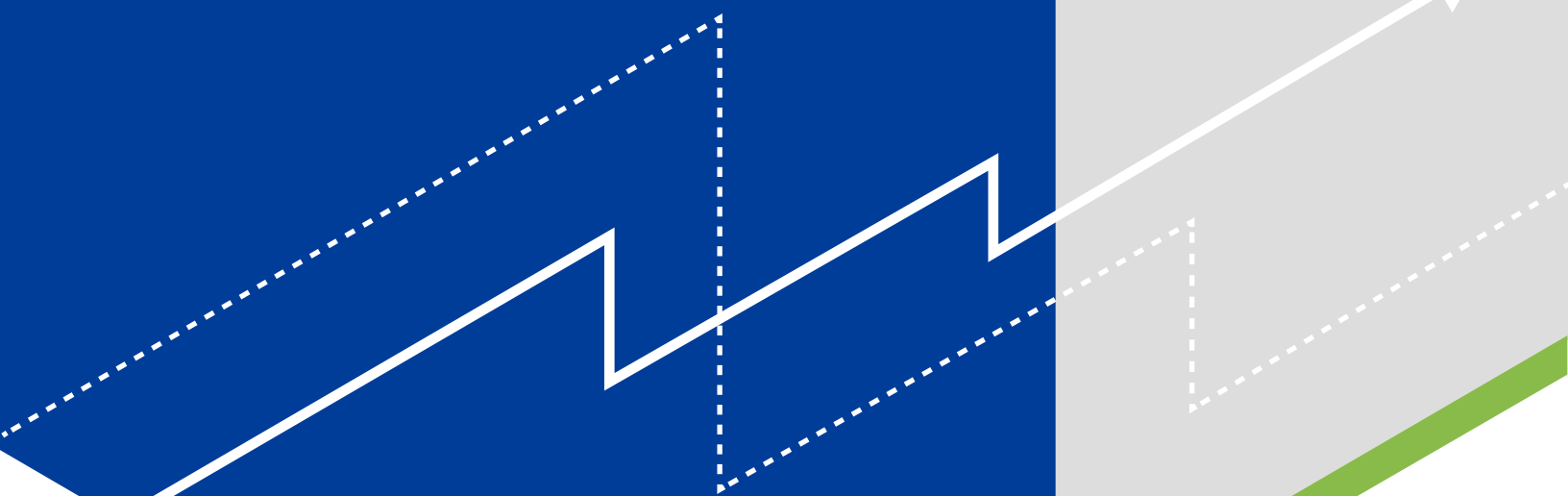
Un document de réflexion élaboré par
Forrester Consulting pour Venafi

Juin 2018

Sécuriser l'entreprise à l'aide de la protection de l'identité des machines



FORRESTER®

Table des matières

Directeur du projet :
Chris Taylor,
Consultant senior sur l'impact marché

Étude associée :
groupe d'étude Forrester sur la sécurité et les risques

FORRESTER®

Les entreprises actuelles ne parviennent pas à suivre et à protéger de manière appropriée toutes les identités existantes des machines. Afin de parvenir à optimiser la protection mise en œuvre, elles ont besoin de capacités d'automatisation.

Résumé

La protection de l'identité des machines est un composant essentiel des programmes de sécurité relatifs à la gestion des identités et des accès (Identity Access Management IAM). La gestion des identités des utilisateurs et des machines, ainsi que celle des accès privilégiés aux données et aux applications de l'entreprise constituent une tâche colossale, laquelle, si elle n'est pas exécutée correctement, a de lourdes conséquences sur la sécurité. L'IAM a toujours été axé sur les personnes. Cependant, les derniers progrès technologiques et les nouvelles capacités informatiques posent de nouveaux défis liés à l'IAM, lesquels exigent une attention accrue sur la protection des identités des machines.

Par exemple, les nouvelles technologies, telles que le Cloud et la conteneurisation, ont élargi la définition de machine pour inclure un large éventail de logiciels qui émulent les machines physiques. De plus, ces technologies génèrent d'innombrables nouvelles machines très évolutives sur les réseaux d'entreprise. Pour gérer et protéger efficacement les identités des machines, les entreprises ont besoin des éléments suivants : une visibilité complète sur toutes les identités de machine sur leurs réseaux ; des renseignements exploitables sur l'identité de chaque machine ; et la capacité d'exploiter efficacement ces renseignements afin de prendre des mesures adaptées au rythme des machines et à grande échelle.

En mars 2018, Venafi a chargé Forrester Consulting d'examiner l'importance de protéger les identités des machines dans les entreprises actuelles et de déterminer l'aptitude des entreprises à mettre en œuvre ces protections. Pour y parvenir, Forrester a mené une étude auprès de 350 décideurs informatiques et de sécurité à travers les États-Unis, le Royaume-Uni, la France, l'Allemagne et l'Australie, dont le rôle consiste à gérer l'infrastructure commerciale, ainsi que la sécurité des programmes de gestion des identités et des accès. Les résultats de l'étude ont révélé que la protection des identités de machines constitue déjà un élément central des efforts IAM. Cependant, les entreprises ne parviennent pas à suivre et à protéger toutes les identités des machines de manière efficace. Afin de parvenir à optimiser la protection mise en œuvre, elles ont besoin de meilleures capacités d'automatisation.

PRINCIPALES CONCLUSIONS

- Quatre-vingt-seize pour cent des entreprises reconnaissent qu'une protection efficace de l'identité des machines et des personnes est essentielle à la sécurité et à la viabilité à long terme de leurs activités. Toutefois, 80 % d'entre elles ne parviennent pas à assurer une protection efficace de l'identité des machines.
- Soixante-dix pour cent des entreprises gèrent moins de la moitié des identités potentielles des machines, en les exposant ainsi à un large éventail de risques de sécurité.
- L'automatisation est essentielle pour relever les défis les plus urgents auxquels les entreprises sont confrontées aujourd'hui liés à la protection des identités des machines (par exemple, la découverte complète des identités des machines, la réponse rapide aux événements de sécurité cryptographiques et le remplacement rapide des certificats et identités vulnérables ou compromis).
- Les améliorations apportées aux programmes de protection des identités de machines généreront des avantages immédiats et à long terme en matière de sécurité, en accélérant la détection et la correction des violations et en réduisant le nombre total de celles-ci.

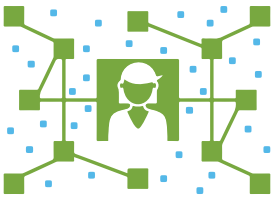
FORRESTER®

Une protection automatisée et efficace des identités de machines est essentielle à la pérennité de l'entreprise

La technologie numérique a permis aux entreprises de transformer leur mode de fonctionnement, tout en améliorant leur relation avec leurs clients. Bien que ces nouvelles fonctionnalités soient bénéfiques pour la rentabilité, il est primordial que l'accès aux machines et l'utilisation de celles-ci, lesquels alimentent cette transformation, soient soigneusement gérés et protégés. Cela peut être un défi de taille pour les entreprises qui ont déjà des milliers, voire des dizaines de milliers d'identités humaines (par exemple, employés, sous-traitants, partenaires et clients) à surveiller et qui doivent également protéger un nombre croissant d'identités de machines, suite à l'adoption du Cloud et de la conteneurisation.

Une protection et une gestion fiables et rentables des identités de machines nécessitent que les entreprises identifient les programmes et les appareils qui se connectent les uns aux autres pour accéder aux informations critiques et sensibles. Ces identités de machines comprennent des clés cryptographiques et des certificats numériques qui régissent l'authentification et la communication chiffrée. Aujourd'hui, près des trois quarts des entreprises admettent la nécessité de gérer et de protéger les identités des personnes et des machines, tout en reconnaissant qu'elles sont tout aussi importantes pour la pérennité de leurs activités.

La nécessité de protéger les identités des machines et des personnes est universellement reconnue comme étant essentielle aujourd'hui et demain. 96 % des entreprises reconnaissent qu'une protection efficace des identités et des accès à la fois pour les machines et les personnes est indispensable à la sécurité et la viabilité à long terme de leurs activités. La mise en place de la technologie appropriée pour assurer la protection automatisée des identités de machines constitue également une priorité absolue. 70 % des entreprises accordent une grande importance à la mise en œuvre de plates-formes dédiées à la protection des identités des machines.



96 % des entreprises reconnaissent qu'une protection efficace des identités et des accès aux identités des machines et des personnes est essentielle pour garantir une sécurité et une pérennité à long terme de leurs activités.

PROTÉGER LES IDENTITÉS DES MACHINES EST AUSSI IMPORTANT QUE DE PROTÉGER LES IDENTITÉS HUMAINES

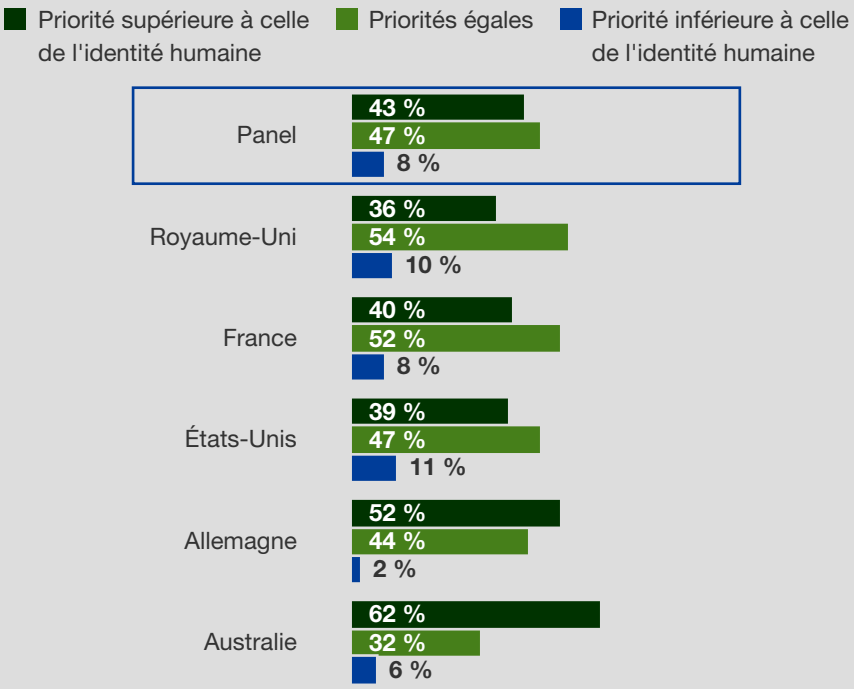
La nécessité de protéger les identités des machines ne fait pas partie d'un cycle technologique qui disparaîtra dans quelques mois : les entreprises d'aujourd'hui sont confrontées à une vague croissante d'identités de machines, suite à l'adoption de nouvelles technologies, notamment l'IoT, le Cloud, la mobilité, ainsi que les nouveaux processus métier automatisés. Outre ces changements, les entreprises font face à un afflux d'initiatives d'automatisation de la sécurité, de DevOps et de conteneurisation, qui complexifient davantage la protection des identités de machines.

Afin de sécuriser les actifs de l'entreprise dans un monde déparamétrisé, les programmes IAM ne peuvent plus se concentrer uniquement sur les identités humaines. Notre étude a révélé que 47 % des entreprises prévoient que les identités des machines et des personnes présenteront une importance similaire au cours des 12 à 24 prochains mois, et 43 % estiment que les identités des machines seront plus prioritaires que les identités humaines. Dans deux des pays interrogés, l'Allemagne et l'Australie, un pourcentage plus élevé d'entreprises estime que la priorité accordée aux identités des machines sera plus élevée à l'avenir (voir la Figure 1).

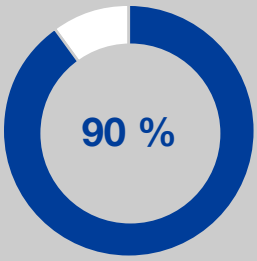
FORRESTER®

Figure 1

« La priorité accordée à la protection de l'identité des machines sera-t-elle supérieure, égale ou inférieure à celle de l'identité humaine au cours des deux prochaines années ? »



mondial : 350 décisionnaires informatiques américains, australiens et de l'EMEA responsables de l'infrastructure commerciale de leur entreprise
Source : étude réalisée par Forrester Consulting pour Venafi, mars 2018
Note : la somme des pourcentages peut ne pas être égale à 100 du fait de l'arrondissement des valeurs.



des entreprises estiment que la protection de l'identité des machines présentera une priorité similaire ou supérieure à celle d'une protection des identités humaines.

La protection de l'identité des machines est une tâche délicate

Les entreprises ont pris conscience aujourd'hui que leurs efforts en matière de sécurité sont axés sur la protection de l'identité des machines. Elles évaluent le succès de leurs efforts en matière de protection de l'identité des personnes et des machines en fonction de trois mesures clés :

- Accélération de la détection des violations.
- Amélioration de la conformité automatisée envers les règles et les réglementations de sécurité.
- Réduction du nombre total de violations.

Même si les entreprises ont conscience que leur pérennité à long terme repose essentiellement sur une protection efficace des identités des machines, c'est malgré tout plus facile à dire qu'à faire. L'ampleur et la complexité du problème ont considérablement augmenté en raison des éléments suivants : augmentation du nombre de machines sur les réseaux ; adoption élargie des workflows basés dans le Cloud ; et nouvelles initiatives DevOps. En ce qui concerne le Cloud et le DevOps en particulier, ces nouvelles initiatives et workflows créent des identités machines très évolutives, dont la gestion doit être efficace. Sans les solutions technologiques adéquates, telles que l'application des règles, la gestion routinière du cycle de vie des identités de machines, ainsi que celle des incidents de sécurité liés à l'identité des machines à l'échelle de l'entreprise, cet environnement à variation rapide peut être dangereux. L'automatisation garantit l'évolutivité des processus

FORRESTER®

de protection des identités machines. L'orchestration manuelle de la création, du provisionnement, de la rotation, du renouvellement et du remplacement des tâches liées aux identités de machines est pratiquement impossible, compte tenu de l'augmentation rapide du volume des identités machines et de la rapidité à laquelle elles évoluent.

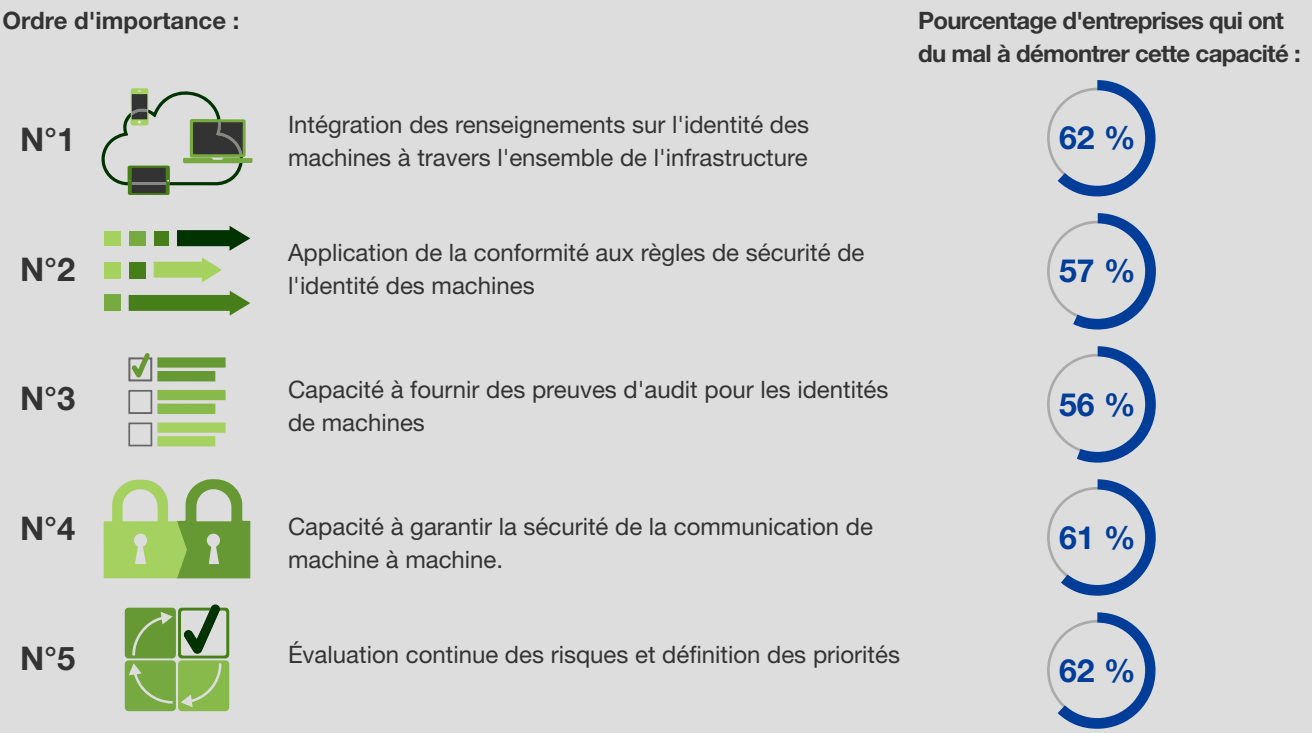
Pour mieux comprendre l'attitude des entreprises interrogées face aux initiatives de protection des identités machines, nous leur avons posé deux questions : 1) quelle est l'importance des capacités dédiées à la gestion de la protection des identités machines et 2) dans quelle mesure leur entreprise parvient-elle à mettre en œuvre ces capacités ? En comparant les résultats de ces deux questions côte à côte, nous avons constaté que les entreprises considèrent que les capacités de protection de l'identité des machines sont importantes, et que la majorité d'entre elles ne parvient pas à les mettre en œuvre efficacement (voir la figure 2). Les trois capacités les plus difficiles à mettre en œuvre étaient :

- Intégration des renseignements sur l'identité des machines à travers l'écosystème.
- Évaluation continue des risques.
- Renseignements exhaustifs sur toutes les identités de machine.

L'intégration, l'application des règles et l'audit des règles relatives à l'identité des machines sont difficiles, car ces capacités ne sont pas souvent intégrées à la plupart des outils. Étant donné que ces capacités clés ne sont pas mises en œuvre, plus de 50 % des entreprises ne parviennent pas à protéger efficacement les identités des machines. Il s'agissait d'une tendance constante à travers toutes les zones géographiques de l'étude.

Figure 2

Les fonctionnalités de protection de l'identité des machines les plus importantes sont difficiles à mettre en œuvre.



Panel : 350 décisionnaires informatiques américains, australiens et de l'EMEA responsables de l'infrastructure commerciale de leur entreprise
Source : étude réalisée par Forrester Consulting pour Venafi, mars 2018

FORRESTER®

Étant donné que les entreprises reconnaissent que leurs systèmes actuels ne parviennent pas à tenir compte des priorités en matière d'identité machines, elles craignent à juste titre les conséquences de leur incapacité à protéger les identités. Soixante et un pour cent des entreprises déclarent que le vol ou la perte de données internes, suivi de près par le vol ou la perte des données clients, constitue leur principale préoccupation en cas d'échec de la gestion des identités et des accès aux machines. À l'heure où la protection des données contribue à générer et à protéger les avantages concurrentiels, il est impératif que les entreprises investissent dans des outils qui assurent la protection complète de l'identité des machines.

LES ENTREPRISES LAISSENT DE NOMBREUSES CLASSES D'IDENTITÉS MACHINES SANS PROTECTION, EN S'EXPOSANT À DES RISQUES ET DES DIFFICULTÉS DE PLUS EN PLUS IMPORTANTS

Les entreprises estiment que la protection de l'identité des machines est une tâche ardue pour deux raisons principales :

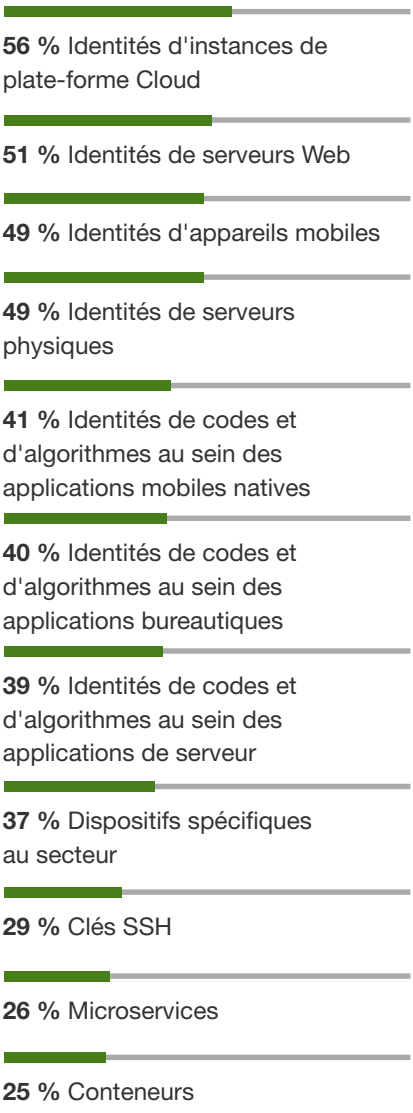
- **De nombreuses formes d'identités machine ne sont ni suivies ni protégées.** Notre enquête a évalué 11 types d'identités de machine communément rencontrées sur les réseaux d'entreprise et, en moyenne, nous avons constaté que les entreprises effectuent un suivi pour moins de la moitié d'entre eux. Les types d'identité incluent les identités de serveur Web, les codes/algorithmes dans les applications, les conteneurs et autres (voir la figure 3). Étant donné que les entreprises n'effectuent pas le suivi de tous les types d'identité de machine possibles, elles risquent de ne pas pouvoir détecter les vulnérabilités existantes, les menaces en constante évolution et les modèles d'attaque. Par conséquent, les machines constituent une cible vulnérable pour les attaques malveillantes. Par exemple, la mobilité existe depuis plus de dix ans, mais l'expansion des initiatives BYOD (Bring-Your-Own-Device) a créé de nouvelles identités de code et d'algorithme machine au sein des applications mobiles natives qui se connectent automatiquement entre elles et aux réseaux de l'entreprise, lesquels doivent être protégés. En outre, l'adoption rapide de conteneurs et de plates-formes Cloud nécessite un ajustement minutieux des programmes de protection de l'identité des machines, car la configuration de ces plates-formes est presque toujours entièrement automatisée. Dans de nombreux cas, les machines créent ou arrêtent d'autres machines en quelques minutes ou secondes. Ces identités peuvent passer entre les mailles du filet si elles ne sont pas soigneusement suivies et protégées.
- **Les entreprises utilisent des outils disparates pour protéger les identités des machines.** Chaque type d'identité de machine présente ses propres défis et complexités. Les entreprises adoptent déjà de nouvelles technologies pour relever ces défis, notamment les modules de sécurité matérielle, les feuilles de calcul/bases de données développées et gérées en interne et les tableaux de bord des autorités de certification. Le problème est que beaucoup de ces outils ont une portée limitée et sont utilisés en silos. Ils sont par conséquent difficiles à maintenir et à faire évoluer. Pour pouvoir évoluer, les entreprises ont besoin de moins d'outils capables d'en faire plus : des outils qui améliorent la visibilité sur tous les types d'identités de machines (partout où elles sont utilisées) et des outils fournissant les informations exhaustives nécessaires à une protection et une réponse automatisées.

L'AUTOMATISATION EST NÉCESSAIRE À LA PROTECTION DE L'IDENTITÉ DES MACHINES

La création d'un inventaire des identités machines permettant d'améliorer la visibilité est un bon début qui peut immédiatement atténuer les risques posés à l'identité des machines. Cependant, ces informations ne suffisent pas si les personnes, les processus et la technologie appropriés ne sont pas en place pour assurer la protection des identités des machines. L'automatisation peut aider les entreprises à atténuer lles problèmes auxquels elles sont actuellement confrontées en protégeant les identités

Figure 3

« Quelles sont les identités de machines qui sont suivies par les entreprises ? »



Panel : 350 décisionnaires informatiques américains, australiens et de l'EMEA responsables de l'infrastructure commerciale de leur entreprise
Source : étude réalisée par Forrester Consulting pour Venafi, mars 2018

En moyenne, les entreprises suivent moins de 50 % de toutes les identités machine possibles.

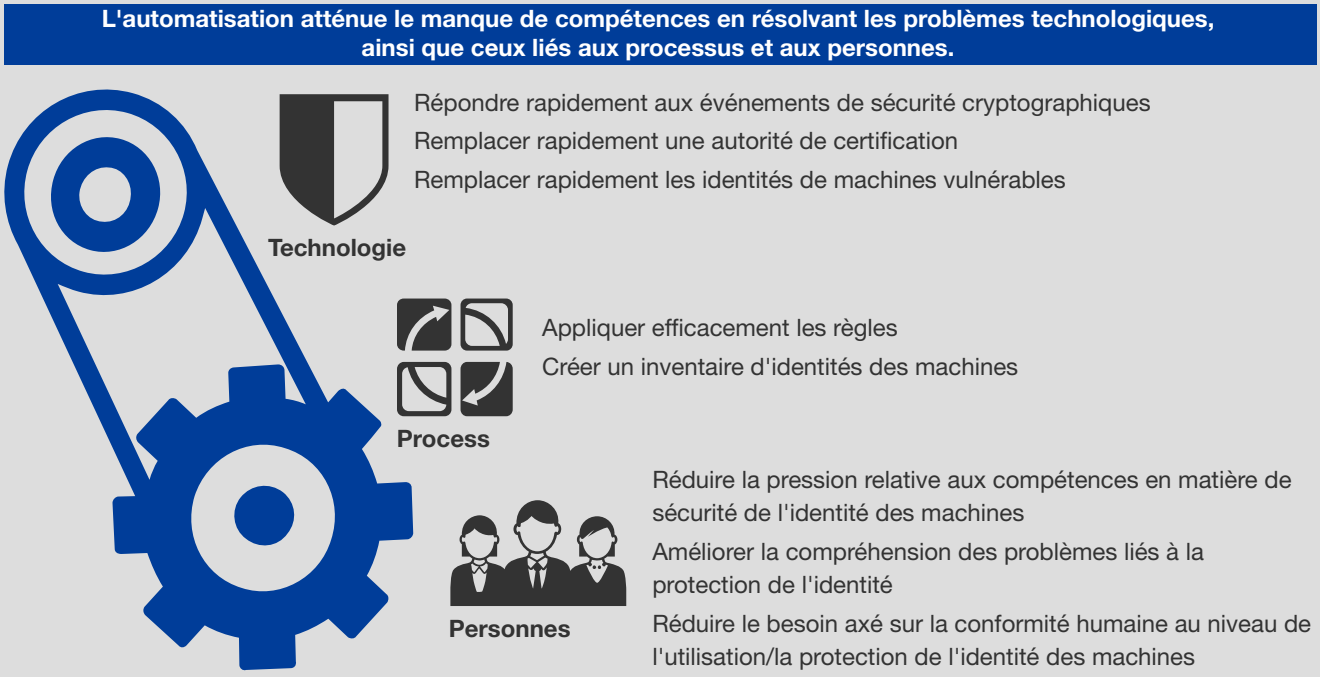
FORRESTER®

des machines et en permettant aux entreprises de :

- **Répondre plus rapidement aux menaces de sécurité.** Les incidents de sécurité sont inévitables, mais le principal défi signalé par les entreprises est leur incapacité à répondre rapidement aux événements de sécurité cryptographiques liés à l'identité des machines et à remplacer/corriger les vulnérabilités (voir la figure 4). Les entreprises souhaitent pouvoir atténuer les risques posés par ces menaces aussi rapidement que possible, et l'automatisation est essentielle pour identifier et répondre aux menaces, avec un temps machine.
- **Suivre les identités et appliquer les règles d'une manière plus efficace.** À la question « quels sont les principaux défis liés aux processus de protection de l'identité des machines ? », le manque d'automatisation pour appliquer les règles et la nécessité de répertorier les identités des machines ont été les réponses les plus fréquentes. De nombreuses entreprises profiteraient grandement de processus plus automatisés susceptibles d'améliorer la surveillance et la protection des identités des machines, d'autant plus que le volume des identités continue de croître rapidement.
- **Réduire le besoin de compétences spécialisées en matière de protection de l'identité des machines.** De nombreuses entreprises estiment ne pas avoir les compétences nécessaires pour mettre en œuvre la protection dont elles ont besoin. Un facteur aggravant est le fait que 37 % des entreprises déclarent ne pas comprendre entièrement les risques commerciaux résultant d'une mauvaise protection de l'identité des machines. L'automatisation peut réduire le nombre de points de contact humains nécessaires à la protection des identités des machines et peut aider les entreprises à axer leurs efforts sur leurs ressources et leurs compétences dans des domaines spécifiques, nécessitant des interactions humaines.

Figure 4

Supprimer les obstacles et renforcer la protection de l'identité des machines grâce à l'automatisation.



Panel : 350 décisionnaires informatiques américains, australiens et de l'EMEA responsables de l'infrastructure commerciale de leur entreprise
Source : étude réalisée par Forrester Consulting pour Venafi, mars 2018

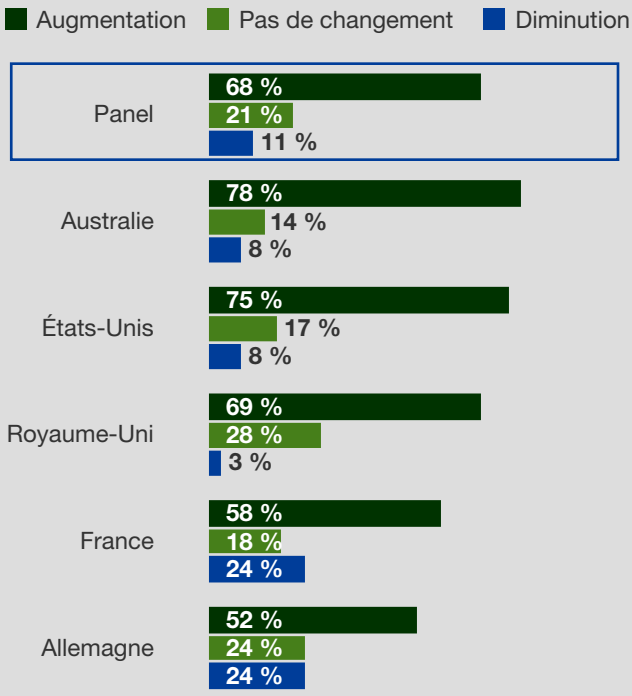
Le renforcement de la sécurité nécessite une attention accrue sur les identités machines

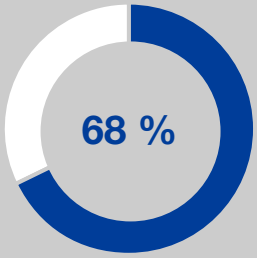
Conscientes de leurs défis actuels en matière d'identité machines, 68 % des entreprises déclarent que la priorité accordée à la protection de l'identité des machines s'accentuera au cours des deux prochaines années. Notre enquête a montré que les décisionnaires en Australie et aux États-Unis étaient beaucoup plus susceptibles de signaler une augmentation anticipée de cette priorité par rapport à d'autres pays (voir la figure 5). Les entreprises interrogées en France et en Allemagne étaient moins enclines à prédire une augmentation de la priorité accordée à la protection de l'identité des machines, étant donné qu'elles reconnaissaient déjà l'importance croissante de la protection des identités des machines, en revoyant leurs priorités en conséquence.

À mesure que la priorité accordée à la protection de l'identité des machines augmente, les entreprises devront se concentrer sur des capacités spécifiques, nécessaires pour relever les défis actuels, notamment :

Figure 5

« Selon vous, quelle sera l'évolution des priorités accordées à la protection de l'identité des machines au cours des deux prochaines années ? »





d'entreprises affirment que la priorité accordée à la protection de l'identité des machines augmentera au cours des deux prochaines années.

mondial : 350 décisionnaires informatiques américains, australiens et de l'EMEA responsables de l'infrastructure commerciale de leur entreprise
Source : étude réalisée par Forrester Consulting pour Venafi, mars 2018

FORRESTER®

› Visibilité continue et renseignements sur toutes les identités de machines à travers l'entreprise : 1) identifier rapidement les accès non autorisés et l'élévation de privilèges et 2) empêcher les attaques latérales à l'aide de clés cryptographiques.

› Des renseignements exhaustifs sur l'ensemble du cycle de vie de l'identité des machines, y compris la génération, l'installation, le déploiement, la rotation et la suppression des certificats pour protéger et sécuriser les communications chiffrées et autorisées entre les machines.

› Des fonctionnalités en libre-service permettant d'éliminer la complexité et de réduire le besoin d'un personnel hautement qualifié pour gérer les opérations de sécurité quotidiennes.

Les entreprises qui investissent plus de temps et d'efforts pour améliorer la protection des identités des machines espèrent en tirer des bénéfices immédiats et futurs (voir la Figure 6). Les principaux résultats sont les suivants :

› **Accélération de la détection des violations.** Il s'agit du résultat à court terme le plus immédiat, que 42 % des entreprises déclarent espérer obtenir. La visibilité et les informations supplémentaires offertes par une meilleure protection de l'identité des machines permettent aux équipes de sécurité de reconnaître et de corriger plus rapidement les menaces envers l'identité des machines.

› **Diminution du risque d'exfiltration de données.** Une fois les violations détectées, les fonctionnalités d'automatisation et d'élévation peuvent rapidement mettre fin à l'accès, révoquer les certificats, assurer la rotation des clés et remédier aux violations afin de minimiser la perte de données. Ce résultat était important pour 39 % des entreprises interrogées.

› **Diminution du nombre de violations.** Bien que les autres résultats soient plus immédiats, 39 % des entreprises ont une vision à long terme de l'amélioration de la protection de l'identité machines, réduisant ainsi de manière mesurable le nombre total de violations. Même si la résolution rapide des problèmes est une bonne chose, il est préférable de prévenir les problèmes avant qu'ils ne surviennent.

Figure 6

Principaux résultats de l'amélioration de la sécurité des identités des machines et des accès privilégiés.

Panel : 350 décisionnaires informatiques américains, australiens et de l'EMEA responsables de l'infrastructure commerciale de leur entreprise
Source : étude réalisée par Forrester Consulting pour Venafi, mars 2018

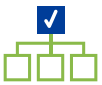
FORRESTER®

Principales recommandations

L'évolution du paysage numérique continue de s'accélérer. Cela signifie que le nombre d'identités machines sur les réseaux d'entreprise continuera de croître de manière spectaculaire, tandis que le nombre de personnes sur les réseaux d'entreprise devrait rester relativement constant. Les entreprises ne peuvent pas se permettre de relâcher leurs efforts relatifs à la protection de l'identité des machines, car le nombre et la variété des identités machines vont continuer à croître. Les programmes de sécurité axés uniquement sur la protection d'un sous-ensemble d'identités de machine (serveurs ou infrastructure critiques par exemple) exposent les entreprises à des risques de sécurité accrus, étant donné que de nouvelles infrastructures mobiles, Cloud, IoT et conteneurisées, telles que la blockchain et l'Intelligence Artificielle, sont utilisées pour prendre en charge les fonctions commerciales.

De nombreuses entreprises ne disposent pas des moyens nécessaires pour résoudre ce dilemme, car elles s'appuient sur des processus manuels ou des outils de protection d'identité des machines en silos qui ne sont pas conçus pour faire face aux complexités inhérentes à la protection de l'identité des machines. Sans les renseignements adéquats, générés par l'automatisation, les entreprises ne parviendront pas à répondre rapidement au nombre croissant de menaces envers liées aux identités machines. En réalité, de nombreuses entreprises sont déjà enlisées dans des processus laborieux et ne sont pas en mesure d'appliquer efficacement les stratégies en matière d'identité machines.

Pour identifier plus rapidement les violations, réduire les pertes occasionnées par les violations et, finalement, réduire le nombre d'infractions, les entreprises doivent mettre en place des mesures de protection d'identités efficaces et automatisées. Pour y parvenir, Forrester recommande aux entreprises de suivre ces bonnes pratiques :



Mettre en oeuvre une capacité de visibilité continue qui surveille activement les identités des machines. La portée et le nombre d'identités des machines dans votre environnement sont plus importants que vous ne le pensez, tout comme la vitesse à laquelle elles apparaissent et évoluent. Outre les technologies déjà évoquées, les connexions aux bases de données, les chatbots, les agents intelligents et les applications prêtes à l'emploi requièrent des identités de machine uniques pour authentifier les connexions aux sources de données sensibles. La condition préalable d'un programme de protection d'identité de machines efficace et automatisé est une compréhension approfondie et continue de vos ressources et des éléments que vous devez protéger.

FORRESTER®

Exploiter les renseignements. Une fois que vous connaissez l'existence d'une identité de machine, vous devez déterminer si elle est conforme à vos règles de sécurité : Provient-elle d'une source connue ? Sa configuration pose-t-elle une menace ? Peut-elle expirer et provoquer la défaillance des systèmes ? Est-elle utilisée de manière inattendue ? Doit-elle être remplacée ? Ces attributs, ainsi que de nombreux autres, doivent être constamment évalués afin de protéger correctement les identités des machines.

Automatisation, automatisation et automatisation. Compte tenu du nombre d'identités de machines et de leur cycle de vie réduit, la protection des identités requiert une approche complètement différente. Les outils et processus manuels ne peuvent pas résoudre les nouveaux défis posés à la protection de l'identité des machines : l'automatisation est le meilleur moyen d'adapter les réponses selon la vitesse et l'ampleur de l'évolution des identités de machines. De plus, la protection de l'identité des machines doit être un processus continu et évolutif capable de gérer les changements rapides de la population d'identités de machines. Elle doit également faire l'objet d'une vérification centralisée. Ces deux fonctionnalités doivent être automatisées.

Synchroniser l'identité des machines et les autres référentiels. Si votre entreprise utilise déjà une combinaison de solutions visant à protéger les clés SSH, les certificats SSL/TLS et d'autres informations d'identification privilégiées pour la communication de machine à machine, consolidez ou au moins synchronisez ces référentiels sur une plate-forme unique avec des API cohérentes, de manière à effectuer un suivi centralisé. Cette interface de sécurité unifiée protège plus efficacement toutes les identités des machines, apporte des améliorations significatives en termes d'efficacité et réduit la complexité.

Intégrer les renseignements relatifs à l'identité des machines à toutes les infrastructures produisant et consommant des identités de machines. Le nombre de consommateurs et de producteurs d'identités machines s'élève à plusieurs milliers au sein des entreprises actuelles. Les serveurs, les VPN, les appareils mobiles, les machines virtuelles, Cloud Workload, les ordinateurs portables, les WAF, les WAP, les CA, les chaînes de bloc, l'IoT, les répertoires actifs produisent ou consomment tous des identités de machines. L'intégration des renseignements relatifs à l'identité des machines à tous les types d'identités de machines est nécessaire pour obtenir une visibilité optimale, un ensemble complet d'informations et une automatisation.

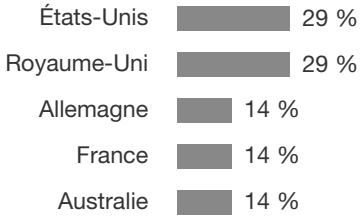
N'essayez pas d'utiliser des outils internes ou des outils non spécifiques à la gestion des identités machines. Ces solutions sont rarement en mesure de faire face à la complexité, à la gestion centralisée des audits et des règles, ainsi qu'aux exigences d'automatisation inhérentes à la protection de l'identité des machines. Déterminez plutôt comment des solutions de protection d'identité de machines spécifiques peuvent répondre à vos besoins.

Annexe A : Méthodologie

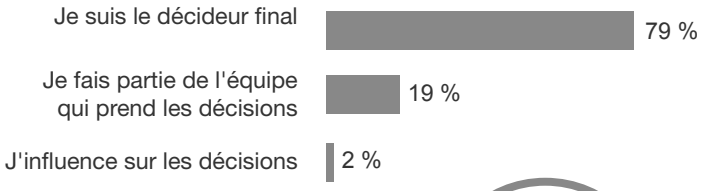
Dans cette étude, Forrester a interrogé 350 décideurs informatiques responsables de l'infrastructure commerciale de leur entreprise, ainsi que de la protection des identités et des accès. Les questions posées aux participants portaient sur l'approche de leur entreprise en matière de gestion des privilèges pour les identités humaines et machines. Les entreprises interrogées étaient installées aux États-Unis, au Royaume-Uni, en Allemagne, en France et en Australie et comptaient au moins 500 employés. Cette étude a été terminée en mars 2018.

Annexe B : Données démographiques

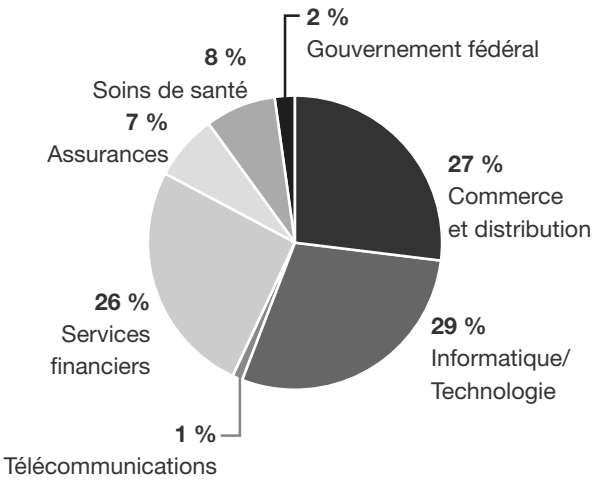
« Dans quel pays vous trouvez-vous ? »

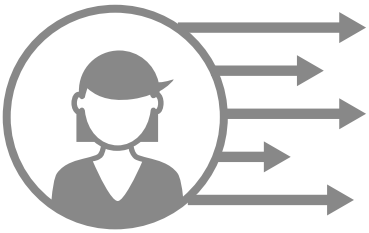


« Quel est votre niveau de responsabilité concernant la la stratégie de sécurité de votre entreprise en matière de gestion des identités et des accès ? »



« Parmi les catégories suivantes, laquelle décrit le mieux le secteur d'activité de votre entreprise ? »





100 % dans les rôles informatiques

Panel : 350 décisionnaires informatiques américains, australiens et de l'EMEA responsables de l'infrastructure commerciale de leur entreprise
Source : étude réalisée par Forrester Consulting pour Venafi, mars 2018

FORRESTER®