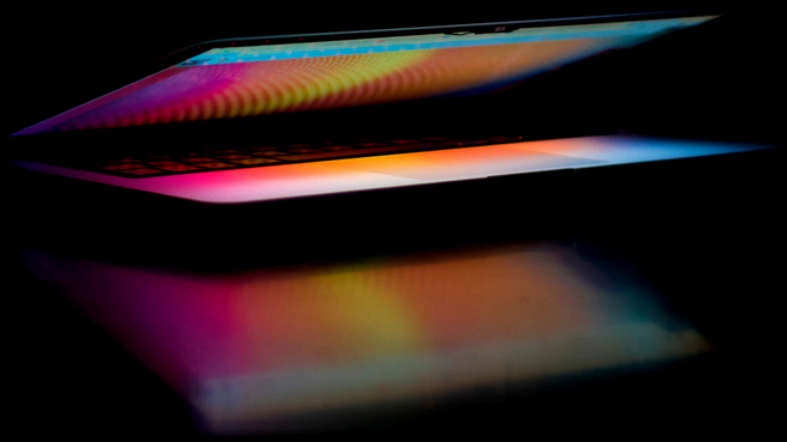
Tableau Comparatif

SAYSE vs FORTINET vs CATO NETWORKS



sayse

A propos de ce document

Comprendre les différences entre WANUP, Fortinet et Cato Networks :

Dans un marché dominé par des acteurs américains bien établis, il peut sembler difficile de distinguer les offres, tant les discours marketing sont rodés et les promesses nombreuses.

C'est pourquoi nous avons conçu ce tableau comparatif objectif. Il vous permet de visualiser les différences majeures entre trois approches du SD-WAN et du SASE :

- WANUP, la solution française éditée par SAYSE,
- Fortinet, pionnier des pare-feu traditionnels,
- Cato Networks, acteur 100 % cloud natif.

Chaque critère a été sélectionné pour refléter les préoccupations réelles des DSI, des RSSI, et des équipes techniques françaises : performance, cybersécurité, simplicité, souveraineté, coût total de possession, résilience...

L'objectif ? Vous aider à faire un choix éclairé, fondé sur les besoins concrets de votre entreprise, et non sur des promesses généralistes.

Comparaison des éditeurs SASE

Fonctionnalités	Sayse (Wanup)	Fortinet (Security Fabric)	Cato Networks (Utopia)
Approche générale	SD-WAN & SASE unifiés, appliances autonomes (centric) avec gestion centralisée (cloud)	Firewall-centric. SD-WAN en option. intégration complexe et modulaire (fortigate, fortisase, fortimanager, fortianalyzer, forticare, …)	Cloud-native avec dépendance à l'infrastructure cloud Cato
Déploiement & Scalabilité	Zero-Touch Provisioning (ZTP), configuration centralisée, modèles applicables en masse, simplification des "objets IP", scalability "one to many touch"	ZTP, configurations spécifiques. Appliances multiples (gamme de modèles) et gestion modulaire des fonctionalités	ZTP, dépendance aux datacenters Cato => complexité d'évolution sur les performances réseau globales par les limites de bande passante
Performance SD-WAN	Optimisées grâce au "local breakout" sur chaque établissement dans le monde, les routages avancés et les modes de QOS automatiques	Dépend des modèles d'appliances locales déployées et de la configuration des QOS	Dépend des PoP Cato et de leurs taux de contention, limitations de bande passante (en standard : 100Mb/s)
Sécurité Intégrée	FWaaS, ZTNA, SWG, IPS/IDS, Toxic IPs, "micro events", AI Vision, intégrés nativement	Firewall local puissant, mais dépend de modules additionnels en option	Sécurité cloud avec filtrage réseau & ZTNA, mais dépendance aux PoP Cato
ZTNA	Nativement intégré, contrôle strict des accès avec politique Zero Trust pour les devices hors du WAN	Nécessite des configurations avancées et client FORTIClient optionnel	Géré dans le cloud avec segmentation stricte
VPN Remote Access	Basé sur des tunnels encryptés WireGuard pour des performances très élevées. Activation "Always-On" pour les télé-travailleurs	IPsec et SSL VPN, configurations complexes et performances limitées par des technologies vieillissantes	VPN Ipsec avec tunnels vers les PoP (cloud) Cato => restriction des performances
Firewall As A Service (FaaS)	Intégré sans option, gestion unifiée	Firewall local robuste, mais nécessite des configurations avancées	Firewall cloud avec filtrage global
IPS/IDS	Intégré nativement, avec détection avancée	Présent sur les appliances haut de gamme ou en option	Fonctionnalité cloud, dépend du routage vers les PoP Cato
Toxic IP's	Filtrage d'IP malveillantes en temps réel via des bases de données agrégées et dynamiques	Peut être configuré via des listes noires uniquement par les clients finaux	Peut être configuré via des listes noires via Gestion centralisée dans le cloud

Comparaison des éditeurs SASE

Fonctionnalités	**Sayse** (Wanup)	**Fortinet** (Security Fabric)	**Cato Networks** (Utopia)
Micro Events (Analyse avancées des signaux faibles)	🟢 Détection des attaques furtives, signaux faibles et des patterns anormaux	🔴 Pas de fonctionnalité spécifique	🔴 Pas de fonctionnalité spécifique
Secure Web Gateway (SWG)	🟢 Filtrage avancé, catégorisation fine, intégré nativement	🔴 Disponible mais nécessite des modules spécifiques optionnels ou intégré dans des packs	🔴 Filtrage cloud, mais dépendance aux PoP Cato
Supervision & Rémédiation	🟢 Interface intuitive avec suggestions de correction et remédiation par AI VISION	🔴 Monitoring via FortiManager, mais pas d'aide à la décision et la rémédiation	🔴 Monitoring cloud Cato, dépendance aux PoP et pas d'aide à la décision et la rémédiation

Glossaire des fonctionnalités

Fonctionnalités	Définitions contractuelles
Local Breakout	Sortie directe vers Internet depuis chaque site, sans concentrateur central.
Full Cloud / Cloud Natif	Architecture basée uniquement sur des nœuds cloud, tous les flux y transitent.
Appliance Autonome	Boîtier capable de traiter localement sans dépendre de la console centrale.
ZTNA (Zero Trust)	Modèle de sécurité qui vérifie systématiquement chaque accès, même en interne.
QoS dynamique	Gestion de la priorité des flux en temps réel selon leur importance métier.
Firewall centric	Approche centrée sur les pare-feu physiques, souvent rigides et complexes.
Cloud Act	Loi américaine autorisant l'accès aux données hébergées par des sociétés US.
Souveraineté numérique	Capacité à garder le contrôle sur ses données et ses infrastructures en Europe.
Taux de contention	Risque de saturation dû à la mutualisation excessive des ressources réseau.
Console centralisée	Interface unique pour gérer le réseau et la cybersécurité de tous les sites.
Micro-événements	Analyse avancée de petits paquets invisibles pouvant signaler des menaces.
Assistance intelligente	Système de supervision avec propositions de remédiation via intelligence artificielle.
Licence tout-en-un	Toutes les fonctions sont incluses dans la licence de base, sans options payantes.
Modèle Carrier Class	Standard de fiabilité élevé, comparable à celui des opérateurs télécoms.

WANUP, une solution pensée pour la performance, sans compromis

SAYSE, en tant qu'éditeur français, propose une solution SD-WAN et SASE conçue pour libérer tout le potentiel de votre réseau.

Ni bridée par le matériel, ni limitée par les licences, ni dépendante d'une architecture cloud centralisée, la solution WANUP s'adapte aux réalités du terrain et aux attentes des entreprises d'aujourd'hui.

Sa conception repose sur un modèle hybride et décentralisé, parfaitement optimisé pour les infrastructures fibre très haut débit — y compris celles bénéficiant de crêtes (burst), fréquentes en Europe.

À l'inverse, ses concurrents ont souvent conçu leurs offres en fonction de standards télécoms plus contraints, issus d'autres marchés.
Avec WANUP, vous bénéficiez d'une liberté technologique, d'une maîtrise budgétaire et d'une souveraineté totale sur votre réseau.

sayse

Prêt à vous sécuriser ?