DELL Technologies

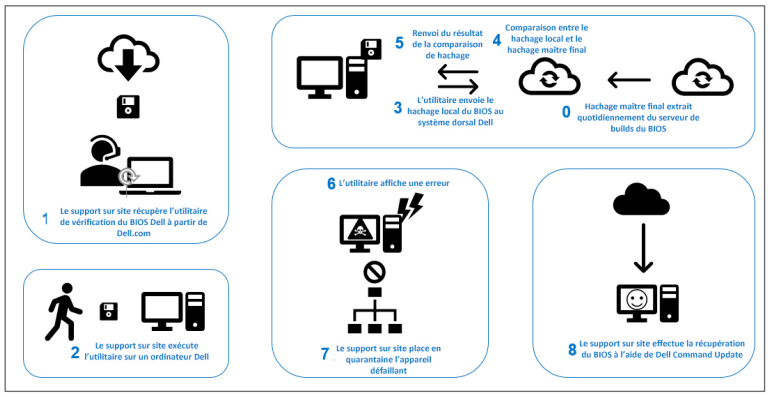
Dell SafeBIOS

SÉCURITÉ INTÉGRÉE SUR LES ORDINATEURS PROFESSIONNELS LES PLUS SÉCURISÉS DU SECTEUR

LA SOLUTION DELL SAFEBIOS RÉDUIT LE RISQUE D'ALTÉRATION DU BIOS AVEC LA DÉTECTION INTÉGRÉE DES ATTAQUES DE FIRMWARE

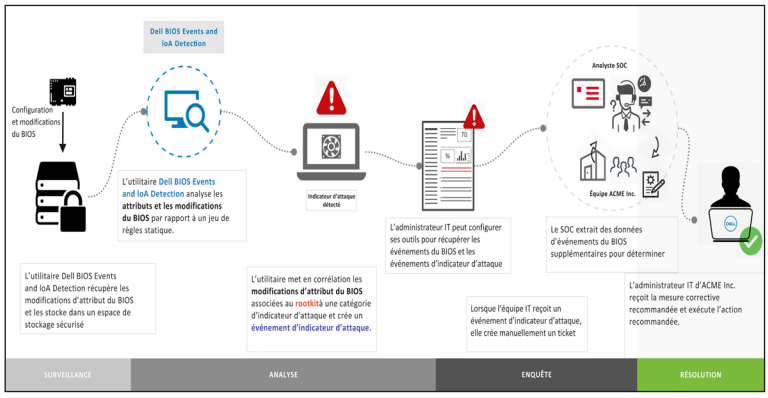
Alerte d'altération du BIOS améliorée

Maintenir la protection des données de l'organisation, qu'il s'agisse de sa propriété intellectuelle ou des informations personnelles identifiables, constitue la base de la sécurité des données. Les pirates ne cessent de rivaliser d'ingéniosité. En effet, les menaces courantes sont plus fréquemment contrées, incitant les cybercriminels à rechercher des méthodes plus avancées pour obtenir ces informations critiques. Les solutions de sécurité des points de terminaison, comme les antivirus de nouvelle génération ou les solutions de détection et réponse au niveau des points de terminaison deviennent plus performantes. Les vecteurs d'attaque sont donc moins nombreux et les pirates sont contraints de se tourner vers d'autres cibles pour leurs cyberattaques.



La protection du BIOS est essentielle pour la stratégie sécuritaire d'une organisation.

Les solutions populaires de sécurité des points de terminaison se concentrent principalement sur le système d'exploitation local et les applications au-dessus. Le niveau le plus bas de la pile de l'ordinateur, le BIOS, est ainsi vulnérable aux attaques malveillantes qui peuvent neutraliser l'intégralité de votre système. Lorsqu'un logiciel malveillant prend le contrôle du BIOS, il devient propriétaire de l'ordinateur et a accès au réseau. Le BIOS est une cible très sensible : les attaques envahissent la racine de confiance de l'ordinateur et s'y ancrent durablement. Si un pirate accède au BIOS, il peut endommager l'ensemble des fonctionnalités de sécurité des points de terminaison d'un appareil, et même l'intégralité du réseau d'une organisation. Ce type d'attaque est très technique et, quand elle atteint sa cible, très destructrice. Cette faille de sécurité flagrante devient de plus en plus préoccupante, car les pirates recherchent de nouveaux vecteurs d'attaque.



Dell SafeBIOS répond à ce changement de paradigme en matière de sécurité

En raison de la multiplication des attaques propres au BIOS et des nouvelles variantes de logiciels malveillants capables de se réinstaller au sein du BIOS, les organisations ont besoin d'une méthode plus sophistiquée pour protéger leurs systèmes, mais aussi pour vérifier en toute confiance que ces derniers ne sont pas déjà infectés.

Dell intègre la vérification post-démarrage à ses ordinateurs professionnels. Le département IT a ainsi la certitude que le BIOS des collaborateurs n'a pas été altéré. Au lieu de stocker les informations du BIOS sur le matériel lui-même, qui est susceptible d'être infecté, la solution Dell SafeBIOS fournit une fonctionnalité de vérification hors hôte du BIOS. SafeBIOS utilise un environnement Cloud sécurisé pour comparer chaque image de BIOS aux mesures officielles contenues dans le laboratoire de conception des BIOS.

Dell SafeBIOS

En outre, Dell automatise la détection précoce des événements et des indicateurs d'attaque du BIOS, ainsi que des configurations à haut risque en offrant une visibilité sur l'historique de configuration du BIOS. L'extraction et l'analyse continues des configurations et des événements du BIOS feront émerger les points de terminaison vulnérables et alerteront les équipes IT en cas d'augmentation des risques, ce qui leur permettra de prendre des mesures correctives.

Si le BIOS est infecté ou altéré, Dell offre à ses clients des options de réinitialisation flexibles. Le BIOS contaminé peut ainsi être analysé afin de comprendre la nature de l'attaque et permettre aux clients de vérifier l'intégrité du BIOS via le processus hors hôte, sans interrompre le processus de démarrage. SafeBIOS offre aux clients une plus grande visibilité sur les modifications du BIOS, ainsi qu'une garantie supplémentaire pour maintenir les menaces à distance.

En outre, si un BIOS est infecté, l'image du BIOS est automatiquement capturée à des fins d'analyse et de correction suite au processus de récupération du BIOS.

Intégrations de partenaires
Ces fonctionnalités combinées permettent d'identifier et de corriger plus rapidement les risques potentiels. La fonctionnalité autonome est actuellement disponible auprès du support Dell.

VMware Workspace ONE fournit à la direction IT une nouvelle visibilité sur l'état du BIOS pour la gestion unifiée des points de terminaison. L'intégration dans VMware Workspace ONE permet au département IT de configurer des workflows automatisés pour envoyer des mises à jour en direct et rétablir la conformité des appareils.

La puissance combinée de VMware Carbon Black Audit and Remediation et de la solution Dell SafeBIOS offre une sécurité de pointe à la fois au-dessus et en dessous du système d'exploitation et permet la télémétrie à partir de l'état de vérification du BIOS hors hôte sur la gamme d'ordinateurs professionnels Dell. La solution intégrée permet aux équipes IT et de sécurité d'automatiser la création de rapports sur l'état de la vérification afin de pouvoir corriger les failles résultant de l'altération du BIOS. Ce partenariat renforce la position de Dell en tant que fournisseur d'ordinateurs professionnels les plus sécurisés du marché.

Dell SafeBIOS fait partie de la gamme plus large de solutions de sécurité de point de terminaison Dell Trusted Devices, qui prennent en charge le point de terminaison au-dessus et en dessous du système d'exploitation pour une approche complète de la protection des données, notamment :

- SafeBIOS : profitez d'une visibilité sur les attaques cachées et les menaces de sécurité qui planent avec l'alerte d'altération du BIOS via la vérification hors hôte du BIOS exclusive de Dell[1], la capture d'images du BIOS et les événements et indicateurs d'attaque du BIOS.
- SafeID : seul Dell sécurise les informations d'identification des utilisateurs finaux dans une puce de sécurité dédiée. Cela permet de les protéger contre les logiciels malveillants qui recherchent et dérobent ce type de données.
- SafeScreen : les utilisateurs finaux peuvent travailler partout, tout en gardant leurs informations confidentielles privées avec un écran de confidentialité numérique intégré.
- SafeData : protégez les données sensibles sur l'appareil pour répondre aux réglementations de conformité et sécurisez les informations dans le Cloud pour offrir aux utilisateurs finaux la liberté de collaborer sereinement.
- SafeGuard and Response (optimisé par VMware Carbon Black et Secureworks) : bloquez, détectez et contrez les cyberattaques et les logiciels malveillants avancés pour rester productif, sans subir les interruptions et pertes de clientèle qu'une attaque peut créer.

Contactez votre spécialiste Dell Endpoint Security dès aujourd'hui à l'adresse endpointsecurity@dell.com pour découvrir comment nous pouvons vous aider à améliorer votre stratégie sécuritaire.

[1] D'après une analyse interne.