

# Dell SafeData

## La plateforme Absolute

### CONSULTEZ ET SÉCURISEZ VOS DONNÉES ET VOS APPAREILS

#### La seule solution intégrée au firmware pour assurer l'intelligence et la résilience des points de terminaison

Vous avez implémenté toutes les stratégies appropriées, mais les outils traditionnels de gestion et de sécurité des points de terminaison présentent des limitations et des angles morts. Ils peuvent être désactivés par les utilisateurs finaux ou être en concurrence avec d'autres programmes pour utiliser les ressources des appareils, et ils peuvent présenter des dysfonctionnements soudains.

Par conséquent, vos points de terminaison deviennent difficiles à consulter, à contrôler et à sécuriser. Cela entraîne des inexactitudes, des inefficacités opérationnelles et des failles de sécurité, ce qui compromet votre capacité à détecter les problèmes de manière fiable et à répondre aux menaces en toute confiance. Le résultat est inéluctable : audits incertains, pertes de ressources, violations de données et de conformité.

Dell intègre la technologie Persistence<sup>®</sup> brevetée d'Absolute dans le firmware, avant que les appareils ne quittent l'usine. Persistence<sup>®</sup> corrige et réinstalle automatiquement l'agent Absolute à chaque séquence de démarrage, même si l'image système a été réinstallée sur l'appareil ou même si le disque dur a été remplacé.

Dès son activation, Absolute fournit la résilience dont vous avez besoin grâce à une attache numérique incassable. Ainsi, vous pouvez toujours consulter et contrôler vos appareils et corriger les failles de sécurité, quoi qu'il arrive.



# INTELLIGENCE SUR LES RESSOURCES

## Visibilité persistante sur les points de terminaison : sur le réseau et en dehors

Absolute garantit que votre attache numérique à chaque appareil reste intacte. Vous bénéficiez ainsi d'une intelligence fiable sur tous vos points de terminaison, que ce soit sur le réseau de votre entreprise ou en dehors.

Vous pouvez maintenir votre inventaire matériel et logiciel toujours à jour, rationaliser la gestion du cycle de vie de vos appareils, accélérer vos audits et vos opérations quotidiennes, recevoir des alertes lorsque les appareils se déplacent, détecter les ressources sous-utilisées pour éviter le gaspillage, et utiliser ces informations pour prendre des décisions plus rentables.

### Vos critères de réussite :



**Intégré et autoréparant** : la seule plateforme optimisée par la technologie d'autoréparation intégrée dans le firmware de votre appareil vous permet de consulter et de contrôler l'ensemble de votre parc à partir d'un tableau de bord unique, quel que soit le réseau ou la plateforme.



**Analytique matérielle** : surveillez chaque point de terminaison et créez un inventaire complet et toujours à jour de tous vos points de terminaison, avec des centaines de points de données par appareil.



**Géolocalisation** : suivez avec précision l'emplacement physique de tous les appareils qui vous intéressent, à tout moment, sur votre réseau ou en dehors, avec notamment les journaux historiques.



**Gestion du cycle de vie à distance** : rationalisez le provisionnement, la réaffectation et la désaffectation des appareils distants, avec notamment la possibilité d'automatiser la maintenance régulière, de résoudre les problèmes liés aux appareils et d'effectuer un effacement certifié en fin de vie.



**Rapports logiciels et alertes** : maintenez votre inventaire logiciel à jour, éliminez l'IT fantôme et détectez l'absence des applications obligatoires.



**Utilisation des appareils** : comprenez la façon dont les appareils sont utilisés et identifiez les ressources inactives pour déterminer lesquelles doivent être réallouées ou désactivées.

# SÉCURITÉ RÉSILIENTE DES POINTS DE TERMINAISON

## Évaluez votre posture de sécurité et appliquez des contrôles de sécurité

À partir d'une console unique basée sur le Cloud, créez des rapports sur la conformité aux normes ou aux réglementations, puis partagez ces informations avec toutes les parties prenantes de votre organisation. Détectez les écarts de configuration et les failles de sécurité, appliquez automatiquement les applications de sécurité et déployez à distance des commandes et des workflows pour traiter les failles de sécurité et automatiser les tâches incontournables.

Absolute est la première et la seule solution de visibilité et de contrôle des points de terminaison qui préserve tout autre contrôle de sécurité. En étendant la résilience d'Absolute à d'autres applications, vous activez l'autoréparation pour l'ensemble de votre pile de sécurité, et étendez cette sécurité renforcée à l'ensemble de votre parc sans intégrer d'appareils. Lorsque les points de terminaison s'éloignent de l'image souhaitée, Absolute les force à s'y conformer à nouveau, afin d'éviter les violations de données catastrophiques et de maintenir la continuité d'activité.

### Vos critères de réussite :



**Analyse comparative des normes** : générez des rapports sur la conformité aux normes de cybersécurité ou aux réglementations en matière de confidentialité des données, signalez les appareils sur lesquels le chiffrement ou un programme anti-logiciel malveillant est manquant, et résolvez l'écart de conformité.



**Renforcement de la configuration** : découvrez les points faibles et les écarts par rapport aux configurations de point de terminaison souhaitées et ajustez-les à grande échelle.



**Continuité des applications** : arrêtez les interruptions de la productivité de l'utilisateur et de la continuité d'activité grâce à l'autoréparation des applications.



**Garantie de protection des données** : renforcez la protection de vos données en préservant des contrôles de sécurité tels que le chiffrement, la protection contre les logiciels malveillants, le VPN, la gestion des points de terminaison et bien plus encore, sans intervention humaine.



**Détection et résolution des failles de sécurité** : localisez les points de terminaison exécutant des versions vulnérables du système d'exploitation et déployez des mises à jour urgentes ou implémentez des solutions de contournement de protection, sur le réseau de l'entreprise ou en dehors.



**Workflows automatisés** : déployez à distance des commandes et des workflows automatisés pour combler les failles de sécurité rapidement et à grande échelle.

## RÉPONSE AUX RISQUES EN TOUTE CONFIANCE

### Détectez les incidents de sécurité, puis répondez-y et récupérez avec succès

Avec Absolute, vous pouvez accéder à vos appareils en profondeur afin de détecter les données sensibles en danger et d'identifier les appareils manquants ou les comportements suspects. À chaque étape d'un incident (précurseur, faille de sécurité, violation ou récupération), Absolute vous offre une suite d'outils persistants pour répondre à l'incident et récupérer de manière fiable.

Recevez instantanément des alertes en cas de failles de sécurité, d'expositions ou de nouvelles activités sur des appareils qui ont disparu. Verrouillez-les et effacez les données qu'ils contiennent. Prouvez aux organismes de réglementation que les données ont toujours été protégées lors d'un incident. Utilisez les journaux historiques pour éviter les notifications de violation, en savoir plus sur la cause première et éviter d'autres incidents similaires.

### Vos critères de réussite :



**Recherche des données des points de terminaison** : localisez les données sensibles, telles que les informations personnelles, les informations personnellement identifiables, les informations sur la santé protégées ou les informations financières personnelles, qui sont en danger ou vulnérables aux violations des réglementations en matière de confidentialité telles que l'HIPAA, le RGPD, le CJIS ou le CCPA.



**Détection précoce des incidents** : recevez une alerte en cas de désactivation des contrôles et de preuves d'altération de l'appareil, et soyez informé quand les appareils contenant des données se retrouvent au mauvais endroit.



**Rapports sur les appareils manquants** : détectez les appareils mis hors ligne pendant un certain temps et signalez-les comme manquants pour être alerté dès qu'ils se connectent à Internet.



**Protection des données en cas d'urgence** : bloquez ou effacez à distance les appareils compromis et obtenez un certificat de nettoyage, évitez le transfert de données et mettez en place de nombreuses autres mesures correctives à grande échelle.



**Experts en investigation** : faites appel à l'équipe Absolute d'enquêteurs expérimentés, qui travaillent en étroite collaboration avec les forces de l'ordre pour poursuivre les criminels, récupérer un appareil volé ou identifier l'utilisateur à l'aide d'outils d'analyse approfondie.

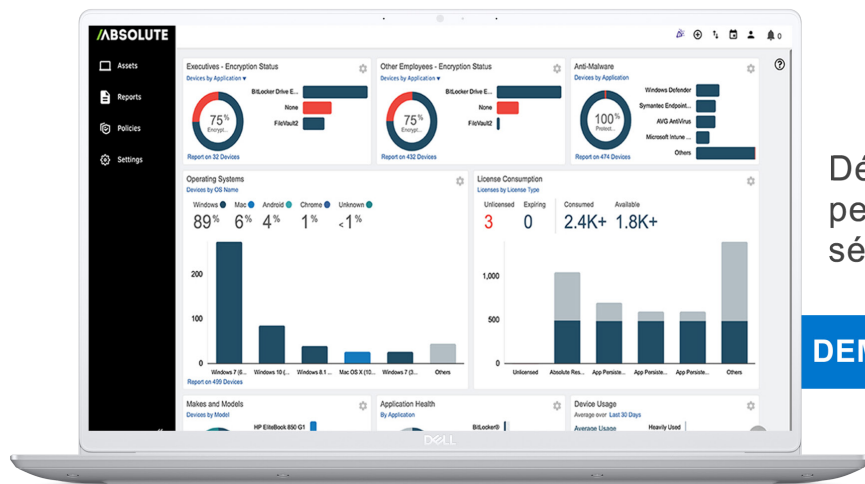


**Preuve de conformité** : utilisez les journaux historiques pour vérifier que la protection des données était en vigueur pendant les incidents et pour en savoir plus sur la cause première, afin d'itérer vos règles de sécurité.

# AYEZ L'ASSURANCE QUE VOS POINTS DE TERMINAISON SONT SÉCURISÉS

Aujourd'hui, les organisations distribuées ont besoin d'une visibilité et d'un contrôle persistants sur les points de terminaison. Pour suivre le rythme des collaborateurs mobiles et atteindre la résilience organisationnelle, les équipes IT et de sécurité s'appuient sur la puissante fusion entre l'intelligence des ressources, la sécurité résiliente des points de terminaison et la réponse aux risques en toute confiance. Elles s'appuient sur la plateforme Absolute.

Pour en savoir plus sur la façon dont Absolute peut vous aider, rendez-vous sur : [absolute.com/platform](https://absolute.com/platform)



Découvrez comment Absolute peut transformer l'IT et la sécurité de votre organisation

**DEMANDER UNE DÉMO**

## Rendez vos applications et outils de sécurité inviolables, uniquement avec Absolute Resilience

Absolute Resilience contient toutes les fonctionnalités de Visibility et de Control, y compris un flux persistant de données, des inventaires automatisés et la possibilité d'effacer les données ou de verrouiller les appareils à risque.



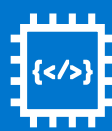
### Persistence des applications

Donnez à vos applications stratégiques la possibilité de se réparer et de se réinstaller elles-mêmes après des tentatives de désactivation, de suppression ou de reconfiguration.



### Recherche des données des points de terminaison

Définissez des règles pour analyser vos appareils Windows et Mac ou les données sensibles à risque, y compris les informations personnelles, les informations financières personnelles, les numéros de sécurité sociale, le RGPD et la propriété intellectuelle, sur votre réseau ou en dehors, puis évaluez le coût de l'exposition.



### Portée absolue

Évaluez et prenez des mesures correctives sur 100 % de vos appareils Windows et Mac, avec une bibliothèque de scripts préconfigurés et personnalisés.



### Investigations

Laissez l'équipe d'Absolute, composée d'anciens membres des forces de l'ordre, retrouver vos appareils perdus ou volés, puis faites équipe avec les forces de l'ordre locales pour les récupérer.

	Absolute Visibility	Absolute Control	Absolute Resilience
Console Absolute	•	•	•
Suivi du matériel	•	•	•
Mesure de l'utilisation des appareils	•	•	•
Surveillance des logiciels installés	•	•	•
Évaluation de la posture de sécurité	•	•	•
Surveillance de l'intégrité des applications stratégiques	•	•	•
Intégration avec des produits tiers	•	•	•
Détection des déplacements d'appareils non autorisés		•	•
Gel à distance des appareils		•	•
Suppression des données à distance		•	•
Activation de la protection du firmware		•	•
Activation de l'autoréparation des applications stratégiques			•
Identification des données sensibles sur les appareils			•
Requête et correction à distance des appareils à grande échelle			•
Enquête et récupération des appareils volés			•

### Plateformes prises en charge :



Contactez votre spécialiste Dell Endpoint Security dédié dès aujourd'hui à l'adresse [endpointsecurity@dell.com](mailto:endpointsecurity@dell.com) pour en savoir plus sur les produits Dell SafeData, qui peuvent vous aider à améliorer votre posture de sécurité.

Pour en savoir plus, consultez le site [DellEMC.com/endpointsecurity](https://DellEMC.com/endpointsecurity)  
© 2022 Dell Technologies et ses filiales.

**ABSOLUTE**<sup>®</sup>