

Protection de vos données sensibles contre les menaces externes et internes

Une nouvelle génération de protection des données

- Protection de la propriété intellectuelle
- Conformité aux réglementations
- Protection des données sur le Cloud

Protection des informations sensibles contre les multiples menaces de notre époque

L'écosystème des entreprises modernes repose désormais sur un modèle ouvert de collaboration et de confiance, et c'est précisément ces deux vecteurs qui font l'objet d'une constante exploitation par les organisations ou les personnes malveillantes. Un flux d'informations constant est vital à l'écosystème des entreprises. Les données sont distribuées et dispersées au travers de l'écosystème qui s'élargit et requiert toujours davantage de protection. Les organisations malveillantes prennent activement pour cible les données critiques de tout l'écosystème, ce qui rend les entreprises de plus en plus exposées et vulnérables.

DIVERSITÉ D'ACTEURS MALVEILLANTS	... EXTRÊMEMENT MOTIVÉS	... QUI CIBLENT VOS DONNÉES SENSIBLES	... ET FONT PESER DES RISQUES INÉDITS SUR VOTRE ORGANISATION
État-Nation	<ul style="list-style-type: none"> • Avantage économique, politique ou militaire 	<ul style="list-style-type: none"> • Secrets industriels • Informations d'affaires • Technologies émergentes • Infrastructure critique 	<ul style="list-style-type: none"> • Perte de l'avantage concurrentiel • Perturbation de l'infrastructure critique
Crime organisé	<ul style="list-style-type: none"> • Gain financier immédiat • Collecter des informations pour des gains financiers ultérieurs 	<ul style="list-style-type: none"> • Systèmes financiers/de paiement • PII, PCI, PHI 	<ul style="list-style-type: none"> • Enquêtes règlementaires et amendes • Actions en justice • Perte financière • Perte de confiance
Hacker	<ul style="list-style-type: none"> • Influencer le changement politique ou social • Pression sur l'entreprise à modifier ses pratiques 	<ul style="list-style-type: none"> • Secrets d'affaires • Informations d'affaires • Informations des cadres, employés clés • PII, PCI, PHI 	<ul style="list-style-type: none"> • Perturbation des activités opérationnelles • Marque et réputation endommagées • Perte de la confiance du consommateur
Internes	<ul style="list-style-type: none"> • Avantage personnel, avantage financier • Revanche professionnelle • Patriotisme 	<ul style="list-style-type: none"> • Ventes, chiffres, stratégies de développement des marchés • Secrets d'affaires, IP et R&D • Opérations d'affaires • Informations personnelles 	<ul style="list-style-type: none"> • Divulgence de secrets industriels • Perturbations des opérations • Marque et réputation • Impact sur la sécurité nationale

Nous protégeons

5
malwares ont lieu
chaque seconde¹

70-90%
des malwares ciblent une organisation
spécifique¹

60%
des cas, les attaques sont capables de
compromettre une organisation
en quelques minutes¹

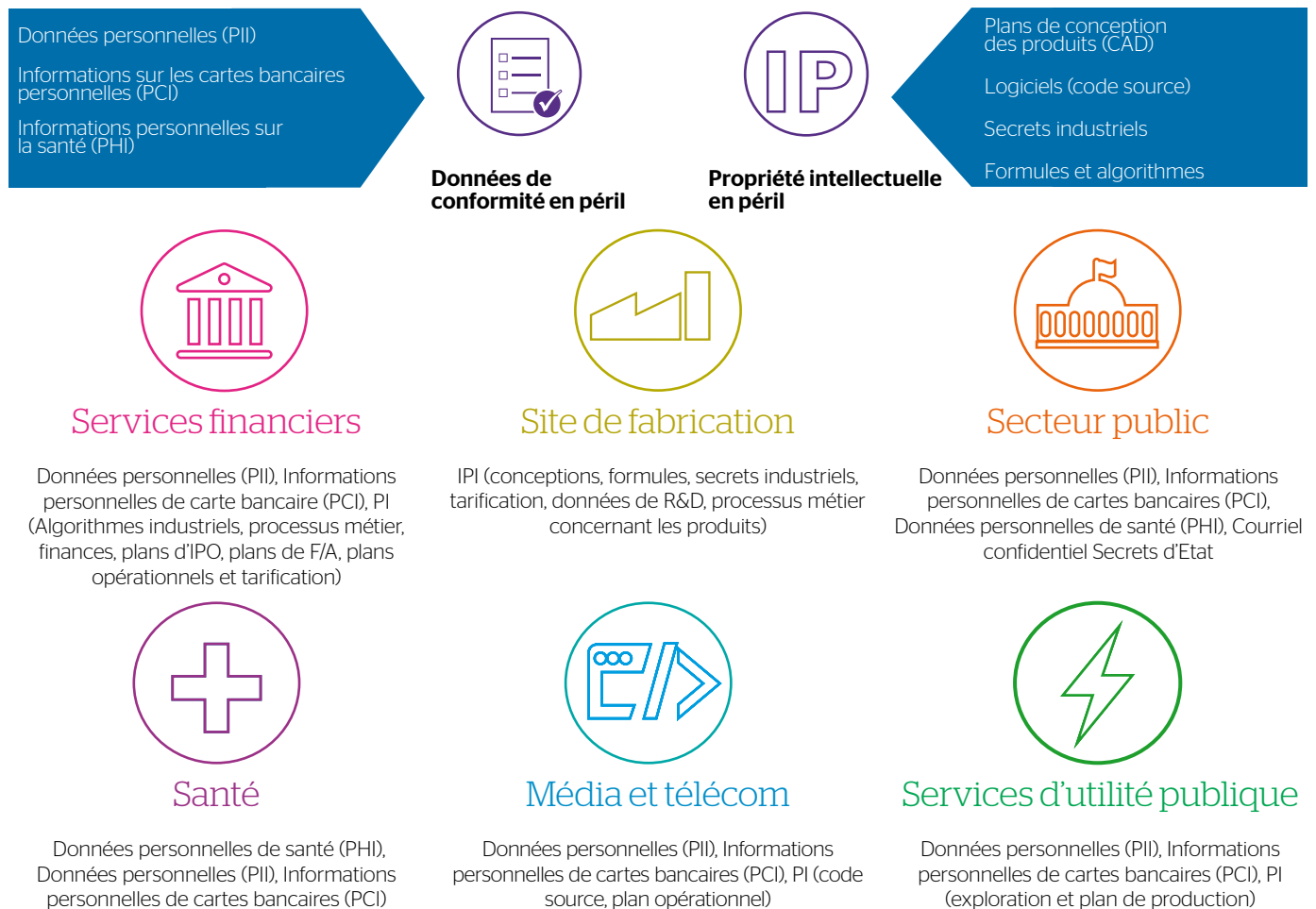
Et il faut plusieurs jours et parfois des mois pour qu'elles soient détectées...

98
jours en moyenne
pour les sociétés de
services financiers²

197
jours en moyenne
pour les sociétés
commerciales³

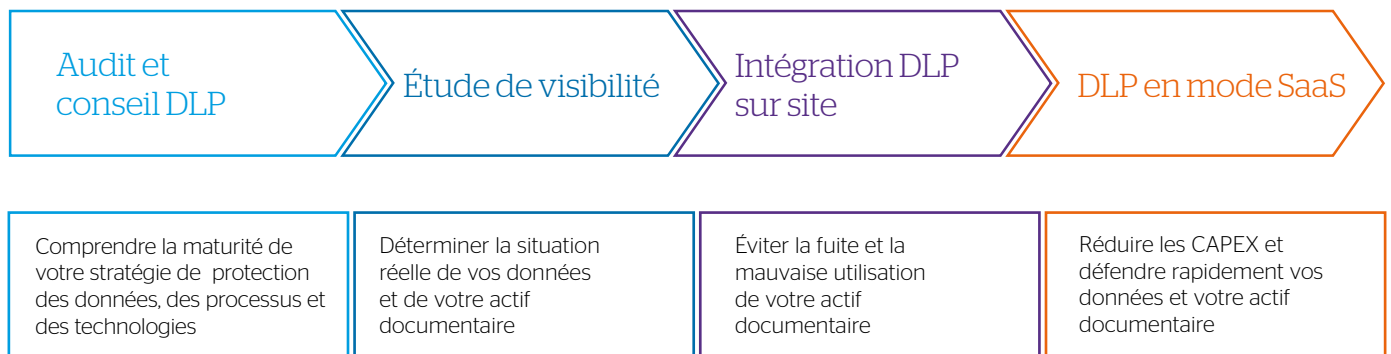
¹ 2015 Data Breach Investigations Report, Verizon
² Advanced Threats in Financial Services: A Study of North America & EMEA, Ponemon Institute
³ Advanced Threats in Retail Companies: A Study of North America & EMEA, Ponemon Institute

La conformité et la Propriété Intellectuelle (PI) sont en péril dans plusieurs secteurs d'activités





Notre approche



Phase 1: Evaluation et étude de visibilité DLP*

Nos spécialistes vous aident à déterminer le niveau de maturité de votre stratégie, vos processus et votre technologie actuels en matière de protection des données et des informations, en fonction des données les plus importantes pour votre secteur. Nous conseillons de mener l'audit DLP de concert avec l'étude de visibilité, pendant laquelle nous vous aiderons à ébaucher une stratégie visant à protéger suffisamment vos données et vos informations sensibles.

L'étude de visibilité Atos est conçue pour fournir des recommandations applicables à la mise en conformité des politiques, l'activité des utilisateurs privilégiés et des initiés, ainsi qu'aux cyberattaques ciblées potentielles. Sur une période de quatre à six semaines et un groupe de 100 utilisateurs, nous vous montrerons ce qui se passe exactement au niveau de vos données et de votre actif documentaire sensibles. Non intrusive, l'étude de visibilité vous donne des renseignements pointus sur le niveau de maturité de la protection des données dans votre environnement. Tout au long de leur mission, nos experts en sécurité vous aideront à examiner les rapports, identifier

les risques, et vous conseilleront sur les étapes concrètes à suivre pour gérer les menaces potentielles.

Phase 2: Intégration DLP* sur site

Si des faiblesses ont été identifiées au sein de votre stratégie, de vos processus et de votre technologie de protection actuels, nous vous aiderons à évoluer. Avec notre partenaire technologique, leader du Gartner Magic Quadrant, Digital Guardian, nous vous proposerons une solution éprouvée riche en différenciateurs uniques :

- ▶ Classification automatique des données (selon le contexte et le contenu)
- ▶ Visibilité complète des points terminaux du système et du comportement des utilisateurs sans politiques prédéfinies
- ▶ Ajustement rapide et précis des règles reposant sur une visibilité élargie
- ▶ Mode furtif et résistance aux altérations
- ▶ Contrôles plus exhaustifs pour stopper la sortie/l'entrée des données et leur expansion
- ▶ Capacité de corréler plusieurs événements au niveau d'un point terminal en temps réel

- ▶ Prise en charge complète des plateformes (Windows, Mac, Linux, appli mobile, Cloud)

Phase 3: DLP* en mode SaaS

DLP est une solution qui vous permet de contrôler vos ressources les plus précieuses.

Cependant, elle doit être protégée. Atos est en mesure d'exécuter la totalité de la plate-forme d'infrastructure et l'application dans un environnement Cloud hautement sécurisé, en mode partagé international pour réduire les coûts, ou en mode local pour la conformité avec les réglementations locales.

Vous en retirez les avantages suivants :

- ▶ Réduction des investissements (CAPEX)
- ▶ Hausse de flexibilité
- ▶ Gestion intégrée de la sécurité
- ▶ Délai de rentabilité rapide
- ▶ Gestion des cybermenaces 24h/7j
- ▶ Accès à la demande à des milliers de politiques de sécurité

*Prévention contre la perte des données



La détection ne suffit pas

Les menaces actuelles qui touchent la sécurité nécessitent une vision globale et une approche corrective intégrée. Le recours à des solutions de sécurité d'appoint ou à des prestataires multiples non intégrés n'apporte aucune garantie de fiabilité, car le délai entre la détection et la correction risque d'avoir des conséquences catastrophiques.

L'avantage d'Atos réside dans son approche intégrée qui combine parfaitement la détection et la réponse aux incidents. Notre approche à trois niveaux, présentée ci-dessous, réunit le centre des opérations de sécurité, la gestion des incidents et des événements, et la correction en un service complet de cybersécurité.

Centre des opérations de sécurité (SOC)

Surveillance des incidents et des événements liés à la sécurité

- Gestion intégrée de la sécurité
- Englobe l'ensemble de l'infrastructure



Atos

CSIRT

Gestion de la réponse aux incidents

- Traitement des incidents prioritaires
- Analyse et résolution

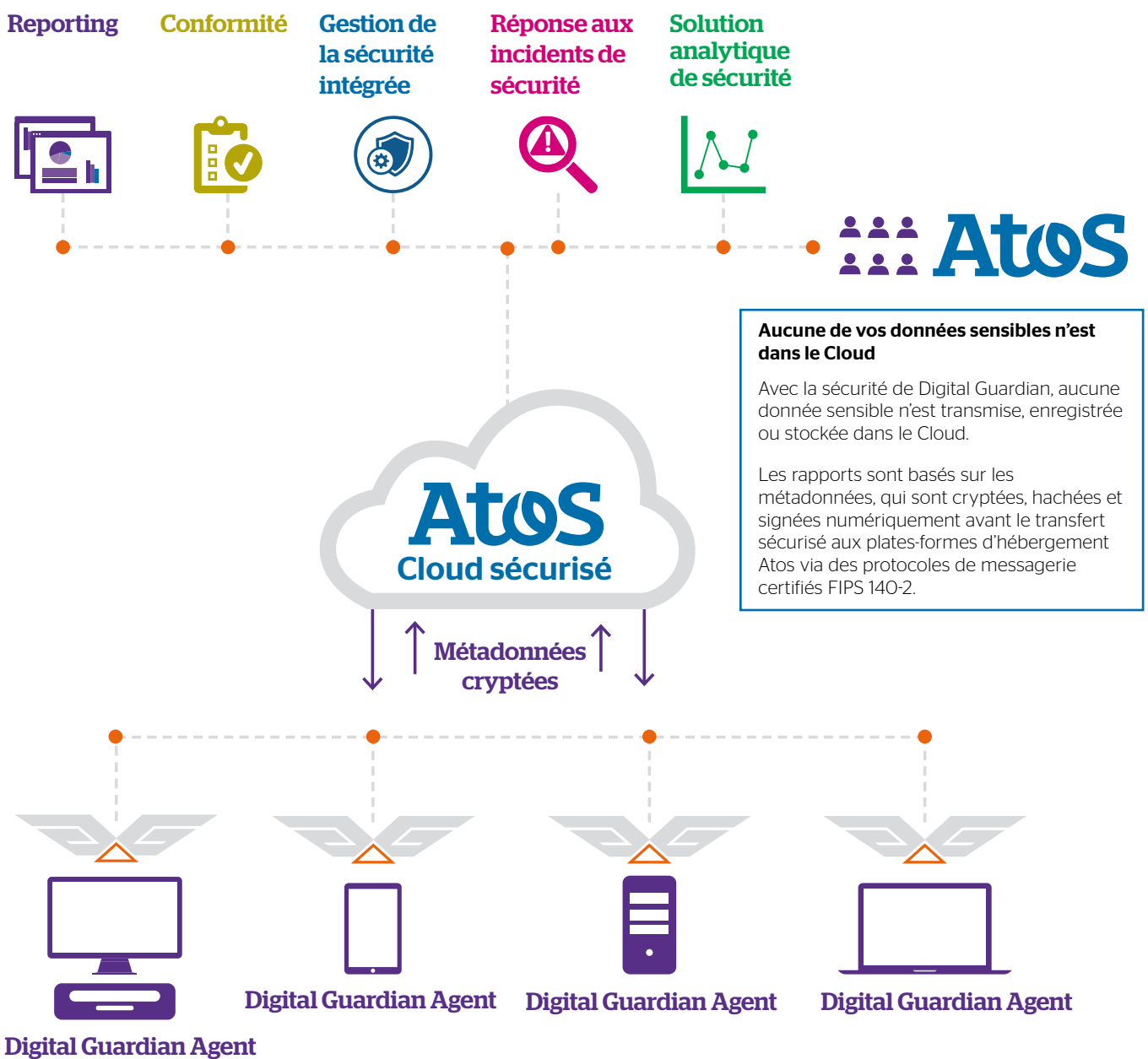
Service de gestion de la sécurité

DLP / Détection APT / IAM

- Service de prévention contre la perte de données (DLP)
- Détection avancée des menaces et correction
- Gestion des identités et de l'accès

Le partenariat entre Atos et Digital Guardian

Ce partenariat réunit le meilleur de deux entreprises de sécurité de pointe : Atos, un leader mondial dans le domaine des services de sécurité et Digital Guardian, leader du Gartner Magic Quadrant logiciels de sécurité pour la protection des données.



La conformité requiert la transparence. La protection requiert le contrôle. La protection des données et des informations d'Atos répond aux deux impératifs.

Votre société gagnera immédiatement en confiance en sachant exactement où se trouvent les données confidentielles, les personnes qui y accèdent et la manière dont elles sont utilisées. Que vous vous attachiez à protéger les informations personnelles, la propriété intellectuelle ou les deux, Atos a la solution adaptée.

- Atos couvre la protection des données et des informations sensibles de bout-en-bout, du conseil, audit et intégration, au services basés sur le Cloud
- Le service de protection des données et des informations d'Atos est le seul véritable service de protection Cloud européen. Grâce à sa capacité Cloud, il confère une protection immédiate aux données
- Protection de l'intégralité de votre environnement, notamment pour les points terminaux Windows, OS X et Linux
- Il s'agit du seul service proposant à la fois la prévention contre la perte de données, la détection d'incidents et l'intervention simultanée aux points terminaux
- La protection des données et des informations d'Atos peut autoriser, aviser ou bloquer l'activité des utilisateurs finaux en fonction de la politique établie. Tout ceci se déroule au niveau du point terminal (point le plus à risque) de sorte qu'aucune intégration complexe avec les périphériques réseau n'est nécessaire
- Délai de rentabilité le plus rapide de toutes les solutions de protection des données grâce à la classification automatique des données
- Simplicité du déploiement et flexibilité des options : déploiement sur Cloud, en infogérance 24h/7j ou sur site
- Seule solution de protection des données évolutive jusqu'à 350 000 utilisateurs avec une seule console de gestion
- Gestion intégrée de la sécurité dans l'ensemble de votre entreprise, avec vue regroupée sur votre niveau de sécurité
- Flexibilité améliorée pour une adaptation rapide aux changements de politiques et d'exigences réglementaires

56%

de hausse des vols en matière de propriété intellectuelle (brevets) en 2015.

(Source : PWC, "The Global State of Information Security® Survey 2016")

À propos d'Atos

Atos SE (Société Européenne), est un leader de services numériques avec un chiffre d'affaires annuel pro forma de l'ordre de 12 milliards d'euros et environ 100 000 collaborateurs dans 72 pays. Atos fournit à ses clients du monde entier des services de conseil et d'intégration de systèmes, d'infogérance, de Big Data et de Sécurité, d'opérations Cloud et des services transactionnels par l'intermédiaire de Worldline, le leader européen des services de paiement. Grâce à son expertise technologique et sa connaissance sectorielle pointue, Atos sert des clients dans différents secteurs : Défense, Services financiers, Santé, Industrie, Médias, Services aux collectivités, Secteur Public, Distribution, Télécoms, et Transports.

Atos déploie les technologies qui accélèrent le développement de ses clients et les aident à réaliser leur vision de l'entreprise du futur. Atos est le partenaire informatique mondial des Jeux Olympiques et Paralympiques. Le Groupe est coté sur le marché Euronext Paris et exerce ses activités sous les marques Atos, Bull, Canopy, Worldline, Atos Consulting, Atos Worldgrid et Unify.

Pour plus d'informations :
atos.net
ascent.atos.net

À propos de Digital Guardian

Le protecteur de données de choix pour les entreprises du monde les plus riches en données.

60 millions de téraoctets de données sensibles sont protégés quotidiennement par plus de 2,5 millions d'agents Digital Guardian dans 54 pays.

- La plateforme nouvelle génération de protection des données conçue pour mettre un terme au vol de données
- Leader en matière de DLP dans le Gartner Magic Quadrant
- La couverture la plus étendue du secteur, en termes de système d'exploitation : Windows, OS X et Linux
- Classification automatique des données (selon le contexte et le contenu)
- Utilisé par le Who's Who des entreprises internationales

Pour plus d'informations :
digitalguardian.com

