SÉCURITÉ CENTRÉE SUR LES PERSONNES

Adopter une sécurité centrée sur les personnes dans le paysage numérique moderne

Comment la plate-forme de protection multicouche complète de Proofpoint met en place une sécurité centrée sur les personnes à l'ère de la transformation numérique

proofpoint®

Résumé

Le paysage numérique moderne a fondamentalement transformé les méthodes de travail. Les entreprises ont résolument adopté le cloud, et les équipes collaborent désormais via une multitude d'environnements divers : email, outils de collaboration et de messagerie, plates-formes de réseaux sociaux, applications SaaS, grands modèles de langage (LLM), services de partage de fichiers, etc.

Cette transition a permis d'accélérer l'innovation et d'accroître la flexibilité. Mais elle s'accompagne aussi de nombreuses nouvelles surfaces d'attaque à la merci des cybercriminels. Les travailleurs du savoir génèrent, stockent et accèdent à des données selon des modalités qui échappent aux stratégies de sécurité traditionnelles, centrées sur la protection des réseaux et des endpoints. Ces bouleversements exigent une architecture moderne, en phase avec le fonctionnement des entreprises et les méthodes de travail des effectifs. Une architecture qui tienne compte du fait que, désormais, ce sont les utilisateurs (et plus l'infrastructure) qui constituent la cible principale des cybermenaces.

Ce livre blanc s'intéresse à une contribution majeure de Proofpoint à cette nouvelle réalité : la plate-forme Human-Centric Security, première en son genre dans le secteur, qui place les personnes au centre de la stratégie de défense moderne.

Ce livre blanc :

- **Explique pourquoi il est plus important que jamais de protéger vos collaborateurs** dans l'environnement de travail numérique actuel
- **Décrit les problèmes centrés sur les personnes** que la plate-forme Proofpoint a été conçue pour résoudre
- **Passe en revue les technologies essentielles** d'une architecture conçue pour détecter les menaces de façon proactive, guider et protéger les utilisateurs en temps réel et simplifier les investigations et la réponse aux incidents

Les collaborateurs en tant que nouveau périmètre de sécurité : pourquoi une sécurité centrée sur les personnes est essentielle

L'être humain est au cœur du défi que représente aujourd'hui la cybersécurité. Les menaces centrées sur les personnes, dont le phishing, la prise de contrôle de comptes, les risques internes et l'exfiltration de données, constituent désormais la majorité des compromissions. Ainsi, la plupart des attaques modernes n'exploitent pas des vulnérabilités techniques, mais le comportement humain. Par la tromperie, la distraction ou la manipulation, les cybercriminels prennent les utilisateurs pour cible au sein d'environnements de travail numériques de plus en plus complexes.

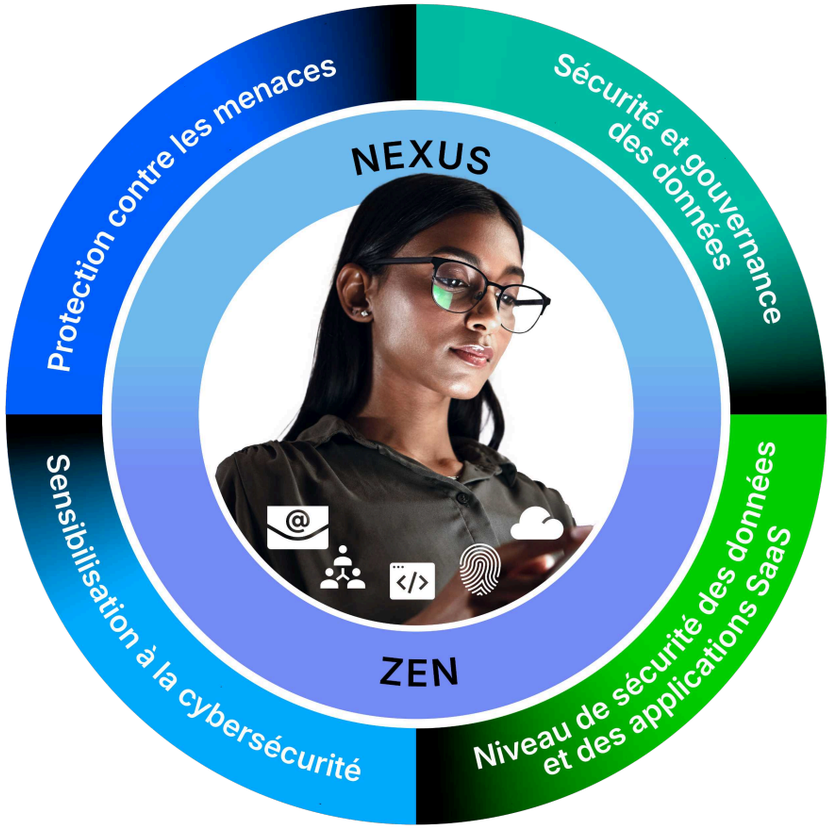
Les modèles de sécurité traditionnels se concentrent sur la protection des réseaux et des endpoints, alors que les menaces modernes ciblent les vulnérabilités de la nature humaine. Grâce à la plate-forme de cybersécurité de Proofpoint, les entreprises peuvent protéger les utilisateurs et les données à l'aide d'une approche centrée sur les personnes. Notre plate-forme propose des solutions de pointe pour répondre à quatre problématiques critiques : le blocage des menaces, la protection des informations, la sensibilisation des utilisateurs et le renforcement du niveau de sécurité des données et des applications SaaS.

PROTECTION CONTRE LES MENACES

Blocage des menaces qui ciblent vos collaborateurs

SENSIBILISATION À LA CYBERSÉCURITÉ

Formation continue à l'intention des collaborateurs



SÉCURITÉ ET GOUVERNANCE DES DONNÉES

Prévention des fuites de données et gouvernance des communications

NIVEAU DE SÉCURITÉ DES DONNÉES ET DES APPLICATIONS SAAS

Correction de l'exposition des données et des applications SaaS

Figure 1. La plate-forme Human-Centric Security de Proofpoint procure des solutions de pointe dans quatre domaines clés.

proofpoint.

Une plate-forme de protection complète et multicouche

La plate-forme complète de Proofpoint repose sur une architecture multicouche qui :

- **Détecte les menaces de façon proactive** dans tout l'environnement de travail numérique grâce à des technologies telles que l'IA avancée, l'apprentissage automatique et une threat intelligence en temps réel
- **Procure une série de points de contrôle au niveau de l'utilisateur final** pour protéger les collaborateurs et les données, où qu'ils se trouvent
- **Alerte les utilisateurs, les guide et les équipe d'outils appropriés** pour assurer leur résilience face aux attaques qui les ciblent
- **Simplifie l'investigation et la réponse aux incidents**

Ces fonctionnalités reposent sur trois technologies phares : Proofpoint Nexus, Zen et Threat Protection Workbench. Les sections qui suivent explorent ces technologies.

Proofpoint Nexus

Détection assistée par l'IA et la threat intelligence

Proofpoint Nexus® est la couche de détection de l'architecture Proofpoint. Il s'agit d'un cadre de détection unifié optimisé par l'IA, l'apprentissage automatique et une threat intelligence en temps réel.

Proofpoint Nexus intègre plusieurs types de modèles d'IA. Chacun de ces modèles est conçu pour analyser des signaux de risques spécifiques associés aux modes de travail des utilisateurs, par exemple l'email, les applications cloud, les outils de collaboration et les navigateurs.

Principaux composants du cadre de détection Proofpoint Nexus

Nexus Threat Intelligence (TI) ingère en continu les signaux associés à des acteurs, campagnes et infrastructures cybercriminels, connus et inconnus, afin de procurer aux solutions Proofpoint des détections contextualisées et la capacité de s'adapter à l'évolution des techniques d'attaque.

Nexus Language Model (LM) utilise la puissance des modèles de langage d'IA avancée pour évaluer le ton, l'emphase et la structure linguistique des messages utilisés dans les attaques d'ingénierie sociale, telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise).

Nexus Relationship Graph (RG) met en corrélation l'activité des utilisateurs, l'historique de leur comportement et le niveau de sensibilité de leur rôle afin d'évaluer la probabilité d'un comportement à risque ou d'attaques ciblées contre des collaborateurs à haut risque.

Nexus Machine Learning (ML) détecte les comportements inhabituels des utilisateurs sur les outils de collaboration et de communication, de façon à identifier les signaux subtils, mais significatifs révélant la compromission de comptes ou une utilisation abusive par des utilisateurs internes.

Nexus Computer Vision (CV) identifie les tactiques d'usurpation de marque et de fraude visuelle en analysant le design, le placement de logos ou la mise en page à la recherche d'imitations frauduleuses. Grâce à une technologie avancée de vision par ordinateur, il détecte les menaces cachées dans des éléments visuels, comme les sites de phishing, les codes QR, les pièces jointes malveillantes et les emails falsifiés.

Proofpoint Nexus détecte les attaques de phishing avancées, le vol d'identifiants de connexion, les tentatives d'usurpation d'identité et les campagnes de ransomwares. À titre d'exemple, Proofpoint Nexus a identifié une fraude à la facturation qui visait un département financier précis, conséquence de la compromission d'un fournisseur. Il a bloqué l'attaque avant qu'elle ne puisse s'exécuter en identifiant des incohérences dans les éléments visuels et le langage employés, et en se basant sur une threat intelligence mondiale.

Proofpoint Nexus excelle également à la protection des données. Dans un autre cas réel, Proofpoint Nexus a détecté une activité anormale au niveau des données sensibles lorsqu'un collaborateur a collé des données client dans un outil d'IA générative non autorisé : il a élevé le score de risque et bloqué l'action.

Proofpoint Nexus analyse plus de **2,6 milliards d'emails et plus de 450 millions d'URL par jour** et corrèle les signaux de centaines de cybercriminels. Ce volume énorme de données garantit à la fois précision et réactivité au sein du paysage des menaces.

proofpoint.

Proofpoint Zen

Points de contrôle et conseils contextuels pour les utilisateurs

Proofpoint Zen™ est la couche chargée de mettre en œuvre les mesures de sécurité et de guider les utilisateurs de l'architecture Proofpoint. Elle applique les règles de sécurité partout où les utilisateurs accomplissent leurs tâches. Les points de contrôle de la suite Proofpoint Zen traduisent la threat intelligence en protection en temps réel et génèrent des messages aux utilisateurs conformément aux règles définies. Ces avertissements aident les utilisateurs à prendre des décisions plus avisées sans nuire à leur productivité.

Principaux composants de la suite Proofpoint Zen

Zen for Outlook transforme les utilisateurs en défenseurs de première ligne en incorporant des outils de sécurité dans leurs workflows de messagerie. Exploitant la threat intelligence en temps réel de Proofpoint Nexus, la solution affiche des avertissements contextuels à l'intention des utilisateurs lorsqu'ils reçoivent des emails suspects et facilite le signalement. Il souligne judicieusement les comportements à risque et émet une alerte en cas de présence de données sensibles dans les emails sortants.

ZenWeb est une extension légère pour les navigateurs Chromium qui sécurise les activités Web sur les outils SaaS, de partage de fichiers et d'IA générative, en plus de protéger les utilisateurs contre les sites de phishing. Grâce aux détections en direct basées sur les modèles de menaces Nexus, ZenWeb détecte et prévient les menaces en temps réel, sans impact sur la productivité.

Zen Endpoint DLP/Insider Threat Management assure la protection des terminaux contre les fuites de données et les menaces internes grâce à la surveillance du comportement des utilisateurs au niveau de l'endpoint. Ce composant surveille l'utilisation des ports USB, le Presse-papiers, les opérations de synchronisation de fichiers et le comportement des applications. Il effectue des captures d'écran des actions utilisateur suspectes et enregistre l'historique des activités des utilisateurs.

Zen Cloud API Connectors étend la sécurité aux plates-formes SaaS dans le cloud telles que Microsoft 365, Google Drive, Slack et Box. Ce composant surveille les chargements de fichiers et détecte les comportements inhabituels tels que les partages excessifs. Il permet également d'établir des workflows personnalisés dans Okta et dans les outils d'orchestration, d'automatisation et de réponse aux incidents de sécurité (SOAR).

Zen Communications Connectors capture les communications sur les plates-formes réglementées, telles que Microsoft Teams, Zoom et Slack, à des fins d'archivage et de supervision. Ce composant ingère des messages à partir de divers canaux et les transforme en un format d'archivage unifié, en plus de s'intégrer avec des outils de supervision destinés aux workflows des départements juridique et des ressources humaines.

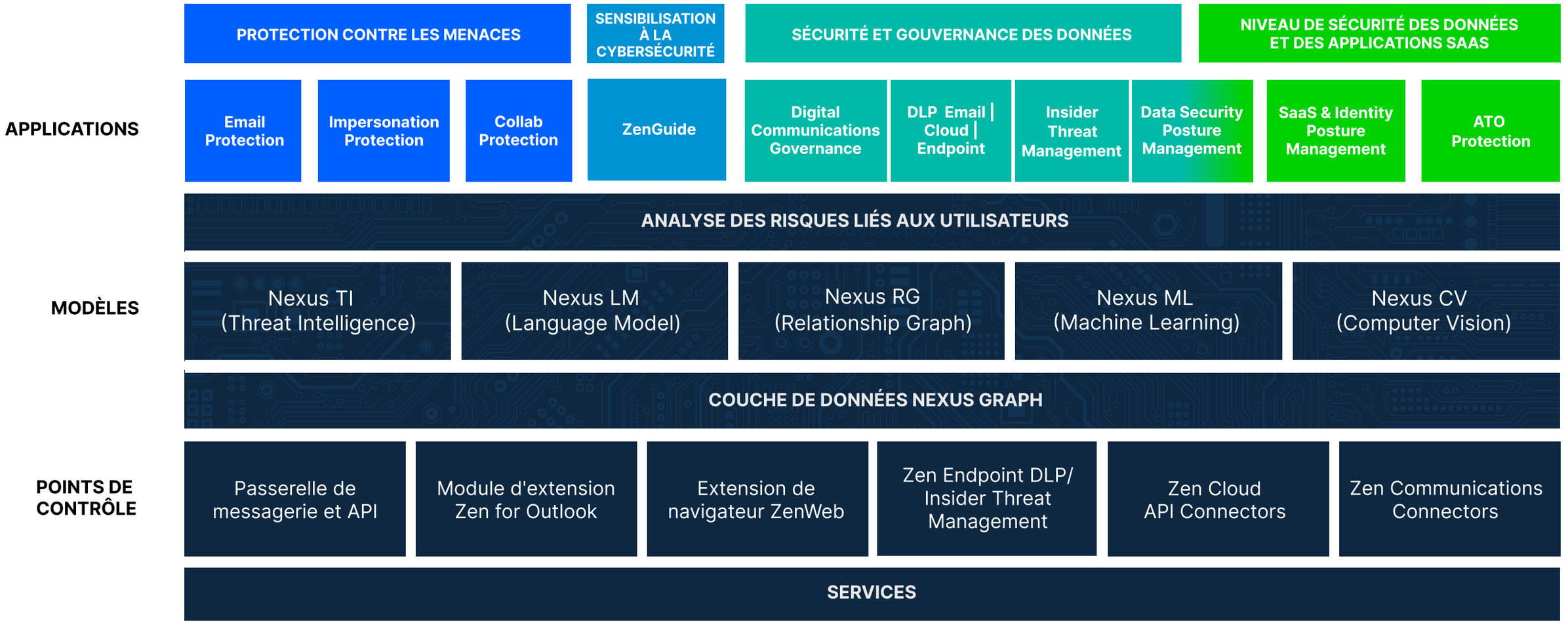


Figure 2. La plate-forme Human-Centric Security de Proofpoint repose sur une architecture multicouche. Les solutions Proofpoint (dans nos domaines d'activité phares que sont la protection contre les menaces, la sensibilisation à la cybersécurité, la sécurité et gouvernance des données et le niveau de sécurité des données et des applications SaaS) exploitent directement les fonctionnalités de nos technologies de base Proofpoint Nexus et Proofpoint Zen.

Proofpoint Threat Protection Workbench

Investigation rapide et correction automatisée

En cas de détection d'une menace ou de signalement de la violation d'une règle, la rapidité d'action et la visibilité deviennent des facteurs critiques. Pour les équipes SOC, la multiplication des consoles et des manipulations nécessaires ainsi que les dépendances vis-à-vis d'autres équipes ralentissent les temps de réponse et accroissent le risque que les attaques aboutissent.

Proofpoint Threat Protection Workbench est la couche d'investigation et d'automatisation de l'architecture Proofpoint. En procurant au SOC une console intuitive et centralisée, il rationalise les investigations sur les menaces et les mesures de correction. Il permet aux équipes de sécurité d'effectuer les opérations de tri, d'analyse et de réponse aux menaces sans les délais qu'entraînent le basculement entre plusieurs outils ou la fragmentation des données.

Les équipes de sécurité emploient Proofpoint Threat Protection Workbench pour traiter les envois aux boîtes email de signalement d'abus, faire remonter les signaux concernant les utilisateurs à haut risque et examiner les campagnes d'attaque. En mettant en corrélation la threat intelligence de Proofpoint Nexus avec les comportements utilisateur et les déclencheurs de règles, Proofpoint Threat Protection Workbench génère des alertes haute fidélité, limitant ainsi les faux positifs.

Exemples de cas d'utilisation de Proofpoint Threat Protection Workbench

- Réponses automatisées lors des investigations sur de possibles prises de contrôle de comptes
- Visualisation de la séquence de clics des utilisateurs ciblés par les attaques
- Synthèse des menaces multicanales complexes

Toutes ces capacités réduisent la charge de travail des analystes ainsi que la durée d'implantation des menaces. Pour répondre aux menaces, les analystes peuvent déclencher directement l'exécution de procédures prédéfinies, ou utiliser des API pour remonter l'information à d'autres composants intégrés dans leurs piles de sécurité plus vastes.

proofpoint.

Conclusion

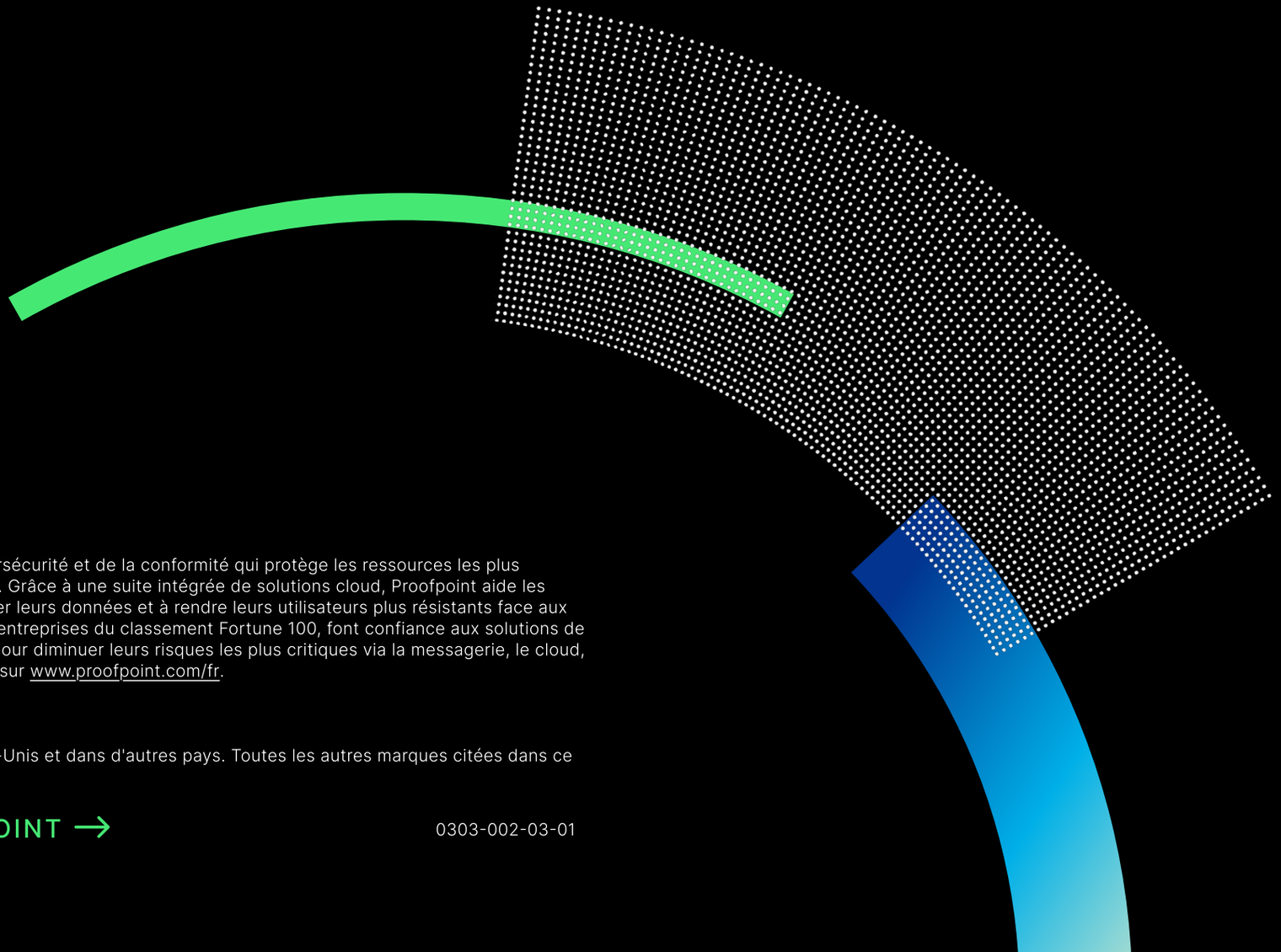
Une architecture spécialisée pour une sécurité centrée sur les personnes

La nature des cyberrisques a changé. Les menaces ne se contentent pas de cibler les systèmes : elles visent les personnes. Et la complexité de l'environnement de travail numérique a pris de court les défenses conçues pour le protéger. Avec des utilisateurs qui emploient désormais indifféremment et en alternance la messagerie électronique, les navigateurs, les outils de collaboration et les applications cloud, l'ancienne approche de la sécurité — basée sur des périmètres statiques et des solutions universelles — ne tient désormais plus la route.

La plate-forme de Proofpoint relève ce défi de taille en alignant son architecture de sécurité sur les nouveaux modes de travail. Avec Proofpoint Nexus, les entreprises disposent d'une visibilité assistée par l'IA sur les menaces centrées sur les personnes, qui s'appuie sur une threat intelligence de pointe et l'analyse comportementale. Avec Proofpoint Zen, notre plate-forme protège et conseille les utilisateurs en temps réel, sans friction. Enfin, grâce à Proofpoint Threat Protection Workbench, les équipes de sécurité sont en mesure de réagir plus rapidement, disposent d'informations plus pertinentes et observent une diminution des frais opérationnels.

Et ce ne sont pas des avantages théoriques. Notre plate-forme offre une architecture éprouvée, conçue pour les environnements de production, qui réduit les risques et établit une résilience à long terme. Les entreprises peuvent ainsi protéger leurs workflows et se préparer à la prochaine évolution des risques centrés sur les personnes.

En associant détection de pointe, contrôles comportementaux incorporés et réponse rapide et intégrée, nous pouvons aider votre entreprise à atténuer les risques là où ils sont les plus critiques : à l'intersection entre les personnes, les données et les menaces.



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

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →

0303-002-03-01