




Faire face aux perturbations

Pourquoi la résilience numérique est devenue une priorité pour les DSI



Que se passe-t-il quand tout s'arrête?

Votre site Web tombe en panne sans avertissement. Ce n'est pas qu'un simple ralentissement. Le site est complètement inaccessible. Très vite, les appels et les messages affluent. Les clients sont les premiers à le remarquer. Les transactions échouent. Les dirigeants envoient des messages, et à l'interne, c'est la course.

Tout le monde pose la même question : que s'est-il passé? S'agit-il d'une attaque DDoS? Quelqu'un a-t-il déployé du code défectueux? Le problème vient-il de votre réseau, ou d'un fournisseur de services infonuagiques que vous ne contrôlez même pas?

Les équipes se précipitent d'un outil à l'autre, d'un tableau de bord à l'autre, d'une salle de crise à l'autre. Les équipes NetOps,

SecOps et ITOps examinent chacune leurs propres données et tentent d'en tirer des conclusions qui ne concordent pas toujours. Les minutes passent. Puis les heures passent. Et tout cela se transforme en temps d'arrêt coûteux, sans vision claire de ce qui s'est réellement produit. Quand l'analyse rétrospective finit par avoir lieu, tout devient clair : le vrai problème, c'est le manque de visibilité sur un environnement numérique complexe et interconnecté.

En tant que directeur informatique, on s'attend à ce que vous évitiez ce genre de situation et que vous preniez les choses en main malgré l'incertitude. Et tout commence par une solide base de résilience numérique qui vous permet de tout voir, d'agir rapidement et de vous adapter à tout.

Résilience numérique : un enjeu de 400 milliards de dollars pour les entreprises

La résilience numérique, c'est la capacité de maintenir votre entreprise opérationnelle et sécurisée, peu importe les obstacles, qu'il s'agisse de cyberattaques, de problèmes technologiques, de bogues logiciels ou de pannes chez des tiers. Maintenir la résilience numérique protège la qualité des

expériences numériques et les résultats de votre organisation. Et une étude récente de Splunk et d'Oxford Economics¹ met encore plus en évidence le coût des temps d'arrêt pour une entreprise : 200 millions de dollars, soit le coût annuel moyen par entreprise du Global 2000. À cela s'ajoutent des coûts indirects : 94 % des dirigeants disent que des pannes majeures retardent l'innovation.

La cause première? C'est un problème de données. Les données opérationnelles restent cloisonnées en raison d'une infrastructure fragmentée et de systèmes déconnectés, résultat de l'évolution des technologies au fil du temps dans les différentes équipes. Résultat : détection tardive, délais d'intervention plus longs et problèmes non résolus qui persistent.

Les éléments essentiels de la résilience numérique

Pour bâtir une véritable résilience, les organisations ont besoin de plus que de solutions ponctuelles. Il leur faut une approche unifiée qui rassemble les équipes ITOps, NetOps, d'ingénierie et SecOps.



Assurance à chaque point de connexion

Assurez une connectivité transparente dans le nuage, sur Internet, sur les réseaux d'entreprise et sur les appareils afin d'assurer la prestation des applications et des services.



Observabilité approfondie pour chaque expérience

Prévenez les temps d'arrêt et optimisez les expériences grâce à une visibilité et à des observations de bout en bout sur l'ensemble des services.



Opérations de sécurité intégrées

Assurez une prévention, une détection, une enquête et une intervention complètes face aux menaces.

Ces trois piliers, **l'assurance**, **l'observabilité** et **la sécurité**, constituent le fondement de la résilience numérique. Mais ce qui fait réellement la différence, c'est la manière dont ces composantes travaillent ensemble.

Comment Cisco aide à renforcer la résilience numérique

Cisco vous offre une visibilité et des observations sur l'ensemble de votre empreinte numérique afin que les équipes puissent détecter les problèmes plus rapidement, automatiser les interventions et offrir des expériences numériques fiables et sécurisées à grande échelle.



Assurer chaque expérience connectée

Cisco ThousandEyes offre une visibilité approfondie sur les réseaux que vous possédez et ceux que vous ne possédez pas, des fournisseurs d'accès à Internet aux applications SaaS en passant par les fournisseurs de services fonduagiques, afin que vous puissiez détecter et résoudre les problèmes plus rapidement, avant qu'ils n'aient des répercussions sur l'entreprise.

Retombées commerciales

- Comblent les lacunes de visibilité sur les réseaux
- Détecter plus rapidement les causes premières, même au-delà de votre périmètre
- Passer d'opérations réactives à des opérations proactives et automatisées



Tout observer, avec contexte

Obtenez une observabilité de bout en bout sur l'ensemble de votre écosystème numérique. Cisco Data Fabric est une architecture unifiée qui permet de gérer et d'activer les données dans tous vos environnements, la plateforme Splunk servant de moteur d'analyse et d'intelligence en temps réel. Elle permet de faire ressortir rapidement des observations et d'aider les organisations à résoudre les problèmes avant qu'ils n'aient une incidence sur l'activité. Splunk a été nommé chef de file dans le Gartner Magic Quadrant 2024 pour les plateformes d'observabilité, ce qui reconnaît sa capacité à offrir une visibilité exploitable en temps réel à l'échelle de l'entreprise, dans les environnements sur site, hybrides et infonuagiques.

Retombées commerciales

- Étendre la visibilité et mettre les événements en corrélation pour obtenir plus rapidement des observations utiles
- Accélérer la détection, l'analyse des causes premières et la résolution des problèmes de performance
- Créer des expériences client exceptionnelles et fiables en tout temps
- Renforcer le contrôle sur les données opérationnelles, le rendement et les dépenses
- Accroître l'efficacité en donnant aux équipes SecOps, NetOps, ITOps et d'ingénierie accès aux mêmes données, au bon moment



Exploiter un environnement sécurisé à grande échelle

Cisco associe une solution SIEM de pointe et une solution XDR innovante afin d'aider les organisations à détecter plus vite les menaces et à y répondre plus rapidement. Splunk Enterprise Security, dix fois chef de file dans le Gartner Magic Quadrant pour les solutions SIEM, offre des capacités d'analyse puissantes et une visibilité étendue sur l'ensemble du paysage de menaces. Cisco XDR intègre les données à l'échelle de toute la pile de sécurité, ce qui simplifie les flux de travail de détection et d'intervention. Et grâce à des fonctionnalités comme Splunk SOAR, Asset and Risk Intelligence et Splunk Attack Analyzer, les équipes peuvent automatiser les enquêtes, hiérarchiser les risques et agir avec plus de rapidité et d'assurance.

Retombées commerciales

- Détecter les menaces et y réagir plus rapidement grâce à l'intelligence artificielle et à l'automatisation
- Mettre fin aux déplacements latéraux avant qu'ils ne se propagent à l'ensemble du réseau
- Unifier la détection des menaces, l'enquête et l'intervention (TDIR) afin de réduire la prolifération des outils

Rester opérationnel en toute sécurité, quoi qu'il arrive

Avec Cisco, la résilience numérique devient un avantage commercial mesurable.

Éviter que les perturbations ne se transforment en catastrophes

Cisco vous aide à détecter de manière proactive les menaces et les problèmes potentiels grâce à une connectivité transparente dans le nuage, sur Internet et sur les réseaux d'entreprise.



WWE utilise ThousandEyes pour détecter les anomalies tôt et réduire le délai moyen de réparation (MTTR).²

Accélérer l'intervention en cas d'incident afin de réduire au minimum les répercussions sur l'activité

Avec Cisco, vous pouvez agir avec agilité quand les choses tournent mal, corriger automatiquement et vous rétablir rapidement.



Progressive Insurance détecte plus rapidement les menaces et résout plus vite les retards de service et les temps d'arrêt grâce à Cisco.³

S'adapter aux nouvelles occasions d'affaires et en tirer parti

En éliminant la complexité des TI et de la sécurité, les équipes peuvent se concentrer sur la création d'expériences client exceptionnelles et investir dans de nouvelles technologies.



Avec Splunk, **Tesco** utilise les données pour mieux comprendre les points de contact avec les clients, simplifier les opérations de la chaîne d'approvisionnement, améliorer le suivi des livraisons et éviter tout temps d'arrêt pendant les pics d'achalandage des Fêtes.⁴



United Airlines a réduit de 50 % le temps de résolution des problèmes en combinant les capacités d'assurance, d'observabilité et de sécurité de Cisco.⁵



Travelport a enregistré une réduction de 95 % des faux positifs et un délai moyen de détection (MTTD) 75 % plus rapide, ce qui lui a permis de dépasser ses objectifs de fiabilité et de disponibilité pour la plateforme de commerce de détail qu'elle fournit.⁶



ManpowerGroup a obtenu des observations 60 fois plus rapidement en centralisant les opérations mondiales de sécurité dans Splunk, ce qui a permis aux équipes de passer de tâches réactives à la création de nouveaux services et à l'amélioration de l'expérience client.⁷



La différence Cisco

Seul Cisco vous offre une visibilité complète sur l'ensemble de votre écosystème numérique en unifiant l'assurance, l'observabilité et la sécurité. Grâce à des observations approfondies propres au domaine et à un contexte en temps réel, vos équipes peuvent détecter, hiérarchiser et résoudre les problèmes plus rapidement, ce qui assure des opérations résilientes et des expériences numériques ininterrompues.



Visibilité complète

Seul Cisco offre une visibilité de bout en bout sur l'ensemble de l'empreinte numérique d'une organisation, y compris les réseaux que vous ne possédez pas, de la périphérie au nuage en passant par les applications SaaS. Peu importe où circulent vos données, Cisco vous aide à voir et à agir plus rapidement.



Données unifiées

Cisco relie les données de NetOps, SecOps, ITOps et de l'ingénierie dans une plateforme commune, tout en préservant les flux de travail propres à chaque domaine. Cette approche favorise la collaboration et accélère le délai de rentabilisation.



Intégré et ouvert dès la conception

Cisco offre des solutions étroitement intégrées qui fonctionnent harmonieusement avec vos outils et vos données existants, ce qui accélère la rentabilisation et génère des résultats concrets à l'échelle de l'entreprise.



Des observations pilotées par l'intelligence artificielle à grande échelle

Grâce à l'ampleur et à la richesse de la télémétrie Cisco, les organisations obtiennent des observations plus précises et exploitables, pilotées par l'intelligence artificielle, qui les aident à garder une longueur d'avance sur les problèmes de performance comme sur les menaces de sécurité.

Les quatre étapes de la maturité en résilience numérique

La résilience numérique n'est pas une destination : c'est un parcours continu. Cisco aide les organisations à passer par quatre étapes :

	Assurance	Observabilité	Opérations de sécurité
1 Visibilité de base Tout voir	Obtenez une visibilité de bout en bout sur l'infrastructure et les réseaux tiers.	Unifiez la télémétrie des applications, des TI et des équipes opérationnelles	Détectez plus tôt les incidents grâce à une vision claire du rendement et des menaces
2 Observations guidées Hiérarchiser ce qui compte	Réduisez le bruit grâce à des observations pilotées par l'intelligence artificielle qui signalent rapidement les véritables problèmes	Mettez les données en corrélation afin de faire ressortir automatiquement des alertes significatives	Triez plus rapidement et évitez de perdre du temps sur les faux positifs
3 Intervention proactive Automatiser et intervenir plus rapidement	Utilisez des guides pour gérer automatiquement les problèmes récurrents	Enrichissez les alertes avec du contexte et accélérez la résolution	Automatisez les interventions pour vous concentrer sur les menaces complexes
4 Flux de travail unifiés Collaborer sans friction	Harmonisez les processus d'intervention entre les équipes TI, réseau et opérations	Collaborez à partir de données partagées afin d'éliminer les cloisonnements	Faites évoluer les flux de travail et les améliorer en continu

Ressources

1. Splunk : « [Les coûts cachés des temps d'arrêt 2024](#) ».
2. Cisco : « [Garantir les expériences, du ring jusqu'à la clientèle internationale.](#) »
3. Splunk : « [Progressive protège ses clients et ses revenus grâce à Splunk](#) »
4. Splunk : « [Carnival navigue dans un océan de données avec Splunk.](#) »
5. Splunk : « [United Airlines aide le service à la clientèle à garder le cap avec Splunk AppDynamics.](#) »
6. Splunk : « [Travelport offre une expérience client exceptionnelle grâce à une observabilité de bout en bout.](#) »
7. Splunk : « [ManpowerGroup utilise Splunk pour obtenir des observations 60 fois plus rapidement et renforcer la sécurité mondiale](#) »

Faites de la résilience numérique un avantage.

Dans un monde où les perturbations sont constantes, la résilience n'est pas facultative. Elle est essentielle. Les organisations qui prospèrent sont celles qui ont une visibilité sur l'ensemble de leur environnement, qui agissent rapidement et qui savent s'adapter à l'inconnu.

Cisco vous permet de faire exactement cela en offrant une visibilité, des observations et une intervention intégrée inégalées à l'échelle de tout l'écosystème numérique.

[Découvrez comment](#) maintenir votre organisation opérationnelle et sécurisée, peu importe la perturbation.

