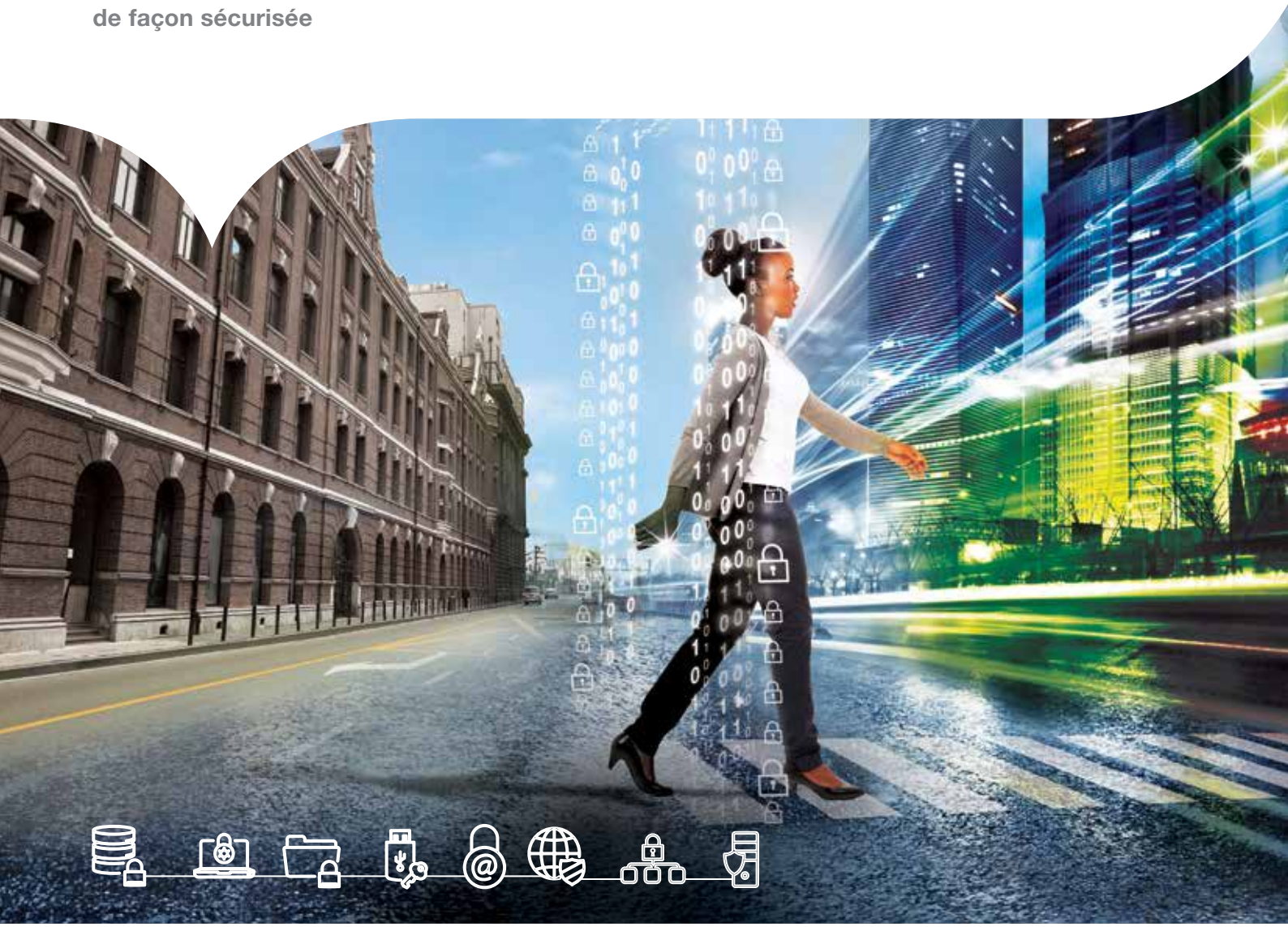
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

La cybersécurité active

Guider les entreprises et organisations publiques dans leur transformation digitale de façon sécurisée



Garantir la sécurité des entreprises à l'ère du tout numérique avec des services de bout en bout basés sur le conseil, la protection et la surveillance en matière de sécurité. Nos services couvrent les domaines critiques de la gestion des accès et identités, des applications, des terminaux et de l'infrastructure.

Sommaire


Login

Une transformation digitale sécurisée

La mise en place d'une stratégie de transformation digitale s'impose comme une évidence, mais la sécurité doit en être la pierre angulaire. C'est ainsi que les entreprises peuvent évoluer et croître en toute sécurité et en toute confiance.

Nous avons introduit la gestion de l'identité 'as a Service' avec une source unique de données client, pour plus de 5 millions d'identités dans 86 applications, avec quelque 600,000 nouvelles inscriptions en cinq mois et plus de 10 millions de visites uniques par mois.

La cybercriminalité est en pleine expansion. Avec une augmentation des cyberattaques de plus de 120 % entre 2013 et 2014[1], il n'est pas surprenant que les entreprises et organisations publiques soient en quête de réponses.

Dans le monde entier, des organisations de toutes tailles souhaitent investir l'univers numérique, la menace est donc plus réelle que jamais. En adoptant les technologies sociales, mobiles, analytiques, cloud, et les objets connectés (regroupés sous l'acronyme SMACT), les DSI savent que leurs organisations deviennent des cibles de choix. La menace se présente de différentes manières, qu'il s'agisse d'organisations criminelles, d'hacktivistes souhaitant faire parler d'eux ou d'attaques appuyées par un État.

Quel est le coût de ces menaces? Le coût annuel moyen de la cybercriminalité pour chaque grande entreprise ayant participé à une étude récente s'élève à 7,6 millions de dollars[2], ce qui représente une hausse de 10,4 % par rapport à l'année précédente. Les principales attaques informatiques peuvent engendrer des dizaines, voire des centaines de millions de dollars de pertes. Et les répercussions des violations de sécurité ne sont pas seulement financières : elles entachent la réputation des entreprises, nuisent à la confiance des clients et entravent la continuité de l'activité.

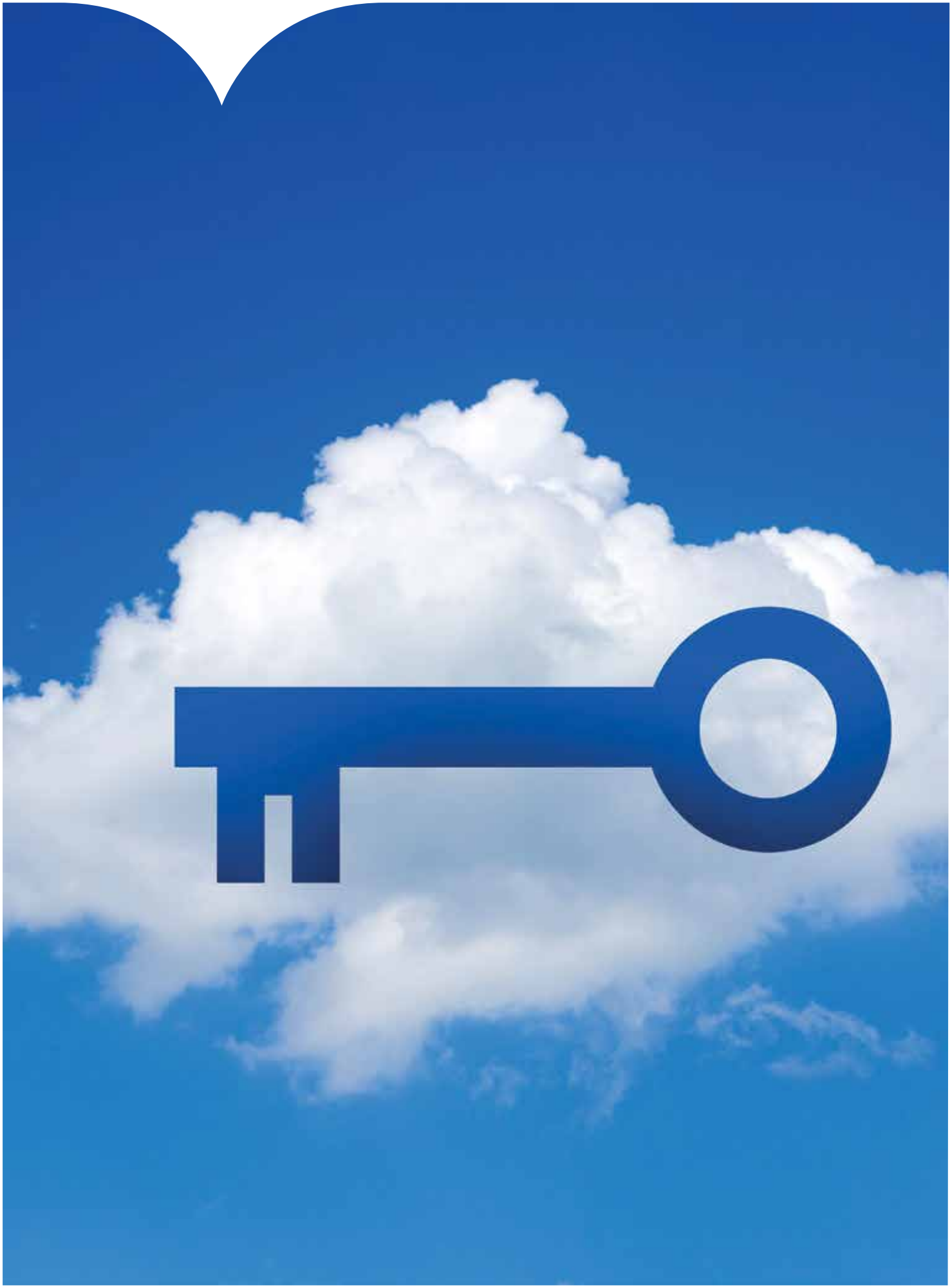
Toutefois, les avantages de la transformation digitale[3] sont tels qu'il est inconcevable, malgré ces menaces, de ne pas aller de l'avant. La mise en place d'une stratégie de transformation digitale s'impose comme une évidence, mais la sécurité doit en être la pierre angulaire. Il convient alors d'identifier et de quantifier les risques inacceptables. La tolérance au risque de l'organisation doit être définie et se traduire dans la conception et la mise en œuvre des contrôles de sécurité.

C'est ainsi qu'à l'ère du tout numérique, les entreprises peuvent évoluer et croître en toute sécurité et en toute confiance.

1 Factiva, base de données « Actualités majeures et publications d'entreprise » Thomson Financial, base de données Investext ; bases de données de différents organismes de sécurité

2 Rapport mondial 2014 sur le coût de la cybercriminalité : Ponemon Institute, octobre 2014

3 L'intérêt du numérique : comment les leaders de l'univers numérique surpassent leurs homologues dans chaque secteur, Capgemini/MIT



Technologies SMACT

L'adoption des technologies SMACT introduit de nouveaux risques pour les données sensibles et autres ressources

Aujourd'hui, de nouvelles méthodes sont mises en place par les entreprises et gouvernements pour travailler et interagir avec les clients. Les nouveaux canaux, comme les réseaux sociaux et mobiles, le Big Data et les systèmes d'analyse, les services dans le cloud, la numérisation de l'activité professionnelle et des processus industriels, exigent une nouvelle approche pour la protection des ressources critiques. Cela est dû à l'adoption des technologies SMACT qui crée de nouveaux risques pour les données sensibles et autres ressources.

Comment ces nouveaux canaux et méthodes de travail influent-ils sur la sécurité ?

- Réseaux **S**ociaux : les utilisateurs font confiance aux réseaux sociaux, ce qui ouvre la voie à divers types d'attaques informatiques. La fuite de données est une source d'inquiétude majeure, avec des informations sensibles (ou inexactes) partagées délibérément ou par inadvertance, puis diffusées rapidement. De plus, si les réseaux sociaux ne sont pas gérés correctement, le risque de préjudice pour la réputation et l'image de la marque est réel.
- Technologies **M**obiles : sécuriser les données d'entreprise, mettre en place des politiques de sécurité appropriées et assurer la conformité des appareils mobiles peut nécessiter différents mécanismes d'authentification de l'utilisateur, de chiffrement et de gestion des flottes mobiles. Ces mécanismes peuvent notamment se traduire par une gestion spécifique des applications et appareils mobiles, ainsi que des identités utilisateurs. Cela peut s'avérer particulièrement complexe lorsque les plates-formes et systèmes d'exploitation sont divers (Bring Your Own Device, par exemple). Êtes-vous en mesure de protéger votre organisation contre la fuite de données et les attaques via des périphériques mobiles accédant à des informations d'entreprise depuis des réseaux publics ? Et qu'en est-il de l'authentification des utilisateurs mobiles et de la sécurisation des applications mobiles ? Ces exigences complexes nécessitent des politiques, des outils et des mécanismes de supervision adaptés.

Nous fournissons des systèmes d'analyse de sécurité, des services SIEM (Security Information and Event Management, gestion des événements et informations de sécurité), ainsi que des services d'analyse forensic aux clients des secteurs privé et public.

Sécurisation de l'expérience client

Offrir aux clients une expérience d'exception, tout en garantissant de hauts niveaux de confiance en termes de gestion des accès et identités, peut s'avérer crucial pour se démarquer de la concurrence. Faire profiter à vos clients des différents canaux disponibles, à l'aide des processus et technologies SMACT, requiert le développement et l'introduction de nouvelles applications mobiles et services Web. La volonté de mise en service accélérée entraîne un risque accru de code contenant des failles pouvant être exploitées par les pirates. Ces vulnérabilités doivent être éliminées via un cycle de développement logiciel sécurisé de manière appropriée.

- Big Data et **A**nalytics : la capacité à exploiter divers types d'intelligence d'entreprise pour une meilleure prise de décision, notamment le renseignement de sécurité, exige l'exploitation de très grandes quantités de données (« big data »). Celles-ci sont gérées de façon innovante, pour un traitement rapide des données et l'intégration sécurisée des instruments relatifs à la science des données. La sécurité au sein de ces très grandes quantités de données n'est pas toujours simple à mettre en place. Les données personnelles doivent systématiquement être manipulées avec prudence, conformément aux réglementations nationales et internationales. Cela est particulièrement vrai lorsque d'immenses quantités de données sont regroupées dans de même lieux.
- **C**loud: la sécurité gagne en complexité tandis que votre organisation migre d'une infrastructure informatique traditionnelle vers un environnement informatique plus agile et virtualisé dans un cloud privé. Généralement, les entreprises commencent par la virtualisation de l'infrastructure afin de consolider les investissements et de réduire les coûts. Ensuite, beaucoup virtualisent les applications critiques. Elles mettent en œuvre une stratégie qui tire parti de l'automatisation et d'un plus haut niveau de gestion, pour ne pas limiter la virtualisation à la plate-forme de traitement et l'étendre à l'ensemble de l'infrastructure, dont le stockage et la mise en réseau. Ces efforts réduisent les coûts opérationnels et améliorent la qualité de service. En revanche, ils nécessitent une analyse minutieuse de la sécurité. Pourtant, il semble que la plupart des organisations n'aient pas adapté leur architecture de sécurité au nouveau modèle de centre de données virtualisé défini par logiciel. Par exemple, elles n'ont pas revu leur approche traditionnelle qui consiste à utiliser des infrastructures de sécurité physiques pour sécuriser des réseaux et centres de données virtualisés.

  En outre, les solutions de cloud public posent certains problèmes. Dans ce cas, le périmètre traditionnel de l'entreprise évolue, et il est essentiel de vérifier le niveau de sécurité offerts par les prestataires de services de cloud public. Votre système de gestion des accès et identités doit être amélioré pour protéger les identités et gérer les accès (particulièrement, par les utilisateurs bénéficiant de privilèges d'accès) aux services dans le cloud. La législation applicable peut également poser des problèmes de sécurité, à moins de pouvoir choisir la région dans

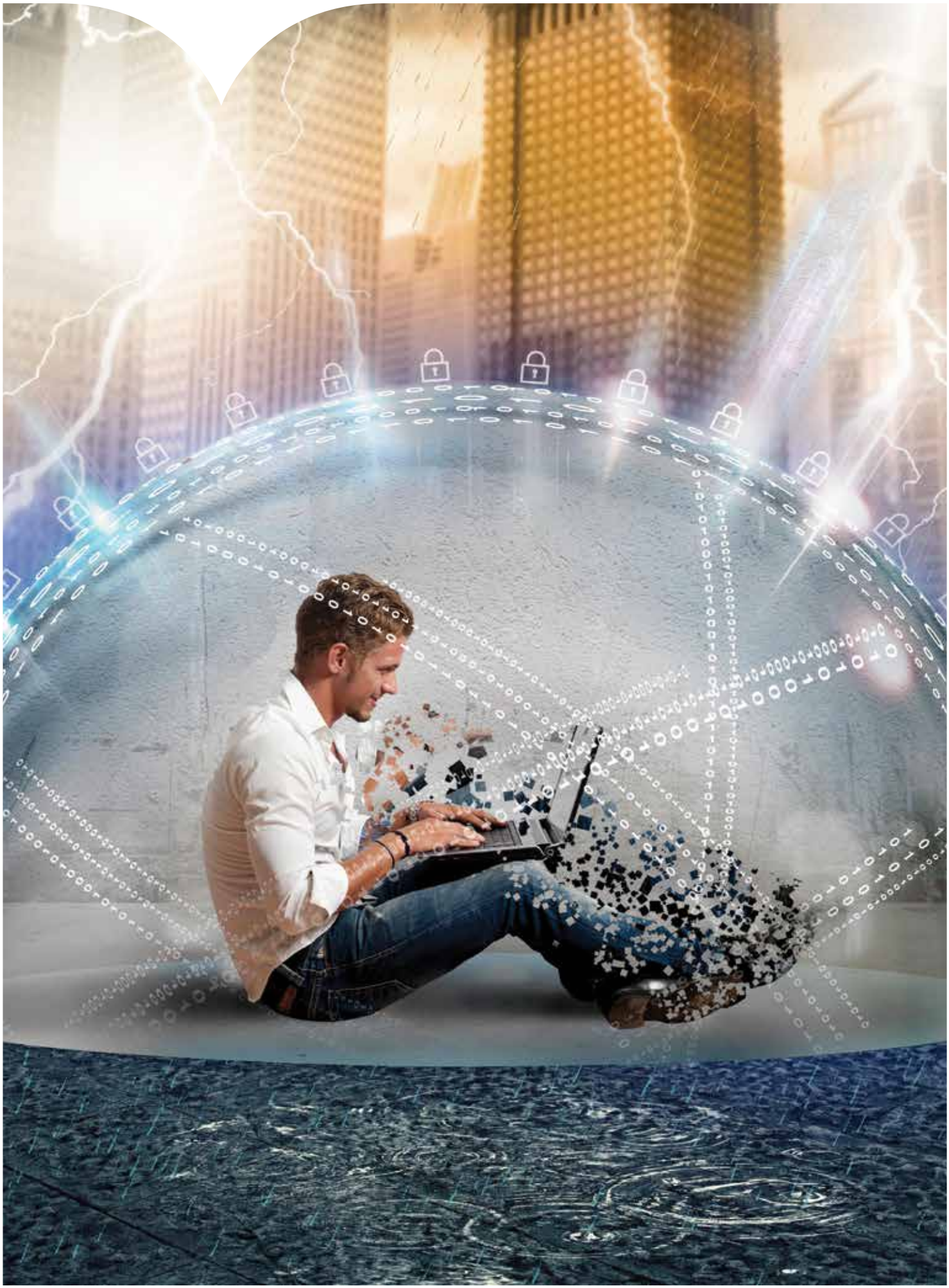
Il est essentiel de vérifier le niveau des services de sécurité offerts par les prestataires de services de cloud public.

Nos solutions de sécurité sont adaptées aux principales applications de gestion commerciale (PGI, GRC, etc.), ainsi qu'aux applications mobiles et Web. Nous développons continuellement nos services afin de nous assurer de pouvoir aider nos clients à sécuriser les systèmes de logiciels 'as a service' dans le cloud qu'ils souhaitent utiliser.

laquelle vos données sont stockées. La législation nationale régissant les prestations de votre fournisseur de services dans le cloud vous convient-elle ?

- Les objets connectés (Internet of **T**hings) : aujourd'hui, il existe également une tendance à l'interconnexion des systèmes de gestion d'entreprise avec l'Internet des objets. Les applications RH et PGI (progiciels de gestion intégrés) sont de plus en plus interconnectées avec les systèmes opérationnels, comme les systèmes de contrôle industriels comprenant des capteurs et systèmes embarqués. Cela accentue la complexité et entraîne de nombreuses vulnérabilités potentielles. En outre, cela étend considérablement le périmètre d'attaque des pirates. Aujourd'hui, les cyberattaques peuvent avoir de graves conséquences non seulement sur les données, mais également sur les infrastructures industrielles, voire sur la sécurité des personnes.

  C'est dans ce contexte que s'inscrit la nécessité absolue d'identifier les vulnérabilités au sein des systèmes de contrôle industriels critiques et de prévenir les cyberattaques. Les différents terminaux composant les systèmes de contrôle industriels d'une organisation requièrent des mécanismes renforcés de supervision, de protection et de gouvernance.



Conseiller, protéger et surveiller

Maintenez le niveau de sécurité dont vous avez besoin pour garantir l'efficacité de votre entreprise tandis qu'elle poursuit sa transformation digitale.

Nous avons recommandé différents périphériques mobiles et les avons connectés à plusieurs services hautement sécurisés, afin de répondre au besoin d'un important service ministériel en termes de sécurité mobile des agents manipulant des ressources ministérielles et des données personnelles sensibles.

Nous savons que transformer votre entreprise pour tirer le meilleur parti de nouvelles méthodes de travail constitue un impératif stratégique. Et pour vous assurer d'atteindre vos objectifs stratégiques, cette transformation doit se faire de façon sécurisée. Vous vous demandez alors où commencer ? Et comment maintenir le niveau de sécurité dont vous avez besoin pour garantir l'efficacité de votre entreprise tandis qu'elle poursuit sa transformation digitale ?

Chez Capgemini, nos 2,500 professionnels de la cybersécurité axent tout leur travail sur la protection de l'activité de clients comme vous. Nous avons conçu un portefeuille de services de cybersécurité de bout en bout couvrant les systèmes IT, des systèmes industriels (OT)[4], ainsi que des objets connectés (Internet of Things). Nous conseillons et contrôlons. Nous protégeons. Nous surveillons.

- Conseil et contrôle : assurez-vous que votre stratégie de cybersécurité est adaptée à votre tolérance au risque et à votre budget. Des évaluations de maturité de la cybersécurité aux feuilles de route, en passant par les évaluations de risque et inventaires de ressources d'information, y compris les contrôles de sécurité comme les tests d'intrusion et audits, nos services de conseil sont conçus pour vous aider à faire les bons choix concernant les éléments à hiérarchiser et les investissements à engager ;

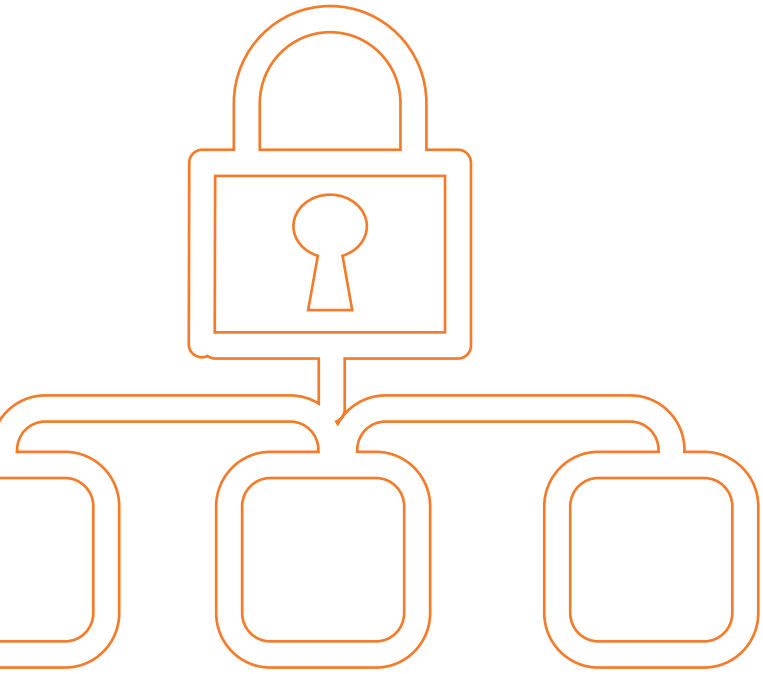
- Protection : nos services de protection établissent la ligne de défense dont vous avez besoin pour sécuriser vos données et systèmes informatiques, industriels et d'entreprise, via vos applications, terminaux, centres de données et dispositifs de gestion des accès et identités ;

- Surveillance : assurez le suivi de vos contrôles de sécurité et des menaces auxquelles vous êtes confrontés grâce à nos services de supervision de sécurité. Vous pourrez ainsi détecter les cyberattaques et y réagir de manière efficace.

Transformez-vous en toute sécurité. Faites en sorte de comprendre et de gérer les risques de cette transformation, tout en exploitant la puissance d'Internet et en vous protégeant des cyberattaques.

4 Gartner : « Les technologies opérationnelles (OT) sont du matériel et des logiciels qui supervisent et contrôlent des appareils physiques et des processus industriels ou de fabrication de l'entreprise »

Pourquoi Capgemini et Sogeti ?



Nous évaluons la cybersécurité en fonction de votre contexte et du degré de transformation de votre entreprise. Nous considérons la sécurité comme un atout et non comme un problème. C'est ce qui nous différencie.

Nous vous accompagnons tout au long de votre transformation digitale tout en assurant votre sécurité. Comment ? En associant notre compréhension et notre expérience de la cybersécurité avec une grande expertise de l'infrastructure informatique et de l'intégration des applications. Nous proposons par exemple des fonctionnalités uniques pour les systèmes critiques, comme les systèmes de contrôle industriels, les systèmes de contrôle et d'acquisition de données (SCADA), ainsi que les systèmes embarqués.

Nous pensons que l'une des meilleures manières de parer les cyberattaques consiste à se mettre à la place des pirates informatiques. Cette approche de la cybersécurité offre une perspective qui vous aide à renforcer vos défenses et rationaliser vos investissements en matière de sécurité.

Grâce à notre ensemble de méthodologies et de services pour une transformation en toute sécurité, nous mettons à votre disposition des pratiques éprouvées, des technologies

et conseils de classe mondiale, ainsi que des services de sécurité de pointe. Cet ensemble se base sur les quatre piliers de la cybersécurité : la sécurité des utilisateurs, des applications, des terminaux et de l'infrastructure, tel qu'illustré ci-contre.

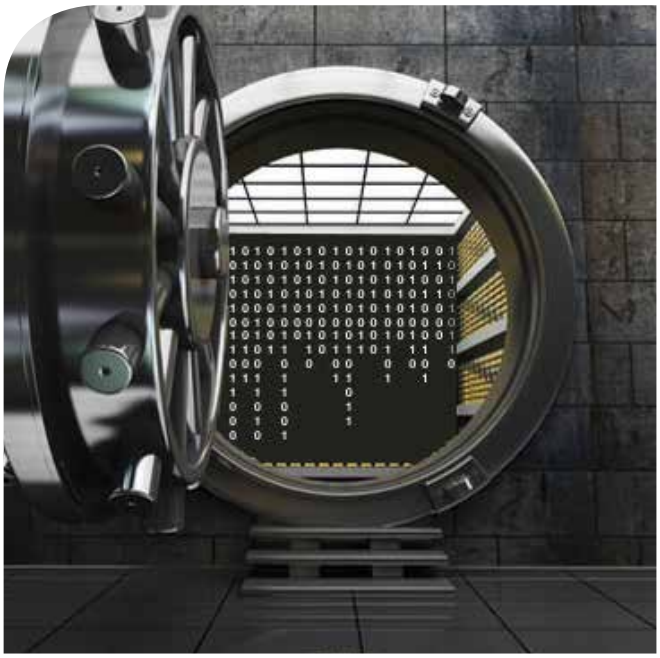
Ces services sont proposés en tant qu'assistance technique, projets à prix fixe, services de conseil et services de sécurité gérés ou hébergés. De plus, nous investissons pour rester à l'avant-garde de la tendance qui agite actuellement le secteur, à savoir le 'as a service'. Cette approche évite à nos clients des dépenses en capital, tout en augmentant la flexibilité et la fiabilité.

Nous adaptons notre écosystème de fournisseurs selon les besoins. Ainsi, nous travaillons avec un large éventail de partenaires technologiques et de fournisseurs spécialisés avec lesquels nous formons des alliances pour répondre aux besoins de chacun de nos clients. Nous pouvons aussi travailler avec un fournisseur spécifique requis par un client particulier.

Grâce à nos centres opérationnels de sécurité mondiaux (disponibles 24 h/24 et 7 j/7) qui deviennent les yeux et les oreilles des services de surveillance de votre entreprise, vous bénéficiez d'un service haut de gamme vous permettant de gérer toutes les menaces, même les plus sophistiquées.

Entre de bonnes mains

Nos clients nous font confiance pour les aider à protéger leurs univers numériques des cyberattaques :



- Gouvernement : pour un service ministériel clé, nous avons créé un portail fournissant une assistance sécurisée pour toutes les applications Web. Ce portail intègre des contrôles de sécurité avancés pour la gestion de volumes importants de transactions sensibles entre les citoyens, avec des services de sécurisation de l'accès à Internet et des systèmes d'authentification externes.
- Santé : nous avons aidé un hôpital en mettant en place des systèmes d'exploitation sécurisés, des mécanismes d'authentification de l'utilisateur, des canaux de communication et des infrastructures hébergées, pour assurer la conformité avec les réglementations en matière de vie privée et la protection des données des patients.
- Transport et service public : nous fournissons une analyse de risque pour des systèmes complets, comme les systèmes de transport ferroviaire et les réseaux d'énergie intelligents.
- Centre de contact client : nous avons conçu et mis en place des contrôles de sécurité pour le centre de contact d'une grande entreprise qui accède à plusieurs systèmes informatiques avec des données sensibles. Nous avons ensuite effectué des contrôles qualité complets de la solution pour confirmer que les niveaux de sécurité requis étaient atteints.
- Services financiers : nous gérons des centres opérationnels de sécurité pour de nombreuses organisations financières. Ces systèmes détectent les tentatives d'attaque au niveau des ressources critiques et surveillent la sécurité globale du réseau.
- Industrie : nous avons aidé un leader international à élaborer sa stratégie de protection des informations et de cybersécurité, ainsi que son programme de transformation. Cela englobait la sécurité de l'infrastructure du groupe, la protection des données au niveau des activités R&D, le modèle de gestion des accès et identités basé sur SAP, ainsi que la sécurité des systèmes industriels.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Pour en savoir plus, contactez :

Franck Greverie
Corporate Vice President des activités Cybersécurité
franck.greverie@capgemini.com

A propos de Capgemini et Sogeti

Fort de près de 145 000 collaborateurs et présent dans plus de 40 pays, Capgemini est l'un des leaders mondiaux du conseil, des services informatiques et de l'infogérance. Le Groupe a réalisé en 2014 un chiffre d'affaires de 10,573 milliards d'euros. Avec ses clients, Capgemini conçoit et met en œuvre les solutions business et technologiques qui correspondent à leurs besoins et leur apporte les résultats auxquels ils aspirent. Profondément multiculturel, Capgemini revendique un style de travail qui lui est propre, la « Collaborative Business Experience™ », et s'appuie sur un mode de production mondialisé, le « Rightshore® ».

Sogeti est l'un des leaders des services technologiques et du test logiciel, spécialisé dans la gestion des applicatifs, des infrastructures et les services en ingénierie. Sogeti propose des solutions innovantes autour du Testing, du Business Intelligence & Analytics, de la Mobilité, du Cloud et de la Cybersécurité, s'appuyant sur sa méthodologie et son modèle global de prestations de services Rightshore®. Présente dans 15 pays avec plus de 100 implantations locales en Europe, aux Etats-Unis et en Inde, la société réunit plus de 20 000 professionnels. Sogeti est une filiale à 100% de Cap Gemini S.A., coté à la Bourse de Paris.

Capgemini et Sogeti, experts en infrastructure IT et intégration d'applications, proposent une offre complète de services de cybersécurité permettant de guider et de sécuriser la transformation digitale des entreprises et des administrations. Nos 2,500 professionnels vous accompagnent pour définir et mettre en œuvre vos stratégies de cybersécurité. Nous sommes à vos côtés pour protéger vos systèmes IT, vos systèmes industriels et vos objets connectés. Nous avons de nombreux atouts pour renforcer vos défenses, optimiser vos investissements et mettre sous contrôle vos risques : des experts en sécurité (infrastructures, applications, terminaux, gestion d'accès et d'identité), une équipe de R&D spécialisée en analyse de malware et forensics, des hackers éthiques, cinq centres opérationnels de sécurité répartis dans le monde (SOC), un centre d'évaluation de la sécurité des technologies de l'information (CESTI) et notre positionnement de leader mondial dans le domaine du testing.

Plus d'informations sur :

www.capgemini.fr/cybersecurite or www.fr.sogeti.com/cybersecurite

MCOS_GI_AP_20150319