

**FORTRA<sup>Δ</sup>**

# **Solutions de Cybersécurité**



# TABLE DES MATIÈRES

## PLATEFORME ..... 3

### SERVICES DE SÉCURITÉ MANAGÉS

Managed Extended Detection & Response ..... 5

Managed Detection & Response ..... 6

Managed Web Application Firewall ..... 7

DLP managée ..... 8

Supervision managée de l'intégrité ..... 9

### SÉCURITÉ DES DONNÉES

Classification des données ..... 11

Transfert sécurisé de fichiers (MFT) ..... 12

Prévention contre la perte de données ..... 13

Collaboration sécurisée ..... 14

Sécurité de la messagerie cloud ..... 15

Protection DMARC ..... 16

Passerelle de messagerie sécurisée ..... 17

Protection face aux risques numériques ..... 18

Solution de sensibilisation à la sécurité ..... 19

## PROTECTION DE L'INFRASTRUCTURE

Gestion des vulnérabilités ..... 21

Logiciel de pen testing ..... 22

Émulation des menaces  
et simulation « red team » ..... 23

Outils de sécurité et services de red teaming ..... 24

Surveillance de l'intégrité ..... 25

Cybersécurité pour IBM i ..... 26

Protection contre les virus  
et les logiciels malveillants ..... 27

Gouvernance et administration de l'identité ..... 28

Gestion des accès privilégiés ..... 29

## OFFRES DE PRODUITS GROUPÉES ..... 30

## MARQUES DE CYBERSÉCURITÉ ..... 31



Fortra™

## PLATEFORME DE CYBERDÉFENSE MULTI-VECTORIELLE NATIVE DANS LE CLOUD

Fortra est une solution de cybersécurité innovante, Cloud based, qui vous protège de différents vecteurs d'attaque. Adapté à un environnement dont les menaces sont en constante évolution, Fortra renforce l'efficacité de votre équipe tout en jetant les bases de l'intégration de nos solutions complètes. Nous prévoyons les attaques, nous renforçons les organisations et en développons la résilience. Fortra améliore les performances en matière de sécurité grâce à la détection, l'agrégation, la corrélation et l'atténuation des menaces les plus. Nous utilisons des technologies de pointe pour gérer les menaces les plus familières; mais nous exploitons également tous les renseignements disponibles pour prévoir l'imprévisible. Enfin, nous avons recours à l'automatisation pour combler les lacunes potentielles. Ceci permet notamment de rationaliser les opérations et d'atténuer les défis opérationnels tout en fournissant des solutions de premier ordre pour un large éventail de vecteurs de menaces le tout dans une plateforme de cybersécurité holistique auprès d'un seul fournisseur.

### Les technologies Fortra en vedette sur la plateforme :

- Fortra Cloud Email Protection pour une protection avancée contre les menaces sur une plateforme intégrée de sécurité de la messagerie dans le cloud
- Fortra Vulnerability Management pour une gestion proactive, précise et intuitive de la gestion des vulnérabilités SaaS
- Fortra Extended Detection and Response pour une visibilité et une couverture complètes des points de terminaison, du réseau et des environnements hybrides

En savoir plus: [www.fortra.com/platform](http://www.fortra.com/platform)



# SERVICES DE SÉCURITÉ MANAGÉS



## Alert Logic

### MANAGED EXTENDED DETECTION AND RESPONSE

Fortra Extended Detection and Response (XDR) offre une visibilité et une couverture de sécurité sur l'ensemble du parc informatique (poste de travail, réseau, identités et cloud) afin de détecter rapidement les menaces et d'y répondre au plus vite. Notre solution XDR managée combine habilement technologies et expertise en matière de sécurité 24 h/24, 7 j/7 pour renforcer rapidement votre posture de sécurité.

#### Fonctionnalités clés :

- Couvre l'ensemble de la surface d'attaque à tous les niveaux de votre environnement
- Augmente l'efficacité et la flexibilité grâce à une réponse automatisée qui simplifie les tâches répétitives
- Intègre les solutions tierces existantes EDR, réseau et d'identités afin de corréliser les données à analyser par notre SOC
- Offre une console unique pour une vision globale de l'environnement informatique
- Utilise un agent Fortra léger, spécialement conçu pour cibler la télémétrie des End Point

En savoir plus: [www.fortra.com/xdr](http://www.fortra.com/xdr)



## Alert Logic

### MANAGED DETECTION AND RESPONSE

Alert Logic de Fortra est le seul fournisseur de services de détection et de réponse managées (MDR) qui offre une couverture complète des clouds publics, des environnements SaaS, On Prem' et hybrides. Notre approche managée de la sécurité et notre équipe d'experts en sécurité protègent votre organisation 24h/24, 7j/7, pour vous garantir une sécurité sans précédent et la réponse la plus efficace aux menaces.

#### Fonctionnalités clés :

- Détection, interception et élimination des attaques dans notre centre d'opérations de sécurité (SOC)
- Surveillance permanente de l'ensemble de votre parc informatique (réseaux, End Point et clouds) pour identifier rapidement les menaces et y répondre au plus vite
- Vue d'ensemble unique de votre environnement avec des tableaux de bord en temps réel sur les menaces et les vulnérabilités
- Vue globale de l'environnement du client, alimentée par des renseignements sur les menaces et des analyses provenant de milliers de clients et de flux
- Mise à disposition d'une équipe dédiée à la fourniture continue de valeur pour vous aider à atteindre vos objectifs et à améliorer votre posture de sécurité

En savoir plus: [www.fortra.com/mdr](http://www.fortra.com/mdr)



## Alert Logic

### MANAGED WEB APPLICATION FIREWALL

Fortra Managed Web Application Firewall (WAF) aide les organisations à obtenir une protection complète des applications Web et des API, en toute simplicité. Exploitez tout le potentiel d'un WAF grâce à une gestion experte et aux renseignements sur les menaces. Grâce au WAF de Fortra, entièrement managé et Cloud ready, vous disposez d'une assistance de SOC 24 h/24, 7 j/7 qui suit et bloque en permanence les attaques visant les applications Web provenant de menaces connues et inconnues.

#### Fonctionnalités clés :

- Bloque les attaques visant vos applications Web et vos API grâce à une protection avancée contre les menaces
- Fournit des stratégies de sécurité, des mesures correctives des faux positifs et des conseils sur les meilleures pratiques
- Protège contre les dix principales menaces identifiées par l'OWASP, les attaques d'identifiants, les DDoS, les robots indésirables et les menaces émergentes grâce à Fortra Threat Brain
- Garantit la sécurité de vos applications entre les cycles de correctifs grâce à des correctifs virtuels de plus de 100 applications majeures
- Fournit une gestion et un affinement continus pour éliminer la complexité de la sécurité et maintenir des protections optimisées pour les applications

En savoir plus: [www.fortra.com/managed-waf](https://www.fortra.com/managed-waf)



## Digital Guardian

### DLP MANAGÉE

Même si votre organisation dispose d'une équipe de sécurité bien préparée, il peut s'avérer difficile de rester au fait de toutes les menaces actuelles. L'équipe de services managés de Digital Guardian de Fortra peut fournir une expertise instantanée et conseiller sur les meilleures pratiques pour faire mûrir votre programme de protection des données et agir comme un niveau d'assistance supplémentaire pour votre équipe de sécurité existante.

#### Fonctionnalités clés :

- Comble votre déficit de ressources en matière de cybersécurité en laissant notre équipe de services managés veiller à ce que les menaces qui pèsent sur vos données sensibles soient stoppées avant toute perte de données
- Augmente l'efficacité opérationnelle et transfère votre charge de travail à nos experts en prévention de pertes de données, ce qui vous permet de vous concentrer sur des projets à plus forte valeur ajoutée
- Améliore la visibilité des données et l'exposition au risque en termes de sécurité des données de votre organisation en faisant confiance à des experts qui ont mis en œuvre des programmes essentiels de sécurité des données, de réponse aux incidents et de conformité destinés aux organisations dans le monde entier
- Tire parti des meilleures pratiques programmatiques et de méthodes éprouvées et fiables, utilisées pour protéger les informations essentielles de centaines de clients dans divers secteurs

En savoir plus: [www.fortra.com/dlp](http://www.fortra.com/dlp)



Tripwire

## SUPERVISION MANAGÉE DE L'INTÉGRITÉ

Tripwire ExpertOps de Fortra est le service managé de Fortra pour la surveillance de l'intégrité des fichiers (FIM), la gestion de la configuration de la sécurité (SCM) et la gestion des vulnérabilités (VM). Il met au service de votre équipe un expert dédié chargé de la gestion des solutions, de la fourniture de conseils personnalisés, de l'assistance en cas d'incident et de l'aide à l'audit. Restez en phase avec les exigences de conformité en constante évolution tout en renforçant la sécurité et l'intégrité de vos systèmes.

### Fonctionnalités clés :

- Agrandit instantanément votre équipe grâce à l'ajout d'un expert spécialisé
- Inclut les logiciels, la gestion par un expert et un hébergement fiable
- Donne la priorité à la réhabilitation pour une réduction maximale des risques
- Suit les progrès réalisés en matière de sécurité et de conformité
- Déployé sous forme d'abonnements de différents niveaux de service

En savoir plus: [www.fortra.com/integrity-monitoring](https://www.fortra.com/integrity-monitoring)



# SÉCURITÉ DES DONNÉES



## Fortra's Data Classification

### CLASSIFICATION DES DONNÉES

La solution de classification des données de Fortra améliore la sécurité des données en appliquant des étiquettes visuelles et des champs de métadonnées pour mieux prendre en charge les politiques DLP. Les recommandations du moteur d'IA aident à réduire les frictions en déterminant quelle étiquette est la meilleure à appliquer, et les employés reçoivent une formation de sécurité réelle qui favorise la visibilité et l'engagement envers les pratiques de sécurité des données dans l'ensemble de l'organisation.

#### Fonctionnalités clés :

- Classifier de manière flexible vos données tout en tenant compte des diverses politiques de conformité, y compris les contrôles réglementaires avancés du gouvernement
- Appliquer des champs de métadonnées enrichies à vos données sensibles pour garantir leur protection et leur contrôle partout où elles se trouvent
- Répondre à vos besoins actuels et futurs en matière de protection des données, de réduction des frictions et de formation des employés aux bonnes pratiques de sécurité

En savoir plus: [www.fortra.com/data-classification](http://www.fortra.com/data-classification)

Windows ●

Mac ●

Google ●

CAD ●

Citrix ●

iOS ●

Android ●



GoAnywhere & Globalscape

## TRANSFERT SÉCURISÉ DE FICHIERS (MFT)

Le transfert sécurisé de fichiers (MFT) sécurise, automatise et audite les transferts de fichiers entre les partenaires commerciaux de diverses organisations et les systèmes internes, le tout à partir d'une plate-forme centralisée. Le MFT chiffre les données en transit ou au repos afin de protéger les fichiers d'un accès non autorisé, tout en facilitant le respect des réglementations. Nos solutions MFT offrent des fonctionnalités de pointe qui simplifient les transferts de fichiers, répondant ainsi aux besoins des organisations en matière d'échanges sûrs et efficaces des fichiers.

### Fonctionnalités clés :

- Protège vos transferts grâce aux normes du secteur : SFTP, FTPS, PGP, HTTPS, AS2/AS3/AS4, etc.
- Automatise les transferts à l'aide d'un calendrier intégré et d'un dispositif de surveillance des dossiers
- Mise à jour d'un journal d'audit détaillé pour toutes les activités de transfert
- Envoi sécurisé des fichiers volumineux via Outlook et fourniture d'un lien HTTPS pour le téléchargement
- Intégrations transparentes à d'autres produits Fortra pour assurer la protection contre les menaces et le transfert de fichiers en toute confiance

En savoir plus: [www.fortra.com/mft](http://www.fortra.com/mft)

IBM i ●  
Windows ●  
Linux ●  
Power ●  
AIX ●  
UNIX ●  
Mac OS ●



## Digital Guardian

### PRÉVENTION CONTRE LA PERTE DE DONNÉES

Digital Guardian de Fortra se déploie rapidement pour vous donner une visibilité immédiate sur les ressources essentielles de votre organisation, en protégeant les données et la propriété intellectuelle où qu'elles se trouvent. Disponibles en mode SaaS ou de déploiement d'un service managé, les tableaux de bord et les stratégies de conformité prédéfinies de Digital Guardian permettent un déploiement plus efficace et vous aident à voir les résultats et à atténuer les risques rapidement.

#### Fonctionnalités clés :

- Réduit les frais généraux, la complexité et les coûts grâce à une simplicité et une rapidité accrues, ainsi qu'à une diminution de la charge de travail des clients
- Fournit une assistance pour les environnements hybrides, notamment la couverture des systèmes Windows, macOS ou Linux, des navigateurs et des applications
- Détecte, surveille, consigne et bloque les menaces qui pèsent sur vos données grâce à des stratégies prédéfinies qui peuvent vous aider à combler les lacunes et à respecter la réglementation en constante évolution
- Soutient les initiatives de mise en conformité et protège des risques graves tout en guidant les utilisateurs vers la meilleure mesure de sécurité suivante

Windows ●  
Mac ●  
Linux ●  
Citrix ●  
VMware ●  
Hyper-V ●  
AWS ●  
Workspaces ●

En savoir plus: [www.fortra.com/digital-guardian](http://www.fortra.com/digital-guardian)



## Digital Guardian

### COLLABORATION SÉCURISÉE

Digital Guardian Secure Collaboration de Fortra chiffre et contrôle l'accès aux fichiers sensibles, quelle que soit leur destination. En adoptant une approche Zero Trust en matière de partage de fichiers, la collaboration avec quiconque - externe ou interne - devient systématiquement rapide et sécurisée, avec la possibilité de révoquer l'accès instantanément et à tout moment.

#### Fonctionnalités clés :

- Sécurise automatiquement les données lorsqu'elles sont partagées en interne et en externe
- Suit les données à mesure de leur accès tout au long de leur cycle de vie
- Vérifie les données tout au long de leurs déplacements et garantit la conformité grâce à une piste d'audit complète
- Révoque l'accès aux données et aux fichiers sensibles partagés avec les employés qui quittent l'entreprise et les fournisseurs tiers

En savoir plus: [www.fortra.com/secure-collaboration](https://www.fortra.com/secure-collaboration)

Windows ●

Mac OS ●

IOS ●

Android ●

Surface ●



Fortra

## SÉCURITÉ DE LA MESSAGERIE CLOUD

Fortra offre une protection avancée contre les menaces et une application performante des stratégies tant dans des environnements On Prem' qu'hybrides. En s'appuyant sur la science des données et la veille économique mondiale sur les menaces, les entreprises peuvent, avec Fortra, relever les difficiles défis de la sécurité de la messagerie, y compris faire face aux menaces avancées telles que la compromission de messagerie d'entreprise (BEC), le hameçonnage et bien plus encore.

### Fonctionnalités clés :

- Advanced Data Science utilise l'apprentissage automatique, les grands modèles de langage et les réseaux neuraux pour évaluer la légitimité des e-mails
- Global Inbox Threat Intelligence révèle les infrastructures de menaces avancées à l'aide d'indicateurs de menaces mondiaux vérifiés et organisés en interne
- L'équipe Email Threat Operations analyse les données relatives aux menaces et élabore des contre-mesures pour lutter contre les campagnes émergentes
- Continuous Detection & Response purge automatiquement les menaces détectées dans l'environnement de messagerie

En savoir plus: [www.fortra.com/agari](http://www.fortra.com/agari)



Agari

## PROTECTION DMARC

La protection Agari Domain-based Message Authentication, Reporting, and Conformance (DMARC) de Fortra assure l'authentification des e-mails pour protéger les clients et les partenaires des attaques par usurpation d'adresse qui peuvent détourner leur marque grâce à l'authentification automatisée des e-mails DMARC en développant des automatisations personnalisées et en orchestrant des processus multi-systèmes complexes.

### Fonctionnalités clés :

- Accélère l'application de la protection DMARC et réduit le délai de rejet en automatisant la mise en œuvre
- Surveille en permanence les domaines d'entreprise pour les protéger contre l'usurpation d'adresse et émet des alertes en cas d'abus
- Améliore la confiance des clients en protégeant leur marque des attaques par hameçonnage
- Maximise l'efficacité du marketing et améliore les taux de livraison grâce à des communications fiables
- Réduit les coûts opérationnels liés à la gestion des canaux de messagerie

En savoir plus: [www.fortra.com/agari](http://www.fortra.com/agari)



Clearswift

## PASSERELLE DE MESSAGERIE SÉCURISÉE

L'apppliance Clearswift Secure Email Gateway de Fortra protège contre la perte de données et les menaces masquées en identifiant et en bloquant de manière granulaire les spams, les virus et les logiciels malveillants et en empêchant les données sensibles de quitter votre organisation, sans perturbation des messages entrants.

### Fonctionnalités clés :

- L'anti-malware « zero hour » et la détection de code actif suppriment les menaces provenant des rançongiciels et autres qui pèsent sur le trafic des e-mails entrants et sortants ; offre l'antivirus Avira ou Sophos et plus encore
- Mécanisme de défense anti-spam multicouche, le meilleur de sa catégorie, qui permet une détection à plus de 99 %
- L'inspection approfondie du contenu élimine les risques tout en maintenant des communications fluides et offre un contrôle souple et granulaire
- Plusieurs options de chiffrement des e-mails sont proposées, notamment TLS, portail, PGP, S/MIME, PDF, Zipet et eDRM
- Compatible avec tous les systèmes de messagerie, notamment Microsoft Office 365, Exchange, Google Workspace, etc.

Linux ●  
Amazon ●  
AWS ●  
Azure ●  
vSphere ●  
Hyper-V ●

En savoir plus: [www.fortra.com/clearswift](http://www.fortra.com/clearswift)



PhishLabs

## PROTECTION FACE AUX RISQUES NUMÉRIQUES

PhishLabs est le leader de la protection face aux risques numériques. Notre solution unifiée protège vos actifs numériques critiques face aux cyberattaques externes, grâce à des renseignements dûment sélectionnés sur les menaces ainsi qu'à un dispositif complet d'atténuation des risques d'usurpation de marque, de fuite de données, d'attaques sur les réseaux sociaux, de piratage de comptes et autres risques numériques.

### Fonctionnalités clés :

- Gagnez en visibilité sur les menaces externes grâce aux données collectées sur le Web visible, le Web profond, le Dark Web, les réseaux sociaux et les flux tiers — grâce à des méthodes avancées d'exploration, d'analyse et anti-évasion
- Accédez à une grande variété d'indicateurs de menaces, collectés et organisés, pour une identification plus rapide, y compris celles qui ont franchi les passerelles Secure Email Gateways et les défenses de première ligne supplémentaires leaders de l'industrie
- Retraits rapides et complets grâce à des partenariats stratégiques avec des fournisseurs de technologies, intégrations de « Kill Switches » (boutons d'arrêt d'urgence), API de retrait, voies rapides, blocage de navigateur — et bien plus encore

En savoir plus: [www.fortra.com/phishlabs](http://www.fortra.com/phishlabs)



Terranova Security

## SOLUTION DE SENSIBILISATION À LA SÉCURITÉ

Terranova Security aide les organisations à travers le monde à réduire les risques cyber liés au facteur humain, à renforcer la résilience des entreprises face aux cybermenaces et à les accompagner pour créer une culture organisationnelle de la sécurité. La solution de formations en sensibilisation à la cybersécurité permet de mettre en place facilement des campagnes selon les risques, grâce à un contenu de qualité et des simulations de phishing basées sur des exemples réels.

### Fonctionnalités clés :

- Stimulez l'engagement, la participation et les taux de complétion des programmes de formation grâce à des cours interactifs et multilingues
- Testez et renforcez vos connaissances sur les cybermenaces grâce à des simulations d'hameçonnage basées sur des exemples réels et entièrement personnalisables
- Surveillez les performances et les progrès en matière de changement de comportement grâce à des rapports et des analyses flexibles et approfondies
- Bénéficiez d'une assistance de premier ordre et notamment de conseils de RSSI pour vous aider à atteindre tous vos objectifs de formation en sensibilisation à la cybersécurité

En savoir plus: [www.fortra.com/terranova-security](http://www.fortra.com/terranova-security)



# PROTECTION DE L'INFRASTRUCTURE



## Beyond Security & Digital Defense

### **GESTION DES VULNÉRABILITÉS**

Nos solutions de gestion des vulnérabilités identifient, évaluent, hiérarchisent et signalent les failles de sécurité pouvant mettre en péril votre organisation. Les solutions de gestion des vulnérabilités de Fortra couvrent l'analyse des vulnérabilités, l'analyse des applications Web, l'analyse des menaces actives et le test de sécurité des applications dynamiques (DAST) qui inclut un fuzzer de boîte noire (BBF).

#### **Fonctionnalités clés :**

- Analyse votre réseau et vos applications pour détecter d'éventuelles vulnérabilités
- Identifie, hiérarchise et signale les vulnérabilités et points faibles identifiés
- Outils évolutifs et simples d'utilisation
- Service clientèle expert et primé

En savoir plus: [www.fortra.com/beyond-security](http://www.fortra.com/beyond-security) et [www.fortra.com/digital-defense](http://www.fortra.com/digital-defense)



## Core Impact

### LOGICIEL DE PEN TESTING

Core Impact de Fortra est un puissant outil de PenTesting qui vous permet d'utiliser les mêmes techniques que celles des auteurs des menaces d'aujourd'hui pour déterminer vos plus grands risques en matière de sécurité. Grâce à des automatisations guidées, vous pourrez exploiter en toute sécurité les faiblesses de sécurité et révéler comment les chaînes de vulnérabilités ouvrent des voies d'accès à vos systèmes et ressources essentiels.

#### Fonctionnalités clés :

- Effectue des évaluations efficaces de l'ensemble de votre infrastructure en testant le réseau, le côté client, les applications Web et le réseau mobile/Wifi
- Utilise une bibliothèque stable et à jour d'exploits de classe mondiale
- Importe et valide les vulnérabilités via différents scanners de vulnérabilités
- Génère des rapports détaillés pour aider à prouver le respect de la conformité aux réglementations telles que PCI DSS, GDPR et HIPAA
- Teste de nouveau les systèmes attaqués pour vérifier l'efficacité des mesures correctives ou des contrôles compensatoires

En savoir plus: [www.fortra.com/core-security](http://www.fortra.com/core-security)



## Cobalt Strike

### ÉMULATION DES MENACES ET SIMULATION « RED TEAM »

Cobalt Strike est un outil robuste d'émulation des menaces, grâce auquel les professionnels de la sécurité peuvent répliquer des attaques avancées et mettre à l'épreuve votre stratégie de réponse aux incidents afin d'améliorer votre sécurité. Idéal pour les exercices de post-exploitation et de red team, cet outil de sécurité proactif a été conçu dans un souci de flexibilité afin d'adapter les engagements à tous vos besoins.

#### Fonctionnalités clés :

- Fournit une charge utile de signature très flexible, Beacon, qui permet de prendre et de conserver le contrôle des systèmes compromis
- Utilise un cadre C2 malléable qui permet aux opérateurs d'apporter des modifications et d'incorporer leurs propres outils
- Donne accès à Cobalt Strike Community Kit, un référentiel d'outils créé et organisé par d'autres opérateurs
- Favorise la collaboration Red Team (équipe rouge) via le partage des données et une communication en temps réel

En savoir plus: [www.fortra.com/cobalt-strike](http://www.fortra.com/cobalt-strike)



## Outflank

### OUTILS DE SÉCURITÉ ET SERVICES DE RED TEAMING

Le Outflank Security Tooling (OST) de Fortra est un vaste ensemble d'outils de red teaming couvrant chaque étape importante de la chaîne de destruction de l'attaquant, de l'intrusion initiale à l'exfiltration des données. Les outils OST sont explicitement développés pour contourner les mesures défensives et les outils de détection, en créant des scénarios authentiques qui simulent une attaque réelle par un auteur de menace avancée ou un groupe de cybercriminels.

#### Fonctionnalités clés :

- Antivirus amélioré et EDR
- Intégrations à d'autres solutions de Red Teaming
- Outils pour chaque phase de la chaîne d'attaque
- Exploits, scripts et autres supports d'engagement
- Communauté Slack privée et dédiée

#### Services de Red Teaming Outflank

Cette Red Team expérimentée et aux spécialisations diverses collabore avec les organisations en vue de mieux les préparer aux cyberattaques. Leurs offres comprennent le Red Teaming et la simulation d'attaques, les tests de pénétration avancés, la réponse aux incidents, le support SOC, le conseil et la formation de Blue Team.

En savoir plus: [www.fortra.com/outflank](http://www.fortra.com/outflank)



Tripwire

## SURVEILLANCE DE L'INTÉGRITÉ

Tripwire est un leader reconnu pour la mise en place de bases solides en matière de cybersécurité. Depuis plus de 20 ans, nous nous adaptons à l'évolution rapide des avancées technologiques pour nous défendre contre les menaces en constante évolution et protéger les plus grandes organisations du monde des cyberattaques les plus dangereuses. Notre gamme de solutions utilise des contrôles de sécurité fondamentaux tels que la surveillance de l'intégrité des fichiers (FIM) et la gestion de la configuration de la sécurité (SCM) pour protéger l'intégrité de votre infrastructure numérique.

### Fonctionnalités clés :

- Déploiement de contrôles de sécurité cohérents sur les infrastructures complexes
- Évaluation et hiérarchisation automatique des modifications détectées grâce à un traitement en temps réel
- Intégration aux systèmes de gestion de parc informatique pour remédier aux modifications détectées
- Gestion automatique de la conformité réglementaire pour s'adapter aux normes industrielles
- Renforcement des systèmes à l'aide des meilleures pratiques et des standards de l'industrie

En savoir plus: [www.fortra.com/tripwire](http://www.fortra.com/tripwire)

AIX  
Linux  
Mac OS  
HP-UX  
Solaris  
Windows



Powertech

## CYBERSÉCURITÉ POUR IBM i

Powertech est la première source de solutions automatisées de sécurité et de conformité pour les environnements IBM i. De la gestion des Exit Points au chiffrement, la gamme d'offres de Powertech combine l'expertise IBM i inégalée de Fortra avec des logiciels de niveau mondial et un support client exceptionnel.

### Fonctionnalités clés :

- Gère les identités et les accès des utilisateurs
- Préviend et détecte les tentatives d'intrusion
- Évalue les vulnérabilités
- Protège votre environnement contre les logiciels malveillants
- Chiffre les données sensibles

En savoir plus: [www.fortra.com/powertech](http://www.fortra.com/powertech)



## Powertech Antivirus

# PROTECTION CONTRE LES VIRUS ET LES LOGICIELS MALVEILLANTS

Powertech Antivirus analyse vos serveurs à la recherche de virus et logiciels malveillants. Conçu spécifiquement pour Linux, AIX et IBM i, il offre la stabilité, la puissance et la protection des scanners, mais prend également en charge les fonctionnalités des systèmes d'exploitation.

### Fonctionnalités clés :

- Analyse en natif les fichiers de vos systèmes, grâce à une solution conçue pour offrir des performances de pointe et une sécurité supérieure
- Renforce votre protection grâce à une liste de signatures de virus parmi les plus complètes qui soient, disponible sur n'importe quelle plateforme
- Utilise des indicateurs analytiques afin de prévenir les nouvelles menaces
- Permet de déterminer avec précision les répertoires à analyser et à quel moment le faire

En savoir plus: [www.fortra.com/antivirus](http://www.fortra.com/antivirus)

IBM i ●  
Linux ●  
PowerLinux ●  
AIX ●  
Solaris ●



## Core Access Assurance Suite

# GOVERNANCE ET ADMINISTRATION DE L'IDENTITÉ

Leader sur le marché des solutions de gestion des identités et des accès, la gestion du cycle de vie des rôles, ou encore la gestion des mots de passe, la suite d'outils Core Access Assurance Suite vous aide à répondre aux exigences de conformité en vigueur. Core Access Assurance Suite permet également à votre organisation de tirer parti d'analyses exploitables pour améliorer la gouvernance et fournir un provisionnement éclairé.

### Fonctionnalités clés :

- Améliore la sécurité de l'organisation et réduit les risques liés à la gestion des identités
- Rationalise les processus de certification pour répondre aux exigences croissantes des auditeurs
- Garantit la conformité aux réglementations gouvernementales et aux normes industrielles
- Améliore l'efficacité opérationnelle, permettant à l'entreprise de faire plus avec moins
- Fait gagner du temps grâce à l'automatisation de la création de comptes et l'attribution de l'accès quel que soit le type d'utilisateur

En savoir plus: [www.fortra.com/access-assurance-suite](http://www.fortra.com/access-assurance-suite)



## Core Privileged Access Manager (BoKS)

### GESTION DES ACCÈS PRIVILÉGIÉS

Core Privileged Access Manager (BoKS) transforme votre environnement hybride de serveurs Linux/UNIX en un domaine unique, sécurisé et géré de manière centralisée. Contrôlez l'accès à vos systèmes et informations essentiels grâce à un déploiement simple et assurez un contrôle total de vos comptes, des accès et des privilèges. Vos équipes informatiques et de sécurité sont ainsi en mesure de prévenir proactivement les attaques internes et externes visant les systèmes essentiels avant qu'elles n'aient effectivement lieu.

Linux  
UNIX

#### Fonctionnalités clés :

- Contrôle complet des comptes, des accès et des autorisations
- Centralisation de l'administration des comptes et des profils d'utilisateurs pour une gestion plus simple et plus évolutive
- Limite les autorisations des utilisateurs afin de s'assurer qu'ils disposent des privilèges minimum nécessaires à l'accomplissement de leur fonction
- Rationalise les demandes d'accès aux comptes et automatise la gestion des mots de passe en libre-service pour Linux et UNIX

En savoir plus: [www.fortra.com/boks](http://www.fortra.com/boks)

## LES OFFRES GROUPÉES EN MATIÈRE DE CYBERSÉCURITÉ DE FORTRA



### PROTECTION CONTRE LES MENACES SFT

Grâce à une intégration transparente à notre Secure ICAP Gateway, cette offre groupée vous permet d'inspecter le contenu transféré avec GoAnywhere MFT de Fortra ou Globalscape EFT de Fortra pour détecter les menaces et les fuites. Sans courir le risque d'être victimes de logiciels malveillants ou de pertes de données, les organisations ont l'assurance que les données seront partagées et reçues en toute sécurité.



### SÉCURITÉ OFFENSIVE

Les auteurs des menaces sont constamment à la recherche de failles de sécurité pour s'introduire dans les réseaux et les applications d'une organisation. Des solutions proactives telles que la gestion des vulnérabilités Fortra et le logiciel de pen testing Core Impact, ainsi que les outils de red teaming Cobalt Strike et Outflank, permettent à votre équipe d'adopter une approche offensive de la sécurité. Ces outils identifient les failles de sécurité, prévoient leur impact potentiel et effectuent des simulations d'attaques qui utilisent les mêmes techniques que celles des auteurs malveillants modernes. Trouvez et corrigez les failles de sécurité de manière préventive grâce à nos offres groupées de sécurité offensive.



### FORMATION ET RÉPONSE

Une excellente formation de sensibilisation à la sécurité incite les utilisateurs à identifier et à signaler les menaces rencontrées dans la boîte de réception, jouant le rôle de deuxième ligne de défense essentielle. Toutefois, les menaces persisteront si les équipes du SOC sont surchargées et mal préparées à examiner les e-mails signalés et à fournir un retour d'information, en particulier si elles manquent de personnel. Mettez fin aux menaces par e-mail en dispensant une formation de sensibilisation à la sécurité de niveau international et en analysant les e-mails suspects.

En savoir plus: [www.fortra.com/bundles](http://www.fortra.com/bundles)

## NOS MARQUES DE CYBERSÉCURITÉ

### **Agari®**

Email Security

### **Alert Logic®**

Managed Security Services

### **Beyond Security®**

Vulnerability Management and  
Application Security Testing

### **Clearswift®**

Email Security

### **Cobalt Strike®**

Adversary Simulations and Red  
Team Operations

### **Core Security®**

Penetration Testing Software and  
Security Consulting Services

### **Data Classification**

Metadata Labeling

### **Digital Defense®**

Vulnerability Management and  
Penetration Testing Services

### **Digital Guardian®**

Data Protection and Secure Collaboration

### **FileCatalyst®**

File Acceleration

### **Globalscape®**

Managed File Transfer

### **GoAnywhere®**

Managed File Transfer

### **Outflank®**

Offensive Security Tooling  
for Red Teams

### **PhishLabs®**

Digital Risk Protection

### **Powertech®**

Cybersecurity for IBM Power Servers

### **Tripwire®**

Integrity Management

### **Terranova Security®**

Security Awareness Training

En savoir plus: [www.fortra.com/solutions](http://www.fortra.com/solutions)

# FORTRA®

## À propos de Fortra

Fournisseur de logiciels de cybersécurité unique sur le marché, Fortra propose à ses clients un futur à la fois plus simple et plus résilient. Nos experts et notre portefeuille, riche de solutions évolutives et intégrées, offrent aux entreprises du monde entier une maîtrise et un équilibre accrus. Acteurs du changement positif, nous vous accompagnons à chaque étape de votre parcours de cybersécurité et vous aidons à garder l'esprit serein. Pour en savoir plus, rendez-vous sur [fortra.com/fr](https://fortra.com/fr).