Technologies émergentes et menaces

Congrès de la CAPA 2026

18 août 2026

Vitesse du risque

La rapidité avec laquelle un risque peut apparaître, se propager et avoir des répercussions sur votre organisme.

Pourquoi est-ce important?

Dans le contexte dynamique d'aujourd'hui, les répercussions d'un risque ne se mesurent plus uniquement à son ampleur, mais aussi à la rapidité avec laquelle il évolue.
Comprendre la vitesse du risque aide les organismes à prévoir les changements, à établir les priorités efficacement et à intervenir avant que les répercussions ne s'aggravent.

Facteurs clés

Accélération technologique
Les nouvelles technologies et la connectivité accélèrent le rythme du changement.

Risques interreliés
Les risques sont davantage corrélés et peuvent déclencher des effets en cascade.

Vitesse de l'information
L'information se propage plus rapidement, tout comme les risques et les réactions.

Volatilité externe
Les bouleversements géopolitiques, économiques et sociétaux s'accélèrent.

Formule pour calculer la vitesse du risque

Vitesse du risque = Taux d'évolution x Taux de propagation x Intensité des répercussions x Exposition

Taux d'évolution
La rapidité avec laquelle les facteurs de risque évoluent.

Taux de propagation
La rapidité avec laquelle le risque se propage au sein de l'organisme ou de l'écosystème.

Intensité des répercussions
Les répercussions possibles si le risque se concrétise.

Exposition
La vulnérabilité de l'organisme au risque.

Visualisation de la vitesse du risque

VITESSE FAIBLE → VITESSE ÉLEVÉE

1. Apparition du risque
Un nouveau facteur de risque fait son apparition dans l'environnement.

2. Propagation du risque
Le risque se propage rapidement entre les fonctions, les systèmes et les emplacements.

3. Augmentation des répercussions
Le risque commence à perturber les activités, le rendement ou la confiance des intervenants.

4. Enjeu
Les répercussions financières, opérationnelles, réglementaires ou en matière de réputation s'intensifient.

5. Réduction du délai d'intervention
Le délai pour détecter le risque, prendre une décision et intervenir devient urgent.

Passer d'une attitude réactive à une attitude proactive

En mesurant et en surveillant la vitesse du risque, les organismes peuvent mettre en place des systèmes d'alerte précoce, se concentrer sur les risques pertinents et agir rapidement et en toute confiance.

Ce que vous pouvez faire

- Surveiller les principaux indicateurs de changement
- Évaluer la vitesse à laquelle les risques peuvent se propager
- Renforcer l'agilité et la capacité d'intervention

Vitesse de la menace

La rapidité avec laquelle une menace peut apparaître, se propager et avoir des répercussions sur votre organisme

Pourquoi est-ce important?

Les attaquants agissent rapidement, en tirant parti de l'automatisation, de l'intelligence artificielle (IA) et de leur portée mondiale. La vitesse de la menace mesure la rapidité avec laquelle les menaces dépassent votre capacité à les prévenir, à les détecter et à intervenir.
Comprendre la vitesse de la menace aide les organismes à renforcer leurs défenses, à déterminer la priorité des risques et à réduire le délai nécessaire à leur maîtrise.

Facteurs clés

Vitesse de l'attaquant
Les attaquants peuvent analyser, exploiter et se déplacer latéralement plus rapidement que jamais.

Élargissement de la surface d'attaque
Le nuage, les tiers, les identités et les dispositifs augmentent l'exposition.

Automatisation et IA
Les outils et l'IA permettent aux attaquants de s'adapter en temps réel.

Information et accès
Le Web clandestin, les fuites de données et les outils faciles à se procurer accélèrent la mise en œuvre des menaces.

Des premiers signes aux répercussions
Le délai entre le début de l'activité et les répercussions concrètes raccourcit.

Formule pour calculer la vitesse de la menace

Vitesse de la menace = **Vitesse de l'attaquant** La rapidité avec laquelle les auteurs de menace peuvent agir et s'adapter. x **Taux de propagation** La rapidité avec laquelle une menace se déplace au sein de votre environnement. x **Répercussions potentielles** Les préjudices potentiels si la menace se concrétise. x **Exposition** La vulnérabilité de l'organisme par rapport à la menace.

Visualisation de la vitesse de la menace

VITESSE DE LA MENACE FAIBLE → VITESSE DE LA MENACE ÉLEVÉE

1. Apparition de la menace
L'attaquant cerne une vulnérabilité ou une possibilité (p. ex. un actif exposé, une possibilité d'hameçonnage, une mauvaise configuration).

2. Déplacement de la menace
L'attaquant obtient l'accès et se déplace rapidement entre les systèmes, les utilisateurs ou les applications.

3. Propagation de la menace
Le mouvement latéral ou la propagation accroît la portée ainsi que l'exposition des données ou des systèmes.

4. Répercussions
Une perte de données, une perturbation, une fraude ou toute autre répercussion importante se produit.

5. Réduction du délai d'intervention
Le délai pour détecter la menace et intervenir est trop court pour que les mesures de contrôle traditionnelles puissent être efficaces.

Passer de la réactivité à la résilience

Réduire la vitesse de la menace en limitant les possibilités pour les attaquants et en accélérant la détection et l'intervention.

Réduire l'exposition | Détecter tôt | Intervenir plus rapidement | Renforcer continuellement

Ce que vous pouvez faire

- Surveiller continuellement les activités externes et internes liées aux menaces.
- Prioriser les mesures correctives en fonction de l'exploitabilité et des répercussions.
- Utiliser les renseignements sur les menaces pour prévoir les activités des attaquants et les perturber.
- Automatiser la détection et l'intervention pour réduire la durée de présence des attaquants.
- Mettre à l'essai, apprendre et s'adapter pour rester à l'avant-garde.

Vitesse de la menace par rapport à vitesse du risque

Deux concepts liés, mais distincts. L'un est axé sur l'attaquant, l'autre sur l'organisme.

Vitesse de la menace

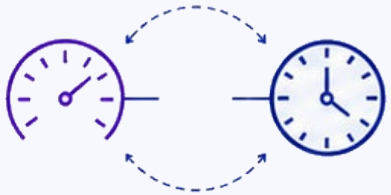
La rapidité avec laquelle une menace peut apparaître, se propager et avoir des répercussions sur votre organisme.

Vitesse du risque

La rapidité avec laquelle un risque peut apparaître, se propager et avoir des répercussions sur votre organisme.

DIMENSION	VITESSE DE LA MENACE	VITESSE DU RISQUE
Accent	Comportement et capacités de l'attaquant	Répercussions opérationnelles et exposition organisationnelle
Question principale	Avec quelle rapidité un attaquant peut-il réaliser ses objectifs?	Avec quelle rapidité les risques qui en découlent pourraient-ils avoir des répercussions sur notre organisme?
Perspective	De l'extérieur vers l'intérieur (perspective axée sur l'attaquant)	De l'intérieur vers l'extérieur (perspective axée sur l'organisme)
Facteurs clés	Vitesse de l'attaquant, outils, tactiques, infrastructure, automatisation et portée	Taux d'évolution, propagation au sein de l'organisme, intensité des répercussions et exposition
Ce qui est mesuré	Vitesse du cycle de vie de la menace : émergence -> déplacement -> répercussions	Vitesse de la concrétisation du risque : émergence -> propagation -> répercussions
Objectif	Renforcer la détection, la prévention et l'intervention en ce qui concerne les activités des attaquants.	Déterminer l'ordre de priorité des risques, affecter des ressources et protéger la valeur.
Exemple	Un auteur de menace peut passer d'un accès initial à l'élévation des privilèges en quelques minutes.	Une attaque par rançongiciel pourrait entraîner le chiffrement de systèmes essentiels à l'échelle de l'organisme en quelques heures.

COMMENT SONT-ELLES LIÉES?



Une vitesse de la menace élevée augmente la probabilité du risque et peut accroître la vitesse du risque.

Réduire la **vitesse de la menace** permet de ralentir l'attaquant.

Réduire la **vitesse du risque** permet de limiter les dommages.

Le fait de miser sur ces deux mesures permet de renforcer la résilience de l'organisme.

POINT À RETENIR

Il est impossible de freiner toutes les menaces, mais il est possible d'influencer la vitesse de la menace et du risque afin de ralentir l'attaquant et de limiter les répercussions si la menace se concrétise.

- Mesurer les deux.
- Améliorer les deux.

Il faut être plus rapide que la menace.

Aperçu des menaces

Les cyberrisques évoluent vers des modes d'attaque mixtes qui combinent automatisation, usurpation d'identité, extorsion, exploitation de vulnérabilités et accès par des tiers. Les dirigeants devraient se concentrer sur la rapidité avec laquelle ces modes d'attaque peuvent avoir des répercussions opérationnelles.

01 Accélération de l'IA

- L'IA générative renforce les techniques d'attaque, notamment les processus de reconnaissance et d'extorsion.
- Les principaux enjeux sont une réduction des efforts que doivent déployer les attaquants, une exécution plus rapide et une fraude psychologique convaincante.
- Il faut considérer l'IA comme un accélérateur pour l'ensemble des modes d'attaque actuels.

02 Identité / logiciel-service (SaaS)

- L'hameçonnage vocal, la saisie de justificatifs d'authentification multifactorielle, l'utilisation malveillante de jetons et la manipulation de services de dépannage peuvent permettre d'obtenir un accès étendu au moyen d'une seule identité.
- Les plateformes SaaS concentrent les données des clients et des employés, les exposant ainsi à un risque d'exfiltration.
- Il faut mettre l'accent sur les comptes présentant un risque élevé et réinitialiser les chemins et les intégrations.

03 Rançongiciel

- Verizon indique que des rançongiciels sont en cause dans près de la moitié des atteintes à la sécurité, l'extorsion demeure un mode d'attaque bien présent.
- L'état de préparation repose sur des procédures de reprise mises à l'essai, les droits en matière de décision, la communication et les processus d'acheminement aux échelons supérieurs.
- Le vol de données peut créer des pressions, même sans un chiffrement complet.

04 Chaîne de vulnérabilité

- Les failles logicielles, les chemins de code malveillant, les secrets dans l'environnement CI/CD (intégration et déploiement continus) et les extensions peuvent passer de la faiblesse à l'interruption.
- La surveillance devrait comprendre des seuils de correctifs, l'exposition et les contrôles des dépôts ainsi que l'accès à ceux-ci.
- Les chemins de développement et d'exploitation peuvent présenter des risques sur le plan de la vitesse ainsi que des risques cachés.

05 Appareils mobiles / réseaux sociaux

- La pression des attaques évolue vers les messages texte, les appels et les flux mobiles pour lesquels les utilisateurs répondent rapidement.
- La sensibilisation doit viser des essais relatifs à l'hameçonnage vocal, à l'hameçonnage par message texte et aux demandes d'approbation urgentes, et non pas uniquement les courriels.
- Les contrôles doivent s'adapter aux méthodes utilisées par les attaquants.

Les 20 principales technologies émergentes – 2027 à 2030

Technologies appelées à transformer le monde des affaires et la société dans les années à venir

2027
Court terme (1 à 2 ans)

1	Génie logiciel soutenu par l'IA augmentée	Accélère le développement, améliore la qualité et diminue les coûts.
2	Agents intelligents (échelle organisationnelle)	Automatise des tâches complexes et améliore la productivité humaine.
3	Nuage hybride (y compris nuage souverain)	Offre flexibilité, contrôle et résilience au sein d'un environnement axé sur « le nuage d'abord ».
4	Réseau maillé de cybersécurité	Renforce la sécurité au moyen d'une protection évolutive à vérification systématique.
5	Tissu de données	Unifie les données dans l'ensemble des sources à l'appui de renseignements fiables et de l'IA.
6	Applications composables	Permet une innovation plus rapide au moyen de blocs fonctionnels modulaires et réutilisables.
7	Réseau 5G/6G privé (adoption précoce)	Offre une connectivité sécurisée à haut rendement pour l'informatique en périphérie et l'Internet des objets.

2028 à 2029
Moyen terme (2 à 3 ans)

8	AI TRiSM (gestion de la confiance, des risques et de la sécurité de l'IA)	Renforce la confiance dans l'IA et assure une adoption sécuritaire et responsable à l'échelle.
9	Jumeaux numériques (échelle organisationnelle)	Optimise les opérations et réduit les coûts, les risques et les temps d'arrêt.
10	Technologies quantiques (cryptographie post-quantique)	Protège les données et les systèmes contre les menaces liées à l'informatique quantique.
11	IA en périphérie	Permet des décisions en temps réel à proximité de l'endroit où les données sont créées.
12	Technologies climatiques (favorisant la carboneutralité)	Accélère la transition vers un avenir plus durable à faibles émissions de carbone.
13	Biologie synthétique (applications industrielles)	Créé de nouveau matériaux, processus et solutions relatifs à la santé et à la durabilité.
14	**Robotique (collaborative et autonome)**	Renforce la main-d'œuvre et améliore la sécurité, la qualité et la productivité.

2030
Long terme (3 ans et plus)

15	Intelligence artificielle générale (IAG)	A le potentiel de révolutionner le travail intellectuel et l'innovation.
16	Informatique spatiale (réalité étendue avancée)	Transforme notre façon d'interagir, de collaborer et de découvrir le monde.
17	Informatique quantique (avantage dans la pratique)	Résout des problèmes complexes que les ordinateurs actuels ne peuvent résoudre.
18	Informatique neuromorphique	Permet une utilisation extrêmement efficace de l'IA à la vitesse et à l'échelle du cerveau humain.
19	Technologies spatiales (échelle commerciale)	Élargit l'accès à l'espace et ouvre la voie à de nouvelles perspectives économiques.
20	Réseaux d'infrastructure physique décentralisés (DePIN)	Crée des réseaux résilients et échelonnables appartenant à des communautés et exploités par celles-ci.

Dix principales technologies à surveiller : technologies de pointe après 2030

1	Interfaces cerveau-machine	Permet une communication directe entre le cerveau et des systèmes numériques.
2	Nanotechnologie (avancée)	Ingénierie à l'échelle atomique pour créer de nouveaux matériaux et dispositifs.
3	Informatique moléculaire	Nouveaux paradigmes informatiques utilisant des molécules pour un traitement extrêmement efficace de l'information.
4	Matière programmable	Matériaux pouvant changer de forme, de propriétés et de fonction sur demande.
5	Stockage d'énergie de longue durée	Stockage de prochaine génération favorisant une énergie propre et fiable.
6	Énergie de fusion	Production d'une énergie abondante, propre et durable.
7	Objets autonomes	Systèmes pleinement autonomes sur les plans de la mobilité, de la logistique et du fonctionnement.
8	Systèmes d'intelligence en essaim	Systèmes répartis collaborant et s'adaptant comme des essaims naturels.
9	Systèmes d'IA superintelligents	Systèmes d'IA qui surpassent l'intelligence humaine dans divers domaines.
10	Technologies de géoingénierie	Interventions à grande échelle visant à restaurer les systèmes terrestres et l'équilibre climatique.

SURFACE D'ATTAQUE

Le périmètre de l'organisme est fragmenté entre différents plans de contrôle que les attaquants peuvent enchaîner plus rapidement que les équipes peuvent les transférer.

Une vue d'ensemble de l'accès, de l'exposition et des mesures d'intervention est nécessaire pour les charges de travail dans le nuage, l'infrastructure en périphérie, les plateformes SaaS et les tiers.

Mission

Réduire les angles morts entre les domaines.

Vision

Détecter, gérer et limiter les accès au niveau des points d'extrémité, des identifiants, du nuage, de la périphérie, des solutions SaaS et des chemins des fournisseurs.

Dispositifs en périphérie

- Détermination des dispositifs exposés.
- Application des correctifs ou isolement rapide.
- Surveillance de l'accès à distance.

Charges de travail dans le nuage

- Configurations de base.
- Centralisation des journaux du nuage.
- Liaison de l'accès à l'identité.

Vue d'ensemble de l'accès, de l'exposition et des mesures d'intervention

Données SaaS

- Contrôle des droits d'administrateur.
- Surveillance des exportations.
- Rotation des jetons à risque.

Tiers

- Vérification des chemins d'accès.
- Essais du transfert des interventions.
- Limitation des privilèges partagés.

IA agentique et IA multi-agent

Agents intelligents. Actions autonomes. Répercussions exponentielles.

L'IA passe progressivement du statut d'outils d'assistance à celui d'agents capables d'agir. D'un agent isolé exécutant des tâches à des réseaux d'agents collaborant pour atteindre des résultats, cette évolution ouvre la voie à de nouveaux niveaux d'autonomie, d'adaptabilité et de valeur.

IA AGENTIQUE

Un seul agent, autonome et axé sur les objectifs.

L'IA agentique désigne les systèmes d'IA capables de percevoir leur environnement, de raisonner, de prendre des décisions et d'agir de manière autonome afin d'atteindre des objectifs spécifiques avec une intervention humaine minimale.

CARACTÉRISTIQUES PRINCIPALES

Perçoit l'environnement
Recueille des renseignements à partir des données et du contexte en temps réel.

Raisonne et planifie
Comprend les objectifs et détermine la meilleure approche.

Passe à l'action
Exécute des tâches et interagit avec des systèmes ou des outils.

Apprend et s'adapte
Améliore son rendement au fil du temps au moyen de la rétroaction et de l'expérience.

Axé sur les objectifs
Travaille à l'atteinte des résultats prédéfinis avec une supervision humaine minimale.

EXEMPLES

Agent de résolution de services de TI
L'agent diagnostique les problèmes, exécute les correctifs et consigne les résultats.

Agent de recherche intelligent
L'agent recherche, analyse et résume des renseignements permettant de répondre à des requêtes complexes.

Agent d'approvisionnement
L'agent détermine les fournisseurs, négocie les modalités et passe les commandes dans le respect des limites fixées par la politique.

IA MULTI-AGENT

Nombreux agents travaillant ensemble pour atteindre les résultats.

Les systèmes d'IA multi-agent sont constitués de plusieurs agents d'IA qui interagissent, collaborent, négocient ou rivalisent entre eux afin d'atteindre des objectifs individuels ou communs.

CARACTÉRISTIQUES PRINCIPALES

Multiples agents
Agents spécialisés ayant des rôles, des compétences ou des points de vue différents.

Interaction et communication
Les agents échangent des renseignements afin de se coordonner et de collaborer.

Coordination et collaboration
Les agents travaillent ensemble pour résoudre des tâches complexes qui dépassent les capacités individuelles.

Négociation et adaptation
Les agents adaptent les plans et règlent les conflits afin d'optimiser les résultats.

Objectifs communs ou individuels
Les agents poursuivent des objectifs communs ou des résultats individuels cohérents.

EXEMPLES

Réseau de détection de fraude
Les agents surveillent les transactions, partagent des indicateurs et prennent des mesures pour prévenir la fraude.

Optimisation de la chaîne d'approvisionnement
Les agents prévoient la demande, gèrent les stocks et coordonnent la logistique.

Équipe de campagne de marketing
Les agents créent du contenu, mettent à l'essai des variantes, optimisent les dépenses et mesurent l'incidence.

COMMENT TRAVAILLENT-ELLES ENSEMBLE?

L'IA agentique est le fondement alors que l'IA multi-agent est le facteur multiplicateur. Ensemble, elles permettent une autonomie évolutive et une coordination intelligente à l'échelle organisationnelle.

IA agentique
Les agents individuels agissent de manière autonome pour atteindre des objectifs définis.

+

IA multi-agent
Les agents collaborent et coordonnent leurs efforts pour atteindre des résultats supérieurs.

→

Une plus grande agilité, de meilleures décisions, une réduction des coûts et de nouvelles possibilités grâce à l'automatisation intelligente.

IA agentique et IA multi-agent

Agents intelligents. Actions autonomes. Répercussions exponentielles.

L'IA passe progressivement du statut d'outils d'assistance à celui d'agents capables d'agir. D'un agent isolé exécutant des tâches à des réseaux d'agents collaborant pour atteindre des résultats, cette évolution ouvre la voie à de nouveaux niveaux d'autonomie, d'adaptabilité et de valeur.

IA AGENTIQUE

Un seul agent, autonome et axé sur les objectifs.

L'IA agentique désigne les systèmes d'IA capables de percevoir leur environnement, de raisonner, de prendre des décisions et d'agir de manière autonome afin d'atteindre des objectifs spécifiques avec une intervention humaine minimale.

CARACTÉRISTIQUES PRINCIPALES

Perçoit l'environnement
Recueille des renseignements à partir des données et du contexte en temps réel.

Raisonne et planifie
Comprend les objectifs et détermine la meilleure approche.

Passe à l'action
Exécute des tâches et interagit avec des systèmes ou des outils.

Apprend et s'adapte
Améliore son rendement au fil du temps au moyen de la rétroaction et de l'expérience.

Axé sur les objectifs
Travaille à l'atteinte des résultats prédéfinis avec une supervision humaine minimale.

EXEMPLES

Agent de résolution de services de TI
L'agent diagnostique les problèmes, exécute les correctifs et consigne les résultats.

Agent de recherche intelligent
L'agent recherche, analyse et résume des renseignements permettant de répondre à des requêtes complexes.

Agent d'approvisionnement
L'agent détermine les fournisseurs, négocie les modalités, et passe les commandes dans le respect des limites fixées par la politique.

IA MULTI-AGENT

Nombreux agents travaillant ensemble pour atteindre les résultats.

Les systèmes d'IA multi-agent sont constitués de plusieurs agents d'IA qui interagissent, collaborent, négocient ou rivalisent entre eux afin d'atteindre des objectifs individuels ou communs.

CARACTÉRISTIQUES PRINCIPALES

Multiples agents
Agents spécialisés ayant des rôles, des compétences ou des points de vue différents.

Interaction et communication
Les agents échangent des renseignements afin de se coordonner et de collaborer.

Coordination et collaboration
Les agents travaillent ensemble pour résoudre des tâches complexes qui dépassent les capacités individuelles.

Négociation et adaptation
Les agents adaptent les plans et règlent les conflits afin d'optimiser les résultats.

Objectifs communs ou individuels
Les agents poursuivent des objectifs communs ou des résultats individuels cohérents.

Réseau de détection de fraude
Les agents surveillent les transactions, partagent des indicateurs et prennent des mesures pour prévenir la fraude.

Optimisation de la chaîne d'approvisionnement
Les agents prévoient la demande, gèrent les stocks et coordonnent la logistique.

Équipe de campagne de marketing
Les agents créent du contenu, mettent à l'essai des variantes, optimisent les dépenses et mesurent l'incidence.

Pertinence pour la Canadian Association of Parliamentary Administration (CAPA) : Ces technologies peuvent agir de manière autonome, prendre des décisions et collaborer avec d'autres agents d'IA, ce qui engendre de nouveaux risques en matière de sécurité et de gouvernance ainsi que des risques opérationnels.

IA en périphérie et dispositifs connectés

L'IA en périphérie désigne l'utilisation de techniques d'IA intégrées dans des produits non informatiques (grand public, commerciaux, industriels), des points d'extrémité de l'Internet des objets (IdO), des passerelles et des serveurs en périphérie. Ces capacités couvrent des applications grand public, commerciales et industrielles, telles que les appareils mobiles, les véhicules autonomes, les diagnostics médicaux avancés et l'analyse en continu. Bien qu'ils soient principalement axés sur l'inférence IA, les systèmes les plus sophistiqués intègrent des capacités d'entraînement local permettant d'optimiser les modèles en périphérie.

Comment fonctionne l'IA en périphérie?

L'IA en périphérie traite les données à l'aide de l'IA directement sur le dispositif ou à proximité de celui-ci, ce qui permet des décisions plus rapides, en temps réel, sans avoir à tout envoyer vers le nuage.

Pourquoi est-ce important?

- Des renseignements et des mesures en temps réel, là où les événements se produisent.
- Une latence plus faible et une réduction des coûts liés à la bande passante.
- Renforcement de la confidentialité et de la sécurité des données.
- Une fiabilité accrue, même hors ligne.
- Une intelligence évolutive dans les environnements répartis.

Comment cela fonctionne-t-il?

1 Dispositifs connectés

Les dispositifs recueillent des données issues du monde physique.

2 Traitement en périphérie avec l'IA

Les modèles d'IA analysent les données localement, sur le dispositif en périphérie.

3 Décision en temps réel

Les renseignements sont exploités immédiatement pour déclencher des actions.

4 Écosystème connecté

Seuls les données ou les événements pertinents sont envoyés vers le nuage.

5 Amélioration continue

Les modèles sont mis à jour et optimisés de manière continue.

Répercussions opérationnelles

Efficacité opérationnelle
Automatisation des processus et réduction des temps d'arrêt

Expérience client
Prestation d'interactions personnalisées en temps réel

Innovation à grande échelle
Nouveaux produits et services intelligents

Résilience et agilité
Intervention plus rapide dans des environnements dynamiques

KPMG

IA en périphérie et dispositifs connectés

Risques et menaces

L'IA en périphérie et les dispositifs connectés fournissent des renseignements en temps réel et apportent une valeur opérationnelle, tout en élargissant la surface d'attaque relative aux dispositifs, aux données et aux environnements répartis.

PRINCIPAUX RISQUES

L'IA en périphérie et les dispositifs connectés entraînent des risques spécifiques dans les domaines de la technologie, des données et des opérations.

Surface d'attaque élargie

Un grand nombre de dispositifs et de points d'extrémité répartis augmente le nombre de points d'entrée potentiels.

Exposition des données et confidentialité

Les données sensibles traitées en périphérie peuvent être exposées en raison de protections insuffisantes ou d'un traitement inadéquat.

Altération de dispositifs et de modèles

Les dispositifs en périphérie et les modèles peuvent être manipulés, donnant lieu à des décisions incorrectes ou à des actions malveillantes.

Connectivité non sécurisée

Des communications peu sécurisées ou non chiffrées entre des dispositifs, des nœuds en périphérie et le nuage créent un risque.

Manque de visibilité et de contrôle

Une visibilité limitée de l'état des dispositifs, des flux de données et du comportement des modèles entrave la détection des menaces.

Perturbation opérationnelle

Les attaques ou les défaillances peuvent perturber les opérations essentielles et avoir une incidence sur la sécurité, le temps de disponibilité et les revenus.

MENACES CIBLANT L'IA EN PÉRIPHÉRIE ET LES DISPOSITIFS CONNECTÉS

Les attaquants ciblent de plus en plus les environnements en périphérie afin de perturber les opérations, de voler des données ou de s'introduire dans les systèmes informatiques et opérationnels.

Logiciels malveillants et rançongiciels

Des logiciels malveillants peuvent infecter des dispositifs en périphérie, chiffrer les données ou perturber les services.

Vol et usurpation de justificatifs d'identité

Des justificatifs d'identité faibles ou volés peuvent être utilisés pour accéder à des dispositifs et compromettre ceux-ci.

Mouvement latéral et pivotement

Des dispositifs en périphérie qui ont été compromis peuvent être utilisés comme porte d'entrée pour accéder à des réseaux plus vastes.

Attaques de modèles d'IA

Les attaquants peuvent empoisonner les données d'entraînement, manipuler les modèles ou exploiter les comportements d'inférence.

Écoute clandestine et attaques par interception

Les attaquants peuvent intercepter ou modifier les données en transit entre les dispositifs, la périphérie et le nuage.

Compromission de la chaîne d'approvisionnement

Les vulnérabilités dans le matériel, les micrologiciels ou les logiciels tiers peuvent être exploitées.

ATTÉNUER LES RISQUES ET RENFORCER LA RÉSILIENCE.

Une approche de sécurité à plusieurs couches est essentielle pour protéger l'IA en périphérie et les environnements connectés.

Sécurisé dès la conception

Intégrer la sécurité dès le départ dans les dispositifs, les modèles d'IA et l'infrastructure.

Gestion rigoureuse de l'identité et de l'accès

Appliquer le principe du « droit d'accès minimal » et l'authentification multifactorielle pour les utilisateurs et les dispositifs.

Protection des données

Chiffrer les données au repos et en transit. Réduire au minimum et anonymiser les données dans la mesure du possible.

Surveillance continue

Maintenir une visibilité de l'ensemble des environnements en périphérie et détecter les anomalies en temps réel.

Gestion des vulnérabilités et des correctifs

Tenir les dispositifs, les micrologiciels et les modèles à jour et réduire l'exposition.

Résilience et intervention

Établir des plans d'intervention en cas d'incident, de reprise et de continuité des activités pour la périphérie.

Pertinence pour la CAPA : L'IA en périphérie et les dispositifs connectés engendrent de nouveaux risques en matière de cybersécurité et de confidentialité ainsi que des risques opérationnels en augmentant la surface d'attaque et certains dispositifs se trouvent à l'extérieur des « limites » de l'organisme.

KPMG

En quoi consiste l'approche de vérification systématique?

La vérification systématique est une approche de sécurité moderne qui élimine la confiance implicite et vérifie continuellement chaque utilisateur, dispositif et connexion avant d'accorder l'accès aux ressources.

La vérification systématique en une phrase

Ne jamais faire confiance, toujours vérifier.

Toujours authentifier et autoriser, et valider continuellement en fonction du principe du droit d'accès minimal et du contexte.

Les cinq piliers de la vérification systématique

1. **Vérifier explicitement**
   Authentifier et autoriser en fonction de tous les points de données disponibles : utilisateur, dispositif, emplacement, temps, comportement et plus.
2. **Utiliser le principe du droit d'accès minimal**
   Accorder uniquement le droit d'accès minimal requis pour effectuer l'action particulière, pas plus, pas moins.
3. **Présumer qu'il y a une intrusion**
   Concevoir en fonction de l'hypothèse que les menaces se trouvent déjà au sein du réseau.
4. **Valider continuellement**
   Surveiller continuellement l'activité de l'utilisateur et revérifier la confiance avant et pendant l'accès.
5. **Protéger tout**
   Sécuriser toutes les ressources (applications, données, charges de travail et interface de programmation d'applications [API[) dans les environnements sur place, dans le nuage et en périphérie.

Vérification systématique par rapport à sécurité traditionnelle

Approche traditionnelle : Confiance, mais avec vérification

Confiance implicite une fois à l'intérieur du réseau

Une fois que les utilisateurs se trouvent au sein du réseau, ils disposent d'un vaste accès aux ressources.

Approche de vérification systématique : Ne jamais faire confiance, toujours vérifier

Vérification continue et droit d'accès minimal requis

Ne jamais supposer que l'accès est accordé. L'accès est continuellement vérifié, limité selon le principe du droit d'accès minimal et surveillé en temps réel.

Le résultat

Réduction du risque
Permet de minimiser l'incidence des intrusions et les mouvements latéraux.

Renforcement de la sécurité
Permet de s'assurer d'accorder le bon type d'accès aux bons utilisateurs et dispositifs.

Agilité opérationnelle
Permet d'assurer un accès sécurisé à un effectif moderne peu importe l'emplacement et le dispositif.

Sécuriser l'accès. Protéger les données. Concevoir en fonction de la vérification systématique.

Vérification systématique : Risques pour l'organisme et menaces connexes

La vérification systématique renforce la sécurité en éliminant la confiance implicite et en vérifiant continuellement toutes les demandes d'accès. Toutefois, les organismes doivent comprendre les risques associés à la mise en œuvre de la vérification systématique et l'évolution des menaces que les attaquants utilisent pour la cibler.

Risques associés à la vérification systématique pour l'organisme

Alors que la vérification systématique réduit le risque, elle engendre également de nouveaux défis que les organismes doivent relever.

Coûts de mise en œuvre et opérationnels plus élevés

La vérification systématique nécessite des investissements dans la technologie, l'intégration, l'automatisation et les ressources qualifiées. La surveillance continue et la gestion des politiques augmentent les frais généraux opérationnels.

Complexité et perturbation opérationnelle

L'intégration de la vérification systématique à tous les niveaux (personnel, processus et technologie) peut s'avérer complexe et risque de perturber les activités opérationnelles si elle n'est pas soigneusement planifiée et mise en œuvre.

Incidence sur l'expérience utilisateur et la productivité

La vérification continue et le principe du droit d'accès minimal peuvent créer des frictions, susceptibles d'avoir une incidence sur la productivité des utilisateurs et l'adoption s'ils ne sont pas bien conçus.

Défis liés à la performance et à l'évolutivité

La vérification, l'inspection et la surveillance en temps réel peuvent avoir une incidence sur la performance des applications et s'avérer difficiles à mettre en œuvre à grande échelle sans une architecture adaptée.

Mauvaise configuration des politiques

Des politiques trop restrictives ou une mauvaise configuration peuvent bloquer des accès légitimes, provoquer des pannes et entraîner l'émergence d'une « informatique fantôme » ou le recours à des solutions de contournement non sécurisées.

Préoccupations liées à la visibilité et à la confidentialité des données

Une surveillance et une collecte de données à grande échelle peuvent soulever des questions relatives à la confidentialité et nécessiter des contrôles rigoureux en matière de gouvernance et de conformité.

Menaces relatives à la vérification systématique

Les attaquants ne cessent de faire évoluer leurs tactiques pour contourner les contrôles, usurper des identités et exploiter les accès privilégiés.

Vol d'identifiants et prise de contrôle de comptes

L'hameçonnage, les logiciels malveillants et le bourrage d'identifiants peuvent permettre de voler des justificatifs d'identité valides et de contourner les contrôles d'accès.

Exploitation des vulnérabilités

Les attaquants exploitent les vulnérabilités présentes dans les applications, les points d'extrémité, les dispositifs réseau et les systèmes d'authentification pour obtenir un accès initial.

Exploitation d'accès et d'autorisations légitimes

Les comptes compromis ou les autorisations excessives peuvent être exploités afin de se déplacer latéralement et d'accéder à des ressources sensibles.

Mauvaise configuration et politiques de sécurité insuffisantes

Des politiques mal configurées, des exceptions et des droits d'accès trop larges peuvent être exploités pour contourner les contrôles de vérification systématique.

Fraude psychologique et menaces internes

Les attaquants ont recours à la manipulation pour inciter des utilisateurs ou des employés malveillants à contourner les contrôles et à obtenir un accès privilégié.

Risques liés à la chaîne d'approvisionnement et aux tiers

Les fournisseurs, partenaires et applications tierces compromis peuvent constituer une porte d'entrée vers votre environnement.

Point à retenir

La vérification systématique n'est pas un produit, c'est un cheminement. La réussite repose sur la recherche d'un équilibre entre la sécurité et les résultats opérationnels, tout en évaluant continuellement les risques et en s'adaptant à l'évolution des menaces.

Mettre l'accent sur ce qui suit :

- Sécurité de l'identité renforcée
- Droit d'accès minimal requis
- Surveillance continue
- Automatisation et orchestration des politiques
- Évaluation et amélioration continues

Il est important de comprendre les risques, de se protéger contre les menaces et de renforcer continuellement votre stratégie de vérification systématique afin de protéger votre organisme, ses données et sa réputation.

Vérification systématique adaptative

Ne faire confiance à personne. Vérifier tout. Un accès sécurisé pour ce qui est important.

La vérification systématique adaptative est une approche de sécurité dynamique vérifiant continuellement chaque utilisateur, dispositif et connexion, s'adaptant en temps réel au risque et au contexte.

PRINCIPES DE LA VÉRIFICATION SYSTÉMATIQUE

Vérifier explicitement

Toujours authentifier et autoriser à l'aide d'une identité forte.

Utiliser le principe du droit d'accès minimal

Accorder uniquement le droit d'accès minimal requis en fonction des besoins et du contexte.

Présumer qu'il y a une intrusion

Valider et surveiller continuellement. Limiter la portée des dommages.

Sécurité de bout en bout

Assurer le chiffrement, la protection et la surveillance dans l'ensemble des environnements.

S'adapter continuellement

Utiliser des indicateurs en temps réel et l'analyse pour ajuster l'accès.

COMMENT FONCTIONNE LA VÉRIFICATION SYSTÉMATIQUE ADAPTATIVE

1. **Demander**
   L'utilisateur ou le dispositif demande l'accès à une ressource.
2. **Vérifier**
   Vérifier l'identité, la posture du dispositif et le risque contextuel en temps réel.
3. **Autoriser**
   Accorder le droit d'accès minimal requis en fonction des politiques et de l'évaluation des risques.
4. **Surveiller**
   Surveiller continuellement le comportement et l'environnement pour relever les anomalies.
5. **Adapter**
   Ajuster l'accès de façon dynamique selon l'évolution des risques et du contexte.

L'intelligence continue favorise l'adaptation

Les indicateurs provenant des utilisateurs, des dispositifs, des applications, des données et de l'environnement alimentent les systèmes d'analyse et d'automatisation afin d'affiner les décisions d'accès en temps réel.

RÉSULTATS OPÉRATIONNELS

Sécurité renforcée

Permet de réduire les risques et de prévenir les intrusions.

Expérience fluide

Permet un accès sécurisé sans compromettre la productivité.

Efficacité opérationnelle

Permet d'automatiser les décisions et de réduire la complexité de la sécurité.

Agilité opérationnelle

Permet de s'adapter au changement et de soutenir les charges de travail modernes.

Conformité et confiance

Permet de respecter les exigences réglementaires et de renforcer la confiance des intervenants.

Pertinence pour la CAPA : Alors que la technologie devient plus complexe et diversifiée (nuage, SaaS, lacs de données), la vérification systématique traite les menaces plus efficacement en vérifiant toujours chaque utilisateur, dispositif et application.

Jumeaux numériques

Modéliser le présent. Prévoir l'avenir.

Optimiser les résultats dans le monde réel.

En quoi consistent les jumeaux numériques?

Un jumeau numérique est une représentation virtuelle dynamique d'un actif physique, d'un processus, d'un système ou d'un environnement, qui est continuellement mise à jour à l'aide de données en temps réel.

En reproduisant le monde réel, les jumeaux numériques permettent aux organismes de surveiller, simuler, analyser et optimiser leur rendement, ce qui contribue à améliorer la prise de décision et les résultats.

Connexion en temps réel

Synchronisation continue avec les données en temps réel provenant des capteurs, des systèmes et des sources.

Simuler et prévoir

Exécution de scénarios et de modèles basés sur l'IA pour prévoir les résultats et évaluer les répercussions.

Surveiller et analyser

Visualisation du rendement, détection des anomalies et mise en évidence des renseignements.

Optimiser et agir

Exploitation des renseignements pour optimiser les opérations, améliorer les résultats et créer de la valeur.

Pourquoi est-ce important?

Les jumeaux numériques comblent le fossé entre le monde physique et le monde numérique. Ils transforment les données en renseignements exploitables, permettent de prendre des décisions plus éclairées et créent un avantage concurrentiel durable.

Jumeaux numériques

Modéliser le présent. Prévoir l'avenir. Optimiser les résultats dans le monde réel.

Quels risques et menaces les jumeaux numériques peuvent-ils engendrer?

Si les jumeaux numériques apportent une valeur considérable, ils peuvent également engendrer de nouveaux risques pour les organismes s'ils ne sont pas gérés efficacement.

Recours excessif aux modèles

Une confiance excessive dans les simulations peut donner lieu à de mauvaises décisions si les modèles sont imprécis ou incomplets.

Biais et résultats inexacts

Des données de mauvaise qualité ou des algorithmes biaisés peuvent donner lieu à des renseignements trompeurs et à des résultats inéquitables.

Confidentialité et exposition des données

Les jumeaux numériques peuvent traiter des données sensibles concernant des personnes, des actifs ou des opérations, ce qui peut entraîner des risques pour la confidentialité.

Coût, complexité et dépendance vis-à-vis d'un fournisseur

Des investissements élevés, des intégrations complexes et des plateformes exclusives peuvent limiter l'agilité et augmenter le coût total.

Responsabilité et responsabilisation

Un manque de clarté quant à la responsabilité des décisions prises en fonction des renseignements tirés du jumeau peut accroître le risque sur le plan juridique.

Quelles sont les menaces qui pèsent sur les jumeaux numériques eux-mêmes?

Les jumeaux numériques constituent des actifs précieux qui doivent être protégés tout au long de leur cycle de vie, depuis l'intégration des données jusqu'à la production de renseignements et à la prise de mesures.

Menaces liées à la cybersécurité

Risque de piratage, de rançongiciel et d'accès non autorisé susceptible de perturber les opérations ou de compromettre la sécurité.

Intégrité et qualité des données

Des données inexactes, incomplètes ou altérées peuvent compromettre la fiabilité du jumeau et donner lieu à des décisions erronées.

Dérive et dégradation du modèle

Sans recalibrage ni validation continue, les modèles peuvent perdre en précision au fil du temps.

Disponibilité et résilience

Les pannes de système ou les problèmes de connectivité peuvent perturber le fonctionnement du jumeau et la prestation de renseignements essentiels.

Menaces liées à l'accès et menaces internes

Des autorisations excessives ou des employés malveillants peuvent entraîner une utilisation abusive ainsi que la manipulation et le vol de données.

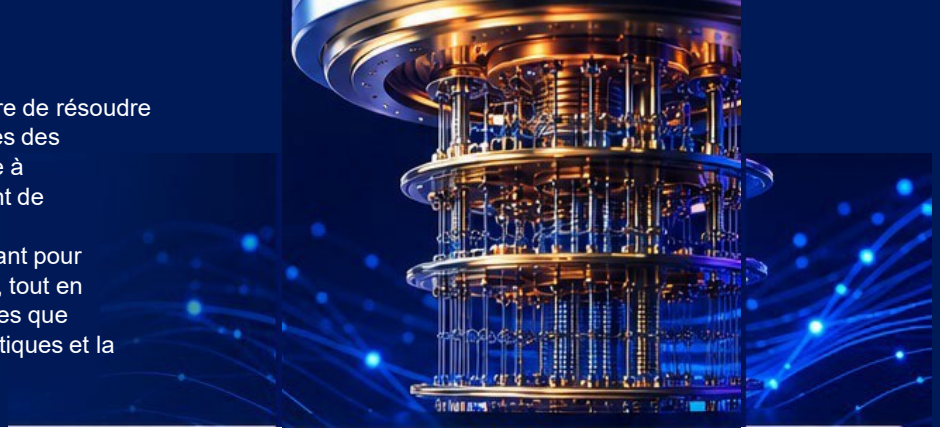
Risques liés aux tiers et à la chaîne d'approvisionnement

Les vulnérabilités présentes dans les API, les plateformes ou les logiciels tiers peuvent exposer les jumeaux à des risques externes.

Pertinence pour la CAPA : Un jumeau numérique peut être utilisé pour simuler l'environnement et l'architecture de TI actuels sans avoir à reproduire intégralement ces environnements. Cela permet de réaliser des essais et des simulations sans affecter la production.

Informatique quantique et cryptographie à résistance quantique

L'informatique quantique pourrait permettre de résoudre des problèmes qui dépassent les capacités des ordinateurs actuels, ce qui ouvrirait la voie à l'innovation, mais elle engendre également de nouveaux risques.
Les organismes doivent agir dès maintenant pour protéger leurs données et leurs systèmes, tout en prenant conscience des nouvelles menaces que pourraient représenter les capacités quantiques et la cryptographie à résistance quantique.



RISQUES ACTUELS RELATIFS À L'INFORMATIQUE QUANTIQUE

Les ordinateurs quantiques pourraient permettre de contourner bon nombre d'algorithmes cryptographiques couramment utilisés aujourd'hui.

1. Percée dans le domaine de la cryptographie

L'algorithme de Shor pourrait venir à bout des systèmes de cryptographie à clé publique largement utilisés (p. ex. RSA, ECC), exposant ainsi les données chiffrées et les signatures numériques.

2. Des données à risque aujourd'hui, déchiffrées demain

Les menaces de type « Récolter maintenant, déchiffrer plus tard » signifient que les données chiffrées recueillies aujourd'hui pourraient être déchiffrées dès que les ordinateurs quantiques seront suffisamment puissants.

3. Répercussions dans tous les secteurs d'activité

Les secteurs fortement réglementés, notamment les services financiers, le secteur de la santé, l'administration publique et les infrastructures essentielles, sont fortement exposés.

4. Perte de confiance et d'intégrité

Une cryptographie compromise pourrait ébranler la confiance dans les services, les transactions et les communications numériques.

5. Conformité et risque juridique

Le fait de ne pas se préparer aux risques post-quantiques pourrait entraîner des infractions réglementaires, engager la responsabilité juridique et nuire à la réputation de l'organisme.

MENACES FUTURES RELATIVES À L'INFORMATIQUE QUANTIQUE ET LA CRYPTOGRAPHIE À RÉSISTANCE QUANTIQUE

Avec l'émergence des capacités quantiques et de la cryptographie à résistance quantique, il faudra faire face à de nouveaux risques et défis.

1. Utilisation abusive de l'informatique quantique

Les ordinateurs quantiques pourraient être utilisés pour contourner le chiffrement, accélérer des attaques ou résoudre des problèmes complexes au profit d'acteurs malveillants.

2. Nouveaux vecteurs d'attaque

Les capacités quantiques pourraient permettre des types d'attaques totalement inédites, qui n'existent pas dans les environnements classiques.

3. Risques liés à la mise en œuvre et à l'adoption de la cryptographie post-quantique

Une cryptographie à résistance quantique mal mise en œuvre pourrait créer des vulnérabilités ou affaiblir la sécurité.

4. Répercussions sur le rendement et les opérations

Les algorithmes à résistance quantique peuvent nécessiter des clés plus longues et entraîner des coûts informatiques plus élevés, ce qui a des répercussions sur les systèmes et les opérations.

5. Risques liés à l'écosystème et à la chaîne d'approvisionnement

La dépendance vis-à-vis de tiers et de fournisseurs ainsi que l'évolution constante des normes peuvent entraîner des risques en matière de compatibilité et de sécurité.

Se préparer à l'ère de l'informatique quantique

1. Évaluer

Évaluer l'agilité cryptographique, recenser les actifs cryptographiques et les flux de données.

2. Définir les priorités

Hiérarchiser les cas d'utilisation et les systèmes en fonction du risque et de la criticité.

3. Planifier

Élaborer une feuille de route pour la transition vers l'informatique quantique.

4. Mettre en œuvre

Tester, mettre en œuvre et intégrer la technologie quantique.

5. Surveiller

Surveiller continuellement les avancées et s'adapter au fil de l'évolution des normes.

Pertinence pour la CAPA : L'avènement de l'informatique quantique est plus proche que nous ne le pensons, la plupart des prévisions tablant sur une disponibilité partielle de cette technologie d'ici à 2030. La cryptographie post-quantique nécessitera une planification et une feuille de route pour la migration.

Prévention de la perte de données

Rechercher. Classifier. Protéger. Surveiller. Intervenir. Protéger les données sensibles au sein de votre organisme.

Qu'est-ce que la prévention de la perte de données (PPD)?

La PPD est un ensemble de politiques et de technologies conçues pour aider les organismes à identifier, surveiller et protéger les données sensibles, ainsi qu'à prévenir tout accès, partage ou exfiltration non autorisés de celles-ci.

La PPD vous aide à :

Protéger les données sensibles
Prévenir l'exposition ou l'utilisation malveillante de données sensibles.

Respecter les exigences en matière de conformité
Contribuer au respect des obligations réglementaires et à la gouvernance.

Réduire les risques
Minimiser les atteintes à la sécurité des données, la fraude et les atteintes à la réputation.

Améliorer la visibilité et le contrôle
Comprendre les flux de données et appliquer les politiques.

Comment fonctionne la PPD?

Le PPD offre une solution de bout en bout permettant de rechercher, classifier, protéger et surveiller les données sensibles à l'aide de politiques adaptatives et de renseignements.

1 Rechercher

Rechercher automatiquement les données sensibles dans l'ensemble de votre environnement à l'aide du balayage et de l'analyse du contenu.

Exemples
- Schéma de données
- Explorateur de contenu
- Évaluation des risques

2 Classifier

Appliquer des étiquettes de sensibilité et des classificateurs avec capacité d'apprentissage pour catégoriser les données en fonction de leur contenu et de leur contexte.

Exemples
- Étiquettes de sensibilité
- Classificateurs avec capacité d'apprentissage
- Texte et correspondance exacte

3 Protéger

Créer des politiques de PPD pour surveiller et protéger les données en cours d'utilisation, en transit et au repos.

Exemples
- Politiques de PPD
- Chiffrement
- Activités authentifiées

4 Surveiller

Relever les cas de non-conformité aux politiques et établir des alertes au moyen de la surveillance et de rapports en temps réel et historiques.

Exemples
- Avis de non-conformité aux politiques
- Gestion du risque lié aux menaces internes
- Explorateur d'activités

5 Intervenir

Enquêter sur les incidents et prendre les mesures nécessaires pour mettre fin aux fuites de données et remédier aux risques.

Exemples
- Enquêtes sur les incidents
- Dérogation aux politiques
- Encadrement des utilisateurs

Plateformes de sécurité des données

(DSPM + PPD appuyée par l'IA + Risque interne)

Une approche moderne et intégrée pour la recherche, la protection et la surveillance des données sensibles au sein de votre écosystème numérique.

Pourquoi est-ce important?

Les données sont omniprésentes
Il y a des données dans le nuage, les SaaS, les points d'extrémité, les bases de données et les outils d'IA.

Les contrôles de sécurité traditionnels ne suffisent pas
Les solutions fondées sur le périmètre ne peuvent pas voir ou protéger les flux de données modernes.

Le risque est dynamique
Les menaces internes, les comptes compromis et l'utilisation de l'IA créent chaque jour de nouvelles vulnérabilités.

Les organismes de réglementation s'attendent à plus
Des exigences plus strictes en matière de confidentialité, de résidence des données et de signalement des intrusions.

Les affaires reposent sur la confiance
La protection des données sensibles renforce la confiance des clients et constitue un avantage concurrentiel.

Le pouvoir de l'intégration

DSPM

Gestion de la posture de sécurité des données (DSPM)

Rechercher, classifier et évaluer continuellement les données sensibles et les mauvaises configurations.

+

PPD appuyée par l'IA

Prévention de la perte de données appuyée par l'IA

Empêcher que les données sensibles quittent l'organisme en s'appuyant sur le contexte, l'intention et la compréhension par l'IA.

+

Risque interne

Gestion du risque interne

Cerner et atténuer les comportements à risque des employés et les menaces en temps réel.

=

Principales capacités

Recherche et classification des données Rechercher et classifier les données sensibles avec précision.

Évaluation continue de la posture Cerner les risques d'exposition et les problèmes de configuration.

PPD appuyée par l'IA et prise en compte du contexte Comprendre le contenu, le contexte et le comportement pour éviter toute perte de données.

Détection du risque interne Cerner les activités à risque avant qu'elles n'entraînent une atteinte à la protection des données.

Surveillance et analyse Obtenir des renseignements en temps réel et déterminer la priorité des risques au moyen de tableaux de bord.

Orchestration des politiques et automatisation Appliquer des politiques uniformes dans l'ensemble des environnements.

Conformité et production de rapports Simplifier les vérifications et respecter les exigences réglementaires.

Résultats opérationnels

Réduire les risques liés aux données
Protéger les données sensibles tout au long de leur cycle de vie.

Prévenir la perte de données
Empêcher l'exfiltration et l'utilisation malveillante avant qu'elles ne se produisent.

Gérer le risque interne
Cerner les comportements internes à risque et intervenir.

Renforcer la conformité
Respecter les obligations réglementaires en toute confiance.

Favoriser l'innovation en toute sécurité
Adopter le nuage et l'IA en toute sécurité grâce à la visibilité et au contrôle.

Réduire les coûts et la complexité Regrouper les outils et simplifier les opérations.

Pertinence pour la CAPA : Alors que la technologie devient plus complexe et diversifiée (nuage, SaaS, lacs de données) et que les auteurs de menaces et les menaces internes se multiplient, la nécessité de gérer les mouvements de données s'accroît.

Plateformes de sécurité des données

(DSPM + PPD appuyée par l'IA + Risque interne)

Une approche intégrée pour la recherche, la protection et la surveillance des données sensibles et l'atténuation des risques au sein de votre écosystème numérique.

Recherche et classification

Protection et prévention

Surveillance et détection

Enquête et intervention

Renseignements appuyés par l'IA

Réduction des risques

DSPM
Rechercher, classifier et évaluer continuellement les données sensibles

PPD appuyée par l'IA
Prévenir la perte de données en s'appuyant sur la compréhension par l'IA et le contexte

Risque interne
Cerner et atténuer les menaces internes en temps réel

RISQUES LIÉS À LA MISE EN ŒUVRE DE PLATEFORMES DE SÉCURITÉ DES DONNÉES

La mise en œuvre d'une plateforme de sécurité des données est une opération complexe. Les organismes sont confrontés à des risques stratégiques, opérationnels et techniques qui peuvent avoir une incidence sur la réalisation de la valeur.

Manque de clarté de la portée et de la stratégie	• Absence d'objectifs clairs et d'indicateurs de réussite • Manque d'harmonisation aux priorités organisationnelles et en matière de risques
Défis liés à la recherche et à la classification des données	• Recherche incomplète dans les environnements hybrides et infonuagiques • Classification inexacte entraînant de faux positifs et de faux négatifs
Intégration complexe et interopérabilité	• Intégration avec divers outils (gestion de l'identité et de l'accès, gestion des informations et des événements de sécurité, agent de sécurité d'accès au nuage, détection des menaces aux points d'extrémité et réponse, etc.) • Incompatibilités relatives aux API, aux formats de données et aux flux de travail
Gestion du changement et adoption par les utilisateurs	• Réticence des utilisateurs opérationnels et des équipes de TI • Manque de sensibilisation et de formation nuisant à l'efficacité
Mise au point des politiques et charge opérationnelle	• Politiques trop strictes nuisant à la productivité • Politiques mal adaptées entraînant une lassitude par rapport aux alertes et une exposition aux risques
Coûts, ressources et risque lié au rendement du capital investi	• Coût total de propriété élevé et prolifération des outils • Difficulté à démontrer le rendement du capital investi et à obtenir des investissements continus
Confidentialité, conformité et risque juridique	• Problèmes d'harmonisation aux exigences réglementaires • Préoccupations liées au traitement des données à l'étranger et à la résidence des données
Évolution des menaces et obsolescence technologique	• Contexte de menaces évoluant rapidement • Risque que la plateforme ne suive pas le rythme de l'innovation

MENACES PESANT SUR LES PLATEFORMES DE SÉCURITÉ DES DONNÉES

Les plateformes de sécurité des données regroupent des fonctionnalités essentielles, ce qui en fait une cible de choix. Les attaquants et les employés malveillants peuvent exploiter les failles présentes dans l'ensemble de la plateforme.

Exfiltration de données dans tous les modes
Les attaquants peuvent contourner les contrôles pour exfiltrer des données sensibles au moyen du système de courriel, du nuage, d'API, de points d'extrémité ou de supports amovibles.

Utilisation abusive de privilèges et prise de contrôle de comptes
Les comptes compromis ou les privilèges excessifs peuvent être utilisés pour désactiver des contrôles ou accéder à des données sensibles.

Politiques et contrôles mal configurés
Des configurations erronées, des règles trop permissives ou des lacunes peuvent exposer des données sensibles.

Menaces internes et vol de données
Des employés malveillants peuvent accéder à des données, voler des données ou causer une fuite de données au moyen d'un accès légitime.

Manipulation de modèles d'IA et évitement
Les attaquants peuvent manipuler des modèles d'IA afin d'éviter la détection ou de générer de faux résultats.

Données fantômes et actifs non gérés
Des données sensibles se trouvant dans des applications non autorisées, des outils d'IA ou des dispositifs de TI fantômes peuvent contourner la surveillance et les contrôles de la plateforme.

Risques liés à la chaîne d'approvisionnement et aux tiers
Des vulnérabilités liées aux intégrations avec des logiciels tiers ou aux fournisseurs peuvent être exploitées pour avoir accès à des données sensibles.

Empoisonnement de données et attaques contre l'intégrité
Les attaquants peuvent modifier les données utilisées pour la classification, l'entraînement ou l'analyse afin de corrompre les renseignements ou affaiblir les contrôles.

Déni de service et perturbation de la plateforme
Les attaquants peuvent perturber la disponibilité de la plateforme, retardant ainsi la détection et l'intervention en ce qui concerne les risques liés aux données.

En résumé :
Plus vous intégrez de capacités, plus il est essentiel de sécuriser la plateforme elle-même. Une surveillance continue, des contrôles d'accès rigoureux et des mesures de défense adaptatives sont indispensables.

PRINCIPAUX FACTEURS DE RÉUSSITE

- **Définir une stratégie et une feuille de route claires**
- **Commencer par les cas d'utilisation à forte valeur ajoutée**
- **Investir dans la recherche et la qualité des données**
- **Mettre en œuvre en s'appuyant sur une gouvernance solide**
- **Surveiller, ajuster et améliorer continuellement**
- **Instaurer une culture de sensibilisation à la sécurité**

PRIORITÉS DES DIRIGEANTS

Les dirigeants devraient financer un programme de cybersécurité pour 2027 qui privilégie la rapidité, l'identité, la gouvernance de l'IA et la résilience plutôt qu'une prolifération généralisée des mesures de contrôle.

La priorité est de concentrer davantage l'attention des dirigeants sur les contrôles permettant de réduire les perturbations, l'exposition des données, la fraude et les délais de prise de décision.

Domaine prioritaire	Mesures à prendre par les dirigeants	
Rapidité	1	Définir des mesures visibles par les dirigeants pour la détection, la prise de décision, le confinement et le tri des vulnérabilités à haut risque.
Accès	2	Financer l'automatisation lorsque celle-ci permet de réduire les délais de réponse sans pour autant éliminer la prise de décisions par des personnes.
	3	Privilégier les méthodes d'authentification qui résistent à l'hameçonnage pour les utilisateurs disposant de privilèges, les dirigeants et les utilisateurs des flux de travail à haut risque.
	4	Élargir la gouvernance de l'identité aux identités non humaines, aux sessions de SaaS, aux jetons et aux agents d'IA.
Résilience	5	Définir le niveau minimal de fonctionnement nécessaire pour les processus les plus critiques en cas de perturbation.
	6	Effectuer des exercices à l'intention des dirigeants permettant de mettre à l'essai des scénarios de rançongiciels, d'extorsion, de problèmes liés aux fournisseurs et d'usurpation d'identité au moyen l'IA.

Point à retenir : Le programme doit permettre de réduire le délai entre le signalement, la prise de décision, la maîtrise de la situation et la reprise des activités en toute confiance.