Forcepoint

Brochure Solution

Les solutions Forcepoint pour répondre aux normes NIST 2.0

Le Défi

- **Risques et réglementations en évolution –** Les entreprises peinent à gérer les cyber-risques croissants et les exigences réglementaires en évolution.
- **Politiques de sécurité incohérentes –** Les contrôles de sécurité fragmentés sur les canaux d'accès créent des failles de conformité.
- **Visibilité et contrôle limités –** L'absence de gestion centralisée et d'alertes rend difficile la détection des risques de sécurité et des violations des politiques.

La Solution

- **Zero Trust Security –** Surveillance continue qui protège les données sur les terminaux, le réseau, le cloud, le Web et les e-mails.
- **Classification basée sur l'IA –** Le moteur de classification des données d'apprentissage continu améliore la précision pour une application efficace des politiques.
- **Déploiement flexible –** Options cloud, sur site et hybrides pour s'adapter aux besoins de l'entreprise.

Résultat

- **Conformité rationalisée –** La protection centralisée et adaptative réduit les risques de perte de données avant que des violations de la conformité ne se produisent.
- **Réduction de la charge opérationnelle –** La gestion unifiée et l'application automatisée minimisent les efforts manuels.
- **Favorise la croissance des entreprises –** Une collaboration sécurisée pour soutenir l'innovation commerciale.

Le cadre de cybersécurité du National Institute of Standards and Technology (NIST) est une pierre angulaire pour de nombreuses entreprises globales qui visent à renforcer leur sécurité sur de nombreux domaines différents, pour protéger les actifs et les données critiques tout en améliorant la gestion et la réponse aux risques et aux menaces.

Avec l'introduction du NIST 2.0 CSF (Cybersecurity Framework) en février 2024, la nouvelle directive aide les entreprises à améliorer leur posture de cybersécurité grâce à une approche plus simplifiée.

Forcepoint reconnaît le rôle important joué par le NIST pour guider les entreprises vers de meilleures pratiques de sécurité. Nous nous engageons à soutenir ces efforts en fournissant des solutions qui aident à identifier, à classer et à protéger les données sensibles tout en permettant la détection et la réponse aux incidents d'exfiltration potentiels. En s'alignant sur les principes du NIST, Forcepoint permet aux entreprises de respecter les normes de conformité, d'améliorer la protection des données et de se défendre contre les risques dans le paysage de plus en plus numérique d'aujourd'hui.

Qu'est-ce que le NIST ?

Le National Institute of Standards and Technology est une agence du ministère américain du Commerce qui fournit des conseils sur la conformité, la protection de la vie privée et la sécurité. Dans le domaine de la cybersécurité, le NIST Cybersecurity Framework (NIST CSF) fournit des informations sur les fonctions de base pour permettre aux entreprises d'élaborer des stratégies et de construire un programme de cybersécurité réussi. Le cadre de travail décrit les fonctions d'identification, de protection, de détection, d'intervention et de récupération avec la fonction globale, Gouverner, qui permet à l'entreprise de déterminer quelles décisions correspondent le mieux à sa stratégie.

Protéger les données contre les menaces émergentes

Le cadre de cybersécurité du NIST permet aux entreprises d'être flexibles dans leur posture de cybersécurité. CSF décrit les résultats souhaités des différents contrôles de sécurité à un niveau élevé, tout en fournissant les outils et les ressources pour un aperçu plus granulaire des processus, des personnes et de la technologie.

Avec l'adoption de plus en plus importante de nouvelles technologies telles que l'IA générative, de nombreuses entreprises sont confrontées au défi de la protection de leurs données sensibles lors de l'utilisation de ces outils. L'abus de ces outils, qu'il soit intentionnel ou non, peut avoir de graves conséquences pour les entreprises. Des informations confidentielles ou sensibles peuvent être divulguées via ces outils, ou la formation d'un modèle d'IA peut être perturbée en raison de contenu malveillant. Forcepoint s'engage à aider les entreprises à obtenir de la visibilité sur leurs données, à les protéger et à empêcher leur utilisation abusive.

Le CSF continue de fournir des conseils et des bonnes pratiques aux entreprises pour la construction, la mise en œuvre et la maintenance de leurs programmes de cybersécurité. Avec les nouvelles technologies, les entreprises devront réfléchir à la façon dont ces outils peuvent être utilisés pour communiquer, mesurer et surveiller les risques.

Protection avec Zero Trust

Incorporer Zero Trust est la reconnaissance que chaque demande peut être une menace potentielle. Les applications, les systèmes et les personnes ne sont pas dignes de confiance à moins qu'ils ne puissent être authentifiés, qu'ils soient au sein du réseau ou en dehors.

Le cadre de travail NIST 2.0 a adopté les principes de l'architecture Zero Trust, dans lesquels les fonctions principales sont axées sur la gestion des identités et des accès et sur la gestion des accès privilégiés. Ces lignes directrices et cette architecture aident les entreprises à atténuer leurs risques tout en protégeant leurs données.

Forcepoint offre des solutions de sécurité axées sur les données en tenant compte de Zero Trust. Cela permet aux entreprises d'atténuer leurs risques en empêchant l'exfiltration des données sensibles et leur permettre de rester en conformité, quel que soit le lieu de localisation de leurs employés ou de leurs données.

Naviguer avec l'évolution des risques de sécurité et des exigences de conformité

Le NIST Cybersecurity Framework (CSF) 2.0 fournit aux entreprises une approche flexible et de haut niveau pour la gestion des risques de cybersécurité. Cependant, la mise en œuvre efficace de ses fonctions principales et la hiérarchisation des contrôles restent un défi. Les entreprises doivent déterminer quelles mesures de sécurité s'alignent le mieux sur leurs besoins commerciaux tout en assurant une adaptabilité à long terme.

Étant donné que le NIST CSF est une directive volontaire, certaines entreprises risquent d'adopter une approche « cases à cocher », en se concentrant uniquement sur la conformité plutôt que sur la construction d'une stratégie de sécurité dynamique et résiliente. Pour maximiser leur efficacité, les entreprises doivent en permanence évaluer les risques, affiner les politiques de sécurité et aligner les ressources pour suivre le rythme des menaces en constante évolution.

Principaux défis de conformité auxquels les entreprises sont confrontées :

- → **Garder une longueur d'avance sur les menaces et les réglementations en constante évolution –** Les entreprises peinent à suivre les cyber-risques de plus en plus sophistiqués et les exigences réglementaires en constante évolution.
- → **Application de politique incohérente –** De nombreuses entreprises n'ont pas de stratégie de sécurité unifiée sur les terminaux, les applications SaaS, le trafic Web et les e-mails, ce qui entraîne des lacunes de sécurité et des risques de conformité.
- → **Lacunes dans la visibilité et le contrôle –** Sans gestion centralisée de la sécurité des données et action en temps réel, il devient beaucoup plus difficile d'identifier les lacunes de sécurité, les violations des politiques et les menaces internes.

Pour adhérer avec succès au NIST 2.0 et renforcer la résilience de la sécurité, les entreprises ont besoin d'une approche proactive et basée sur les risques qui assure une application de politique unifiée, la détection des menaces en temps réel et une surveillance continue sur tous les environnements numériques.

Une approche unifiée et adaptative de la sécurité des données

Les entreprises qui adoptent le NIST CSF 2.0 ont besoin d'une approche structurée de la gestion des risques, de l'application de politique et de la protection des données, qui s'aligne sur les fonctions principales du cadre. Forcepoint fournit des solutions conçues pour aider les entreprises à répondre à ces exigences tout en améliorant les opérations de sécurité, en réduisant la complexité de la conformité et en s'attaquant aux risques de sécurité, avant qu'ils ne deviennent des violations de la conformité.

Cadre de sécurité Zero Trust

L'architecture de sécurité des données de Forcepoint est basée sur les principes de Zero Trust, qui garantissent que l'utilisation des données est surveillée et vérifiée en permanence, que les politiques de moindre privilège sont appliquées et que les risques potentiels – externes et internes – sont atténués en temps réel. Cette approche s'aligne sur les recommandations du NIST pour la gestion proactive des risques et le contrôle d'accès.

Gestion unifiée des politiques et de la conformité

- → **Politiques de sécurité unifiées –** Un cadre de politiques unique applique des contrôles de sécurité cohérents sur les terminaux, les applications SaaS, le Web et les e-mails, répondant aux besoins du NIST en matière de gestion intégrée de la sécurité.
- → **Contrôles de conformité automatisés –** Les politiques préconstruites et personnalisables pour la protection des données, le contrôle d'accès et la réponse aux incidents sont alignées sur les recommandations du NIST CSF 2.0.
- → **Classification des données basée sur l'IA –** Identifie et catégorise avec précision les données sensibles au repos, en mouvement et en utilisation, réduisant les angles morts de la conformité.

Détection et application basées sur le comportement

- → **Risk-Adaptive Protection –** Utilise des analyses comportementales pour ajuster automatiquement l'application des politiques en fonction des niveaux de risque en temps réel.
- → **Criminalistique et enquêtes sur les incidents –** Fournit des journaux et une analyse détaillés des événements de sécurité et des violations des politiques, aidant les entreprises à renforcer leurs processus de réponse aux incidents.

Flexibilité et évolutivité du déploiement

- → **Options cloud, sur site et hybrides –** Les entreprises peuvent déployer les solutions de Forcepoint en fonction de leurs besoins en infrastructure de sécurité, tout en maintenant la cohérence des politiques.
- → **Gestion évolutive de la sécurité –** À mesure que les besoins en matière de sécurité et de conformité évoluent, Forcepoint permet aux entreprises d'étendre leur protection sans perturbation opérationnelle.

Les solutions de Forcepoint sont conçues pour aider les entreprises à opérationnaliser les directives NIST 2.0, à appliquer les politiques de sécurité à grande échelle et à renforcer leur posture globale de cybersécurité.

Simplifier la conformité pour permettre l'innovation et la croissance

L'alignement sur le NIST CSF 2.0 fournit une approche structurée et basée sur les risques de la cybersécurité, qui aide les entreprises à renforcer la protection des données tout en rationalisant la conformité. La surveillance continue et les contrôles adaptatifs réduisent les risques de perte de données et de violation, en identifiant de manière proactive les vulnérabilités avant qu'elles ne deviennent des violations de la réglementation.

En intégrant la sécurité moderne des données aux opérations commerciales, les entreprises peuvent activer une collaboration sécurisée, soutenir la transformation numérique et stimuler l'innovation sans compromettre la conformité. Une approche structurée et basée sur les risques renforce la sécurité, optimise les opérations et permet aux entreprises de se concentrer sur la croissance.

Protection des données

L'approche de la sécurité des données en tout lieu de Forcepoint protège les informations sensibles sur tous les canaux d'accès clés, en unifiant l'application de la sécurité et en simplifiant la gestion.

SOLUTIONS DE SÉCURITÉ DES DONNÉES FORCEPOINT
Forcepoint Data Loss Prevention (sur site / hybride / cloud) – Terminal, réseau, découverte, e-mail, applications SaaS, Web
Forcepoint DSPM (Data Security Posture Management, sur site / cloud)
Forcepoint Risk-Adaptive Protection (sur site / cloud)

Protection réseau

Les solutions de sécurité de Forcepoint offrent une protection complète sur les réseaux, les applications cloud, les e-mails et le Web pour prévenir la perte de données, contrôler l'accès et assurer la conformité.

SOLUTIONS RÉSEAU DE FORCEPOINT
Forcepoint (CASB et ZTNA)
Forcepoint Web Security (sur site / hybride / cloud)
Forcepoint Email Security (sur site / cloud)
Forcepoint NGFW et Secure SD-WAN
Forcepoint RBI (Remote Browser Isolation) avec CDR (Content Disarm and Reconstruction)

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
IDENTIFIEZ			
ID.AM-02	Des inventaires des logiciels, des services et des systèmes gérés par l'entreprise sont maintenus	Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent fournir des journaux et des rapports qui peuvent aider les entreprises à comprendre le trafic Web, les applications cloud et l'utilisation des données. Les contrôles des politiques permettent également aux entreprises de déterminer quels sites Web et applications cloud sont appropriés, tout en identifiant ou en bloquant les catégories et les applications cloud inappropriées ou dangereuses.
ID.AM-03	Les représentations des communications réseau autorisées de l'entreprise et des flux de données des réseaux internes et externes sont maintenues	Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent surveiller l'utilisation des réseaux, du Web, du cloud et des applications privées pour les réseaux/appareils gérés et non gérés. Grâce aux contrôles des politiques, les solutions de Forcepoint peuvent identifier ou bloquer l'accès à ces destinations en fonction des risques, de la conformité ou même de la perte de productivité.
ID.AM-04	Les inventaires des services fournis par les fournisseurs sont maintenus	Solutions Réseau de Forcepoint	Forcepoint CASB, Web Security et NGFW peuvent également détecter, gérer et bloquer le trafic, ainsi que l'accès aux sites externes et aux applications SaaS gérées et non gérées. En outre, Forcepoint NGFW peut surveiller la santé des services.
ID.AM-05	Les actifs sont hiérarchisés en fonction de la classification, de la criticité, des ressources et de l'impact sur la mission	Solutions de sécurité des données Forcepoint	Forcepoint aide à classifier, à identifier et à hiérarchiser les données pour leur protection grâce à Forcepoint DSPM, à Forcepoint Classification, à Data Detection and Response (DDR), à Enterprise DLP et à Risk-Adaptive Protection (RAP). Les solutions de réseau de Forcepoint peuvent également appliquer des règles de qualité de service et une surveillance de la santé.
ID.AM-07	Des inventaires de données et de métadonnées correspondantes pour les types de données désignés sont maintenus	Solutions de sécurité des données Forcepoint	Forcepoint permet aux entreprises de découvrir, d'inventorier et d'étiqueter les données au sein de l'environnement, y fournit la possibilité de tenir un registre des données et des parties responsables.
ID.AM-08	Les systèmes, le matériel, les logiciels, les services et les données sont gérés tout au long de leur cycle de vie	Forcepoint Data Security	Forcepoint DSPM + DDR surveille en permanence les données tout au long de leur cycle de vie pour les classifier et les re-classifier au fur et à mesure qu'elles changent, en suivant la lignée et même en signalant les données ROT à la fin de leur cycle de vie.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
IDENTIFIEZ			
ID.RA-01	Les vulnérabilités des actifs sont identifiées, validées et enregistrées	Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent identifier les risques pour les sites Web en temps réel et appliquer les scores de risque pour les applications cloud. Forcepoint offre un aperçu des raisons pour lesquelles ces ressources cloud sont risquées, avec des notifications à l'écran ou une messagerie dans la console. En outre, \ Forcepoint NGFW IPS/Inspection évaluent les vulnérabilités en dehors des canaux Web standard.
ID.RA-02	Les informations sur les cybermenaces proviennent de forums et de sources de partage d'informations	Solutions Réseau de Forcepoint	Les solutions de Forcepoint intègrent des flux de menaces provenant de diverses sources, ainsi que nos propres équipes dédiées qui recherchent et analysent les cybermenaces. Ces informations sont alimentées dans notre ACE (Advanced Classification Engine) et, conjointement, dans notre réseau ThreatSeeker Intelligence, utilisé pour aider à identifier et à bloquer les cybermenaces avec nos solutions. Grâce à ces informations, les entreprises peuvent également créer des catégories personnalisées pour les solutions de Forcepoint Web Security.
ID.RA-03	Les menaces internes et externes à l'entreprise sont identifiées et enregistrées	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Toute menace détectée ou bloquée par les solutions Forcepoint est journalisée et enregistrée. Les entreprises peuvent utiliser ces informations pour identifier la source, la destination et d'autres détails associés à l'événement.
ID.RA-04	Les impacts potentiels et les probabilités de menaces exploitant les vulnérabilités sont identifiés et enregistrés	Solutions Réseau de Forcepoint	Toute cybermenace que Forcepoint identifie et bloque est journalisée et enregistrée. En outre, Forcepoint met à jour quotidiennement ses moteurs de détection des menaces. D'autres solutions de Forcepoint, telles que Remote Browser Isolation, Content Disarm and Reconstruction et Advanced Malware Detection, sont conçues pour identifier et arrêter les menaces zero-day.
ID.RA-05	Les menaces, les vulnérabilités, les probabilités et les impacts sont utilisés pour comprendre les risques inhérents et pour orienter la hiérarchisation des réponses aux risques	Solutions Réseau de Forcepoint	Pour toute cybermenace détectée/bloquée par Forcepoint, des journaux disponibles permettent aux entreprises de comprendre la source et le type de menace. En outre, les menaces sont classées par niveau de gravité en fonction de leur type.
ID.RA-06	Les réponses aux risques sont choisies, hiérarchisées, planifiées, suivies et communiquées	Solutions Réseau de Forcepoint	Forcepoint y aide en fournissant des informations et un suivi en fonction de la menace détectée ou bloquée, en fournissant des informations telles que la source, la destination, le type de menace, etc.
ID.RA-07	Les changements et les exceptions sont gérés, évalués pour l'impact sur les risques, enregistrés et suivis		Toute modification de configuration dans les solutions Forcepoint est enregistrée afin que les entreprises puissent examiner et réimplémenter les politiques en fonction de leur évaluation. En outre, Forcepoint prend en charge un cadre de flux de travail et une API bidirectionnelle pour intégrer des solutions tierces de gestion des tickets.
ID.RA-09	L'authenticité et l'intégrité du matériel et des logiciels sont évaluées avant leur acquisition et leur utilisation		Forcepoint fournit des hachages pour tous les fichiers logiciels téléchargeables publiés.
ID.RA-10	Les fournisseurs critiques sont évalués avant l'acquisition	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint peut partager toutes les informations relatives aux produits que nous offrons, par exemple, la façon de les administrer ainsi que tous les détails concernant le contrat.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
IDENTIFIEZ			
ID.IM-02	Les améliorations sont identifiées à partir de tests et d'exercices de sécurité, y compris ceux effectués en coordination avec les fournisseurs et des tiers pertinents		Les solutions de Forcepoint fournissent des détails concernant les cybermenaces ou les événements de sécurité des données. Les rapports générés à partir de ces informations peuvent aider les entreprises à déterminer les domaines qui doivent être améliorés.
ID.IM-03	Les améliorations sont identifiées à partir de l'exécution des processus, des procédures et des activités opérationnels		Les solutions de Forcepoint fournissent des détails concernant les cybermenaces ou les événements de sécurité des données. Les rapports générés à partir de ces informations peuvent aider les entreprises à déterminer les domaines qui doivent être améliorés.

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
PROTÉGER			
PR.AA-01	Les identités et les informations d'identification sont gérées pour les appareils et les utilisateurs autorisés	Solutions de sécurité des données Forcepoint	Indirectement impliqué, Forcepoint aide à limiter les interactions avec les données sensibles qui quittent l'environnement avec Enterprise DLP et DLP for Email. En outre, Forcepoint CASB peut offrir un accès conditionnel pour les applications SaaS en fonction de l'authentification SAML SSO.
PR.AA-02	Les identités sont vérifiées et liées à des informations d'identification en fonction du contexte des interactions	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint fournissent des journaux d'activité détaillés qui peuvent aider les entreprises à identifier les utilisateurs ou les systèmes qui exécutent des actions. Avec Risk-Adaptive Protection, les informations d'identification sont liées au contexte des utilisateurs locaux, des systèmes et des actions de données.
PR.AA-03	Les utilisateurs, les services et le matériel sont authentifiés	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint mettent en œuvre des méthodes Zero Trust pour authentifier les utilisateurs. En outre, les connexions à Active Directory, à l'authentification unique et aux services d'authentification multi-facteur sont utilisées.
PR.AA-04	Les assertions d'identité sont protégées, transmises et vérifiées	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint qui utilisent un SSO SAML 2.0 ou une authentification par l'intermédiaire de systèmes fédérés respectent les normes de l'industrie.
PR.AA-05	Les autorisations, les droits et les autorisations d'accès sont définis dans une politique, gérés, appliqués et examinés, et intègrent les principes du moindre privilège et de la séparation des tâches	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les entreprises peuvent utiliser Forcepoint pour restreindre l'accès aux ressources Web, aux applications privées, aux données et aux réseaux. . En outre, les solutions de Forcepoint offrent des contrôles d'accès basés sur les rôles qui peuvent interdire l'accès à des zones des solutions. En fonction du rôle, les utilisateurs peuvent avoir accès pour créer/modifier des contrôles de politique, exécuter des rapports et gérer la configuration de l'infrastructure ou de la plateforme.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
PROTÉGER			
PR.AT-01	Le personnel est sensibilisé et formé afin de posséder les connaissances et les compétences nécessaires pour effectuer des tâches générales en tenant compte des risques de cybersécurité	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent fournir une messagerie sur mesure pour la formation. Cette forme de coaching des utilisateurs peut permettre aux entreprises d'être plus conscientes des menaces potentielles de cybersécurité.
PR.AT-02	Les personnes occupant des rôles spécialisés reçoivent une sensibilisation et une formation afin de posséder les connaissances et les compétences nécessaires pour effectuer des tâches pertinentes en tenant compte des risques de cybersécurité	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint exige que nos partenaires suivent notre formation sur les produits et encourage les utilisateurs de nos solutions à les suivre aussi. Forcepoint fournit également de nombreux articles, des vidéos pratiques et de la documentation pour fournir des compétences et des connaissances aux utilisateurs de nos solutions.
PR.DS-01	La confidentialité, l'intégrité et la disponibilité des données au repos sont protégées	Solutions de sécurité des données de Forcepoint	Forcepoint peut découvrir et classifier les données au repos avec Forcepoint DSPM. Les solutions sont capables de fournir cette capacité aux ressources sur site et dans le cloud, tout en étant une solution déployée hybride.
PR.DS-02	La confidentialité, l'intégrité et la disponibilité des données en transit sont protégées	Solutions de sécurité des données Forcepoint	Forcepoint DLP peut protéger les données sensibles en transit sur les ressources Web telles que les sites Web, le cloud et les applications personnalisées, les e-mails et les terminaux. Les solutions sont capables de fournir cette capacité pour les ressources sur site et dans le cloud, tout en étant une solution déployée hybride.
PR.DS-10	La confidentialité, l'intégrité et la disponibilité des données utilisées sont protégées	Solutions de sécurité des données Forcepoint	Forcepoint DLP protège les données sensibles en empêchant l'exfiltration non autorisée des données coupées/copiées/collées, des applications accédant aux fichiers, de l'impression, des supports amovibles et des e-mails. Les contrôles d'application de la DLP sont actifs, quel que soit l'endroit où se trouve la machine de l'utilisateur. Les contrôles sont actifs sur site et à distance. Les solutions sont capables de fournir cette capacité pour les ressources sur site et dans le cloud, tout en étant une solution déployée hybride.
PR.PS-01	Les pratiques de gestion de la configuration sont établies et appliquées	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint disposent de contrôles prédéfinis qui peuvent permettre aux entreprises d'appliquer les meilleures pratiques pour les contrôles réseau et les besoins de sécurité des données. Ces politiques prédéfinies permettent aux entreprises de déployer rapidement des contrôles de sécurité pour l'environnement.
PR.PS-04	Des journaux sont générés et mis à disposition pour une surveillance continue	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les entreprises peuvent utiliser les solutions Forcepoint pour surveiller l'activité des utilisateurs sur différents canaux, pour s'assurer qu'ils sont conformes aux politiques de l'entreprise. Cela inclut les canaux réseau et les canaux d'exfiltration des données. Forcepoint DLP conserve les enregistrements de données criminalistiques pour les futurs audits.
PR.PS-05	L'installation et l'exécution de logiciels non autorisés sont empêchées	Solutions Réseau de Forcepoint	Forcepoint peut empêcher le téléchargement de charges utiles potentiellement malveillantes, en empêchant de manière proactive leur exécution sur la machine de l'utilisateur.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
PROTÉGER			
PR.IR-01	Les réseaux et les environnements sont protégés de l'accès et de l'utilisation logiques non autorisés	Solutions Réseau de Forcepoint	Les solutions de réseau de Forcepoint peuvent empêcher les utilisateurs d'accéder à des catégories spécifiques d'applications Web et cloud, et peuvent détecter et empêcher le trafic entrant/sortant vers les réseaux, en plus du trafic est-ouest via SD-WAN/NGFW.
PR.IR-02	Les actifs technologiques de l'entreprise sont protégés des menaces environnementales	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions Forcepoint peuvent être déployées dans des configurations à haute disponibilité pour se conformer aux plans de reprise après sinistre.
PR.IR-03	Des mécanismes sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions cloud de Forcepoint disposent de mécanismes pour maintenir la disponibilité. Pour tout déploiement sur site, Forcepoint recommande la haute disponibilité et les déploiements hybrides.

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
DÉTECTER			
DE.CM-01	Les réseaux et les services réseau sont surveillés pour détecter les événements potentiellement indésirables	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint surveille le trafic Web et réseau pour détecter la perte de données potentielle, le trafic réseau malveillant général et la surveillance des menaces internes via Risk-Adaptive Protection et Forcepoint Insider Threat.
DE.CM-03	L'activité du personnel et l'utilisation de la technologie sont surveillées pour détecter les événements potentiellement indésirables	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent surveiller l'activité des utilisateurs grâce à un calcul des risques en temps réel pour surveiller les événements liés au réseau et aux données. En outre, Forcepoint Risk-Adaptive Protection peut surveiller l'activité des utilisateurs grâce à des calculs des risques en temps réel pour plus de 130 indicateurs de comportement.
DE.CM-06	Les activités et les services des fournisseurs de services externes sont surveillés pour détecter les événements potentiellement indésirables	Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent surveiller l'activité des utilisateurs et les applications de la solution grâce à un calcul des risques en temps réel pour surveiller les événements liés au réseau et aux données. En outre, les contrôles de Forcepoint, tels que ZTNA, peuvent aider à surveiller les connexions externes aux applications internes pour identifier et bloquer les événements potentiellement indésirables.
DE.CM-09	Le matériel et les logiciels informatiques, les environnements d'exécution et leurs données sont surveillés pour détecter les événements potentiellement indésirables	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint calculent des risques en temps réel pour surveiller les événements liés au réseau et aux données. Les solutions de surveillent/bloquent l'exfiltration des données et le trafic réseau pour déterminer si les événements sont indésirables en fonction des contrôles des politiques établis.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
DÉTECTER			
DE.AE-02	Les événements potentiellement indésirables sont analysés pour mieux comprendre les activités associées	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint fournit des détails sur les incidents qui peuvent aider à déterminer si un événement est indésirable ou non en permettant aux équipes SOC de disposer de détails et d'analyses approfondis des journaux.
DE.AE-03	Les informations sont corrélées à partir de plusieurs sources	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent fournir des rapports centralisés pour aider à consolider les incidents et aider les entreprises à répondre de manière appropriée. En outre, le réseau ThreatSeeker est capable de corréler entre tous les déploiements de Forcepoint pour aider à identifier les menaces.
DE.AE-04	L'impact et la portée estimés des événements indésirables sont compris	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint peuvent fournir de riches détails sur les incidents ainsi que des classements de gravité et de risque pour aider les entreprises à comprendre l'impact.
DE.AE-06	Les informations sur les événements indésirables sont fournies au personnel et aux outils autorisés	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint fournissent des informations détaillées sur les événements qui peuvent être contrôlés pour la consultation par RBAC. Lorsque Forcepoint détecte un incident, des alertes peuvent être générées pour être envoyées aux équipes appropriées par des alertes de tableau de bord, par e-mail et par une intégration à des outils tiers (par exemple, SIEM, systèmes de billetterie).
DE.AE-07	Les informations sur les cybermenaces et d'autres informations contextuelles sont intégrées à l'analyse	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les politiques de Forcepoint utilisent des analyses contextuelles et des intégrations à d'autres flux (par exemple, SIEM, flux de renseignements tiers) pour identifier les événements à risque ou identifier et bloquer les actions d'exfiltration des données.
DE.AE-08	Les incidents sont déclarés lorsque les événements indésirables répondent aux critères d'incidents définis	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint fournit des détails sur les incidents basés sur des contrôles de politique établis violés pour aider les entreprises dans le processus de déclaration.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
INTERVENIR			
RS.MA-01	Le plan de réponse aux incidents est exécuté en coordination avec les tiers concernés une fois qu'un incident est déclaré	Solutions de sécurité des données de Forcepoint Solutions Réseau de Forcepoint	Les politiques de Forcepoint offrent des actions proactives et réactives qui s'alignent sur les plans de réponse aux incidents de l'entreprise. L'API bidirectionnelle aide également aux flux de travail de réponse aux incidents avec des solutions tierces.
RS.MA-02	Les rapports sur les incidents sont triés et validés	Solutions de sécurité des données de Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint fournissent une gestion et des rapports centralisés pour aider à trier et à enquêter sur les menaces.
RS.MA-03	Les incidents sont catégorisés et hiérarchisés	Solutions de sécurité des données de Forcepoint Solutions Réseau de Forcepoint	Les incidents de Forcepoint peuvent être triés en fonction de la source, de la gravité, de la politique, etc. La hiérarchisation peut être basée sur le plus récent, le plus grand degré de gravité, le score de risque le plus élevé, etc.
RS.MA-04	Les incidents sont intensifiés ou élevés en fonction des besoins	Solutions de sécurité des données de Forcepoint Solutions Réseau de Forcepoint	Forcepoint fournit des informations détaillées sur les incidents avec des niveaux de gravité / scores de risque qui peuvent aider à prioriser les incidents / les cas à remonterà la hiérarchie.
RS.MA-05	Les critères d'initiation de la reprise des incidents sont appliqués	Solutions de sécurité des données de Forcepoint Solutions Réseau de Forcepoint	Forcepoint peut fournir des informations détaillées sur un incident qui peut contribuer aux processus de reprise des incidents.
RS.AN-03	Une analyse est effectuée pour établir ce qui s'est passé lors d'un incident et la cause première de l'incident	Solutions de sécurité des données de Forcepoint Solutions Réseau de Forcepoint	Forcepoint peut fournir des informations détaillées sur un incident, en incluant la source, la destination, le canal et les règles violées, ainsi que des informations scientifiques sur les événements de sécurité des données détectés.
RS.AN-06	Les actions effectuées lors d'une enquête sont enregistrées, et l'intégrité et la provenance des enregistrements sont préservées	Solutions de sécurité des données de Forcepoint Solutions Réseau de Forcepoint	Forcepoint conserve une piste d'audit des activités administratives ainsi que des détails des incidents judiciaires, qui peuvent être conservés dans un emplacement crypté.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
INTERVENIR			
RS.AN-07	Les données et les métadonnées des incidents sont collectées, et leur intégrité et leur provenance sont préservées	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les solutions de Forcepoint collectent et stockent les informations sur les incidents judiciaires qui sont stockées dans une réserve cryptée.
RS.AN-08	L'ampleur d'un incident est estimée et validée	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint fournit des informations détaillées sur les incidents avec des niveaux de gravité / scores de risque qui peuvent aider à prioriser les incidents / les cas à remonter à la hiérarchie.
RS.CO-02	Les parties prenantes internes et externes sont informées des incidents	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint peut fournir des informations sur les incidents et envoyer des alertes aux parties désignées. Avec Forcepoint DSPM, le registre des actifs peut informer les différents propriétaires de données des détections et des changements dans la classification ou le risque des données dont ils sont responsables.
RS.CO-03	Les informations sont partagées avec des parties prenantes internes et externes désignées	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les politiques de Forcepoint utilisent des analyses contextuelles et des intégrations à d'autres flux (par exemple, SIEM, flux de renseignements tiers) pour identifier les événements à risque ou identifier et bloquer les actions d'exfiltration des données.
RS.MI-01	Les incidents sont contenus Forcepoint	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les politiques de Forcepoint offrent des actions proactives et réactives qui s'alignent sur les plans de réponse aux incidents de l'entreprise. Forcepoint DLP peut bloquer/mettre en quarantaine automatiquement les données pour empêcher l'exfiltration.
RS.MI-02	Les incidents sont éradiqués Forcepoint	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Les politiques de Forcepoint offrent des actions proactives et réactives qui s'alignent sur les plans de réponse aux incidents de l'entreprise.

Les solutions de Forcepoint cartographiées au NIST CSF 2.0

FONCTION ET SOUS-CATÉGORIE	DESCRIPTION	PRODUITS FORCEPOINT	VALEUR
RÉCUPÉRER			
RC.RP-01	La partie de récupération du plan de réponse aux incidents est exécutée une fois lancée à partir du processus de réponse aux incidents	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	L'examen des incidents et des réponses de Forcepoint DLP peut être intégré aux plans de reprise et d'amélioration de l'entreprise.
RC.RP-06	La fin de la reprise des incidents est déclarée en fonction de critères, et la documentation liée aux incidents est achevée	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint peut aider les entreprises dans ce processus en fournissant les détails des incidents.
RC.CO-04	Les mises à jour publiques sur la reprise des incidents sont partagées à l'aide de méthodes et de messagerie approuvées	Solutions de sécurité des données Forcepoint Solutions Réseau de Forcepoint	Forcepoint peut aider les entreprises en fournissant les détails des incidents sur une violation détectée par les solutions Forcepoint afin qu'une mise à jour et un message puissent être effectués.

forcepoint.com/contact