CATO
NETWORKS

Les PME face aux organisations cyber criminelles

Comment agir?

Protéger votre PME face aux cybermenaces n'est plus une option.

Voici un guide pour vous aider à relever ce défi.

Préambule

« J'ai souhaité écrire ce livre blanc pour sensibiliser les PME aux risques cyber, mais surtout avec l'objectif de dire aux dirigeants des PME françaises que l'accès aux technologies de pointe n'est plus réservé uniquement aux grands groupes disposant de moyens humains, techniques et financiers énormes. C'est l'une des raisons qui m'a incité à rejoindre la société Cato Networks, dont le fondateur rêve d'offrir le meilleur de la cybersécurité à n'importe quelle entreprise privée ou publique. Cela implique une approche simple, rapide, efficace et économiquement accessible.»

Adrien Porcheron,

Country Manager chez Cato Networks.

Pourquoi devons-nous nous préoccuper des PME ?

Les PME représentent une part essentielle de l'économie française. **Elles constituent 99,9% des entreprises en France et emploient 45,5% des salariés** (source Ministère du travail).

99,9%

des entreprises en France

45,5%

des salariés

Leur rôle est crucial dans la création d'emplois, l'innovation et la croissance économique. Cependant, leur vulnérabilité aux cyberattaques peut avoir des conséquences dévastatrices non seulement pour elles-mêmes mais aussi pour l'économie nationale.

Les PME françaises ne disposent que très rarement des moyens humains, techniques et financiers des ETI ou des grands groupes. Pourtant, elles ont les mêmes enjeux. De ce fait, les PME les plus vulnérables se retrouvent à risque et deviennent la cible privilégiée des groupes cybercriminels organisés.

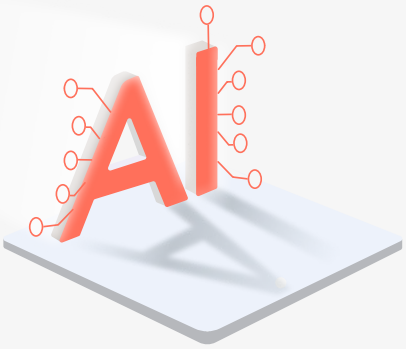
Le monde change et les PME doivent prendre conscience de la gravité des cybermenaces et adopter des mesures de cybersécurité robustes pour se protéger efficacement. Il n'y a plus de doute quant au fait que l'espace numérique est devenu le nouvel eldorado des pirates du web.

Pour comprendre les enjeux il faut saisir l'ampleur des Cybermenaces

Les PME en France sont particulièrement vulnérables aux cyberattaques, et les statistiques montrent une tendance inquiétante. Voici des chiffres clés qui illustrent l'ampleur de la menace.

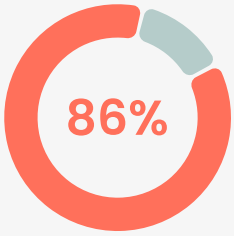
Le temps entre l'infiltration des assaillants dans le système d'information et de l'exfiltration des données est passé de **10 jours en 2021 à quelques minutes en 2025**.

La volumétrie d'attaque a été multipliée par **100 en 3 ans**. Le nombre de nouvelles attaques et de nouveaux scénarios d'attaques non reconnues par les systèmes de sécurité traditionnels (attaques de type Zero Day) est en constante augmentation, on observe en moyenne **plus de 2 millions de nouvelles attaques créées par jour.**



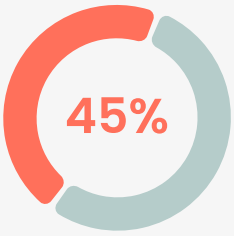
La barrière à l'entrée pour les organisations criminelles est devenue anecdotique. **La majorité des attaques sont produites par des moteurs d'IA qui vont élaborer des nouvelles combinaisons**, des nouveaux scénarios pour contourner les défenses des équipements traditionnels qui sont impuissants face à cette vague gigantesque et imprévisible.

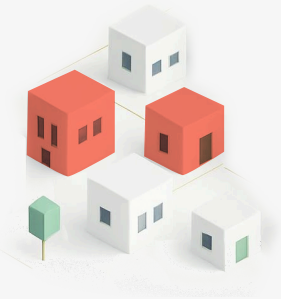
PME victimes de cyberattaques en quelques chiffres



330 000 PME ont été victimes de cyberattaques en 2022. Cela représente 86% des 385 000 cyberattaques subies par les entreprises françaises cette même année.

Encore 45% des entreprises françaises ont subi au moins une cyberattaque réussie au cours de l'année 2024 (selon l'enquête du CESIN).





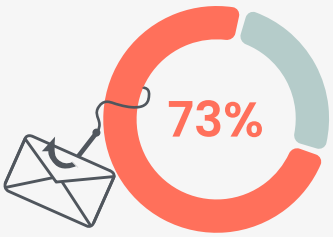
2 PME sur 5 sont touchées par une attaque de type Rançongiciels.

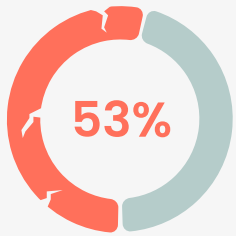
- 59% arrivent à récupérer leurs données.
- 1 entreprise sur 3 paie la Rançon et subit une nouvelle attaque dans les 12 mois.

Types de cyberattaques courantes

Les cyberattaques peuvent prendre plusieurs formes, mais certaines sont particulièrement fréquentes :

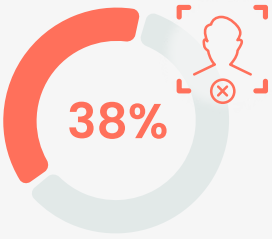
Phishing: 73% des entreprises concernées ont été victimes de tentatives de phishing. Cette méthode consiste à tromper les employés pour qu'ils divulguent des informations sensibles.





Exploitation de failles: 53% des entreprises ont subi des attaques exploitant des vulnérabilités dans leurs systèmes.

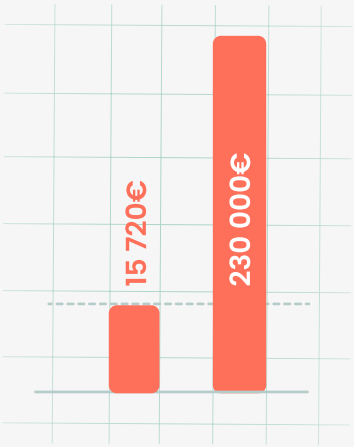
Arnaque au président: 38% des entreprises ont été ciblées par des attaques où les cybercriminels se font passer pour des dirigeants pour obtenir des transferts d'argent.



Impact économique des cyberattaques

Les conséquences financières des cyberattaques peuvent être dévastatrices :

- Les pertes financières moyennes par cyberattaque s'élèvent à environ **15 720€**.
- Une entreprise sur huit rapporte des coûts dépassant les **230 000€**.
- Les interruptions d'activité, la perte de confiance des clients et les dommages à la réputation sont des impacts courants.



Réactions des entreprises

Face à ces menaces, les entreprises prennent des mesures pour renforcer leur sécurité :

- **70%** des entreprises ont prévu d'augmenter leur budget consacré à la cybersécurité.
- **56%** des entreprises envisagent d'embaucher des spécialistes supplémentaires.

Ces chiffres (sources : ANSI, Cigref, CESIN) montrent l'importance cruciale de la cybersécurité pour les PME en France. Les cyberattaques peuvent avoir des impacts dévastateurs sur l'économie et la stabilité des entreprises. Il est essentiel que les PME prennent des mesures proactives pour se protéger contre ces menaces.

Les cyberattaques, de plus en plus fréquentes et sophistiquées, représentent une menace constante pour les PME. L'exemple du groupe de cybercriminels LockBit, responsable de près d'un tiers des attaques par ransomware détectées en 2022, illustre parfaitement l'ampleur du problème. Ce groupe a été impliqué dans 846 attaques, soit une augmentation de 94% par rapport à l'année précédente. L'un des défis majeurs est de pouvoir contrôler les angles morts et faire face à l'ensemble des nouvelles vulnérabilités « les attaques Zero Day ».

Quels sont les enjeux pour la France dans notre contexte géopolitique?

La cybersécurité est devenue un enjeu stratégique majeur dans le contexte géopolitique actuel. Les cyberattaques peuvent être utilisées comme des armes de déstabilisation par des acteurs étatiques ou non étatiques. La France doit renforcer ses capacités de cyberdéfense pour protéger ses infrastructures critiques, ses entreprises et sa souveraineté nationale.

Les tensions géopolitiques, comme celles observées entre la Russie et l'Ukraine, montrent l'importance de la résilience cybernétique pour la sécurité nationale.

Pourquoi les entreprises doivent réagir?

Ces attaques ont des conséquences dévastatrices, tant sur le plan financier qu'opérationnel, pouvant aller jusqu'à l'arrêt total des activités.

Les entreprises doivent réagir pour plusieurs raisons :

- **Protection des données:** Les cyberattaques peuvent entraîner des fuites de données sensibles, affectant la confidentialité et la réputation des entreprises
- **Continuité des activités:** Les interruptions causées par les cyberattaques peuvent paralyser les opérations et entraîner des pertes financières importantes
- **Conformité réglementaire:** Les entreprises doivent se conformer aux réglementations en matière de protection des données, comme le RGPD et NIS2, sous peine de sanctions.
- **Confiance des clients:** La sécurité des données est essentielle pour maintenir la confiance des clients et des partenaires commerciaux.

En outre, l'impact opérationnel ne doit pas être sous-estimé. Les cyberattaques peuvent perturber les processus internes, paralyser les systèmes d'information et même interrompre complètement les activités, affectant la productivité, les chaînes d'approvisionnement, le service client et l'image de l'entreprise.

L'impact économique d'une cyberattaque ne se limite pas à une rançon potentielle ou à une fuite de données. Les frais de remédiation, les pertes de chiffre d'affaires, les dommages à la réputation, les pénalités réglementaires et la perte de confiance des clients peuvent faire grimper la facture à des niveaux sans précédent.

Face à cette menace omniprésente et en constante évolution, il est crucial pour les entreprises de toutes tailles de se doter des meilleurs outils pour protéger leurs systèmes d'information. C'est un enjeu vital pour leur pérennité et leur développement.

Feuille de route du décideur en 12 étapes et 12 mois

Mois 1

Cartographier

Comprendre votre environnement technologique est la première étape cruciale vers une meilleure sécurité de votre système d'information.

Vous devez savoir quels types de données votre entreprise manipule, où ces données sont stockées et qui y a accès. La cartographie des actifs de votre entreprise, y compris les données sensibles et le matériel informatique, vous aide à évaluer leur niveau de sensibilité et à mettre en place des mesures de protection appropriées.

Cette compréhension approfondie de votre environnement informatique est la base sur laquelle vous pouvez bâtir une stratégie de sécurité globale solide.

Mois 2

Évaluer

Réaliser un audit de sécurité pour identifier les vulnérabilités. Une fois que vous avez une vue claire de votre environnement, l'étape suivante est de l'évaluer pour identifier les vulnérabilités potentielles.

Un audit de sécurité informatique est un processus systématique qui examine et teste votre système d'information pour découvrir les failles qui pourraient être exploitées par des attaquants.

L'audit peut déceler des problèmes tels que les configurations erronées, les logiciels obsolètes et les failles de sécurité dans les applications. Les résultats de l'audit peuvent ensuite guider les efforts pour corriger les vulnérabilités et renforcer la sécurité vers une approche plus moderne et simple à piloter.

Mois 3

Former

Sensibiliser les employés aux bonnes pratiques de cybersécurité. Vos collaborateurs sont votre première ligne de défense.

Malheureusement, ils peuvent aussi être le maillon faible s'ils ne sont pas correctement formés pour reconnaître et gérer les menaces. Une formation en cybersécurité peut aider vos employés à comprendre les risques, à reconnaître les signes d'une attaque possible et à savoir comment réagir.

Une équipe bien formée et consciente des enjeux de la cybersécurité peut être un atout majeur pour la protection de votre entreprise. La formation est un exercice continu, appropriez-vous des campagnes de tests mensuelles et communiquez sur les résultats à vos salariés.

Mois 4

Définir vos critères

Définir les critères de succès pour atteindre vos objectifs en fonction de vos cas d'usages et des résultats d'audit.

Plusieurs services sont indispensables pour construire une barrière efficiente et tendre vers une approche Zero Trust:

- **L'authentification:** L'authentification multi facteur est la base de la sécurité.
- **Contrôle des accès avec des permissions granulaires:** Assurez-vous que les utilisateurs n'ont accès qu'aux applications et aux données dont ils ont besoin pour leur travail. Utilisez des rôles et des permissions pour limiter l'accès.
- **Protection de la navigation internet:** Contrôler l'accès de vos utilisateurs à la navigation sur internet.
- **Supervision des usages:** Pour comprendre et agir il est nécessaire de disposer d'informations pertinentes sur son exposition aux vulnérabilités. Mettez en place des outils de surveillance pour suivre les activités des utilisateurs et détecter les comportements anormaux. Les audits réguliers permettent de s'assurer que les politiques de sécurité sont respectées.

- **Classification des données sensibles:** Identifiez et documentez les services numériques essentiels. Assurez-vous que ces données soient classifiées et accessibles par des personnes accréditées.
- **Shadow IT:** Bien que cela puisse améliorer l'innovation et la productivité, le Shadow IT présente également des risques importants en matière de sécurité et de conformité.
- **Contrôler l'accès aux applications SaaS:** face à l'adoption de nouvelles applications SaaS, il est essentiel de mettre en place des mesures de sécurité robustes et adaptées aux besoins de votre entreprise.
- **Sauvegardes hors-ligne:** Cela consiste à créer des copies de vos données qui ne sont pas connectées à Internet ni au réseau principal de votre entreprise. Suivre la règle du 3-2-1: Conservez trois copies de vos données, stockez deux copies sur des supports différents et gardez une copie hors site. Tester les sauvegardes: Vérifiez régulièrement que vos sauvegardes peuvent être restaurées correctement pour éviter les mauvaises surprises en cas de besoin.

Mois 5

Tester les Solutions

Évaluer les solutions à travers un pilote technique et fonctionnel.

Pour évaluer les solutions à travers un pilote technique et fonctionnel, il est important de suivre une méthodologie structurée qui permet de tester et de valider les différentes options avant de les déployer à grande échelle. Voici quelques étapes clés:

- **Identifier clairement les objectifs** que vous souhaitez atteindre avec le pilote. Cela peut inclure la validation de la faisabilité technique, l'évaluation des performances, la vérification de la compatibilité avec les systèmes existants, et la satisfaction des utilisateurs.

- **Élaborer un cahier des charges fonctionnel et technique:** Rédigez un cahier des charges détaillé qui décrit les fonctionnalités requises, les contraintes techniques, les critères de performance, et les attentes des utilisateurs. Ce document servira de référence tout au long du pilote.
- **Sélectionner les solutions à tester:** Choisissez les solutions qui répondent aux critères définis dans le cahier des charges. Assurez-vous de sélectionner des options variées pour avoir une comparaison complète.
- **Mettre en place l'environnement de tests:** Créez un environnement de test qui simule les conditions réelles d'utilisation. Cela peut inclure des configurations réseau, des applications métiers SaaS/On Premise, des sites existants et bien entendu un panel d'utilisateurs représentatifs.
- **Exécuter les tests techniques:** Testez les solutions sur des aspects techniques tels que la performance, la sécurité, la compatibilité, et la stabilité. Utilisez des outils de monitoring pour collecter des données et analyser les résultats.
- **Évaluer les fonctionnalités:** Vérifiez que les solutions répondent aux besoins fonctionnels définis dans le cahier des charges. Cela peut inclure des tests d'utilisabilité, des démonstrations, et des retours d'utilisateurs.
- **Analyser les résultats:** Comparez les performances des différentes solutions en fonction des critères définis. Identifiez les points forts et les faiblesses de chaque option.
- **Prendre une décision:** sur la base des résultats du pilote, choisissez la solution qui répond le mieux aux objectifs et aux besoins de votre entreprise. Préparez un rapport détaillé pour documenter le processus et les conclusions.

Engager votre projet de modernisation et planifier le déploiement

Une fois la solution choisie, planifiez son déploiement à grande échelle en tenant compte des leçons apprises lors du pilote. Assurez-vous d'avoir des plans de contingence en place pour gérer les éventuels problèmes.

Passer en phase d'exploitation de la solution retenue

Passer en phase d'exploitation de la solution retenue est une étape cruciale qui nécessite une planification minutieuse et une exécution rigoureuse. Voici les étapes clés pour réussir cette transition:

- **Planification détaillée:** Élaborez un plan de déploiement détaillé qui inclut les étapes, les ressources nécessaires, les responsabilités et les échéances.
- **Formation des utilisateurs:** Assurez-vous que les utilisateurs soient formés à l'utilisation de la nouvelle solution. Organisez des sessions de formation et fournissez des documents de support.
- **Paramétrage de la solution:** Configurez la solution selon les besoins spécifiques de votre entreprise. Cela peut inclure la personnalisation des interfaces, des workflows et des permissions.
- **Intégration avec les systèmes existants:** Assurez-vous que la nouvelle solution s'intègre bien avec les autres systèmes en place.
- **Tests de performance:** Effectuez des tests de performance pour garantir que la solution fonctionne correctement sous charge.
- **Validation fonctionnelle:** Vérifiez que toutes les fonctionnalités répondent aux attentes et aux besoins des utilisateurs.
- **Déploiement progressif:** Envisagez un déploiement progressif pour minimiser les risques. Commencez par un groupe pilote avant de généraliser à l'ensemble de l'entreprise.
- **Surveillance et support:** Mettez en place des outils de surveillance pour suivre les performances et détecter les problèmes. Assurez-vous que le support technique est disponible pour résoudre rapidement les incidents.
- **Collecte de feedbacks:** Recueillez les retours des utilisateurs pour identifier les points d'amélioration.
- **Amélioration continue:** Utilisez les feedbacks pour apporter des améliorations et optimiser l'utilisation de la solution.
  En suivant ces étapes, vous pouvez assurer une transition en douceur vers la phase d'exploitation de la solution retenue et maximiser ses bénéfices pour votre entreprise.

Mois 8

Lancer une campagne de pentest.

Le test de pénétration est un exercice de sécurité dans lequel un expert en cybersécurité tente de trouver et d'exploiter les vulnérabilités d'un système informatique. L'objectif de cette simulation est d'identifier les points faibles dans la défense d'un système dont les pirates pourraient tirer profit. Un pentest est la meilleure option pour évaluer sa nouvelle posture de sécurité et peaufiner les règles d'accès aux ressources de l'entreprise.

Mois 9

Définir un plan de gestion de crise

Préparez-vous à la gestion de crise. Il est nécessaire de développer et tester un plan de réponse aux incidents. Testez ce plan régulièrement pour vous assurer de sa pertinence et de sa performance.

Mois 10

Plan de continuité

Planifier la mise en place d'un plan de continuité d'activité

Prévoir un PRA/PCA: Un plan de reprise d'activité (PRA) ou un plan de continuité d'activité (PCA) est essentiel pour minimiser l'impact d'une cyberattaque et assurer la reprise rapide de vos activités.

Tests de pénétration: réalisez des tests de pénétration pour vérifier la robustesse des défenses.

Mois 11

Analyser, réviser et améliorer votre posture

Révision et amélioration: Révisez les mesures de sécurité et apportez des améliorations basées sur les résultats des tests. Documentez les actions menées et les résultats obtenus.

Mois 12

Souscrire à une assurance Cyber

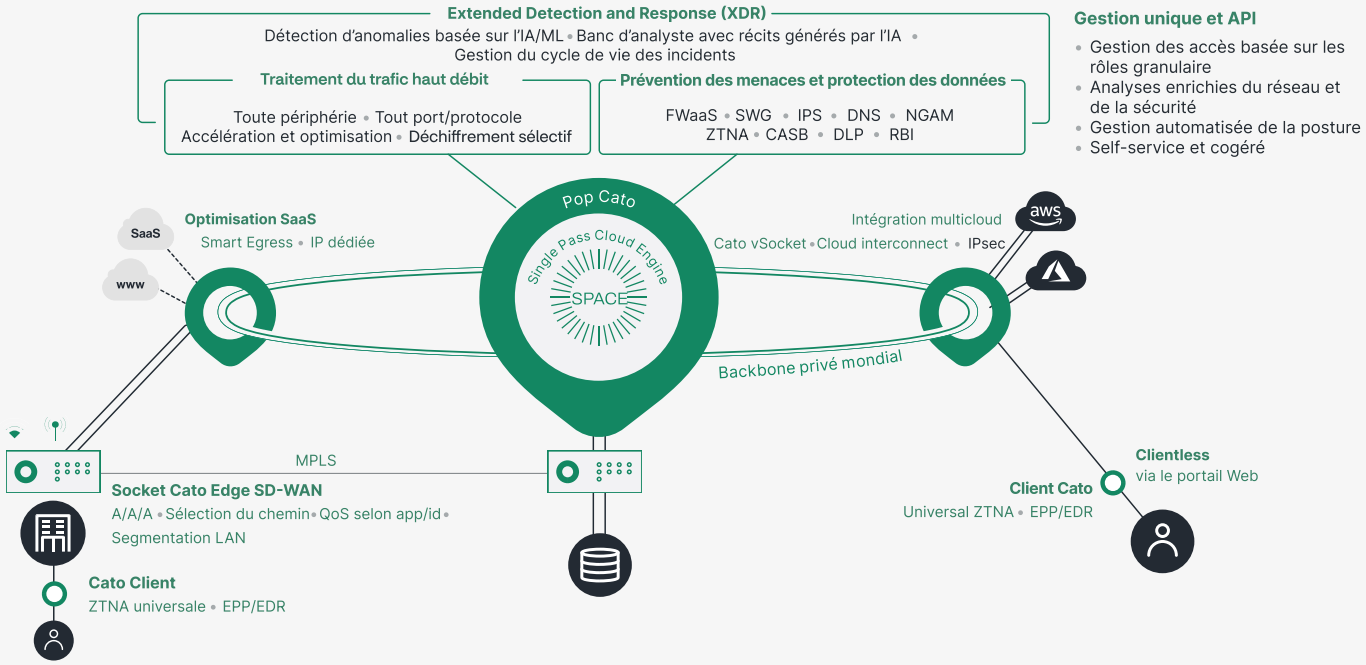
Respecter cette feuille de route peut effectivement améliorer les chances **d'obtenir une cyber assurance de qualité**. Les assureurs, comme AXA, évaluent les mesures de sécurité mises en place par les entreprises pour déterminer leur niveau de risque.

En suivant les étapes de cette feuille de route, les PME peuvent démontrer leur engagement envers la cybersécurité et réduire leur exposition aux cybermenaces, ce qui est favorable pour obtenir une couverture d'assurance optimale.

Comment l'approche Zero Trust de Cato Networks permet d'apporter une réponse fiable, souveraine, autonome avec un coût maîtrisé pour les PME?

Notre mission chez Cato Networks est de simplifier et de rendre transparents les services de Réseau et de Sécurité afin de libérer du temps aux équipes pour se focaliser sur des projets à plus forte valeur ajoutée.

Plusieurs centaines de PME ont choisi Cato Networks pour se protéger des risques de cyberattaque. Voici les principales raisons qui ont poussé ces PME à choisir la plateforme Cato SASE Cloud.



Simplification et transparence

Cato Networks simplifie la gestion des réseaux et de la sécurité en intégrant tous les services dans une plateforme unique, le Cato SASE Cloud. Cela permet aux PME de gérer facilement leurs infrastructures sans avoir à jongler avec plusieurs outils et solutions.

La plateforme offre une sécurité complète avec des fonctionnalités telles que le pare-feu de nouvelle génération (NGFW), la passerelle web sécurisée (SWG), la prévention des intrusions à travers une combinaison de moteurs d'inspection (IPS, DNS, NGAM, UEBA) reposant sur un service de Cyber Threat Intelligent (CTI) intégré dans la souscription, le contrôle d'accès granulaire aux applications (CASB) et aux données (DLP).

Sécurité avancée

Cela garantit que les données et les applications de l'entreprise sont protégées contre les menaces. L'approche Zero Trust de Cato Networks est simple à implémenter et nous intégrons les principes clés pour vous apporter une maitrise complète de cette approche:

- **Vérification forte de l'identité:** Utilisation de l'authentification multi facteur pour vérifier l'identité des utilisateurs.
- **Analyse comportementale:** Surveillance des comportements pour détecter les anomalies et les intrusions potentielles.
- **Micro-segmentation:** Application de contrôles de sécurité granulaires autour de chaque ressource.
- **Contrôles de moindre privilège:** Limitation des privilèges des utilisateurs et des applications pour réduire les risques.
- **Contrôle continu** durant toute la vie de la session utilisateur

Réduction des coûts

En utilisant la combinaison des services de SDWAN, SSE, ZTNA et XDR de Cato, les PME peuvent réduire les coûts associés aux réseaux MPLS et au maintien en condition opérationnelle de différents équipements.

Cato Networks se charge de gérer pour vous les montées de version et les mises à jour, tout en améliorant les performances, la résilience et la sécurité des accès aux ressources. Le backbone privé de Cato Networks permet une connectivité mondiale optimisée, ce qui est particulièrement bénéfique pour les entreprises ayant des sites répartis en France ou à l'international.

Cato Networks permet aux PME de s'adapter rapidement aux changements et de croître sans contraintes. La plateforme cloud native est conçue pour évoluer avec les besoins de l'entreprise, offrant une agilité et une réactivité accrues.

Notre architecture est conçue sur la base d'un backbone privé mondial constitué de plus de 90 POPs autour du monde connectés entre eux pour offrir un réseau full mesh résiliant avec des SLA de 99,999%. Pour assurer une souveraineté au marché français nous avons signé des accords avec des opérateurs nationaux pour intégrer 4 POPs privés sur le territoire.

Flexibilité et évolutivité

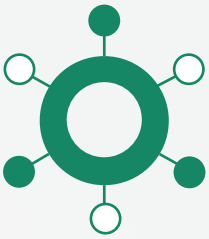
Gestion centralisée

La console de management unifiée de Cato permet de surveiller et de gérer l'ensemble de l'infrastructure réseau et de sécurité à partir d'un seul endroit. Cela simplifie la gestion et améliore la visibilité sur l'état de santé de l'infrastructure.

Le maintien en condition opérationnel est complètement opéré et industrialisé par Cato Networks ce qui permet de tendre vers une sécurité en mode Zero Day.

Que ce soit pour les employés mobiles ou sédentaires, Cato Networks assure un accès sécurisé aux ressources de l'entreprise, qu'elles soient sur site, dans le cloud ou en SaaS. Cela permet aux PME de garantir la sécurité des données tout en facilitant le travail à distance.

Accès sécurisé pour les collaborateurs



Exploitation simplifiée et adaptée à la taille de structures des PME

Cato Networks propose un service XDR (Extended Detection and Response), qui combine les technologies d'EDR (Endpoint Detection and Response) et de NDR (Network Detection and Response), et qui peut être opéré par nos partenaires MSP.

Voici quelques points clés sur les fonctionnalités de Cato XDR

- **Détection et réponse étendues:** Cato XDR offre une visibilité et un contrôle sur les endpoints, les réseaux et les infrastructures cloud. Cela permet de détecter et de répondre rapidement aux menaces potentielles.
- **Intégration des données:** Le service collecte des données brutes à partir de capteurs natifs de la plateforme Cato SASE Cloud, ainsi que des événements provenant de capteurs externes comme les solutions EDR tierces.
- **Algorithmes avancés**: Cato XDR utilise des algorithmes d'IA et de ML pour la chasse aux menaces et la détection des anomalies. Ces algorithmes aident à identifier les menaces dans un vaste lac de données et à les présenter de manière gérable pour l'analyse et la résolution.
- **Réponse rapide:** Les équipes de sécurité peuvent exécuter des actions de remédiation directement depuis la plateforme, comme la mise en place de règles de pare-feu pour contenir les attaques et le déclenchement de scans EPP pour nettoyer les endpoints compromis.

Avantages pour les PME :

- **Efficacité accrue:** En consolidant les outils de sécurité, Cato XDR améliore l'efficacité des équipes de sécurité en réduisant le temps nécessaire pour détecter et remédier aux incidents.
- **Visibilité complète:** La solution offre une vue d'ensemble des activités suspectes et des menaces potentielles, facilitant ainsi la gestion proactive de la sécurité.
- **Gestion centralisée:** Toutes les actions de sécurité peuvent être gérées à partir d'une seule application, simplifiant ainsi la gestion et la coordination des réponses.
- **Conformité et souveraineté:** Pour les entreprises, cela implique de respecter des règles spécifiques concernant la collecte, le stockage, et le traitement des données. Cela signifie également que les données doivent être stockées et traitées dans des juridictions offrant des protections juridiques adéquates.

En résumé, Cato Networks offre une solution complète et intégrée qui répond aux besoins spécifiques des PME en matière de réseau et de sécurité, tout en offrant des avantages en termes de coût, de flexibilité et de gestion.