SÉCURITÉ CENTRÉE SUR LES PERSONNES

Un multiplicateur de force dans les architectures de cybersécurité modernes

Pourquoi une sécurité centrée sur les personnes est un élément essentiel de toute stratégie de défense moderne, qui s'adapte à vos investissements de cybersécurité existants, s'y connecte et les optimise

proofpoint®

Résumé

Il incombe aux RSSI modernes de déterminer les investissements stratégiques à consentir dans l'architecture de cybersécurité de leur entreprise. Par ailleurs, certains piliers de sécurité bien établis, tels que le SASE (Secure Access Service Edge), la détection et la réponse avancées aux incidents (XDR) et l'identité, doivent être au cœur de la stratégie de défense des entreprises. Ces piliers ne peuvent pas fonctionner de manière indépendante — ils doivent travailler de concert pour s'assurer que l'architecture déjoue les menaces actuelles et prémunit l'entreprise contre celles de demain. Cependant, bien que chacun de ces piliers soit une composante fondamentale de toute stratégie de défense, aucun ne tient compte de la plus grande menace : les personnes et leurs actions.

Une sécurité centrée sur les personnes permet de boucler la boucle : de la boîte de réception à l'endpoint, de l'identité aux menaces internes. En effet, derrière chaque brèche se cache une personne négligente, malveillante ou dont le compte a été compromis.

Ce livre blanc explique pourquoi une sécurité centrée sur les personnes est un élément essentiel — et transformateur — des architectures de cybersécurité modernes.

Ce livre blanc :

- **Explique en quoi une sécurité centrée sur les personnes joue un rôle déterminant** dans votre architecture globale en éliminant les angles morts dans votre protection existante et en détectant les risques liés aux utilisateurs au sein des espaces de travail numériques.
- **Présente la plate-forme Human-Centric Security de Proofpoint.** Ce livre blanc décrit comment Proofpoint fait office de plan de contrôle stratégique en optimisant vos investissements de sécurité existants et en protégeant votre entreprise contre les menaces centrées sur les personnes.

Au-delà des périmètres et des produits isolés : la faille

De nombreux RSSI luttent toujours contre les menaces modernes au moyen de modèles d'ancienne génération, c'est-à-dire de contrôles cloisonnés, d'informations fragmentées et d'outils incapables de s'adapter assez rapidement. Cependant, face à l'évolution de la surface d'attaque, notre réponse doit suivre le mouvement.

La nouvelle réalité est la suivante : les cybercriminels ciblent aujourd'hui les personnes, pas les ports. Avec l'élargissement des espaces de travail numériques, les cyberpirates ciblent des personnes par le biais de la messagerie électronique et de nombreux autres canaux numériques (outils de collaboration et de messagerie, plates-formes de réseaux sociaux, applications cloud, grands modèles de langage ou LLM, services de partage de fichiers, etc.). Les cybercriminels peuvent également pirater des communications d'entreprise de confiance, ce qui nuit aux relations avec les fournisseurs et les clients.

Les fuites de données ne se produisent pas par magie. Derrière chacune d'elles se cachent des actions humaines. Les utilisateurs négligents gèrent des données sensibles ou critiques de manière inappropriée. Les utilisateurs malveillants les emportent avec eux. Les cyberpirates compromettent des comptes utilisateur pour les voler. Les collaborateurs qui rejettent les règles les utilisent de manière abusive.

S'il demeure important de choisir des outils de pointe, les RSSI modernes doivent également se concentrer sur la création d'une architecture intelligente et cohésive, qui évolue avec le paysage des menaces et s'assure que ces outils fonctionnent de concert pour offrir une défense efficace.

Proofpoint a développé quelque chose d'unique dans le secteur : une plate-forme complète de sécurité centrée sur les personnes qui fait office de multiplicateur de force en optimisant vos investissements de sécurité au niveau de la messagerie électronique, de l'identité, des données et des accès.

Nous ne nous contentons pas de corriger les failles de sécurité. Grâce à des intégrations étroites avec des partenaires tels que CrowdStrike, Okta, Zscaler, Microsoft et Palo Alto Networks, nous réduisons la durée d'implantation des cybercriminels, neutralisons les attaques à un stade plus précoce et allégeons la charge de travail de votre équipe de sécurité.

Si vous utilisez uniquement notre solution de protection de la messagerie, vous ne connaissez pas encore tous nos atouts. Découvrez notre plate-forme.

proofpoint.

Les piliers fondamentaux d'une architecture de cybersécurité moderne

Tous les RSSI les connaissent. Ce sont les piliers fondamentaux d'une architecture de cybersécurité moderne : **le SASE, le XDR, l'identité, ainsi que les SecOps et l'automatisation.** Comme décrit ci-après, chacun de ces piliers est essentiel et résout un large éventail de préoccupations liées aux risques. Toutefois, aucun ne tient compte du plus grand risque dans le paysage actuel de la sécurité : les personnes. **C'est la raison pour laquelle une sécurité centrée sur les personnes constitue aujourd'hui le pilier le plus important de tous.**

SecOps et automatisation

Rationalisent la détection, l'analyse et la neutralisation des menaces en éliminant les efforts manuels et les workflows cloisonnés. Réduisent les problèmes de longs délais de réponse, de baisse de vigilance face aux alertes et d'inefficacité opérationnelle. Proofpoint automatise le tri des menaces et l'application des règles grâce à des stratégies intégrées, à des informations enrichies sur les risques liés aux utilisateurs et à des API flexibles. Les équipes du centre d'opérations de sécurité (SOC) peuvent ainsi intervenir plus rapidement et avec plus de précision.

SASE

Offre un accès sécurisé et optimisé aux applications et aux données, quels que soient l'emplacement de l'utilisateur et le terminal dont il se sert. Prend en charge les effectifs distribués, les accès au cloud et l'application cohérente de règles dans les environnements de télétravail. Lorsqu'il est nourri par des signaux de risques centrés sur les personnes, le SASE peut prioriser la protection pour les utilisateurs ou les comportements à haut risque.

Sécurité centrée sur les personnes

Place les personnes au centre de la protection, étant donné que ce sont les utilisateurs, et non les infrastructures, qui sont les principales cibles des cybermenaces. La plate-forme Human-Centric Security de Proofpoint lutte contre le phishing, les fuites de données et les compromissions de comptes en combinant détection des menaces basée sur l'IA et formation en temps réel des utilisateurs. Pour réduire les risques centrés sur les personnes, nos technologies Nexus et Zen identifient de manière unique et avec précision les utilisateurs, comportements et expositions à risque.

XDR

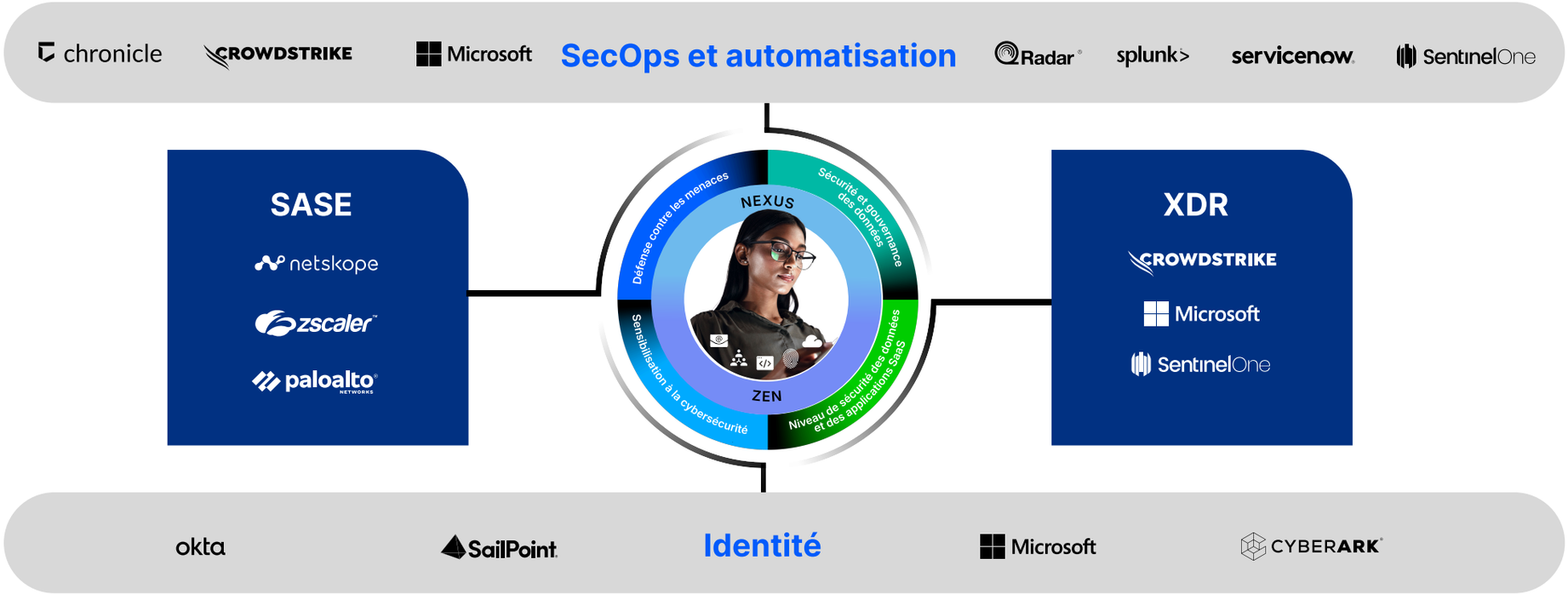
Unifie les données télémétriques au niveau de la messagerie électronique, des endpoints, du cloud et des réseaux, afin de rationaliser la détection, l'analyse et la neutralisation des menaces. Réduit les problèmes de silos de visibilité et de longs délais de réponse. Les données télémétriques centrées sur les personnes de Proofpoint, notamment les informations sur les personnes ciblées et à risque, peuvent optimiser le XDR grâce à des renseignements contextuels précoces et exploitables.

Identité

Sécurise les identités et les accès des utilisateurs au niveau du cloud et des environnements sur site en détectant les prises de contrôle de comptes, les utilisations abusives d'identifiants de connexion et les erreurs de configuration d'applications SaaS. Réduit les risques d'attaques visant les identités et d'accès non autorisés grâce à la surveillance continue des autorisations, des comportements de connexion et des configurations des applications à risque. Étant donné que Proofpoint sait qui a accès à quoi et pourquoi, les équipes de sécurité peuvent prévenir les déplacements latéraux et appliquer le principe du moindre privilège.

proofpoint.

La sécurité centrée sur les personnes, un multiplicateur de force



La plate-forme Human-Centric Security de Proofpoint fait office de plan de contrôle stratégique dans votre architecture de cybersécurité. Elle s'intègre à vos investissements de sécurité existants en fournissant des signaux de risques centrés sur les personnes qui boostent leur efficacité.

Notre plate-forme s'appuie sur la compréhension de la classification des données, de l'intention des utilisateurs et du contexte des menaces. Elle a recours à l'IA, à l'apprentissage automatique et à une threat intelligence en temps réel pour extraire des informations pertinentes et permettre la prise de décisions automatisées en matière de règles.

Voici quelques-unes des nombreuses façons dont la plate-forme Human-Centric Security de Proofpoint s'intègre aux autres piliers de votre architecture afin de transformer votre protection globale :

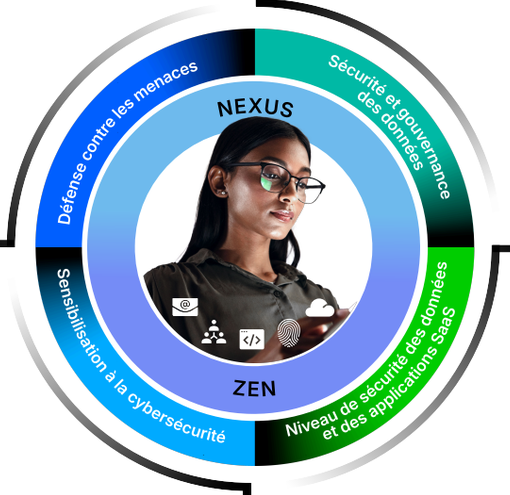
Réponse accélérée et automatisée

Proofpoint s'intègre à des systèmes de gestion des événements et des incidents de sécurité (SIEM) et à des plates-formes d'orchestration, d'automatisation et de réponse aux incidents de sécurité (SOAR) afin de réduire le délai moyen de détection, d'analyse et de neutralisation des menaces grâce au déclenchement d'alertes centrées sur les personnes et à l'automatisation des actions de réponse. Les signaux de risques de Proofpoint déclenchent, dans Cortex XSOAR ou Splunk SOAR, des stratégies automatisées qui mettent les utilisateurs en quarantaine ou réinitialisent les identifiants de connexion. Les alertes enrichies disponibles dans Splunk ou Microsoft Sentinel réduisent les faux positifs et accélèrent le tri. Les renseignements sur les menaces et les données télémétriques sur les comportements des utilisateurs de Proofpoint sont partagés entre les systèmes afin de garantir des workflows unifiés.

SASE et contrôle adaptatif des accès

En collaboration avec des partenaires comme Zscaler et Palo Alto Networks, Proofpoint intègre une threat intelligence et des informations comportementales qui influencent les règles d'accès en temps réel. Les utilisateurs ciblés sont soumis à une authentification renforcée ou voient leur accès bloqué via Zscaler ou Palo Alto Prisma Access. Les activités malveillantes déclenchent l'application immédiate de règles.

Il s'agit d'une architecture SASE informée par des personnes, et pas seulement par des paquets.



Un XDR qui s'applique dès le point d'entrée

Le phishing demeure le principal point d'entrée. Notre partenariat avec CrowdStrike, Microsoft Sentinel et SentinelOne nous permet de boucler la boucle. Le signalement d'un email déclenche l'isolation de l'endpoint dans CrowdStrike ou SentinelOne en quelques secondes seulement, et non en plusieurs heures. L'attribution d'un score de risque aux utilisateurs et les informations contextuelles ciblées sur les menaces de Proofpoint enrichissent les alertes dans Microsoft Sentinel.

Proofpoint offre une visibilité dès le point d'entrée, afin que votre solution XDR bénéficie d'informations exhaustives.

Protection des identités et des accès à privilèges

Nous partageons des informations contextuelles sur les risques avec Okta, CyberArk et SailPoint afin d'influencer dynamiquement le contrôle des accès. Nous identifions vos utilisateurs les plus à risque et partageons ces renseignements avec nos partenaires. Un comportement suspect ? Nous appliquons l'authentification multifacteur. Un utilisateur à haut risque ? Nous appliquons des règles et des contrôles adaptatifs. Un compte compromis ? Nous révoquons l'accès. Ensemble, nous donnons vie au Zero Trust grâce à une mise en œuvre adaptative et tenant compte de l'identité.

proofpoint.

Vos prochaines actions doivent être stratégiques, pas tactiques

La question n'est pas de savoir quel est le prochain outil à utiliser, mais comment développer une plate-forme capable de s'adapter à vos investissements existants, de s'y connecter et de les optimiser.

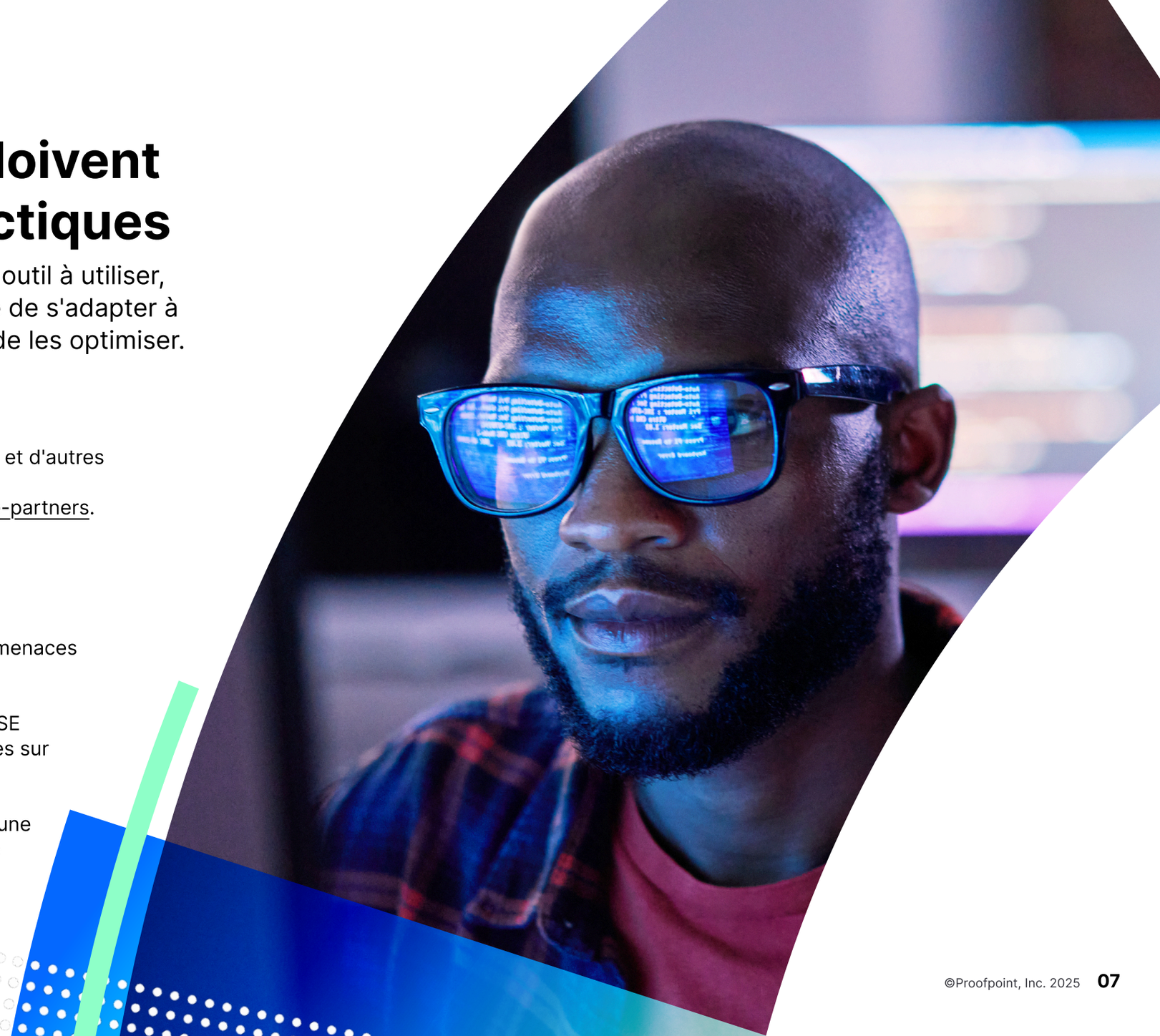
En savoir plus sur nos intégrations

Découvrez d'autres cas d'utilisation d'intégration entre Proofpoint et d'autres composants de votre architecture de cybersécurité.
Consultez la page proofpoint.com/fr/partners/technology-alliance-partners.

Prenez contact avec Proofpoint

- **Évaluez** si votre architecture de sécurité est prête à gérer les menaces centrées sur les personnes.
- **Déterminez** comment vos investissements existants (XDR, SASE et identité) peuvent être optimisés par nos informations unifiées sur les risques liés aux utilisateurs.
- **Découvrez** à quoi ressemble vraiment une sécurité basée sur une plate-forme et quelles sont les premières étapes vers une telle approche. Nous vous montrerons comment convertir des informations centrées sur les personnes en une sécurité transformatrice.

proofpoint.



proofpoint.

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises du classement Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

Suivez-nous : LinkedIn

0303-001-03-01

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →