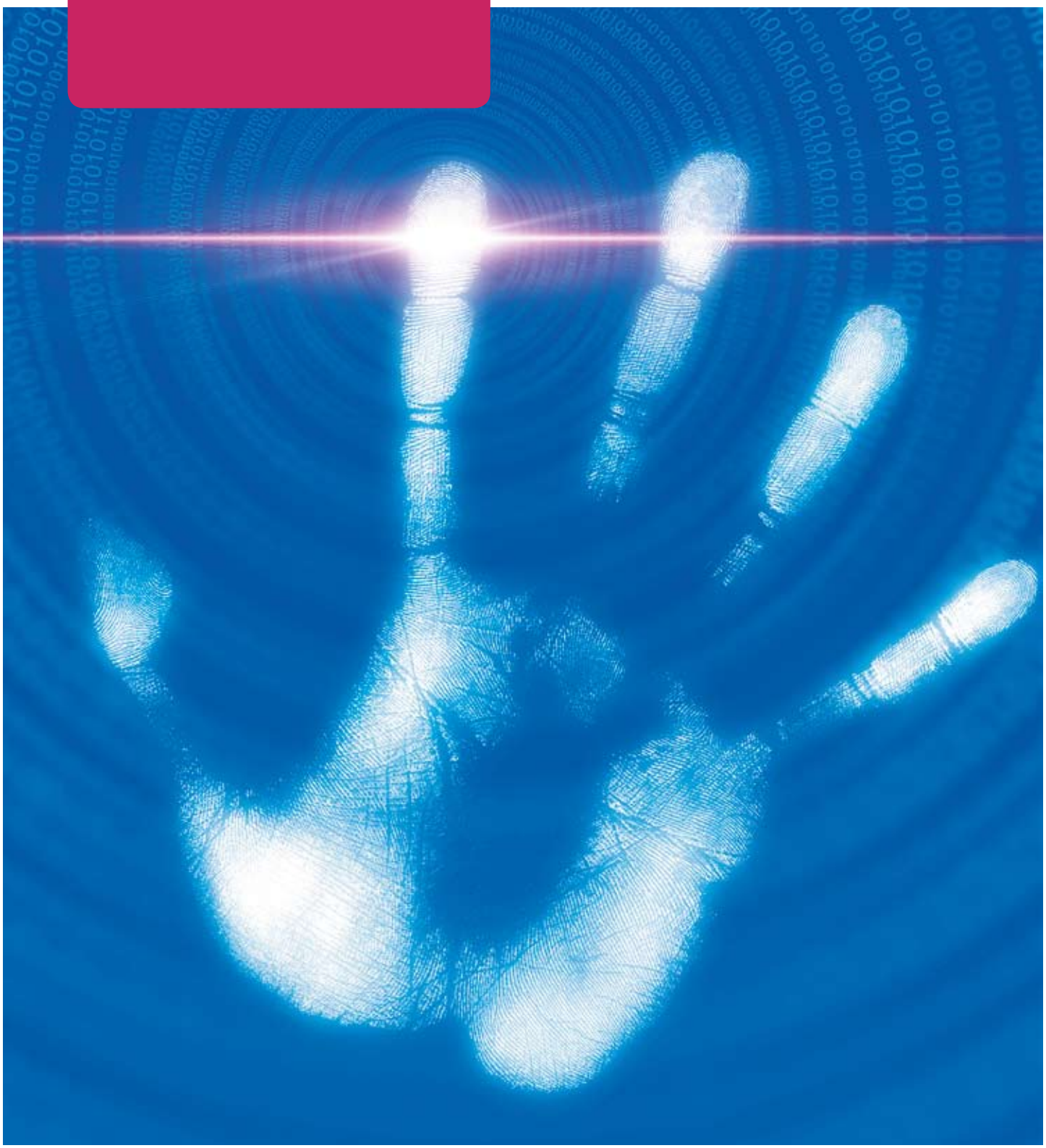
Projet de solution d'investigation numérique Dell



Le défi :
le tsunami numérique

Ces dernières années, les activités numériques des criminels et des groupes terroristes ont connu une croissance exponentielle, tant au niveau du volume que de la rapidité, de la diversité et de la sophistication, et ce partout dans le monde. Aujourd'hui, la plupart des délits commis présentent une composante numérique. Ce phénomène est parfois appelé le tsunami numérique.

Cette évolution a été exacerbée par des avancées considérables dans le domaine du matériel électronique. La diversité croissante des équipements électroniques grand public, associée à une capacité accrue de mémoire et de stockage, fournit aux criminels et aux terroristes un nombre incalculable d'opportunités de masquer les données malveillantes.

Il n'est pas rare de trouver des ordinateurs de bureau ou portables offrant une capacité de stockage de plusieurs centaines de gigaoctets. Les disques durs les plus récents permettent même d'étendre la capacité à 2 ou 4 téraoctets. Sachant qu'un téraoctet permet de stocker 200 DVD, cela représente une quantité de stockage impressionnante, et donc une source de problèmes qui ne vont pas cesser de se multiplier.

Des PC aux ordinateurs portables, des téléphones mobiles aux clés USB et même aux consoles de jeux, les forces de police et de sécurité n'en finissent plus de cloner, d'ingérer (ou de créer des images), d'indexer et d'analyser des quantités croissantes de données suspectes tout en préservant la chaîne de conservation des preuves numériques et en protégeant les citoyens.

Lorsqu'elles arrêtent des suspects et saisissent leurs équipements informatiques, les forces de police et les agences sont soumises à une pression considérable pour traiter et analyser les preuves potentielles dans un délai très réduit et dans des environnements informatiques souvent imparfaits. Lorsque ce sont des entreprises qui sont suspectées d'avoir commis des activités délictueuses ou terroristes, la quantité d'équipements à analyser est encore plus importante.

La création d'images des données prend du temps

Il faut d'abord copier ou « cloner » les disques durs afin de ne pas contaminer la source de données. Cela constitue une problématique majeure pour les forces de police ou les organismes concernés, car la conservation des données copiées à partir des clones requiert des capacités de stockage considérables. La copie et le traitement des disques durs et des systèmes sur lesquels ils étaient exploités peuvent prendre des heures, voire des jours. Ces opérations nécessitent en outre d'être réalisées avec le plus de précautions possibles et une grande attention aux détails.

Des directives strictes permettent de préserver la chaîne (ou la continuité) de conservation. La documentation doit inclure les conditions indispensables au rassemblement des preuves.

L'identité de tous les détenteurs de preuves doit être spécifiée. La durée de conservation des preuves, les conditions de sécurité applicables lors de la manipulation ou du stockage des preuves, ainsi que la manière dont les preuves ont été transmises aux détenteurs suivants doivent être indiquées... Or, cela prend du temps.

Les problèmes actuels liés à l'ingestion et à l'analyse

Une fois clonées, les données sont « ingérées » par les experts en investigation numérique sur une ou plusieurs stations de travail ou sur des PC hautes performances. Là encore, l'opération peut prendre beaucoup de temps selon la quantité de données ingérées avant leur indexation, leur tri et leur analyse.

En raison des quantités importantes de données à analyser et du risque de perte de données, les experts doivent réaliser leurs analyses au sein de laboratoire. Par ailleurs, il arrive que la législation locale interdise les examens à distance des disques durs saisis pour être analysés par des unités de police scientifique équipées de moyens haute technologie.

Il n'est donc pas surprenant que les retards de traitement des disques durs saisis soient importants : de 18 à 24 mois[1], le plus souvent. Dans le meilleur des cas, les données peuvent être partagées entre les serveurs de fichiers mais doivent tout de même être analysées en laboratoire, nécessitant en outre des capacités réseau de pointe afin de transférer les données entre les serveurs gérés de manière centralisée et les PC des analystes. Généralement, cela ne permet pas de partager les données entre les analystes travaillant sur un même site, encore moins sur des sites distants. Le partage en temps réel entre des organismes ou même des pays, voire entre plusieurs services publics, est hors de question.

Actuellement, pour réaliser des analyses complémentaires, il faut donc obligatoirement se rendre au laboratoire. Par ailleurs, si l'image clonée contient un code malveillant, celui-ci peut endommager la station de travail de l'expert chargé de l'investigation, auquel cas une restauration peut être nécessaire, obligeant à recommencer entièrement le processus d'ingestion ou risquant de compromettre la chaîne de conservation si le code n'est pas détecté.

Les défis du marché

- Manque d'expertise et de ressources combiné au volume exponentiel de données suspectes conduisant à un retard de traitement de 18 à 24 mois[1].
- Approche informatique ad hoc et non structurée, axée sur une infrastructure comptant un ou plusieurs PC.
- Délais d'investigation coûteux centrés sur la gestion des technologies, la duplication des données et la sécurisation de la chaîne de conservation.
- Accès limité aux données hors site. Enquêteurs obligés de rester au laboratoire pour éviter les risques de fuite d'informations.
- Code malveillant pouvant altérer les stations de travail des analystes, ce qui entraînerait une restauration du système et une possible contamination des preuves.
- Variation des approches en matière de sauvegarde des données suspectes en fonction des autorités. Risque de dysfonctionnement des appareils/supports au fil du temps.

Avantages de la solution

- Simplification de la création d'images, du partage et de l'archivage des données entre les experts et les équipes, d'où la possibilité d'une hausse spectaculaire de la productivité.
- Standardisation de l'infrastructure informatique d'investigation et définition d'une procédure claire pour l'échange sécurisé d'informations électroniques.
- Concentration de l'expertise d'investigation sur l'analyse des données suspectes en proposant une interface utilisateur unique pour différentes applications d'investigation.
- Analyse et examen des données suspectes et des preuves réalisables sur site ou de manière sécurisée à distance.
- Possibilité d'exécuter un code malveillant dans un environnement « isolé », sans affecter l'intégrité du système.
- Configurations optionnelles de sauvegarde, de restauration et d'archivage et de reprise après sinistre définissant une procédure claire qui contribue à sécuriser la chaîne de conservation ainsi que la partage et la destruction des informations.

Solution d'investigation numérique Dell

L'approche Dell en matière d'investigation numérique reprend les principes de la procédure séquentielle et y applique les principes de l'informatique en nuage en utilisant la capacité du datacenter pour permettre le traitement simultané et parallèle des preuves numériques.

Phase 1 (tri)

Grâce à l'association d'un ordinateur portable Dell Latitude™ E6400 XFR ultrarobuste et du logiciel de tri Spektor® d'Evidence Talks, les experts en investigation numérique ont la possibilité de récupérer rapidement des preuves potentielles sur des équipements suspects afin de les examiner sur site. Outre le gain de temps que cela représente, toutes les données récupérées le sont en intégralité, soit en les exportant en tant que fichier EO1 pour les charger directement dans le datacenter, soit en créant une image de la manière habituelle, chargée via une interface USB sur le système de stockage central pour être traitée au laboratoire.

Phase 2 (ingestion)

Comme dans les pratiques actuelles, les données suspectes sont clonées. Mais au lieu de créer une image sur une seule station de travail, les données sont ingérées dans un référentiel central de preuves plutôt que sur le PC d'un analyste.

L'ingestion immédiate des données par le datacenter contribue à réduire les transmissions de données entre équipements, ce qui augmente la disponibilité des données pour différents analystes, améliorant considérablement leur productivité et leur efficacité.

Phase 3 (stockage)

Le stockage direct des données suspectes dans le datacenter permet aux analystes de se concentrer sur l'analyse au lieu de chercher à savoir s'ils disposent de suffisamment d'espace sur le disque dur de leur PC pour stocker et indexer les données. Cela leur permet de ne pas perdre de temps avec la sauvegarde d'autres travaux d'investigation sur des supports enregistrables, de type DVD.

Le stockage centralisé des données permet également de partager plus efficacement les données et les charges de travail et de diminuer les délais nécessaires pour copier des jeux de données très volumineux d'un appareil à l'autre, améliorant ainsi la productivité. Cette opération peut prendre plusieurs heures, même sur les réseaux haut débit les plus récents, d'où une immobilisation inefficace du PC et des ressources du réseau.

Phase 4 (analyse)

Avec le stockage centralisé des données, il est possible d'indexer et de trier les données au sein du datacenter sur des serveurs hautes performances au lieu de recourir à des PC dédiés d'analystes.

De cette façon, il est possible d'exécuter en même temps sur une ou plusieurs stations de travail plusieurs sessions d'analyse exploitant des logiciels tels que AccessData, FTK et Encase® de Guidance Software, augmentant considérablement la productivité. L'analyste peut ainsi consacrer son temps à l'analyse des données plutôt qu'à leur administration.

Chaque instance d'application est exécutée sur une session indépendante de serveur, ce qui contribue à protéger le reste du système des codes malveillants et des virus, contribuant ainsi à préserver l'intégrité du système. Lorsqu'il est nécessaire d'exécuter un code malveillant ou des applications à des fins de compréhension et de preuve, les analystes peuvent les exécuter dans des environnements sécurisés et isolés.

Auparavant, lorsqu'un code malveillant était exécuté par erreur, cela pouvait compromettre l'intégrité d'une preuve potentielle, la chaîne de conservation et le temps déjà consacré à l'analyse. Par conséquent, cela nécessitait généralement une restauration de la station de travail de l'analyste et la reprise depuis le début des procédures de création d'image et d'analyse.

Phase 5 (présentation)

Une fois les données traitées et les domaines d'intérêt potentiels identifiés, les équipes d'investigation pouvant inclure jusqu'à 200 agents de police (selon la taille de l'infrastructure d'investigation) peuvent être autorisées à accéder en temps réel et de manière sécurisée aux preuves potentielles. Par ailleurs, la nature formalisée de cette infrastructure permet d'accéder facilement à distance et de manière sécurisée aux experts qualifiés. En effet, il n'est pas nécessaire que les équipes d'investigation se déplacent sur le terrain pour traiter des cas importants et il est inutile de prendre le risque d'exposer des preuves sur des CD.

Cycle de vie de l'investigation numérique selon Dell

1. **Tri**
   Grâce à l'association de l'ordinateur portable Dell Latitude™ E6400 XFR ultrarobuste et du logiciel de tri Spektor® d'Evidence Talks, les analystes chargés de l'investigation peuvent rapidement visualiser les preuves les plus accessibles disponibles sur les équipements suspects, directement sur les lieux du délit.

2. **Ingestion**
   Une fois clonées, les données suspectes sont ingérées directement dans un référentiel centralisé de preuves et non pas sur une station de travail. La solution permet d'ingérer simultanément plusieurs équipements.

3. **Stockage**
   Copier directement les données sur les systèmes de stockage à grande vitesse Dell™ EqualLogic™ et EMC² permet de transférer en toute transparence les données entre les serveurs et les systèmes de stockage, améliorant ainsi la productivité

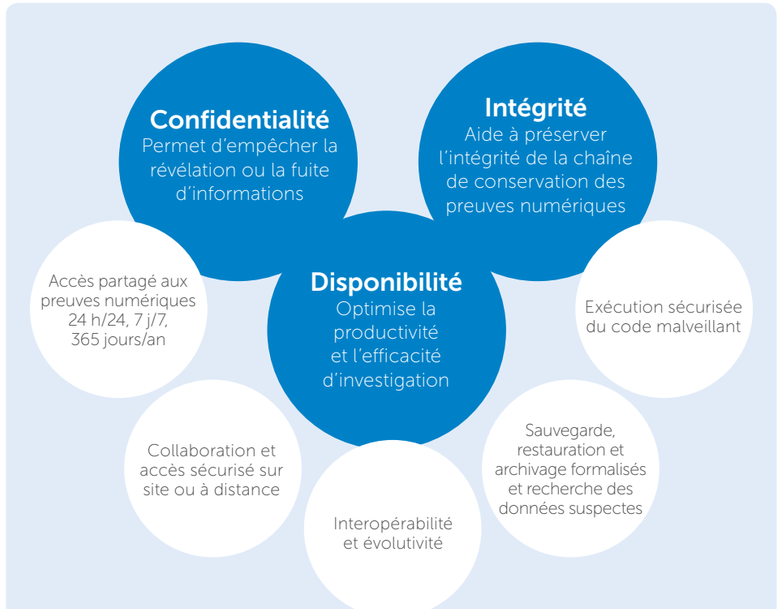


Fig 1. Répartition du processus d'investigation numérique en 5 phases séparées.

4. **Analyse**
   Plusieurs sessions d'analyse peuvent être exécutées simultanément sur un ou plusieurs PC Dell OptiPlex™, accroissant encore la productivité.

5. **Présentation**
   La solution permet d'adapter selon les besoins le nombre d'équipes d'investigation sur site ou à distance disposant d'un accès sécurisé aux données de l'affaire : 24 h/24, 7 j/7, 365 jours/an.

6. **Archivage et recherche**
   Les options standard de sauvegarde, de restauration et d'archivage contribuent à préserver l'intégrité de la chaîne de conservation des preuves numériques, d'échanger des données en toute sécurité et de coopérer en situation de crise.

Phase 6 (archivage et recherche)

Le « modèle » Dell de solutions d'investigation numériques modulaires peut contribuer à créer un environnement modulaire et évolutif pouvant être étendu et mis à niveau afin de s'adapter aux exigences croissantes de traitement et de stockage. L'intégration d'une infrastructure formalisée de sauvegarde, de restauration et d'archivage permet d'optimiser la coopération entre les agences et les forces de police, y compris d'un pays à l'autre.

Par ailleurs, les installations de sauvegarde, de restauration et d'archivage standard permettent d'alléger les tâches administratives des analystes, d'assurer l'homogénéité entre les laboratoires, en particulier en cas de crise, et de diminuer les risques pour la chaîne de conservation des preuves numériques lorsque les preuves potentielles sont sauvegardées sur des DVD enregistrables et des équipements de sauvegarde de type « domestique ». Cela simplifie considérablement le transfert sécurisé des informations entre les laboratoires de police scientifique hautes technologies.

Par ailleurs, le projet de solution d'investigation numérique de Dell inclut un composant de rechercher en option qui permet de corréler les informations entre les différents jeux de données ingérés. L'analyste peut ainsi exécuter rapidement une recherche de type Internet sur la banque de données complète d'une affaire comprenant à la fois du contenu actif en ligne et des documents archivés lors d'affaires antérieures.

Analyser des données plus rapidement pour confirmer des convictions

Fig 2. Exemple de solution d'investigation numérique de Dell montrant une station de travail équipée de deux écrans exécutant simultanément plusieurs instances d'AccessData ftk (versions 1.8 et 2.2) et de Guidance Encase.

Solution d'investigation numérique Dell

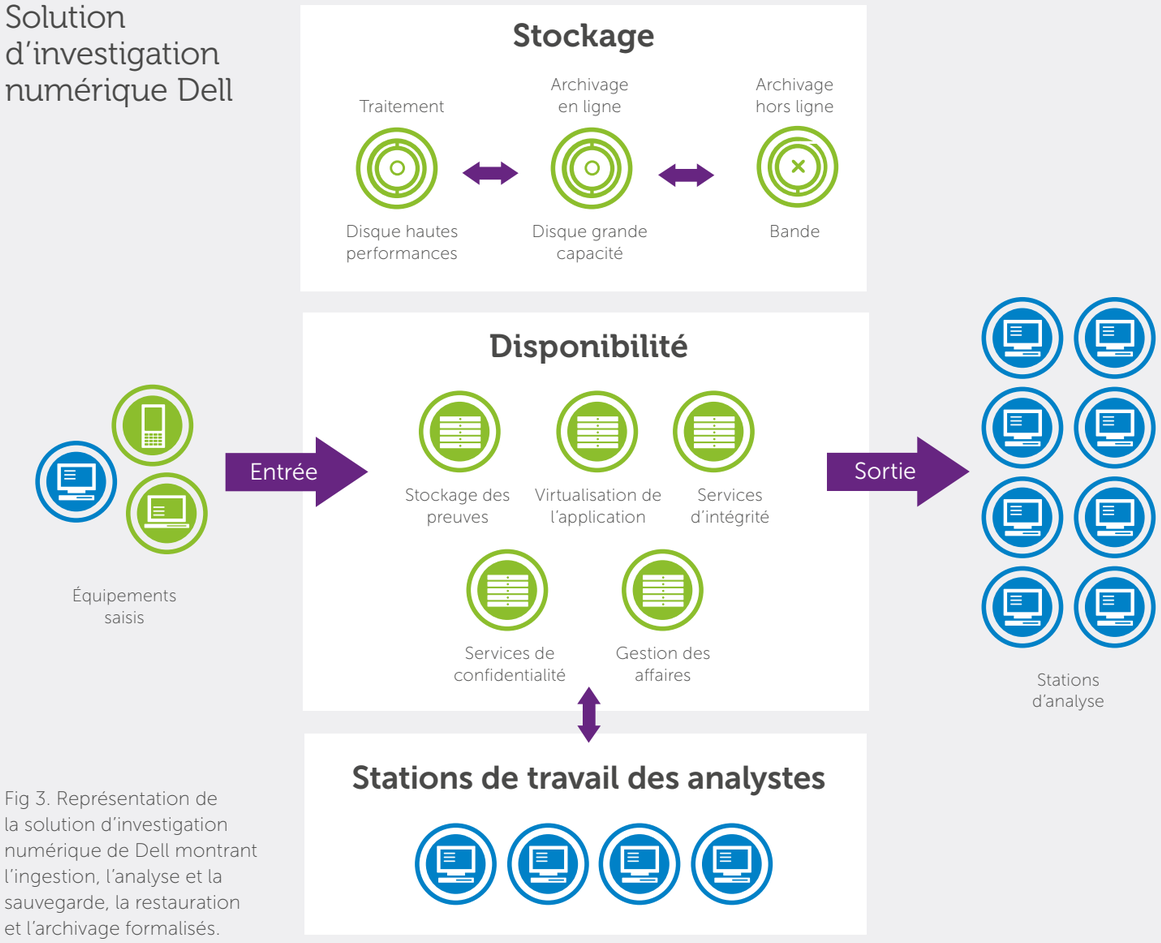


Fig 3. Représentation de la solution d'investigation numérique de Dell montrant l'ingestion, l'analyse et la sauvegarde, la restauration et l'archivage formalisés.

Résumé

La solution d'investigation de base comprend une suite de services de serveur, de stockage et de logiciels à haute disponibilité conçue pour traiter et stocker des données d'investigation numériques tout en protégeant la sécurité et l'intégrité de ces données tout au long du cycle de vie. Les éléments de la solution illustrée à la Figure 3 sont les suivants :

- Stockage des preuves : une plateforme de stockage modulaire commune composée d'une combinaison d'équipements de stockage hautes performances et haute capacité. Les données peuvent ainsi être traitées rapidement et transférées de manière transparente sur des supports de stockage moins coûteux en vue de leur conservation à court terme (en ligne) et à long terme (hors ligne).
- Services d'application : toutes les applications d'investigations principales sont exécutées dans le datacenter, diminuant l'activité/la latence du réseau et améliorant les performances. L'analyste d'investigation peut ainsi exécuter plusieurs instanciations d'applications à partir d'une seule station de travail sans aucune dégradation des performances.
- Services d'intégrité : suite de produits logiciels commerciaux prêts à l'emploi qui protège les applications et les données contenues au sein du système contre tout code illégal ou malveillant. Elle permet toutefois à un analyste d'exécuter tout code ou application suspect(e) dans un environnement isolé et sécurisé.
- Services de confidentialité : périmètre de sécurité permettant d'éliminer les fuites de données non autorisées.
- Gestion des affaires : intégration optionnelle avec le logiciel existant de gestion des affaires des forces de police ou des agences.
- Services supplémentaires : Dell peut ajouter des services supplémentaires à sa solution de base, comme la traduction (de texte, de bandes audio et de vidéos) et la recherche d'entreprise.

À propos de Dell

Dell a été fondée en 1984 par Michael Dell sur la base d'un concept simple : en vendant des systèmes informatiques directement à nos clients, nous serions en mesure de mieux comprendre leurs besoins et de leur fournir efficacement la solution informatique la plus performante et la plus adaptée. Notre stratégie commerciale en constante évolution combine notre modèle de relation directe avec le client avec de nouveaux réseaux de distribution qui nous permettent de satisfaire les clients dans le monde entier, qu'il s'agisse d'administrations publiques, d'entreprises ou de particuliers. Dell travaille en collaboration avec les forces de police, les agences de sécurité, les intégrateurs de systèmes et les fournisseurs de solutions spécialisées pour simplifier les complexités liées à la gestion et au traitement actuels des données et des informations suspectes. Dell conçoit, fabrique et personnalise ses produits et services, des solutions mobiles embarquées sur les véhicules aux solutions d'investigation numérique évolutives de niveau entreprise. Nous pouvons fournir aux forces de police et aux agences de sécurité un accès sécurisé, distant et en temps réel aux informations essentielles et au travail collaboratif.

Les produits Dell permettant d'améliorer les décisions, d'accélérer les actions et d'optimiser la souplesse sont notamment les suivants :

- Ordinateurs portables Latitude™ pour un usage mobile et souple y compris via des solutions embarquées dans des véhicules pour des communications en temps réel.
- Stations de travail Dell™ Precision™ et serveurs PowerEdge™ pour les applications de calculs intensifs telles que l'investigation numérique, la simulation et la modélisation de datacenters économes en énergie, ainsi que les infrastructures de commande et de contrôle.
- Solutions de stockage Dell/EMC, Dell EqualLogic™ et PowerVault™ fournissant un accès évolutif, protégé et interopérable ainsi que des solutions de sauvegarde, de restauration et d'archivage pour les informations sensibles et le renseignement.
- Les services internationaux de Dell peuvent fournir un ensemble de plans pratiques et réalisables pour simplifier l'environnement informatique, notamment des services de conseil en infrastructure, des services de déploiement, des services gérés et Dell ProSupport.

1. La police recherche de nouvelles solutions d'analyse des disques durs à distance, The Register, 29 avril 2009 www.theregister.co.uk/2009/04/29/remote_hard_drive_forensics