai (trace)	Ingénierie DevOps, SWE
Entraîne un problème d'infrastructure (métrique)	Ingénierie DevOps, SRE
Conduit à un problème de configuration (métrique)	Ingénierie DevOps, Opérations
Entraîne une fuite de mémoire dans une application (log)	Développeur/SWE



Puissance trois

Pour certaines organisations, les métriques fournissent suffisamment d'informations pour effectuer l'essentiel du dépannage. Dans les services IT dotés d'infrastructures simples qui génèrent des quantités de données relativement faibles, les métriques peuvent suffire. Et toutes les organisations n'ont pas besoin d'identifier les problèmes dans des délais aussi courts. Les entreprises traditionnelles qui n'ont que peu ou pas de présence numérique en dehors de leur site web n'ont pas besoin d'identifier et de résoudre instantanément les problèmes rencontrés par les clients.

Mais si vous lisez ceci, vous êtes probablement responsable des performances des systèmes dans une entreprise axée sur le numérique et évoluant dans un secteur dynamique. Pour vous, combiner métriques, traces et logs représente une avancée majeure dans la modernisation de l'IT.

Obtenez des informations plus utiles à partir de vos données

Tout comme les solutions de supervision modernes vous signalent les problèmes avant qu'ils ne surviennent, une solution d'observabilité qui combine métriques, traces et logs peut apporter plus rapidement des informations plus complètes et de meilleure qualité pour faciliter votre travail.

Évoluez à la vitesse dont vous avez besoin

L'observabilité est plus qu'un outil pratique. Dans les entreprises visionnaires, l'observabilité est vue comme un avantage compétitif qui permet d'évoluer et de se développer au rythme rapide de la transformation numérique. Pour être prêtes, elles réalisent des investissements durables dans leurs outils de supervision.

Corrélez les données de l'ensemble de votre réseau, conteneurs et microservices inclus

Si vous utilisez des conteneurs et des microservices, les avantages pour vous sont encore plus nets. Le contexte supplémentaire apporté par le traçage est essentiel au dépannage dans les environnements hybrides, car il fournit beaucoup plus d'informations sur la localisation probable d'un problème dans un réseau distribué.

Accélérez votre passage au cloud

Enfin, il faut savoir que le passage au cloud entraîne immanquablement une augmentation exponentielle de la quantité de données système à superviser et à comprendre. L'observabilité est parfaitement adaptée au cloud.

Si l'observabilité est l'un des sujets les plus discutés en informatique, c'est pour une bonne raison. Si vous n'avez pas encore réfléchi à l'implémentation de l'observabilité dans votre environnement, la première étape consiste à déterminer comment votre système utilise les métriques, les traces et les logs.

Pourquoi Splunk ?

Splunk est la **seule solution de supervision multicloud axée sur l'analyse** de l'industrie, et elle couvre tous les environnements. Splunk offre la vitesse, l'évolutivité et les informations dont vous avez besoin pour relever vos défis IT. Splunk est la seule solution qui vous permet :

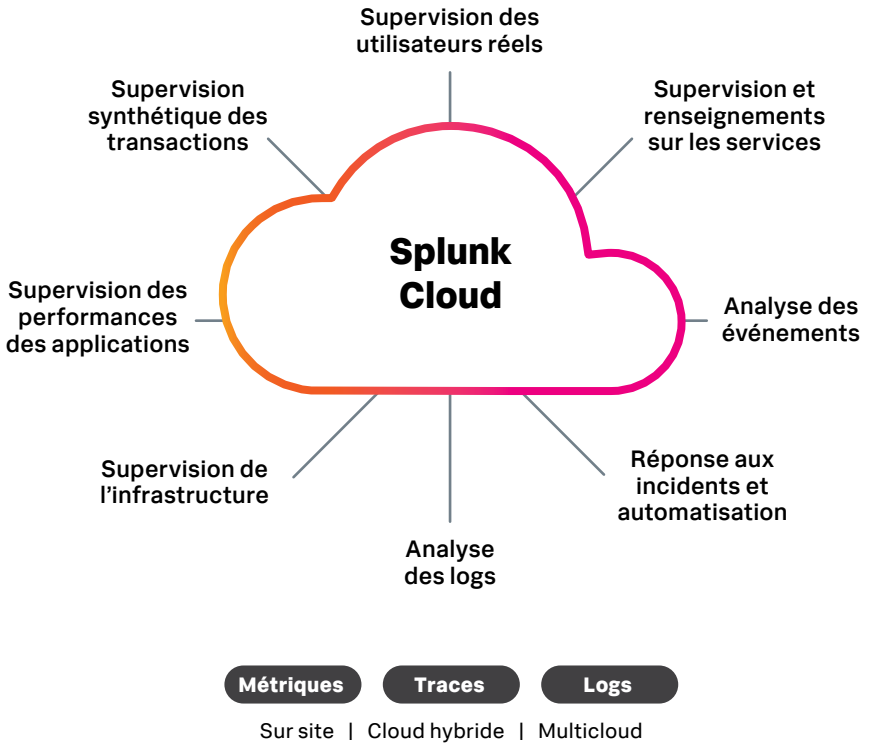
- d'identifier la cause profonde avec un dépannage rapide en temps réel, rechercher et corriger les problèmes dès qu'ils surviennent, et parvenir à la résolution en quelques secondes seulement ;
- de corréler les données de multiples sources, dans plusieurs formats et issues de divers outils, pour produire des informations exploitables au sein d'une solution unique ;
- d'obtenir rapidement des informations sur l'ensemble de votre environnement, qu'il soit local, hybride, multicloud ou basé des conteneurs et des microservices ;
- de démarrer rapidement et facilement avec des centaines d'intégrations prêtes à l'emploi, des graphiques et des tableaux de bord prédéfinis, et la découverte automatique des services ;
- de générer plus rapidement de la valeur pour votre organisation grâce à une supervision et un dépannage hautement performants et simples d'utilisation, pour détecter et résoudre rapidement les problèmes ;
- de réduire les coûts et la complexité en unifiant et en standardisant les outils de supervision sur la plateforme de données leader du marché ;
- de pérenniser votre investissement avec une solution complète, évolutive et flexible, basée sur les données et capable d'évoluer avec votre organisation ;
- d'analyser et de corréler les données pour obtenir des informations précieuses qui réduisent le bruit des événements et prédisent les dégradations futures.

Splunk fournit la solution de dépannage et de supervision la plus complète, la plus robuste et la plus flexible dans les environnements locaux, hybrides et multicloud à n'importe quelle échelle.

Splunk est reconnu par les plus grands analystes comme la meilleure solution du marché pour l'ITIM et l'ITOM, ainsi que comme un leader des solutions d'observabilité du cloud.

Les plus grandes entreprises du monde, dont 90 % appartenant au Fortune 100, font confiance à Splunk.

L'ensemble le plus complet de **capacités d'observabilité**



Témoignages de clients : Quantum Metric

À l'heure où de plus en plus d'industries comprennent la nécessité d'une transformation numérique accélérée, des entreprises toujours plus diverses se tournent en masse vers Quantum Metric pour maximiser leur potentiel. Pour la licorne de 2021, un tel afflux de clients était synonyme d'une augmentation massive des flux de données, et d'une complexification de l'environnement d'ingénierie englobant aussi bien des clusters Kubernetes que des moteurs Docker.

Brent Miller, Directeur principal des opérations cloud, déclare : « Nous voulons faire la même chose que nos clients : créer de meilleurs produits, évoluer rapidement, produire des itérations, expérimenter ; et le faire en toute sécurité. ». Eric Irwin, Directeur de l'ingénierie, ajoute : « Résoudre un problème sur différents scénarios d'utilisation nécessite une solution d'observabilité suffisamment extensible et robuste pour les traiter tous sans nous pousser dans une seule direction ».

Quantum Metric cherchait une solution d'observabilité flexible qui les aiderait, ainsi que leurs clients, à créer de meilleurs produits, plus rapidement. C'est pourquoi l'équipe a opté pour Splunk Observability Cloud.

Grâce à l'importation des données de log, des métriques et des traces en haute-fidélité, l'équipe sait désormais ce qui se passe dans son infrastructure et ses applications, et obtient ainsi des informations qui seraient autrement impossibles à collecter. Avec une visibilité complète de bout en bout sur l'intégralité de la pile, l'équipe s'assure du bon fonctionnement des sites de démonstration et comprend les interactions entre ses services pour apporter une valeur ajoutée à ses clients.

Des résultats axés sur les données

80 000 $

80 000 $ d'économies avec l'adoption de Splunk, grâce à une meilleure analyse de la réduction des effectifs et à une meilleure planification des capacités

96 %

Développement d'applications 96 % plus rapide, productivité des développeurs accrue

95 %

Réduction de 95 % des tâches CI en attente grâce à une meilleure évaluation des besoins en capacité

Conclusion

Il y a une raison pour laquelle on dit qu'il faut toujours avoir de la visibilité sur ses données. La raison est simple, et vous la connaissez probablement déjà. Le volume de données à superviser et à comprendre en tant que professionnel de l'IT ne fera que croître. Le rythme du changement ne peut qu'accélérer. La clé de votre valeur en tant que professionnel de l'IT réside dans votre capacité à garder une longueur d'avance sur ces changements et à contribuer au succès de votre entreprise. L'observabilité est la meilleure technologie pour rendre vos tâches aussi faciles, efficaces et performantes que possible.

Pour résumer :

- les métriques, les traces et les logs nous fournissent des données sur le fonctionnement de notre infrastructure, de nos services et de nos applications ;
- chaque élément répond à un besoin unique, propre à un cas d'utilisation spécifique ;
- leur combinaison produit une image complète ;
- ensemble, ils nous donnent une vision holistique permettant la supervision, l'analyse et l'adaptation aux changements de nos environnements.

Vous souhaitez tirer le meilleur parti de vos logs, métriques et traces ? Démarrez votre parcours de modernisation dès aujourd'hui avec la version d'essai de Splunk Observability Cloud.

21-19531-Splunk-Supercharge Your IT Monitoring With the Three Pillars of Observability-EB-106

splunk> turn data into doing™