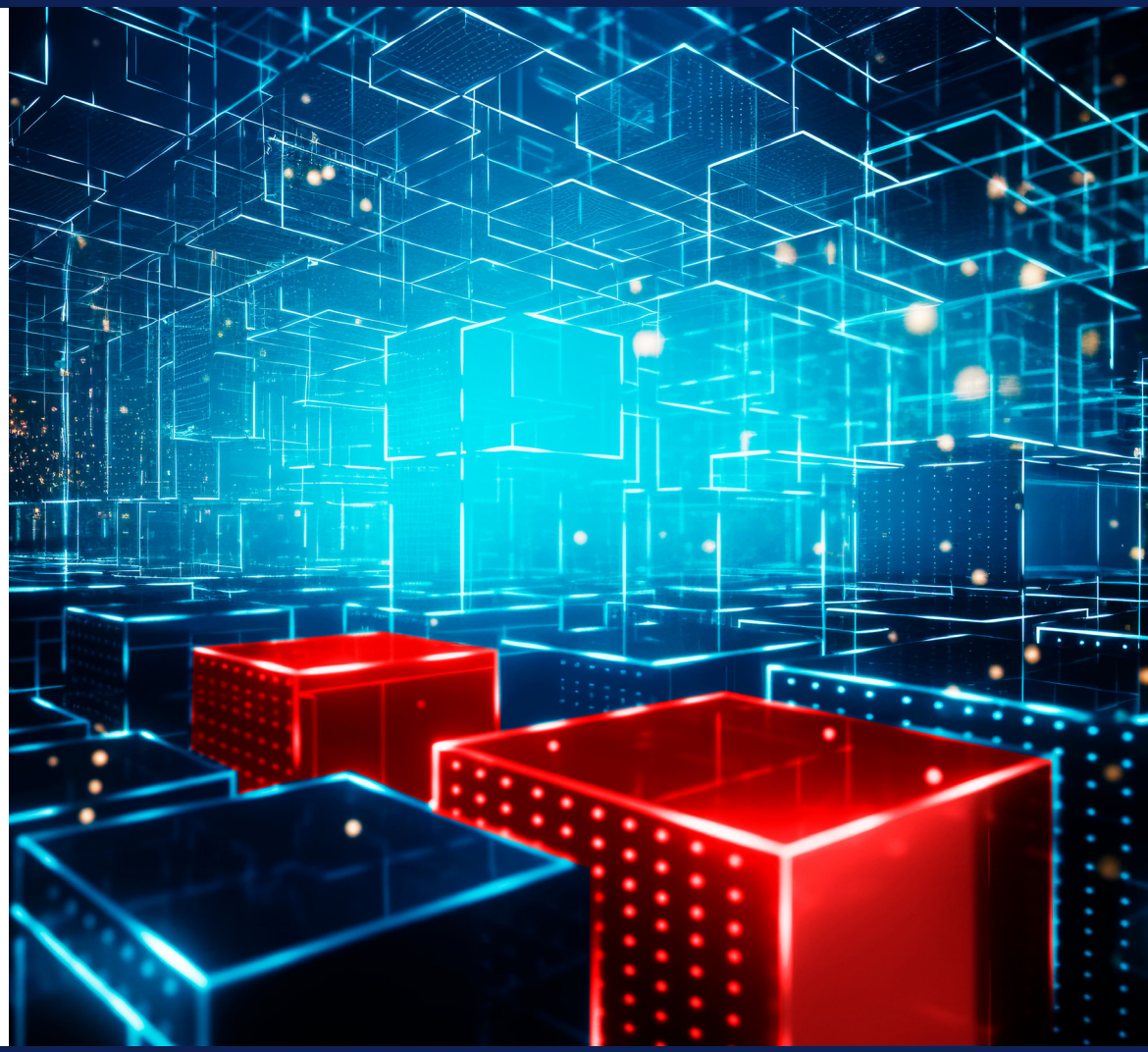
Utilisation sécurisée de l'IA au niveau des points de terminaison

Protégez les charges applicatives d'IA intégrée en utilisant des appareils sécurisés et modernes tout en tenant compte des menaces.



Résumé

L'IA intégrée présente d'énormes avantages, mais elle n'est pas exempte de cyberrisques. Dans cet e-Book, nous vous expliquons comment positionner votre entreprise en toute sécurité pour tirer parti de l'innovation en matière d'IA au niveau des points de terminaison.

Sommaire

Surface d’attaque de l’IA intégrée

Cibles potentielles

Toutes les technologies émergentes présentent un risque de cybersécurité pour une seule raison : leur nouveauté. Vous êtes face à l’inconnu. Nous avons été confrontés au même défi avec d’autres technologies telles que le Cloud Computing et la blockchain. Il en est de même pour l’IA intégrée. Pour atténuer ce risque, la meilleure approche consiste toujours à s’informer.

Avant de parler de la sécurité à mettre en place pour minimiser la surface d’attaque, il est utile d’identifier ce que nous sécurisons et les raisons. Imaginez un système de tuyaux dans un bâtiment commercial qui abrite plusieurs entreprises. Ces tuyaux transportent notamment l’eau et le gaz dans l’ensemble du bâtiment à diverses fins. Si ce contenu est contaminé ou bloqué, il devient inutile. Si les tuyaux qui le transportent sont endommagés ou corrompus, ils deviennent également inutiles. Tant les tuyaux que leur contenu doivent être en bon état de fonctionnement pour répondre aux besoins de leurs cas d’utilisation respectifs.►

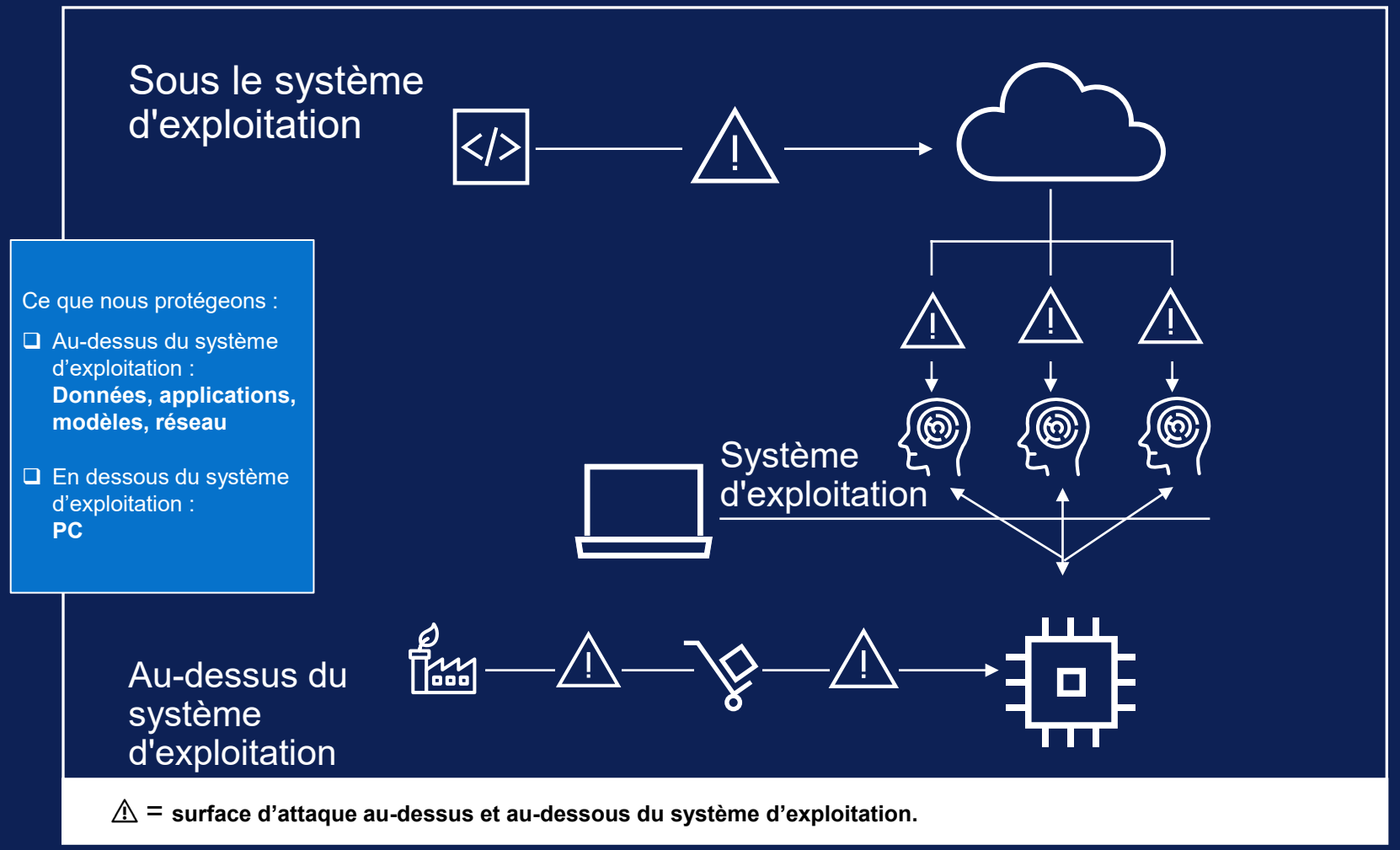
Surface d’attaque de l’IA intégrée (suite)

Cibles potentielles (suite)

Retour à l’IA au niveau des points de terminaison :

- Les tuyaux sont votre infrastructure : vos PC, vos réseaux d’entreprise. Votre méthode et votre lieu de travail.
- Le contenu des tuyaux représente les données, les applications et les modèles qui alimentent divers cas d’utilisation de l’IA. Les actifs et les ressources dont vous avez besoin pour travailler.

Vous l’avez deviné : les cyberattaquants ciblent les deux. Ils peuvent voler la propriété intellectuelle pour obtenir une rançon ou contaminer des données ou des modèles afin de perturber les opérations. Dans tous les cas, les conséquences peuvent être graves (dommages financiers et atteinte à la réputation et/ou examens réglementaires).►



Risques de sécurité au niveau des points de terminaison

Tactiques d'accès utilisées par les attaquants

À présent, abordons les méthodes utilisées par les attaquants pour accéder aux deux cibles.

Compromission des appareils. Comme expliqué dans le document Endpoint Security Market Insights de Forrester Research, Inc. (mars 2025), les PC font partie des principales cibles des cybermenaces modernes. Ce type d'attaques peut se produire bien avant que les tâches d'IA intégrée ne commencent (une **attaque de la chaîne logistique matérielle ou logicielle**, par exemple). Tout au long de la chaîne logistique, il existe des dizaines de points, voire des centaines, où une partie malveillante peut modifier des composants (circuits, firmwares, par exemple) pour introduire des vulnérabilités afin de les exploiter ultérieurement. Imaginez le désastre auquel s'expose une société d'investissement qui reçoit de tout nouveaux PC contenant des composants contrefaits.

Compromission des identités. Les violations basées sur le vol ou la compromission d'informations d'identification sont l'un des vecteurs d'attaque à la croissance la plus rapide. Ce n'est pas étonnant. Des informations d'identification valides permettent aux attaquants de se connecter à un PC, de se déplacer librement sur le réseau de l'entreprise et de rester indétectables pendant de longues périodes. D'après le dernier rapport sur le coût d'une violation de données d'IBM, l'identification et la maîtrise de ces violations ont nécessité en moyenne 292 jours, soit le délai le plus long de tous les vecteurs d'attaque étudiés. Les acteurs malveillants ne peuvent tout simplement pas ignorer un tel niveau d'accès. D'après une étude de Zscaler, les parties malveillantes utilisent l'IA générative pour optimiser le vol d'informations d'identification afin d'améliorer et de faire évoluer les attaques par hameçonnage. Appliqué à des données sensibles d'entraînement ou d'inférence ou directement à des modèles, cet accès non autorisé est classé comme une **attaque de la chaîne logistique des modèles**.

Menace interne. Selon une étude récente, comparées à d'autres vecteurs d'attaque, les **attaques internes malveillantes** ont entraîné les coûts les plus élevés, avec une moyenne à 4,99 millions de dollars. N'oubliez pas que les attaques internes peuvent se produire tout au long de la chaîne logistique du matériel, des logiciels et des modèles.►

Temps moyen qui s'écoule avant qu'un utilisateur ne soit victime d'un **hameçonnage** par e-mail : < 60 secondes*

292 jours : durée moyenne nécessaire pour détecter et maîtriser **la compromission d'informations d'identification****

Les attaques internes malveillantes coûtent en moyenne 4,99 millions de dollars**

** Source : Verizon DBIR, 2024*
*** Source : IBM Cost of a Data Breach, 2024*

Contre-mesures à mettre en place

Approches réduisant les risques

Aucune de ces cibles d'attaque n'est fondamentalement nouvelle. Les objectifs finaux des attaquants sont également les mêmes. Comme toujours, nous voulons nous concentrer sur la sécurité et la résilience de votre parc. **L'application de plusieurs contre-mesures** peut aider à réduire la surface d'attaque et à détecter immédiatement tout comportement suspect.

Une **approche Zero-Trust** permet de limiter les risques sur l'ensemble de votre parc. Ces principes (ne jamais faire confiance, toujours vérifier et surveiller en permanence) vous aident à garder une longueur d'avance sur les attaquants. Il est impossible de bloquer 100 % des attaques. Pour disposer d'une posture de sécurité solide, vous avez besoin **de visibilité et de contrôle** sur l'ensemble de votre écosystème IT.

En gardant ce cadre à l'esprit, réévaluez votre infrastructure, en particulier les systèmes et les processus qui interagissent avec l'IA. Quelles contre-mesures réduisent le risque de compromission des appareils, de compromission des identités et de menaces internes ?►

Ces principes Zero-Trust aident à se prémunir contre les risques et à réduire le champ d'action de la cyberactivité

Contre-mesures à mettre en place (suite)

Approches réduisant les risques (suite)

Il existe deux catégories globales de contre-mesures.

La sécurité « au-dessous du système d'exploitation » protège les appareils IA sur lesquels vous travaillez. Nous pouvons la diviser en deux parties :

- Protégez votre parc avec des appareils **conçus de façon sécurisée**. Pour cela, utilisez des PC IA qui sont sécurisés dès leur conception. Ces appareils sont développés sur la base de principes de conception sécurisés dans une chaîne logistique sécurisée.
- Protégez votre parc avec des appareils dotés d'**une sécurité intégrée**. Les PC IA sécurisés intègrent des couches de protection qui offrent une visibilité immédiate, jusqu'au BIOS et au silicium.

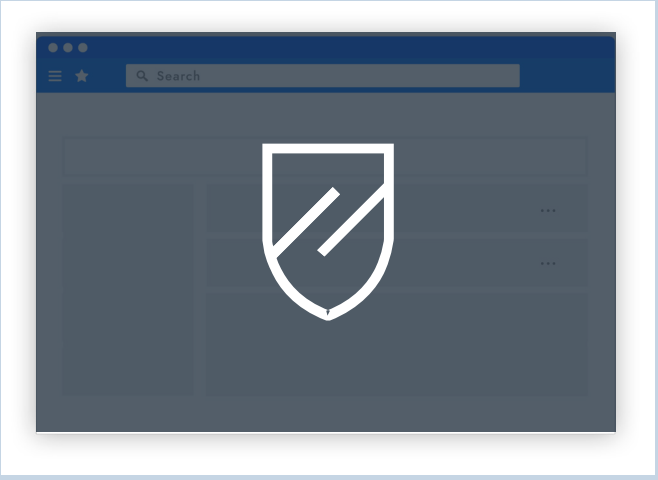
La sécurité « au-dessus du système d'exploitation » protège l'accès aux modèles d'IA. Protégez les données et les modèles *avec* lesquels vous travaillez ainsi que les réseaux d'entreprise *sur* lesquels vous travaillez avec **la sécurité logicielle**. Il est essentiel de protéger les opérations de sécurité de l'apprentissage automatique et de surveiller le trafic réseau des charges applicatives d'IA déployées.►

Sécurité sous le système d'exploitation

PC IA sécurisés

Sécurité du matériel et du firmware, sécurité de la chaîne logistique, base silicium

Sécurité au-dessus du système d'exploitation



Sécurité logicielle

Couche de sécurité supplémentaire pour les points de terminaison, les réseaux et les environnements Cloud

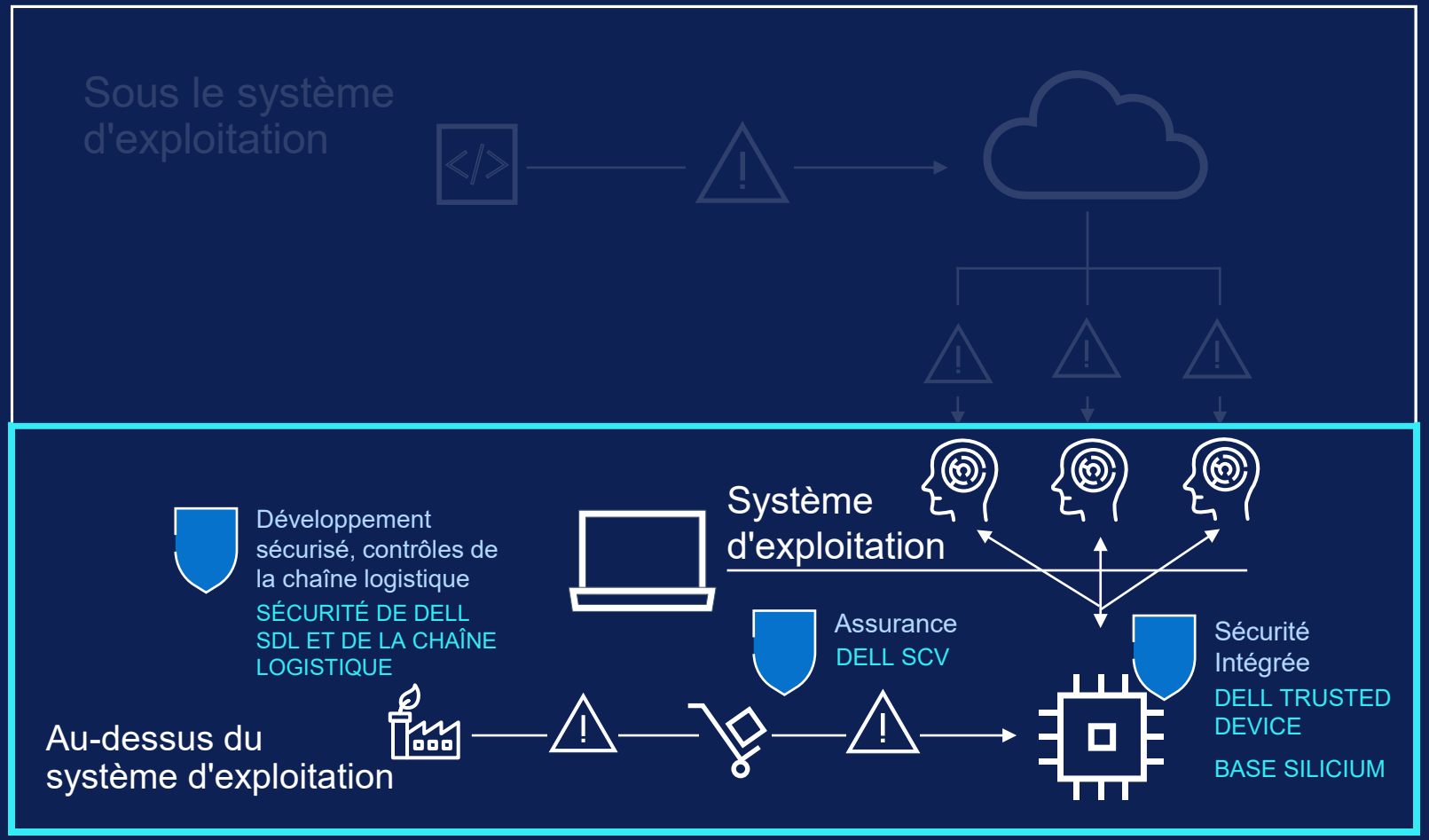
Services de sécurité et expertise disponibles pour une approche globale.

Application des meilleures pratiques à votre parc

PC IA de Dell : bénéficiez d'une sécurité de base pour votre parc

C'est là que Dell Trusted Workspace peut vous aider. Nos experts en technologies conçoivent et développent la sécurité de nos ordinateurs IA professionnels avec une compréhension approfondie des menaces.

Au-dessous du système d'exploitation, la conception sécurisée, les contrôles robustes de la chaîne logistique et la garantie de la chaîne logistique (facultative) garantissent la sécurité des PC dès le premier démarrage. La sécurité intégrée du matériel et du firmware protège le PC pendant son utilisation. Par exemple, les détections de modification au niveau du BIOS (Dell SafeBIOS) et la sécurité des informations d'identification sans mot de passe (Dell SafeID), exclusivités* de Dell, assurent la protection contre les accès non autorisés. De plus, les technologies de silicium Intel® fournissent une base pour protéger divers aspects de l'IA dans le cadre de son utilisation par les clients des PC IA. Par exemple, Intel aide à sécuriser les données d'IA au repos sur le client grâce à l'accélération du chiffrement des modèles sur disque.►



Application des meilleures pratiques à votre parc (suite)

PC IA de Dell : bénéficiez d'une sécurité de base pour votre parc (suite)

Pour compléter cette sécurité au-dessous du système d'exploitation, la technologie Persistence de notre partenaire Absolute peut être intégrée en usine pour une visibilité et un contrôle accrus tout au long du cycle de vie des PC. Cela permet, par exemple, la géolocalisation des appareils en cours d'acheminement et l'autoréparation des applications stratégiques dans le pire des cas.

Dell a créé un écosystème de solutions partenaires logicielles, notamment CrowdStrike Falcon XDR et Absolute Secure Access, qui mettent en œuvre les principes Zero-Trust pour protéger votre chaîne logistique de modèles contre les accès non autorisés **au-dessus du système d'exploitation**. Ces solutions vous permettent de créer et d'appliquer des stratégies avec des contrôles d'accès granulaires (par exemple, contrôle d'accès basé sur les rôles) afin de limiter le risque que des acteurs internes malveillants accèdent à vos modèles d'IA ou les manipulent.►

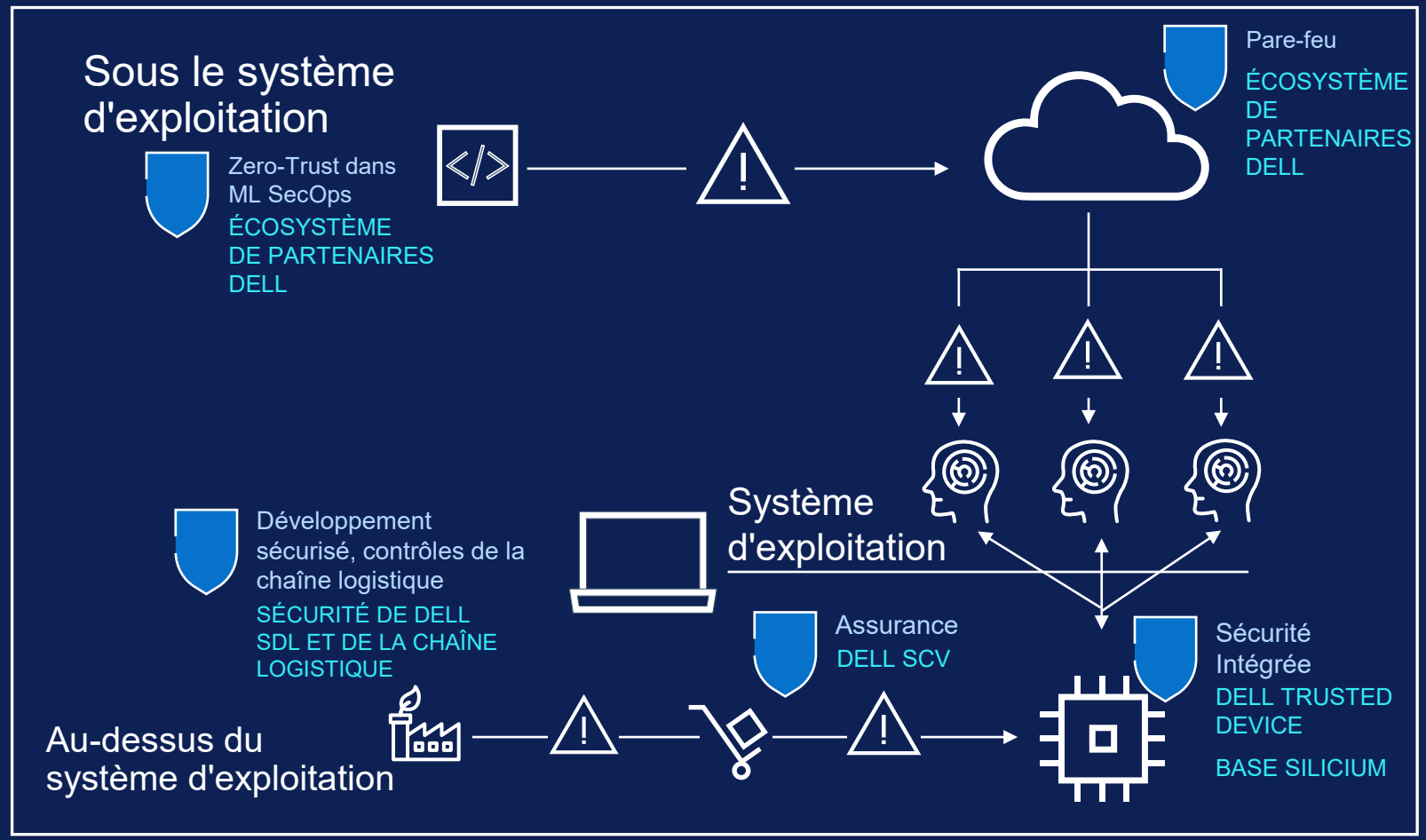
Application des meilleures pratiques à votre parc (suite)

PC IA de Dell : bénéficiez d'une sécurité de base pour votre parc (suite)

Tout cela constitue la ***Sécurité pour l'IA.*** Ces fonctionnalités protègent les charges applicatives d'IA intégrée contre les cyberattaques, ce qui vous permet de rester concentré sur l'innovation et l'augmentation du nombre de contrats ►

Bloquez les attaques avancées sur les points de terminaison grâce à des défenses matérielles et logicielles coordonnées

En collaboration avec Intel et CrowdStrike, Dell intègre la sécurité assistée par matériel dans les couches au-dessous et au-dessus du système d'exploitation. *En savoir plus >*



Éléments clés à retenir et étapes suivantes

Sécurisez l'IA au niveau des points de terminaison avec Dell

L'IA suscite beaucoup d'enthousiasme auprès des entreprises, mais celles-ci ne sont pas encore prêtes pour l'IA, comme l'indique une récente enquête menée par Absolute auprès des RSI. Une analyse portant sur des millions d'appareils a révélé que les PC étaient incapables d'absorber les nouvelles fonctionnalités d'IA de façon générale. **Dell peut apporter toutes les réponses.**

Développez et déployez des modèles d'IA sur une base sécurisée et moderne. La fin du support de Windows 10 est prévue pour octobre 2025. Les PC ne bénéficieront plus des mises à jour de sécurité, des mises à jour de fonctionnalités, ni du support Windows 10. Les appareils plus anciens peuvent ne pas répondre aux exigences de Windows 11 et ne pas disposer des dernières améliorations intégrées en matière de performances, de sécurité et d'IA. Optez pour des **Dell Pro** ou **Dell Pro Max équipés de processeurs Intel® Core™ Ultra avec Intel vPro®** afin d'optimiser la sécurité et de protéger les charges applicatives d'IA avec les **PC professionnels les plus sécurisés au monde*.** ►

Le support Windows 10 s'arrête en octobre.

Optez pour les derniers PC IA Dell équipés de processeurs Intel pour optimiser la sécurité et bénéficier d'améliorations en matière d'IA :

Boutique Dell Pro ● Dell Pro Max

*Les PC IA professionnels les plus sécurisés au monde**

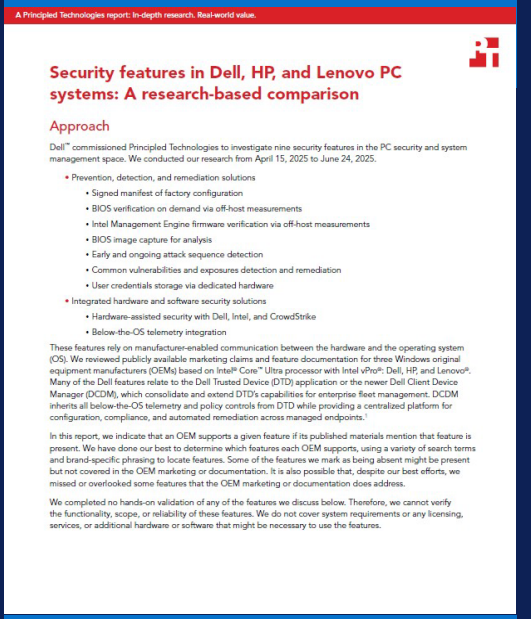
Découvrez les logiciels et services à valeur ajoutée qui améliorent votre posture de sécurité :

Logiciels et intégrations

Services

LEADER DU SECTEUR

Principled Technologies a constaté que la sécurité des PC IA professionnels de Dell et Intel l'emportait sur ses homologues


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Lire l'étude

Clauses de non-responsabilité

* D’après une analyse tierce réalisée par Principled Technologies comparant les PC IA professionnels Dell avec processeurs Intel avec HP et Lenovo, juillet 2025. Basé sur une analyse interne menée par Dell sur le marché mondial des PC, octobre 2024. S’applique aux PC équipés de processeurs Intel. Toutes les fonctionnalités ne sont pas disponibles sur tous les PC. Certaines fonctionnalités sont vendues séparément.

Pour en savoir plus :

Contactez-nous à l’adresse : Global.Security.Sales@Dell.com

Rendez-vous sur : Dell.com/Endpoint-Security

Suivez-nous : LinkedIn @DellTechnologies | X @DellTech

À propos de Dell Endpoint Security

La sécurité est un sujet complexe, quelle que soit la taille des organisations. **Faites appel à un partenaire expérimenté en matière de sécurité et de technologie pour moderniser la sécurité de vos points de terminaison**.

Dell Trusted Workspace permet de mieux sécuriser les points de terminaison pour un environnement IT moderne adapté au Zero-Trust. Réduisez la surface d’attaque et améliorez la cyberrésilience grâce à une gamme complète de solutions matérielles et logicielles de sécurité, caractéristiques de l’innovation Dell. Hautement coordonnée, notre approche de la sécurité allie solutions de protection intégrées et surveillance continue pour neutraliser d’éventuelles menaces. Les utilisateurs finaux maintiennent leur niveau de productivité et les équipes IT travaillent en toute sérénité avec des solutions de sécurité pensées pour l’univers Cloud actuel.