CONFIANCE NUMÉRIQUE : ÉTAT DES LIEUX 2024

LEADERS

RETARDATAIRES

PKI

CONFORMITÉ

DIGITAL TRUST POUR LE MONDE RÉEL

IoT

INTERRUPTIONS DE SERVICE

XX
ALERTE DE SÉCURITÉ

BONNES PRATIQUES

digicert®

CONFIANCE NUMÉRIQUE : ÉTAT DES LIEUX 2024

En 2022, DigiCert a lancé le tout premier état des lieux de la confiance numérique. À l'heure où la transformation digitale bat son plein dans tous les secteurs, la confiance numérique s'impose plus que jamais pour garantir non seulement la légitimité des personnes et appareils avec lesquels nous nous connectons, mais aussi la sécurité de ces interactions.

Selon Jennifer Glenn, Directrice de recherche pour IDC, la confiance numérique est « la base d'un monde connecté sûr et sécurisé. Elle représente donc un élément indispensable à toute entreprise qui cherche à rassurer ses clients, collaborateurs et partenaires quant à la fiabilité de ses processus et interactions en ligne. »

Leader de la confiance numérique, DigiCert apporte aux entreprises et aux particuliers les outils qui leur permettent d'échanger et de communiquer de façon sereine et sécurisée dans l'univers du digital. D'où l'importance de ce baromètre annuel de la confiance numérique dans les organisations, tant en termes de perception du concept que d'avancées concrètes dans l'établissement, la gestion et l'extension de la confiance numérique.

Approfondir l'analyse initiale

Le premier état des lieux réalisé en 2022 a révélé que la totalité des entreprises sondées attachait de l'importance à la confiance numérique. Et presque toutes (99 %) pensaient que leurs clients pourraient se tourner vers la concurrence en cas de perte de confiance dans leur marque. Un point confirmé par plus de deux tiers des consommateurs (68 %) qui déclaraient attacher de l'importance à la confiance numérique.

Pour l'édition 2024, nous souhaitions aller plus loin dans notre analyse et nous pencher sur des domaines et workflows spécifiques de la confiance numérique.

Méthodologie

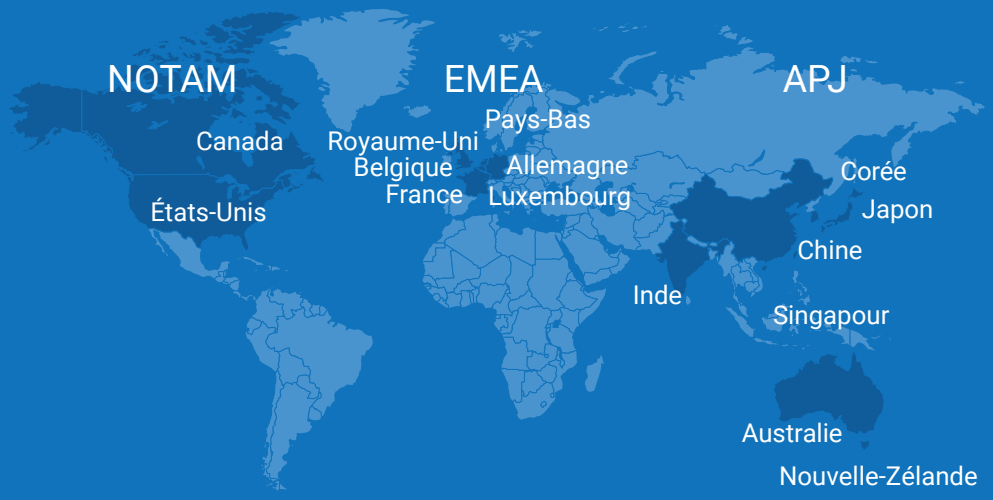
Au troisième trimestre 2023, Eleven Research, un spécialiste des études de marché basé à Dallas, a dressé un état des lieux de la confiance numérique pour 2024. Pour les besoins de l'enquête, le cabinet a interrogé par téléphone 300 dirigeants d'entreprises de taille intermédiaire et de grands groupes dans les régions Amérique du Nord, EMEA et APJ.

Les participants travaillaient dans différents secteurs, notamment la tech, l'industrie et les services financiers. Les structures de l'échantillon comptaient des effectifs allant de 1 000 à plus de 10 000 salariés.

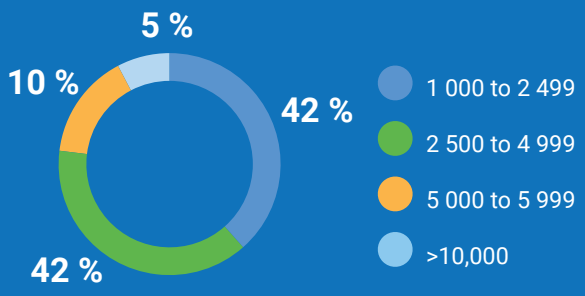
Pour bien cerner les initiatives spécifiques de confiance numérique, Eleven Research a ciblé son étude sur les responsables de quatre sous-domaines de la confiance numérique :

- Entreprise : sécurisation des communications, des données et des accès pour les collaborateurs, les applications et les clouds
- Appareils IoT et objets connectés : protection des appareils et services connectés comme les glucomètres
- Logiciels : protection des logiciels et des applications contre toute atteinte à leur intégrité et toute attaque de la supply chain logicielle
- Signatures électroniques : protection de l'authenticité et de l'intégrité des documents et de leur contenu

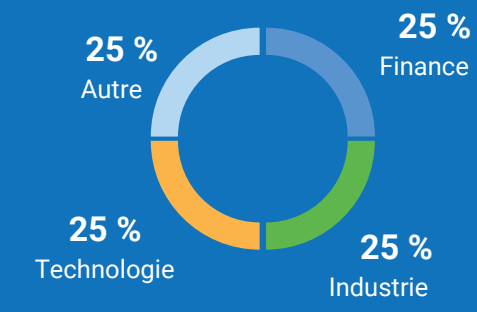
RÉGIONS ET PAYS



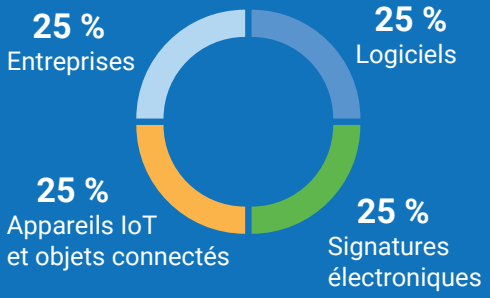
TAILLE DES ENTREPRISES



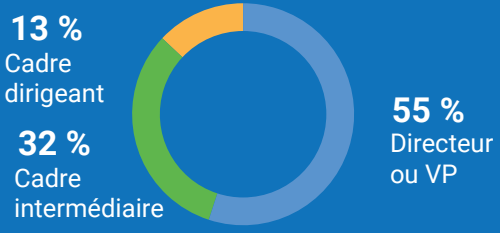
SECTEURS



PERSONAS



NIVEAU HIÉRARCHIQUE



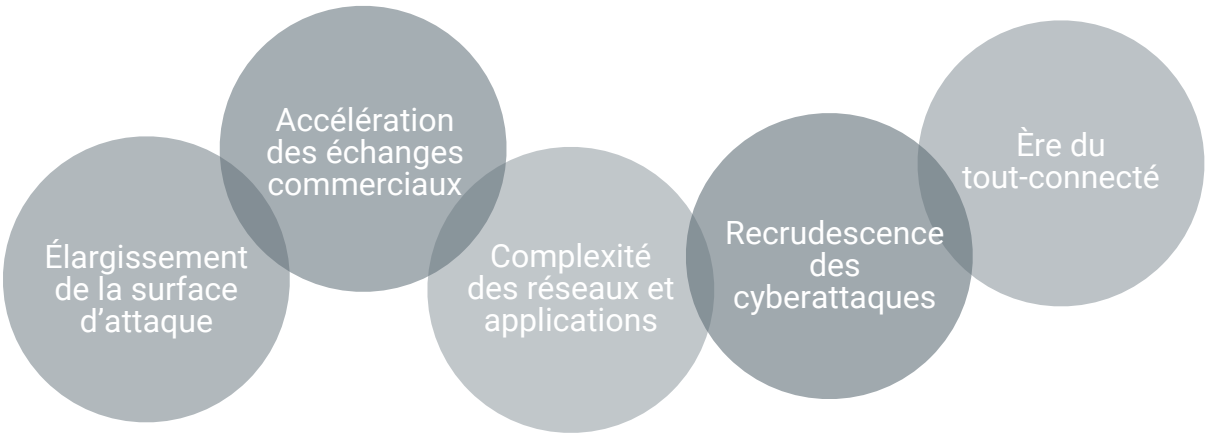
LA CONFIANCE NUMÉRIQUE RESTE AU CŒUR DES PRÉOCCUPATIONS DES ENTREPRISES

Vu l'intérêt généralisé pour la question dans l'édition précédente, c'est sans surprise que les entreprises restent focalisées sur la confiance numérique, et ce pour trois grandes raisons :

- Le nombre de télétravailleurs n'a jamais été aussi élevé
- Les réseaux ne cessent de se développer (notamment à la périphérie et par interconnexion avec les partenaires et clients)
- Surtout, les clients exigent cette confiance numérique

TROIS PRINCIPAUX RESSORTS

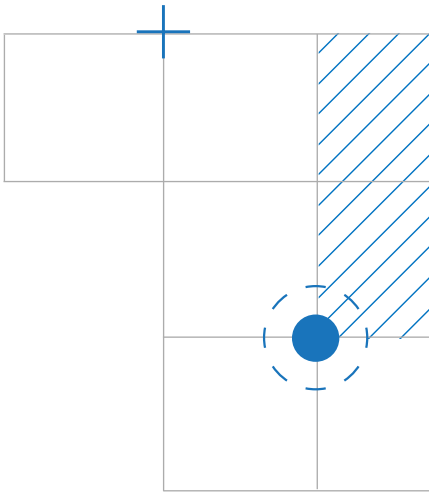
AUTRES RAISONS



Toutefois, l'établissement, le suivi et la gestion de la confiance numérique n'ont rien d'une formalité. Les entreprises se heurtent en effet à cinq grands défis :

- **Le manque d'expertise des équipes.** La confiance numérique étant une discipline relativement nouvelle, nombre de professionnels ignorent encore comment la mettre en place et la gérer de manière centralisée. Quant à leur PKI privée vieillissante et sujette aux pannes, elle représente un véritable frein à l'acquisition des compétences essentielles.
- **La complexité croissante des réseaux et des applications.** Les environnements technologiques des entreprises ne cessent de se complexifier. D'abord sur le plan des réseaux où les organisations ne se contentent plus de data centers traditionnels, de sites distants et d'une présence dans le cloud. Aujourd'hui, leurs réseaux s'étendent à la périphérie (Edge), à de multiples clouds et aux domiciles de milliers de collaborateurs en télétravail.

  Quant aux applications, elles sont passées d'une structure monolithique à des architectures de microservices ultra-distribuées, dont une majorité échappe au contrôle direct de l'entreprise. Autant dire que face à une telle complexité, l'instauration et l'optimisation de la confiance numérique prennent des allures de mission impossible.
- **L'ampleur des ressources à protéger.** À l'heure où la transformation digitale gagne du terrain, le nombre de ressources numériques critiques augmente constamment, de même que la surface à sécuriser.
- **Le manque de soutien de la part de la direction.** Dans une conjoncture inflationniste au sortir de la pandémie, les Comex ont dû faire des choix difficiles, comme en témoignent les quelque 240 000 licenciements dans le secteur de la tech, sur la seule année 2023[1]. On ne s'étonnera donc pas de voir un certain fléchissement dans l'engagement des instances dirigeantes envers les initiatives de confiance numérique.
- **L'explosion des ressources cryptographiques, et leur gestion complexe et chronophage.** Les certificats numériques constituent la clé de voûte des initiatives de confiance numérique, tant privée que publique. Le problème, c'est que l'essor rapide du portefeuille de certificats rend leur gestion difficile pour les entreprises.



[1] Tech Crunch

CONFIANCE NUMÉRIQUE : LES AVANCÉES DES ENTREPRISES

Où en sont les entreprises dans la mise en place de la confiance numérique ? La réponse à cette question est à la fois longue, complexe et tout en nuances. Pour faire court, nous dirons que la marge de progression reste importante.

Force est de constater que les résultats varient sensiblement selon le domaine numérique en question. C'est pourquoi nous avons mesuré la confiance numérique sur quatre grands pans :

- Entreprise
- Appareils IoT et objets connectés
- Logiciels
- Signatures électroniques

Entreprise : les pratiques de confiance

En général, la gestion de la confiance numérique en entreprise relève de la fonction IT. Elle inclut le plus souvent les missions suivantes :

- Gestion des certificats
- Gestion des identités et des accès (IAM)
- Sécurité des e-mails
- Sécurité des terminaux

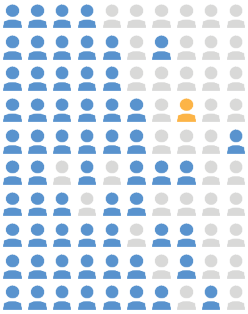
Alors que nous nous attendions à observer une assez grande maturité, dans le domaine « entreprise », la confiance numérique reste à l'état embryonnaire. Rares (seulement 1 sur 100) sont les responsables de la confiance numérique qui estiment leurs pratiques « très matures ». Pire encore, 87 % décrivent leurs initiatives comme cloisonnées.

Les certificats numériques permettent d'authentifier et de sécuriser les communications des utilisateurs, appareils (ex. : smartphones) et serveurs de l'entreprise. Le problème, c'est qu'avec l'extension et la complexification des réseaux et des cas d'usage, le nombre de certificats nécessaires s'envole.

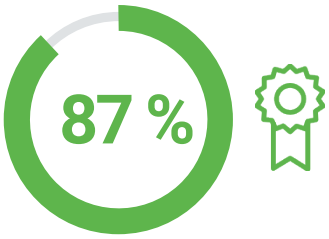
Ainsi, environ la moitié (52 %) des structures sondées confient la gestion des certificats au département IT, tandis qu'un tiers (37 %) opte pour un autre département. Dans une entreprise sur neuf (11 %), les certificats ne sont pas du tout gérés.

Notons par ailleurs que dans la plupart des entreprises, les certificats sont émis par 5 départements ou moins, même si elles sont majoritairement favorables à une augmentation de ce nombre.

Seulement **1 répondant sur 100** estime ses pratiques de confiance numérique très matures



La plupart les considèrent comme « assez matures »



décrivent leurs initiatives de confiance en entreprise comme cloisonnées

Dans la plupart des entreprises, les départements qui émettent des certificats sont au nombre de 5 ou moins

La majorité estime que davantage de départements devraient émettre des certificats

Fonctions responsables de la gestion des certificats

Gérés par le département IT

Gérés en dehors du département IT

Non gérés

Entreprise : les résultats des initiatives de confiance

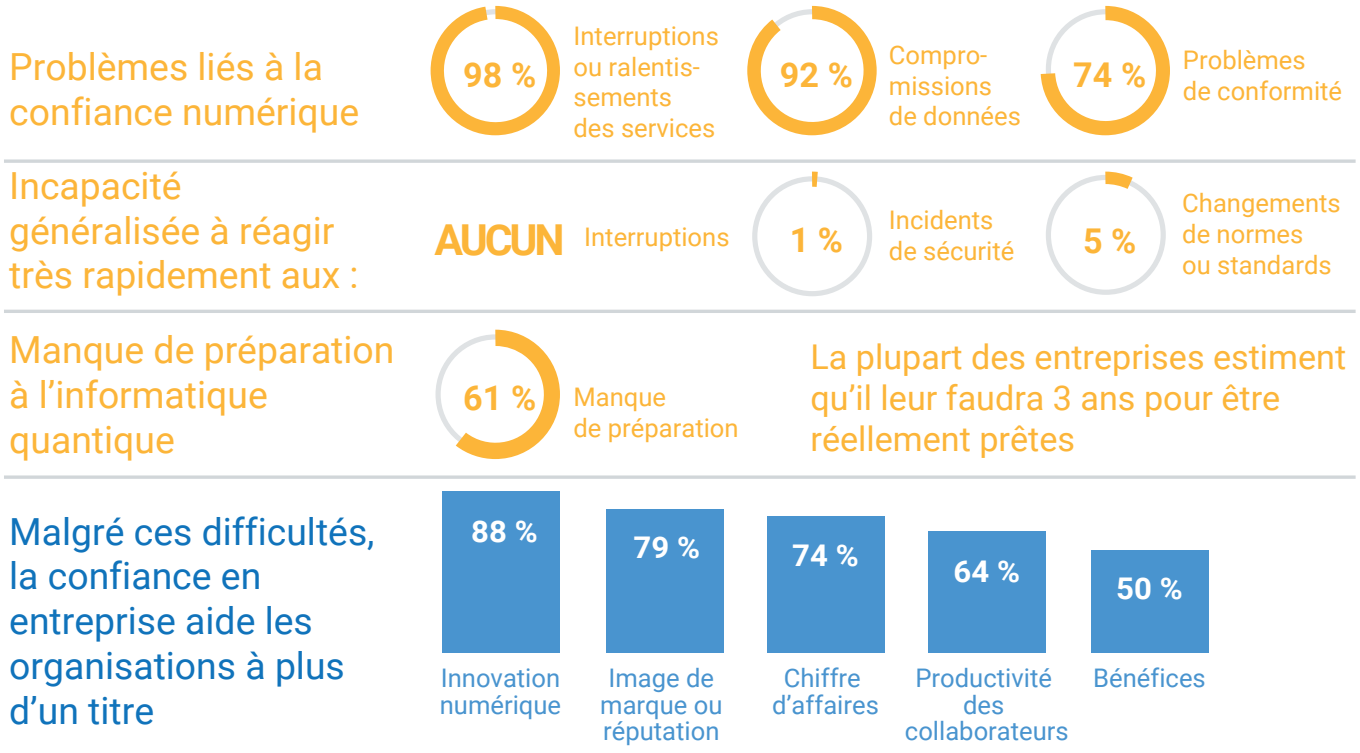
Les initiatives de confiance numérique portent-elles leurs fruits dans les entreprises ? À vrai dire, elles pourraient mieux faire. Voici un aperçu des principaux problèmes rencontrés par les responsables interrogés :

- **La quasi-totalité (98 %)** mentionne quelques interruptions ou ralentissements des services
- **La majorité (92 %)** a subi des compromissions de données
- Et **une grande partie (74 %)** s'est heurtée à des problèmes de conformité

Pour avoir une vision plus détaillée, nous avons mesuré leur agilité en matière de confiance numérique.

- **Aucune entreprise** n'est en mesure de réagir très rapidement en cas d'interruption de service
- **Presque aucune (1 %)** ne peut réagir très vite en cas d'incident de sécurité
- **Peu (5 %)** sont capables de réagir très rapidement aux changements de normes ou standards
- **La majeure partie (61 %)** se dit mal préparée à l'ère post-quantique, la plupart d'entre elles estimant à trois ans le temps nécessaire pour être réellement prêtes

Malgré ces points d'achoppement, les responsables de la confiance numérique en entreprise considèrent que leurs initiatives ont globalement eu des effets positifs dans différents domaines, tant en termes financiers que d'innovation et d'image de marque.



Appareils IoT et objets connectés : les pratiques de confiance

Pour ce volet, l'enquête s'est intéressée aux entreprises qui fabriquent et vendent des appareils IoT et objets connectés (capteurs industriels, montres connectées, thermostats intelligents, etc.). Nous nous sommes donc entretenus avec les personnes chargées des missions suivantes :

- Mesures d'authentification pour les appareils IoT et objets connectés
- Chiffrement sur les appareils IoT et objets connectés
- Signature des mises à jour de logiciels et de firmwares pour les appareils IoT et objets connectés
- Protection des appareils IoT et objets connectés via la cryptographie

Là encore, les responsables de la confiance numérique pour les appareils IoT et objets connectés font état d'une forte marge de progression. Seulement un répondant sur sept qualifie ses pratiques de très matures. La plupart d'entre eux les jugent « assez matures »

Mais le plus déroutant, c'est qu'ils sont **une grande majorité (87 %)** à transférer des données à caractère personnel provenant des appareils IoT ou objets connectés via des canaux non chiffrés.

La plupart des entreprises (88 %) sondées emploient un responsable sécurité des produits. Toutes recourent à des certificats numériques pour identifier les appareils déployés sur le terrain et imposent une authentification forte aux utilisateurs.

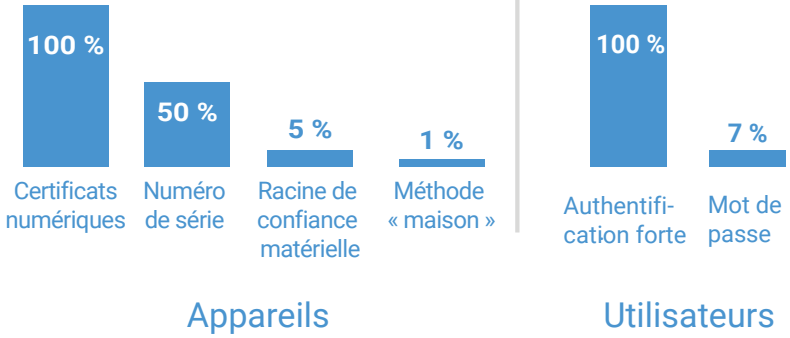
Seulement **1 répondant sur 7** estime ses pratiques de confiance numérique très matures

La plupart les considèrent comme « assez » matures

des personnes sondées transfèrent des données à caractère personnel provenant des appareils IoT ou objets connectés via des canaux non chiffrés

de tous les appareils IoT ou objets connectés sont gérés par un responsable sécurité des produits ou selon des pratiques centralisées

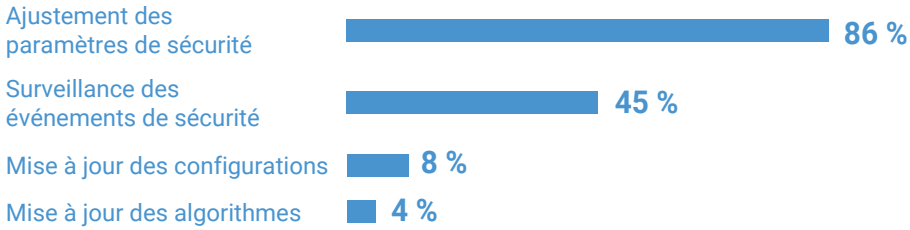
Mode d'identification de leurs appareils et utilisateurs sur le terrain



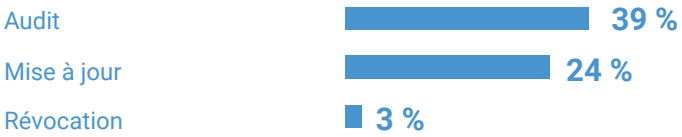
Nous avons demandé aux participants d'évaluer leurs capacités dans différents domaines liés aux appareils IoT et objets connectés. La gestion des appareils du parc obtient des résultats mitigés. Si les répondants excellent dans la gestion des paramètres de sécurité et s'en sortent plutôt bien sur la surveillance des événements de sécurité, la mise à jour des appareils laisse à désirer.

La gestion des identités d'appareils, tout particulièrement la révocation des identités, leur pose régulièrement problème. Un point positif toutefois : ils maîtrisent généralement bien la sécurité des logiciels, même s'ils sont souvent à la traîne sur la livraison sécurisée des mises à jour.

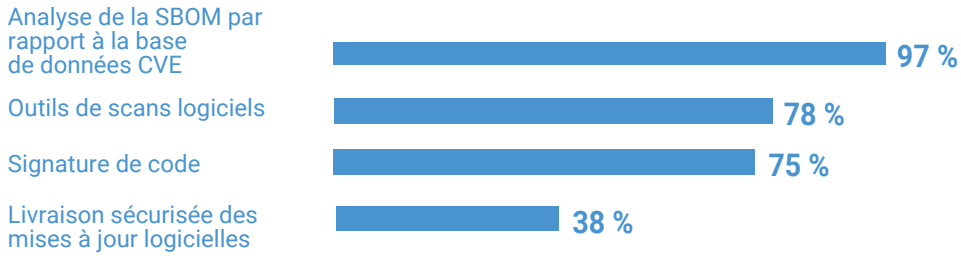
Fonctionnalités des appareils sur le terrain : Très bonne capacité de...



Gestion des identités des appareils :



Mesures prises pour sécuriser les mises à jour de logiciels et de firmwares :



Appareils IoT et objets connectés : les résultats des initiatives de confiance

Au vu de ces pratiques (ou de leur absence), les fabricants d'appareils IoT et d'objets connectés que nous avons interrogés nous ont semblé éprouver quelques difficultés :

- **La plupart d'entre eux (93 %)** ont subi des compromissions de données. Dans bien des cas, des appareils mal sécurisés ont servi de point d'entrée sur le réseau
- **La même proportion (93 %)** a connu des interruptions et ralentissements de service
- En lien avec le premier point, **84 %** des répondants ont été victimes d'une intrusion malveillante

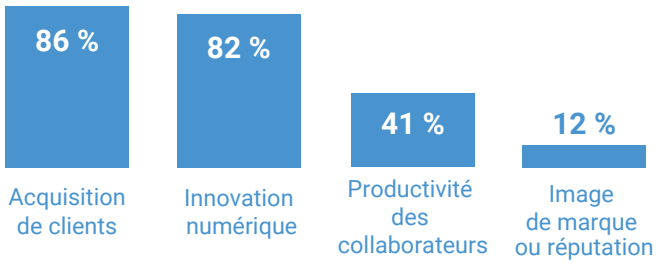
Certaines pratiques ont toutefois porté leurs fruits :

- **86 % des fabricants** ont constaté un effet de levier sur l'acquisition de nouveaux clients
- **82 % d'entre eux** ont noté une amélioration en matière d'innovation numérique

Pour autant, de sérieux progrès restent à faire en matière de confiance numérique pour les appareils IoT et objets connectés.

Problèmes liés à la confiance numérique

Malgré ces difficultés, la confiance pour les appareils IoT et objets connectés aide les organisations à plus d'un titre :



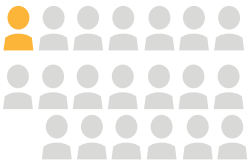
Logiciels : les pratiques de confiance

Il s'agit ici d'instaurer une confiance numérique dans les logiciels que les entreprises vendent à leurs clients (ou du moins mettent à leur disposition). Une fois de plus, le constat relève du « peux mieux faire ». Seulement 1 participant sur 20 (5 %) estime que ses pratiques de confiance pour les logiciels sont très matures. Par ailleurs, les entreprises n'utilisent pas toutes la signature de code aux mêmes fins :

- **La quasi-totalité (99 %) d'entre elles** l'emploie pour le code source du logiciel
- **84 %** y recourent pour les fichiers binaires du logiciel
- **62 %** s'en servent pour les scripts de build et la configuration de l'infrastructure
- **33 %** signent les containers et environnements sans serveurs
- **Une grande majorité (67 %) des participants** déclarent stocker les clés privées sur des équipements conformes au standard FIPS 140-2

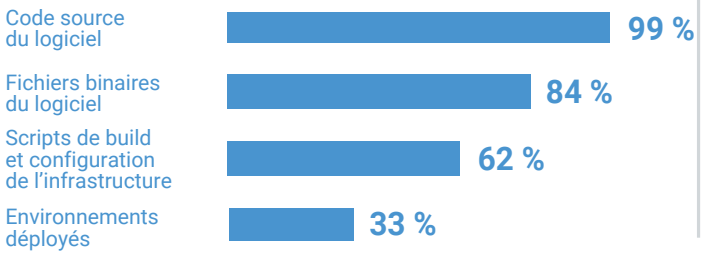
En cas de compromission d'une de leurs clés privées de signature de code, aucune entreprise n'a déclaré pouvoir identifier très rapidement toutes les applications pour lesquelles cette clé a été utilisée.

Seulement **1 répondant sur 20** estime ses pratiques de confiance numérique très matures

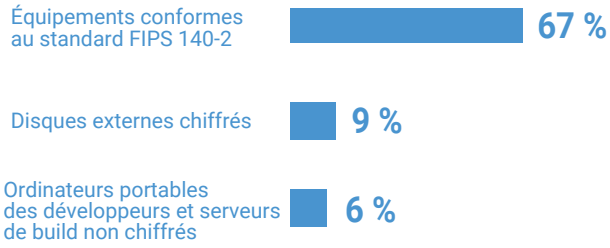


La plupart les considèrent comme « assez » matures

Ce que les entreprises protègent avec la signature de code :



Supports de stockage des clés privées de signature de code



En cas de compromission d'une de leurs clés privées de signature de code, **AUCUN PARTICIPANT** ne serait en mesure de détecter rapidement les applications pour lesquelles cette clé a été utilisée

La quasi-totalité des répondants crée une nomenclature des composants logiciels (SBOM) pour chaque application développée

La quasi-totalité des participants soumet les logiciels externes à un cahier des charges en matière de risque, de sécurité et de conformité réglementaire

Logiciels : les résultats des initiatives de confiance

Où en sont les entreprises dans la conformité de leurs logiciels aux réglementations ? Seulement 1 répondant sur 8 déclare très bien s'en sortir. Ils sont également nombreux à faire état de problèmes impactant la confiance dans leurs logiciels :

- **86 % d'entre eux** ont subi des compromissions de données
- **80 %** ont signalé des compromissions de l'infrastructure de build
- **79 %** ont connu des pannes logicielles dues à l'expiration de certificats de signature de code
- **78 %** ont livré un logiciel contenant un malware ou d'autres vulnérabilités
- **75 %** ont dû retarder leur lancement à cause d'un problème de signature de code ou de malware

Si, pour les éditeurs de logiciels, la sécurité de leurs clients passe par l'intégrité de leurs produits, sécuriser la totalité des clés nécessaires à la signature de code peut s'avérer un véritable casse-tête.

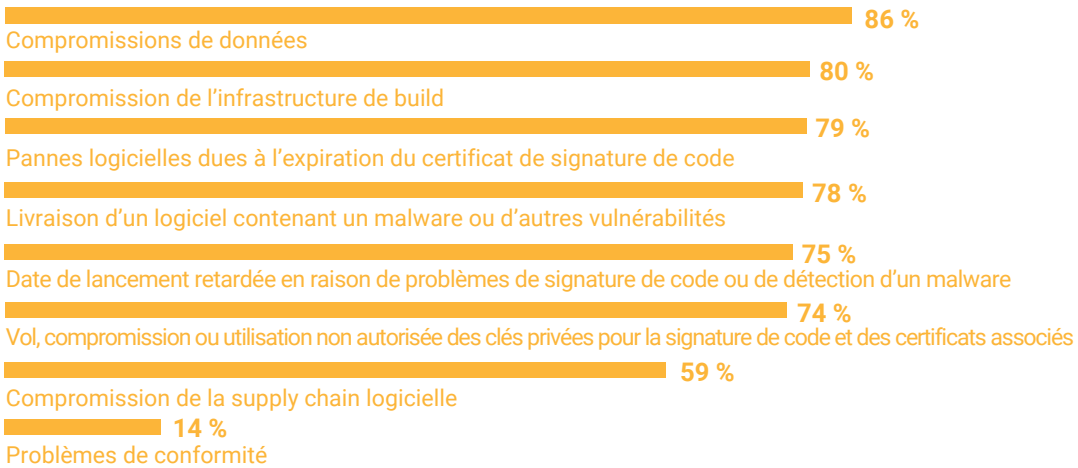
D'après notre étude, ils sont peu nombreux à pouvoir facilement produire une nomenclature complète des composants entrant dans les logiciels qu'ils produisent.

Cela dit, les responsables de la confiance pour les logiciels notent deux effets bénéfiques de leurs initiatives sur l'entreprise en général : 1) l'innovation numérique et 2) la productivité des collaborateurs.

Excellent au niveau de la conformité réglementaire de leurs logiciels

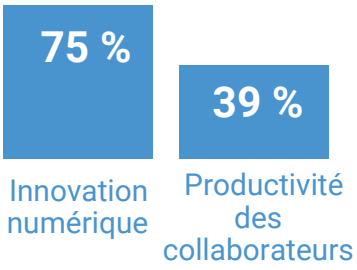
S'en sortent assez bien

Problèmes liés à la confiance numérique



des répondants trouvent très facile de créer une nomenclature des composants (et de leurs configurations) entrant dans les logiciels qu'ils développent

Malgré ces difficultés, la confiance pour les logiciels aide les organisations à plus d'un titre :



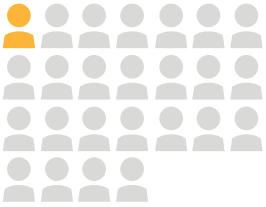
Signatures électroniques : les pratiques de confiance

Un certificat de signature de document permet à des personnes physiques, des équipes et des organisations d'apposer une signature numérique électronique à une grande variété de formats de fichiers. L'objectif est triple : 1) prouver leur droit de propriété sur le document concerné ; 2) garantir l'intégrité du document ; et 3) protéger les informations sensibles qu'il contient.

Nous avons demandé aux répondants d'évaluer le degré de maturité de leur confiance pour les signatures électroniques. Ils ne sont que 1 sur 25 (4 %) à qualifier leurs pratiques de très matures, soit le taux le plus bas des quatre catégories de confiance numérique étudiées. Cela s'explique en partie par une des spécificités des signatures électroniques, à savoir qu'elles ne sont pas gérées par l'IT, mais par d'autres départements (juridique, RH, achats, etc.). Or, dans ces équipes, seulement une personne sur 8 a une bonne compréhension des différences entre des signatures électroniques de base et des signatures numériques basées sur des certificats.

- **Près de la moitié des répondants (48 %)** apposent des cachets électroniques (eSeal) sur des documents (juridiques, contrats de vente ou d'achat, etc.)
- **La plupart d'entre eux (86 %)** vérifient l'authenticité des signataires grâce à des signatures numériques basées sur des certificats émis par un tiers de confiance

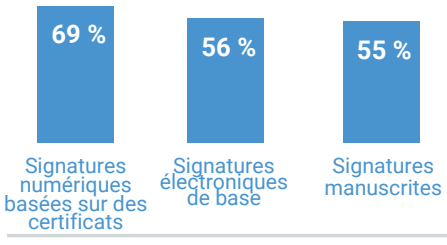
Seulement **1 répondant sur 25** estime ses pratiques de confiance numérique très matures



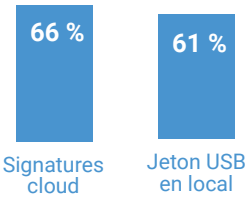
La plupart les considèrent comme « assez » matures

des répondants maîtrisent les différences entre les signatures électroniques de base et les signatures numériques basées sur des certificats

Types de signatures utilisées :



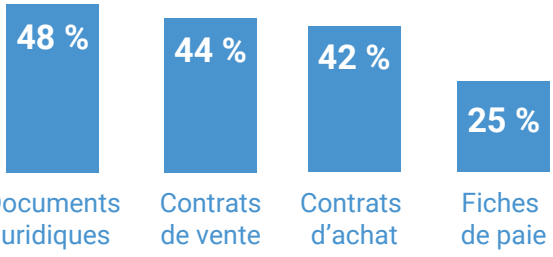
Types de signatures électroniques :



des répondants vérifient l'authenticité des signataires grâce à des signatures numériques basées sur des certificats émis par un tiers de confiance

La moitié des participants apposent des cachets électroniques (eSeal) sur des documents

Cas d'usage les plus fréquents :



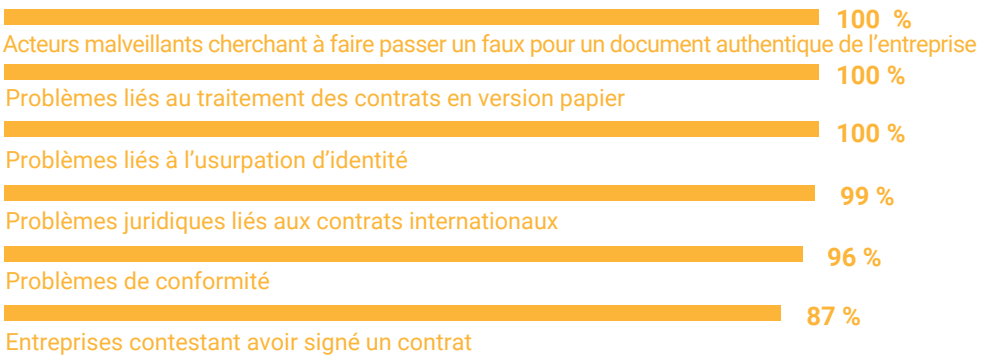
Signatures électroniques : les résultats des initiatives de confiance

Cette catégorie est la plus touchée par des problèmes en lien avec la confiance numérique :

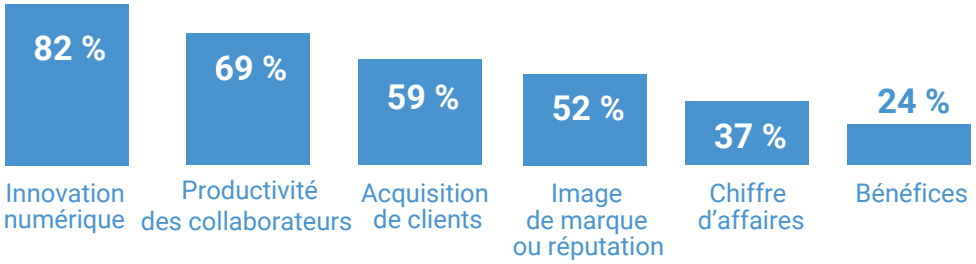
- **100 % des répondants** ont eu affaire à des acteurs malveillants cherchant à faire passer un faux pour un document authentique de leur entreprise
- **100 % d'entre eux** signalent des problèmes liés au traitement des contrats en version papier
- **100 % d'entre eux** font état de problèmes liés à l'usurpation d'identité
- Presque tous **(99 %)** ont rencontré des problèmes juridiques en lien avec des contrats internationaux
- **96 % d'entre eux** ont connu des problèmes de conformité
- **87 % d'entre eux** ont vu des entreprises contester avoir signé un contrat

Malgré ces nombreuses difficultés, leurs initiatives ont eu des effets positifs pour l'entreprise, et ce à plusieurs niveaux : innovation numérique, productivité des collaborateurs, acquisition de clients, et bien plus encore.

Problèmes liés à la confiance numérique



Malgré ces difficultés, la confiance en entreprise aide les organisations à plus d'un titre



LEÇONS DU « DIGITAL TRUST COGNOSCENTI »

Jusqu'à présent, notre analyse s'est concentrée sur les résultats globaux des entreprises combinées. Toutefois, à y regarder de plus près au sein d'un même groupe, certaines structures s'en sortent mieux, voire beaucoup mieux que la moyenne.

Intrigués par ces disparités, nous avons classé et comparé nos données. Pour ce faire, nous avons noté chaque question sur des métriques du type : « Avez-vous constaté des compromissions », et « Quel est le temps nécessaire à votre entreprise pour réagir en cas d'incident ? ». Nous avons attribué une note positive pour les bons résultats, et une note négative pour les mauvais, puis additionné le tout pour obtenir un score final pour chaque répondant.

Les entreprises arrivant dans le premier tiers du tableau, toutes catégories confondues, ont été classées au rang des « leaders de la confiance numérique ». Quant à celles du dernier tiers, nous les avons qualifiées de « retardataires de la confiance numérique ».

L'objectif était de comprendre les différences de pratiques et de résultats entre ces deux groupes, et ce dans chacun des quatre grands domaines de confiance numérique étudiés.

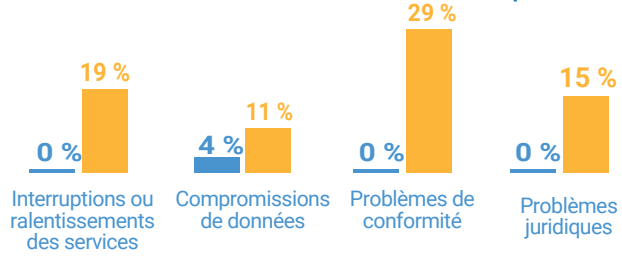
Confiance en entreprise

Dans la catégorie « Confiance en entreprise », les leaders s'en sortent nettement mieux que les autres. Ils rencontrent beaucoup moins de problèmes en la matière (presque pas d'interruptions, peu de compromissions de données et aucun problème de conformité légale ou réglementaire).

Près des trois-quarts des leaders (74 %) déclarent pouvoir réagir très rapidement en cas d'interruption de service, contre 59 % des retardataires.

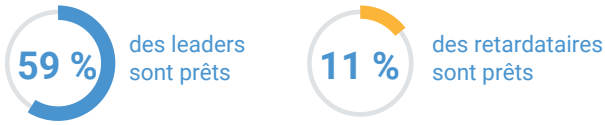
Les leaders sont presque six fois plus nombreux à se déclarer prêts pour l'ère post-quantique **(59 % contre 11 % des retardataires)**.

Diminution des problèmes liés aux initiatives de confiance en entreprise



Accélération de la réponse en cas de pannes

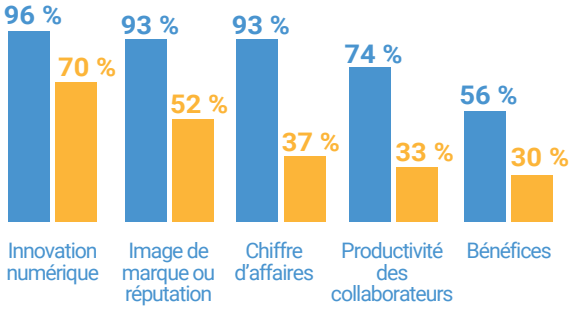
Meilleure préparation à la PQC



Accélération de la préparation à la PQC

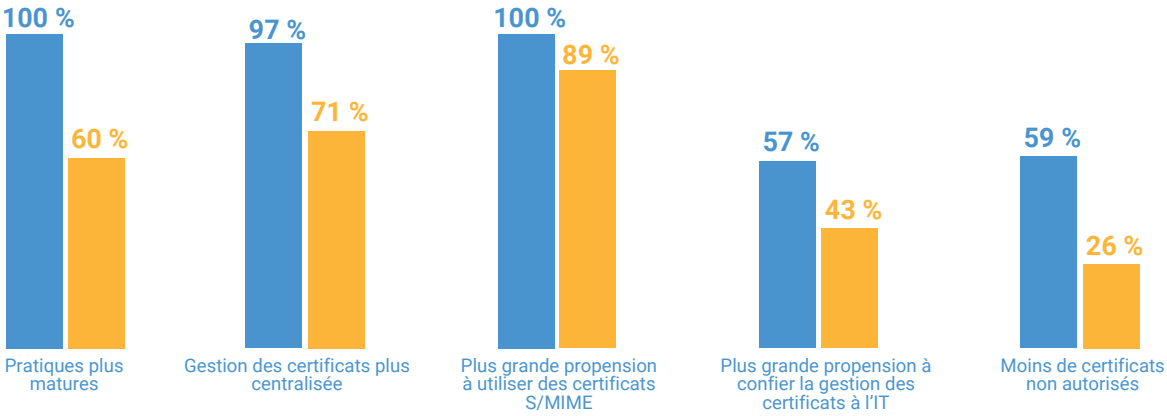
Les leaders estiment qu'il leur faudra 2 ans pour être prêts, contre 3 ans pour les retardataires

La confiance en entreprise a eu des effets très positifs dans ces domaines :



Comment les leaders tirent-ils leur épingle du jeu ?

Tout d'abord, 100 % des leaders de la confiance en entreprise estiment avoir des pratiques très matures en la matière. Ils tendent davantage à gérer leurs certificats de façon centralisée au sein de l'IT et à utiliser des certificats S/MIME pour sécuriser les e-mails. En outre, ils recensent moins de certificats non autorisés.

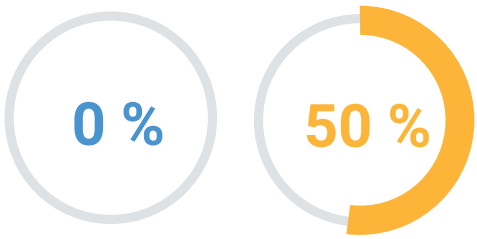


Confiance pour les appareils IoT et objets connectés

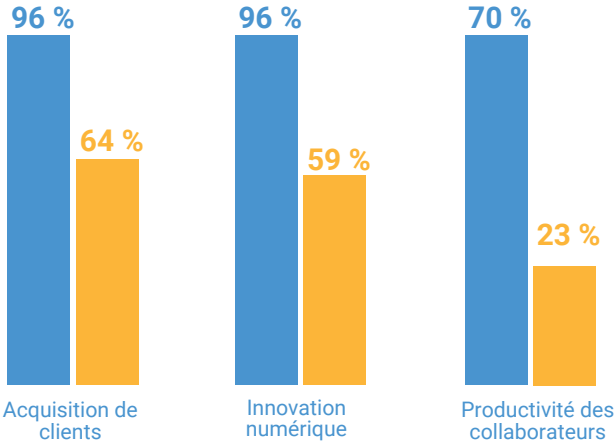
Nous nous sommes ensuite intéressés aux professionnels de la confiance pour les appareils IoT et objets connectés. Là encore, les leaders surclassent nettement les retardataires. Ils n'ont rencontré aucun problème de conformité réglementaire, contrairement à **50 %** des retardataires.

Par ailleurs, selon les leaders, leurs initiatives de confiance pour les appareils IoT et objets connectés ont davantage de retombées positives sur leur entreprise. Presque tous (96 %) constatent ainsi un effet de levier sur l'acquisition de clients et l'innovation numérique. La productivité des collaborateurs y gagne aussi pour la plupart (70 %) d'entre eux. Par comparaison, les retardataires notent des avantages bien moindres, avec respectivement 64 %, 59 % et 23 %.

Baisse des problèmes de conformité



La confiance pour l'IoT a eu des effets très positifs pour l'entreprise dans différents domaines :

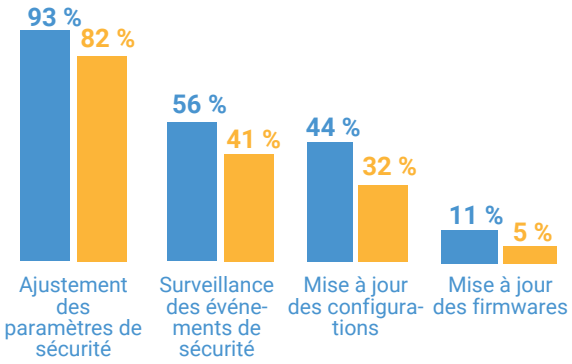


En quoi leurs pratiques diffèrent-elles ?

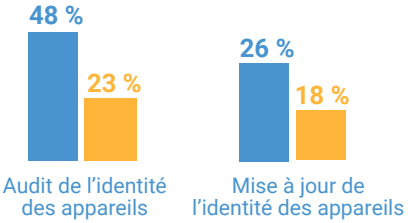
D'abord, les leaders ont une meilleure capacité à modifier et à surveiller les appareils déployés sur le terrain, mais aussi à auditer et à mettre à jour les identités de ces appareils.

Enfin, ils sont 19 % à se dire totalement prêts à faire face à des problèmes de confiance numérique pour l'IoT, contre 0 % chez les retardataires.

Plus grande capacité à modifier les appareils déployés sur le terrain :



Capacité améliorée dans ces domaines :



Meilleure préparation aux problèmes de confiance pour l'IoT

Confiance pour les logiciels

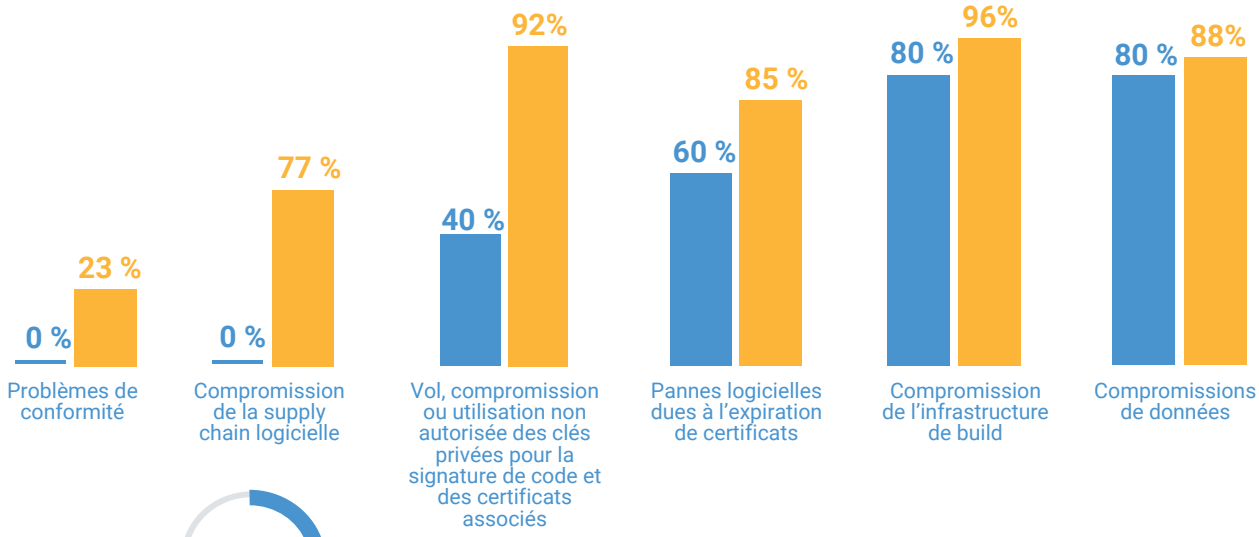
Nous nous sommes ensuite penchés sur le cas des professionnels de la confiance pour les logiciels. L'avance des leaders sur les retardataires est une fois de plus notable : ils connaissent moins de problèmes de confiance au niveau de leurs logiciels. Par exemple, ils n'ont eu à gérer aucun problème de conformité ni aucune compromission de leur supply chain logicielle, contre respectivement 23 % et 77 % chez les retardataires.

En outre, un leader sur cinq **(20 %)** dans cette catégorie affiche des pratiques très matures, contre 0 % chez les retardataires

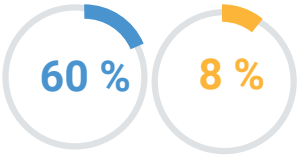
Côté conformité réglementaire, les leaders creusent aussi l'écart : 60 % obtiennent d'excellents résultats contre 8 % des retardataires.

Par ailleurs, les initiatives de confiance pour les logiciels s'avèrent bien plus payantes globalement dans les entreprises des leaders que celles de retardataires, notamment sur le plan de l'innovation numérique, de l'acquisition de clients et de la productivité des collaborateurs.

Les leaders rencontrent moins de problèmes liés à des accidents de confiance pour les logiciels :

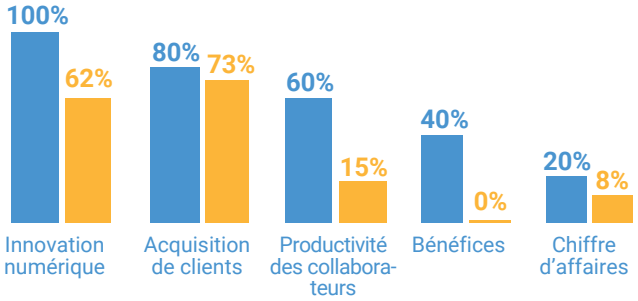


des leaders affichent des pratiques très matures en matière de confiance logicielle, contre 0 % chez les retardataires



des leaders obtiennent de très bons résultats sur la conformité réglementaire

La confiance pour les logiciels a eu des effets très positifs pour l'entreprise dans différents domaines :



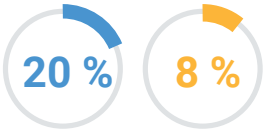
Comment les leaders font-ils la différence ?

Les leaders sont deux fois plus nombreux que les retardataires à recourir à un processus d'approbation formel pour accéder aux clés cryptographiques (80 % contre 38 %).

De même, ils tendent plus à trouver très facile de créer une nomenclature des composants (et de leur configuration) entrant dans les logiciels qu'ils développent (20 % des leaders contre seulement 8 % des retardataires).

Plus grande propension à appliquer un processus d'approbation pour accéder à tout type de clé

Les leaders trouvent très facile de créer une nomenclature des composants (et de leurs configurations) entrant dans les logiciels qu'ils développent



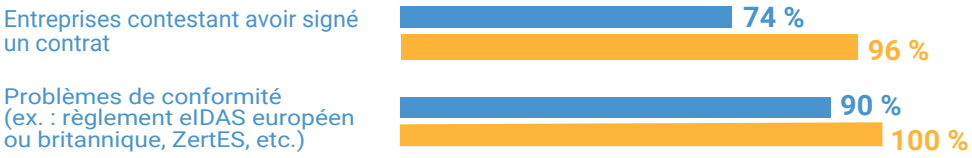
Confiance pour les signatures électroniques

Le dernier groupe de cette comparaison détaillée rassemble les professionnels de la confiance pour les signatures électroniques. Fait notoire, cette catégorie est souvent composée d'équipes non techniques (comme des responsables RH, juridiques ou commerciaux). Or, faute d'implication de la fonction IT, certaines spécificités techniques des initiatives de confiance numérique échappent à ces responsables métiers. Et cela se voit dans les résultats.

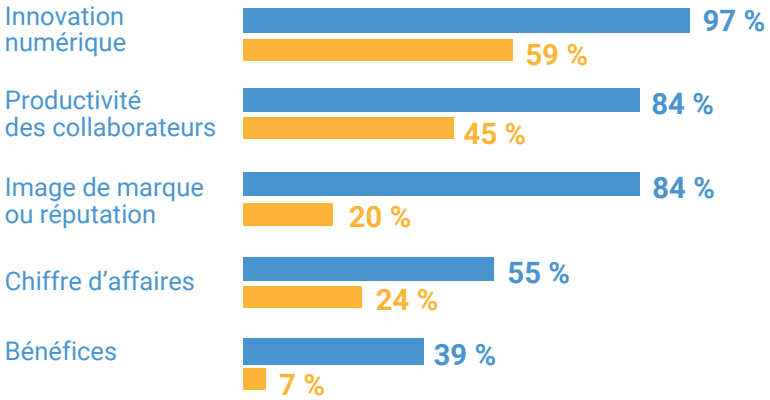
Ainsi, même si les leaders sont plus nombreux que les retardataires à recourir à des pratiques très matures au niveau des signatures électroniques, leur proportion (10 %) reste faible en valeur absolue. Par ailleurs, les leaders sont moins confrontés que les retardataires aux problèmes de confiance pour les signatures électroniques et constatent davantage les effets positifs de leurs pratiques sur l'entreprise.

des leaders affichent des pratiques très matures en matière de confiance pour les signatures électroniques, contre 0 % chez les retardataires

Les leaders rencontrent moins de problèmes de confiance pour les signatures électroniques :

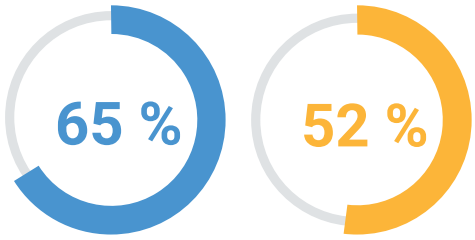


La confiance pour les signatures électroniques a eu des effets très positifs pour l'entreprise dans différents domaines :



En quoi les leaders sortent-ils du lot ?

La différence entre le premier et le dernier tiers tient à une qualité fondamentale : la maturité des leaders en matière de compréhension, de mise en place et de gestion des politiques et des pratiques de gouvernance des signatures et cachets électroniques.



Les leaders font preuve d'une plus grande maturité en matière de compréhension, de mise en place et de gestion des politiques et des pratiques de gouvernance des signatures et cachets électroniques

LE POINT DE VUE DE DIGICERT

À mesure que le champ des menaces s'étend, l'écart se creuse entre les entreprises à la pointe de la confiance numérique et les organisations à la traîne. Si les leaders et les retardataires savent pertinemment où ils se situent, le danger vient plutôt du faux sentiment de sécurité qu'entretiennent parfois les entreprises du tiers intermédiaire. Le relatif manque de vigilance qui en résulte parfois pourrait ainsi avoir des conséquences très sévères.

Dès lors, que doivent faire les entreprises pour optimiser leurs initiatives de confiance numérique, globalement et dans les domaines spécifiques étudiés (IT d'entreprise, logiciels, appareils connectés et documents) ?

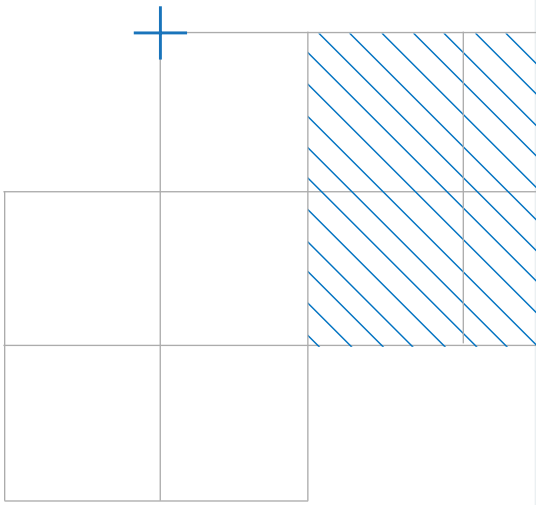
Leader de la confiance numérique, DigiCert apporte aux entreprises et aux particuliers les outils qui leur permettront d'échanger et de communiquer de façon sereine et sécurisée dans l'univers du digital. À la lumière de notre expérience forgée au cours des deux dernières décennies, nous conseillons aux entreprises souhaitant emboîter le pas des leaders d'envisager les mesures suivantes :

Dresser un inventaire

L'adage selon lequel on ne peut gérer que ce l'ont voit vaut aussi pour la confiance numérique. D'où l'importance d'établir un état des lieux complet de la manière dont vos identités numériques et vos clés cryptographiques sont créées, protégées et utilisées dans votre entreprise. Vous avez le choix entre deux méthodes : le recensement manuel de tous les processus métiers ou le recours à des outils pour analyser votre environnement en continu et ingérer des données provenant d'autres sources, comme les systèmes de gestion des ressources IT.

Définir des politiques

Il existe toutes sortes de politiques pour vous guider sur la voie de la confiance numérique. Pour protéger vos équipes en présentiel et en distanciel, instaurez des politiques de sécurisation des appareils et d'authentification des utilisateurs. Identifiez celles indispensables à votre conformité réglementaire, surtout si votre entreprise fabrique des dispositifs médicaux ou appartient à un secteur ultra-réglementé. Votre organisation édite des logiciels stratégiques ? Mettez en place des politiques garantes de la sécurité de la supply chain logicielle. Par ailleurs, misez sur le Zero Trust, en particulier pour vos workloads cloud-native qui traitent des données sensibles et réglementées. Évidemment, tous ces exemples s'inscrivent en complément des politiques essentielles qui régissent l'usage de la cryptographie et de l'infrastructure à clés publiques (PKI) au sein de votre entreprise.



Centraliser la gestion PKI

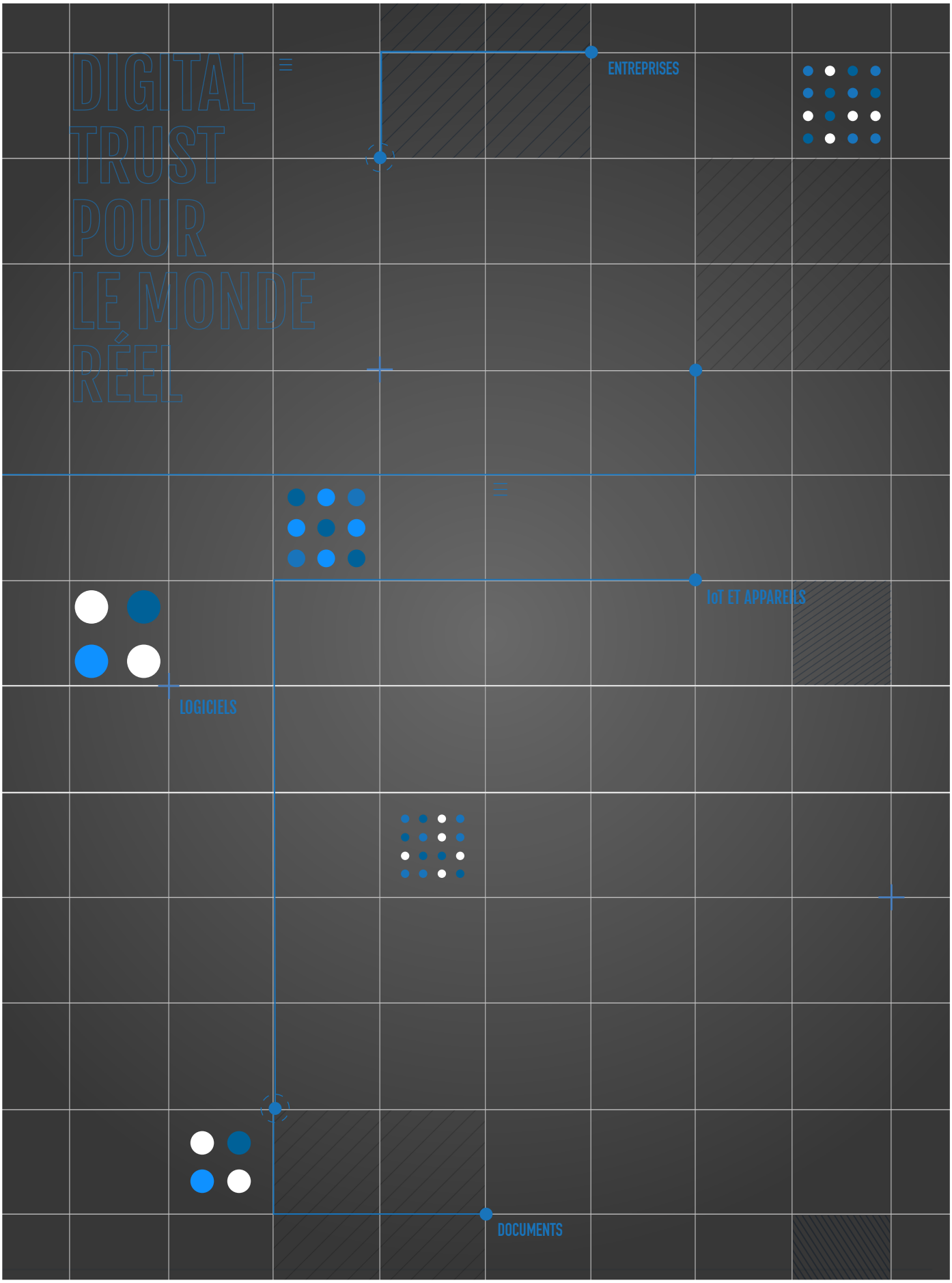
Les organisations doivent désormais faire preuve de crypto-agilité, c'est-à-dire la capacité de mettre à jour et de corriger rapidement leurs ressources cryptographiques. Pour limiter les risques et les perturbations, déployez des outils de gestion centralisée et d'automatisation de la PKI et des certificats numériques. Sécurité renforcée, gain d'efficacité, administration simplifiée… cette approche a beaucoup à offrir.

Prioriser en fonction de l'impact sur vos activités

Le but de l'inventaire est d'identifier les ressources entrant directement dans des processus et applications critiques. C'est là que vous devrez agir en priorité. Commencez par corriger toutes les failles de sécurité avant d'implémenter des solutions de simplification des tâches relevant de la confiance numérique. Il s'agira par exemple de permettre aux utilisateurs d'enregistrer automatiquement et facilement leurs appareils pour sécuriser les accès distants, et ce, sans faire appel à l'IT. Ou encore de renforcer la sécurité du cloud grâce à l'émission et à l'installation rapides de certificats de serveurs pour protéger les données et les communications.

Conclusion

Consolidation de leur image de marque, réduction des cyber-risques, amélioration de l'efficacité opérationnelle… les entreprises en pointe sur la confiance numérique n'y voient que des avantages. Leurs clients, partenaires et parties prenantes aussi, car la sécurité robuste et la gouvernance transparente les rassurent. Une confiance numérique forte, c'est une meilleure capacité à braver la complexité des réglementations, à s'y conformer et à ainsi réduire les risques juridiques et financiers. Et c'est aussi une protection des données et une résilience renforcées pour mieux faire face aux nouvelles menaces à l'ère du digital.


DIGITAL TRUST POUR LE MONDE RÉEL
ENTREPRISES
IoT ET APPAREILS
LOGICIELS
DOCUMENTS