

snowpack

B E C O M E I N V I S I B L E



Si les hackers ne
vous voient pas,
ils ne vous
attaquent pas!

*Protégez vos utilisateurs, vos
données, vos services web et votre
système d'information
des pirates informatiques !*



#Innovation #Deeptech #Cybersecurité #Europe #Start-up



Spin-off du CEA*
créée en mai 2021

*Siège à Paris-Saclay
Bureaux à Paris & Vienne*

*Technologie basée sur sept années de R&D et
protégée par 4 brevets internationaux*

+2 M€ de financement
d'amorçage en 2022

bpifrance



concours d'innovation
i-Lab

Ecosystème

#cybersecurité #innovation



HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Generate
S'entraîner pour innover

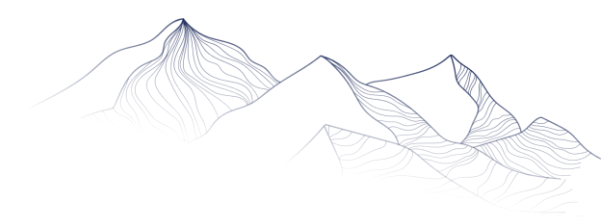


TECH4 TRUST



PÔLE D'EXCELLENCE
CYBER

* Commissariat à l'Énergie Atomique et aux énergies alternatives : plus grand centre français de recherche appliquée

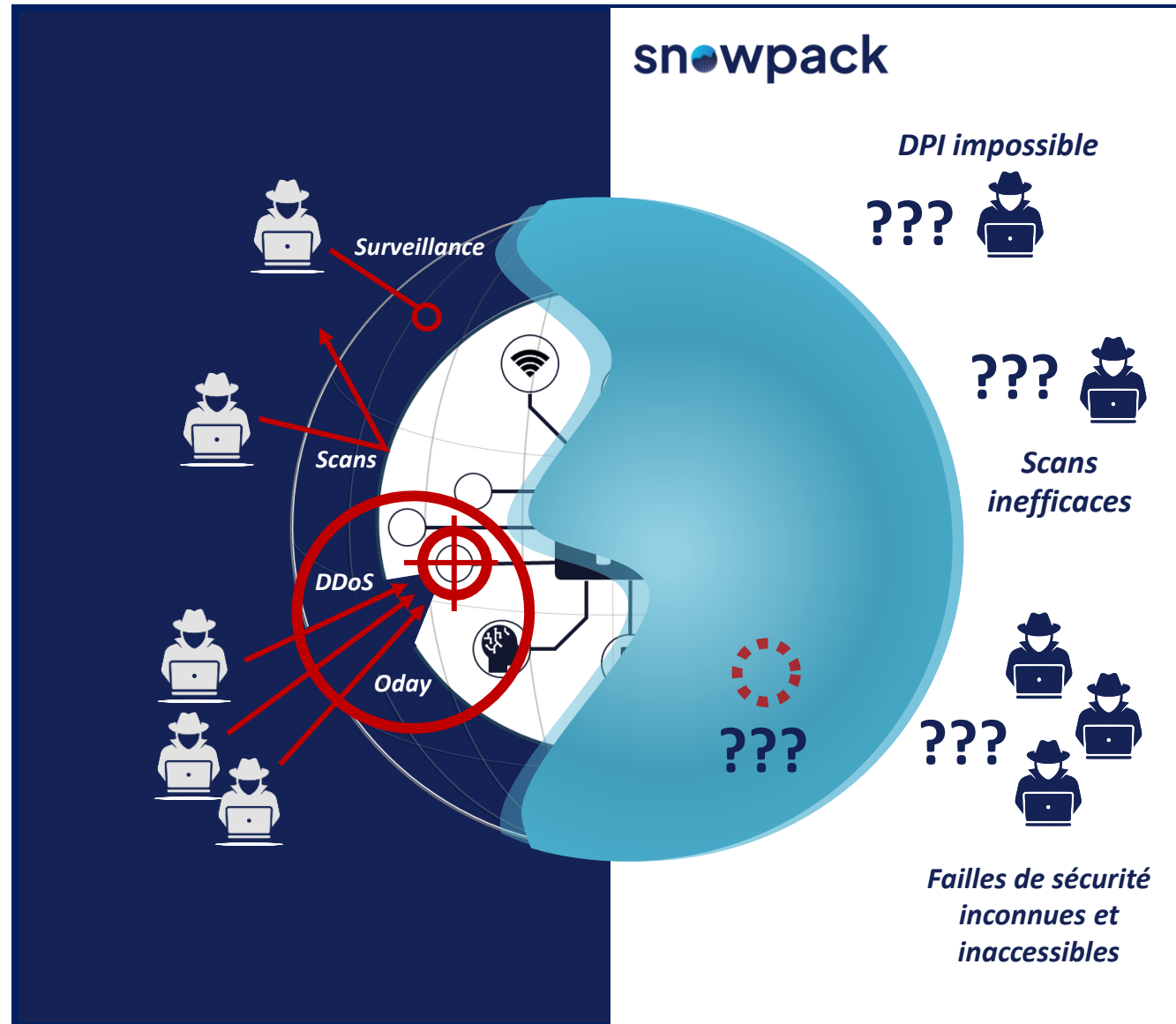


snowpack | Si les hackers ne vous voient pas, ils ne vous attaquent pas !

'Visible'

Les vulnérabilités peuvent être exploitées à partir de :

- **Métadonnées** sur les données en transit
- **Port(s)** d'écoute sur les serveurs
- **Tiers de confiance**



'Invisible'

Pas d'exploitation des vulnérabilités à partir de l'Internet :

- Pas de métadonnées
- Pas de port d'écoute
- Pas de tiers de confiance

Notre réseau privé virtuel invisible (VIPN) cache et protège vos activités.

Activez notre solution, et devenez invisible



Invisible Access

Surfez sur Internet sans aucune trace

Naviguez sur le Clear, Deep & Dark Web de manière véritablement anonyme et sans tiers de confiance



Invisible Services

Protégez vos services web sensibles

Rendez vos services web sensibles exposés sur internet invisibles pour les pirates informatiques

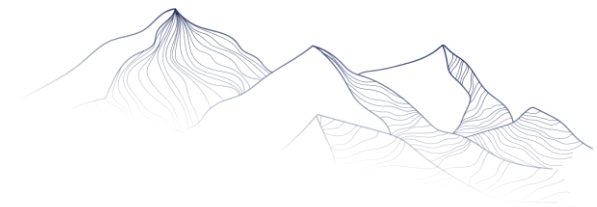


Invisible Infra

Masquez votre surface d'attaque

Protégez vos end-points et vos données des pirates informatiques et empêchez l'exploitation des vulnérabilités

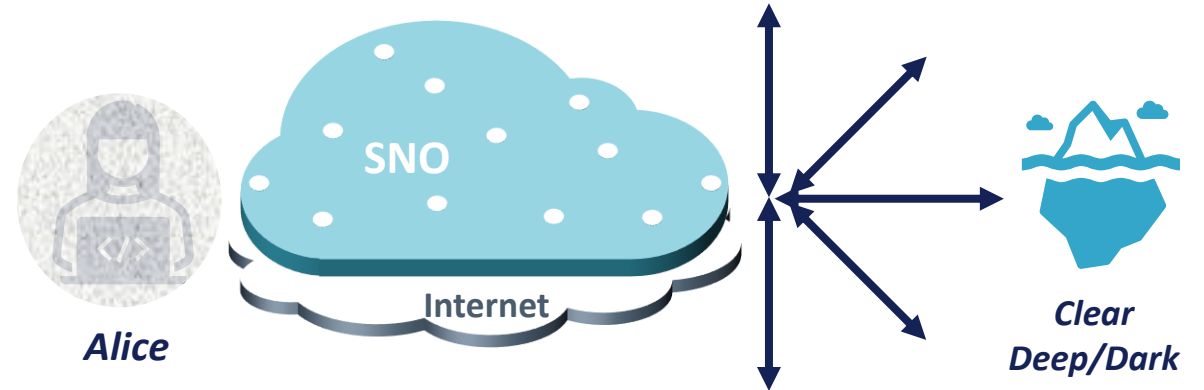
← *Egalement disponibles via l'API « **Invisible by Snowpack** » pour l'intégration dans vos logiciels et systèmes.* →





Invisible Access

*Cachez vos utilisateurs
et leurs opérations sur Internet*



Mode « Privacy » : Pas de tiers de confiance, QoS, pas de MITM

Télétravail et mobilité

Osint - OpSec

(Investigation en ligne, renseignement,...)

- Protégez les **utilisateurs sensibles** et leurs communications : *VIPs d'entreprise, soldats sur théâtres d'opération, accès distants, avocats, journalistes, etc.*
- Aidez les professionnels ayant **un fort besoin d'invisibilité** pour leurs opérations: *Red Team, Cyber Threat Intelligence, légal, Investigation sur le clear/deep/dark web, etc.*

snowpack | Cas d'usage 1 : Protection des communications sensibles



PROBLEMATIQUE

- Risque d'**espionnage** stratégique et industriel élevé*
- Télétravail, nomadisme
- Ingérence étrangère

CONSEQUENCES

- **Identification** des individus, de leurs communications, de leur localisation,
- **Interception** des communications et **vol** de données et informations sensibles

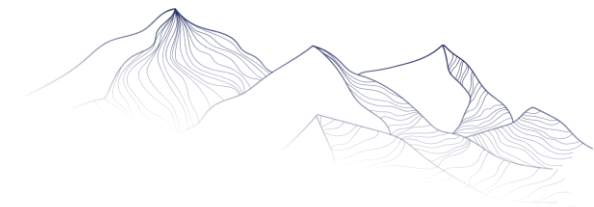
SOLUTION

SNOWPACK INVISIBLE ACCESS

- Masquer sa présence sur Internet quel que soit son point d'accès
- Protéger les communications des utilisateurs sur Internet
- Empêcher les attaques de type Man-In-The-Middle

RESULTATS & BENEFICES

- Protection des **utilisateurs** , des **communications sur IP** (*télétravail, visio, voix...*) et des échanges de **données** sensible entre l'utilisateur, son entreprise et ses partenaires.



snowpack | Cas d'usage 2 : OSINT OPSEC



PROBLEMATIQUE

- Infrastructures d'anonymisation (VPN, Tor, ad-hoc) difficiles à **mettre en place**, à maintenir & impliquant des tiers de confiance & des logs
- Bulle de filtrage (géoloc, qualité IP, recherches, cookies...)
- Systèmes de gestion des bots (captchas, WAFs, outils de détection des bots...)
- Faible qualité de service

CONSEQUENCES

- Temps consacré à l'infra au lieu de l'op.
- Détection, interdiction ou intoxication des données
- Falsification du trafic
- Partage des opérations avec le fournisseur d'anonymisation
- Attribution des opérations

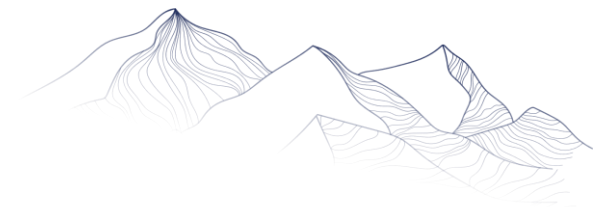
SOLUTION

SNOWPACK INVISIBLE ACCESS

- Réglage fin de l'invisibilité et plug-in avec son propre outil (CLI)
- Opérations secrètes en ligne véritablement sécurisées (réel anonymat, pas de MITM)
- Infra avec des adresses IP de haute qualité et permissives (IP résidentiel et outils de surveillance IP)
- Haute qualité de service

RESULTATS & BENEFICES

- Pas de risque d'attribution
- Modus operandi dissimulé

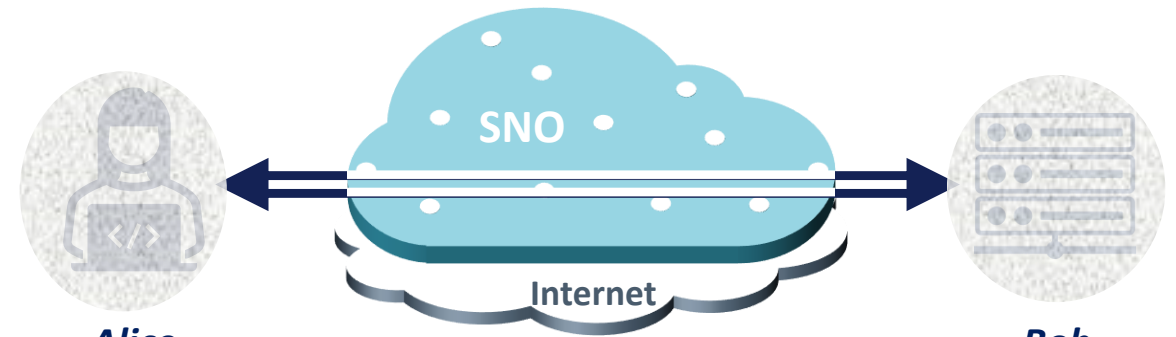


snowpack | [Invisible Services & Infra] Masquez votre surface d'attaque !



Invisible Services & Infra

*Masquez la surface d'attaque
de votre système d'information*



Mode « Tunnel » : end-points (serveurs,...) masqués, QoSec,
résilience dès la conception, pas de MITM

Réduire la **surface d'attaque externe** du SI

Sécuriser les **accès distants** au SI

Sécuriser la **Supply Chain**

Faciliter la **gestion de l'obsolescence** (IT/OT)

Implémenter **ZTNA & Micro-segmentation**

- **Rendez invisibles** aux pirates les **services sensibles** d'entreprise exposés sur Internet: *sites web, APIs, services web, etc.*
- **Protégez les composants d'infrastructure** exposés sur Internet (*serveurs, end-points, VPN, etc.*) contre les attaques externes (*par ex. scan, DDoS, Oday*).

snowpack | Cas d'usage 3 : Réduction de la surface d'attaque du SI

Ivanti Connect Secure zero-days exploited by attackers (CVE-2023-46805, CVE-2024-21887)

Vulnerability in 150K+ Fortinet Devices Let Hackers Execute Arbitrary Code Remotely

Palo Alto Networks warns of PAN-OS firewall zero-day used in attacks

Critical GitLab flaw allows account takeover without user interaction, patch quickly! (CVE-2023-7028)

LockBit Ransomware Affiliates Leverage Citrix Bleed Vulnerability (CVE-2023-4966)

Cisco IOS XE zero-day exploited by attackers to deliver implant (CVE-2023-20198)

CISA confirms that SonicWall vulnerability is getting exploited (CVE-2024-40766)

CVE-2024-24919 Detection: Zero-Day Vulnerability Actively Exploited for In-the-Wild Attacks Against Check Point's VPN Gateway Products



PROBLEMATIQUE

- Services et composants du SI exposés sur internet :
 - non mis à jour en temps réel
 - non forcément dédiés à un grand nombre d'utilisateurs
- Présence de failles, vulnérabilités, ou mauvaises configurations.

CONSEQUENCES

- Attaques par exploitation des failles et vulnérabilités (*zero day, n-day*)
- Attaque par déni de service distribué (DDoS)

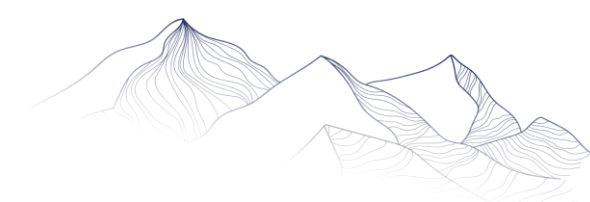
SOLUTION

SNOWPACK INVISIBLE SERVICES / INFRA

- Rendre **invisible** les services et composants du SI exposés sur Internet
- Ne les laisser accessibles qu'aux seuls utilisateurs autorisés

RESULTATS & BENEFICES

- Diminution** de la surface d'attaque du Système d'Information
- Gain de temps** pour mettre à jour ses services et serveurs en cas de CVE, notamment sur les composants « **Invisible by Snowpack** » nativement



snowpack | Cas d'usage 4 : Cybersécurité des SI Industriels



PROBLEMATIQUE

- Équipements **obsolètes** et non mis à jour depuis longtemps
- Absence de **segmentation** des réseaux **IT/OT**
- **Ouverture** du SI industriel (*télé maintenance, télétravail*)

CONSEQUENCES

- **Exposition accrue** aux menaces externes (*+ attaques ciblées APT*)
- Augmentation des **vecteurs d'attaques**
- Risque **d'intrusions malveillantes**

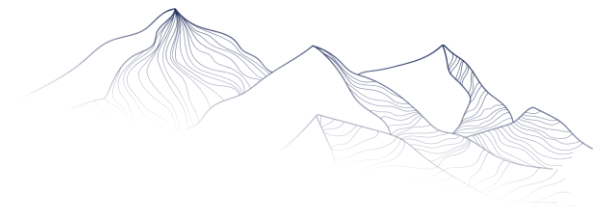
SOLUTION

SNOWPACK INVISIBLE SERVICES / INFRA

- Rendre **invisibles** les points d'entrée (services, serveurs ..) exposés sur Internet et ne les laisser accessibles qu'aux seuls utilisateurs autorisés
- **Cloisonner / Segmenter** les zones exposées

RESULTATS & BENEFICES

- **Diminution** de la surface d'attaque du SI industriel
- Protection **rapide, simple, accessible** pour tout type d'organisation
- **Gain de temps** pour travailler en profondeur sur :
 - La mise à jour des composants obsolètes
 - La refonte du SI industriels



snowpack | Cas d'usage 5 : Cyber-assurabilité des TPE/PME/ETI



PROBLEMATIQUE

- *TPE/PME/ETI** :
 - Menace & Risque cyber élevés
 - Budgets restreints
- *Courtiers/Assureurs*
 - Critères d'éligibilité aux offres de cyber-assurance restrictifs**

CONSEQUENCES

- Eligibilité compliquée des TPE/PME/ETI aux offres de cyber-assurance*, pourtant quasi obligatoires opérationnellement

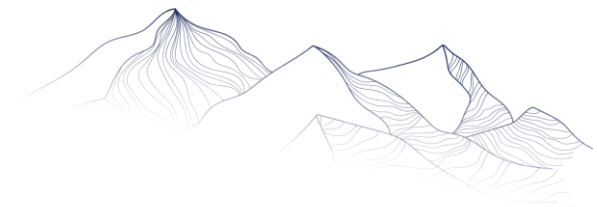
SOLUTION

SNOWPACK INVISIBLE SERVICES / INFRA

- **Masquer la surface d'attaque** externe des TPE/PME/ETI et les protéger des cybermenaces sans recourir à l'empilement complexe de couches de sécurité traditionnelles, souvent coûteuses et non infaillibles

RESULTATS & BENEFICES

- **Diminution** de la surface d'attaque externe des TPE/PME/ETI
- **Accès** à un produit de cyber-assurance
- **Gain de temps** pour améliorer leur cyber-sécurité
- Solution **rapide, simple, et accessible**



* Etude [Impact Cyber](#) de cybermalveillance.gouv.fr

** [rapport LUCY de l'AMRAE](#) 2024

Technologie

Virtual Invisible Private Network (VIPN) & Snowpack Network Overlay (SNO)

Comment rendre les utilisateurs, les données et composants du système d'information intraquables et invisibles sur Internet sans devoir faire confiance à un tiers ?

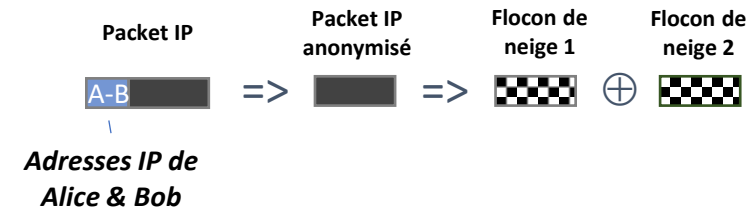


4 principes clés brevetés pour garantir l'invisibilité, l'anonymat et l'indépendance technologique

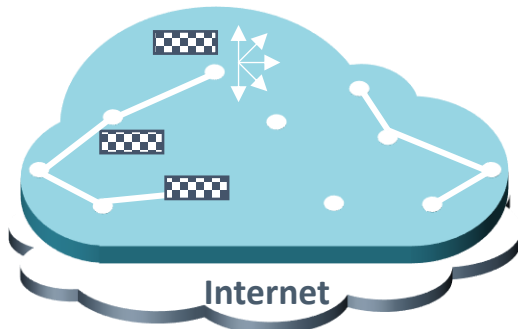
1. Réseau Overlay Distribué (SNO)



2. Fragmentation des paquets IP en bruits anonymes (flocons de neige)

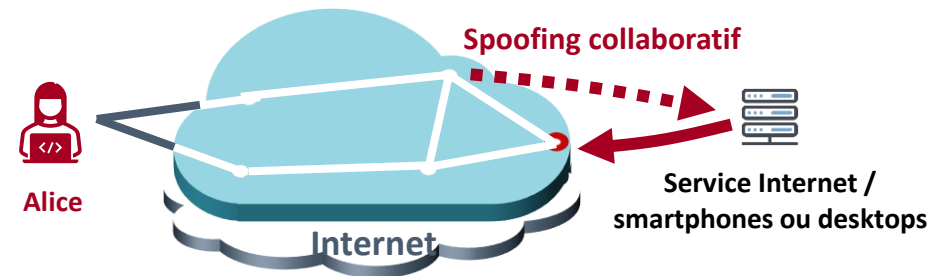


3. Distribution des flocons sur des routes, autodécouverte des nœuds



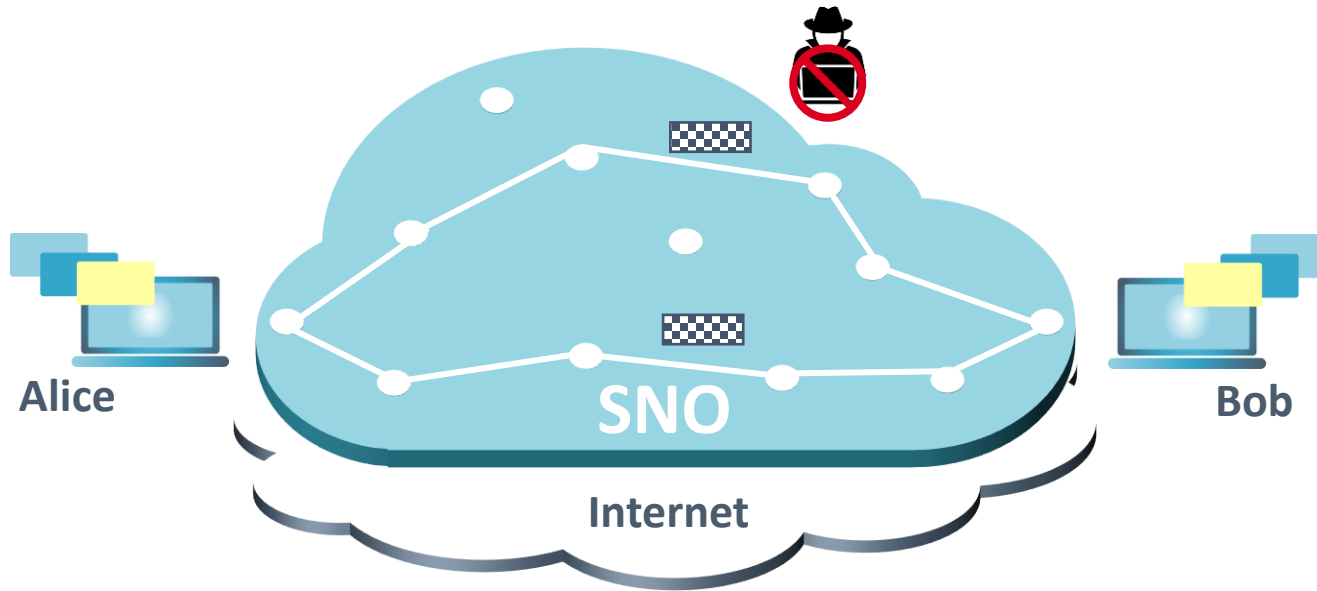
Les nœuds ne peuvent pas connaître l'intégralité de l'itinéraire / du chemin (quelle que soit la puissance de calcul)

4. Nœuds de sortie distribués



Aucun élément du SNO ne peut avoir une connaissance totale de {l'expéditeur, du destinataire, du contenu}.





Les flocons transitent à travers le SNO

Points forts de la solution

Aucune attaque MITM possible



Pas de tiers de confiance



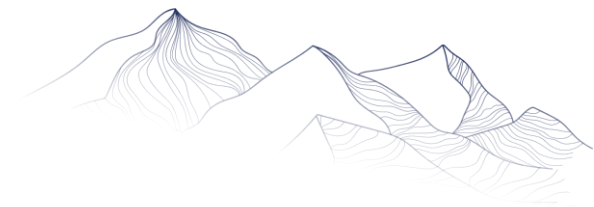
Dissimulation de l'infra & des Services



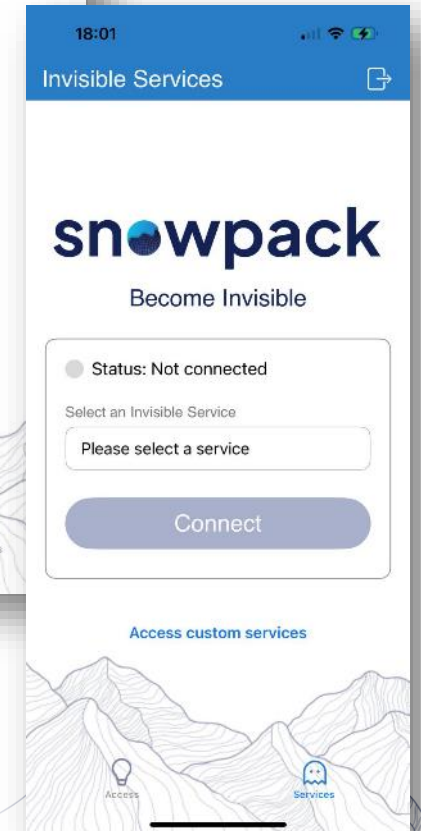
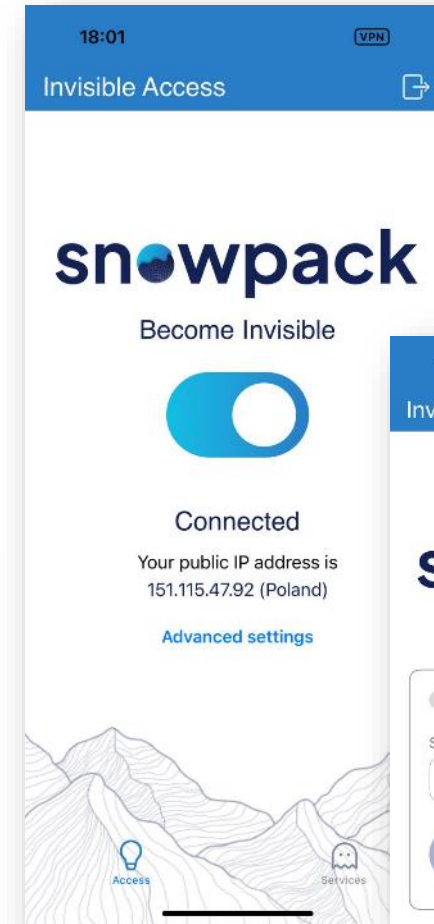
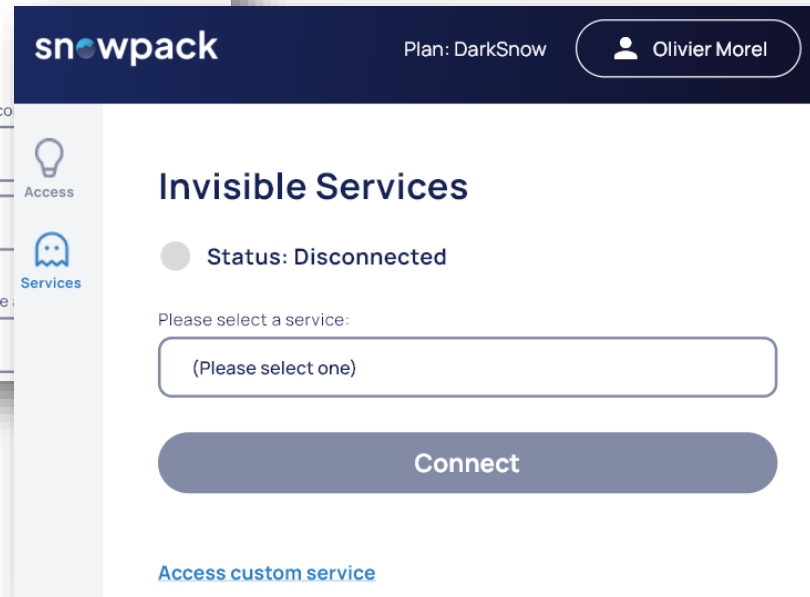
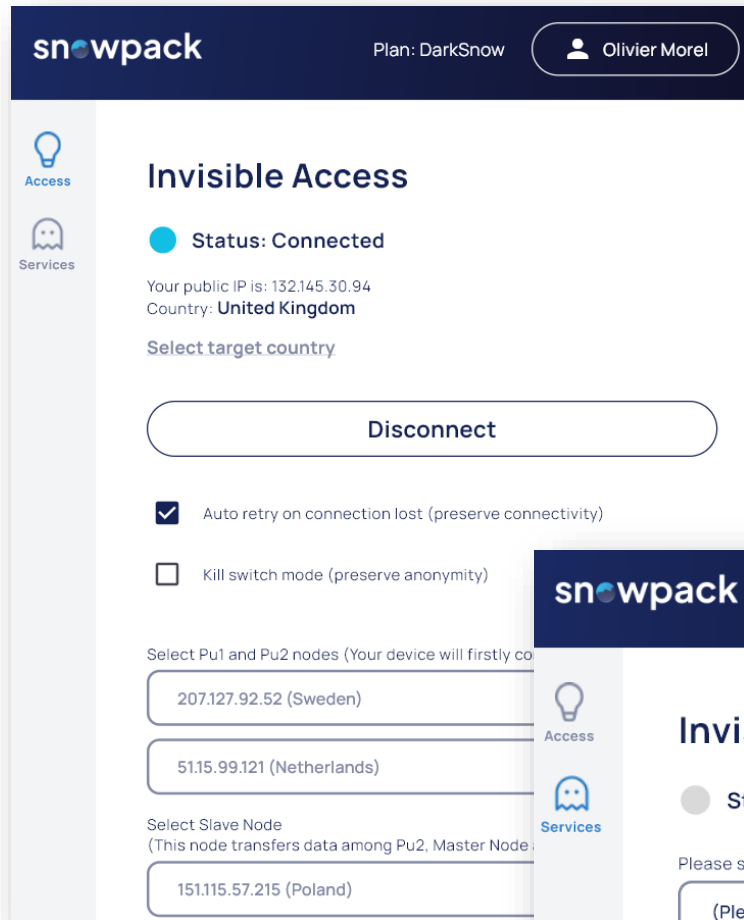
Haute qualité de service et résilience



Installation simple et rapide,
expérience utilisateur facilitée



snowpack | VPN : 'deeptech', mais très simple pour l'utilisateur ...



snowpack | ... et simple à installer et à administrer !

The dashboard features a sidebar with the following navigation links: Overview, Profile, Plan and payments, Invisible Services, My services, Services management, and Users and access. Three arrows point from the 'My services', 'Services management', and 'Users and access' links to their respective sections.

My Services

Status	Tenant ↓	Service	Public IP	Local URL
Active	DEMO-Raph	TEST DEMO LIVE	14.20.42.14	https://14.20.42.14:443
Active	Snowpack Company Demo	Invisible Demo	14.20.42.14	https://14.20.42.14:443

Services management

Create + Number of services: 2 / 5

Status	Nickname ↓	Public IP	Local URL	Number of assigned users	Actions
Active	My-Invisible-Service-01	14.20.42.14	https://14.20.42.14:443	3 / 100	Edit More
Active	My-Invisible-Service-02	14.20.42.14	https://14.20.42.14:443	2 / 100	Edit More

Users and access

Invite + Number of users: 4 / 10

Name ↓	Email	Assigned services ▼	Actions
Baptiste-test	baptiste.p@snowpack.eu	• My-Invisible-Service-01	Edit More
Fred (Not yet accepted)	frederic.m@snowpack.eu	• My-Invisible-Service-02	Edit More
Olivier-DarkSnow	olivier.m@snowpack.eu	• My-Invisible-Service-01 • My-Invisible-Service-02	Edit More
Raphael-test	raphael.d@snowpack.eu	• My-Invisible-Service-01	Edit More

snowpack | Véritable Zero-trust...



Architecture VPN

Contrôle total mais :

- Conçu pour les **architectures centralisées**
- Gestion des droits d'accès **mauvaise**
- Passerelle est **vulnérable**

Architecture SASE

Conçues pour les architectures **décentralisées**
avec une **gestion des droits d'accès simple**
+ **Résilience**

Mais

Nécessite de **faire confiance au fournisseur**



Architecture VIPN

Contrôle total et...

- Gestion **aisée** des droits d'accès
- **Pas de tiers de confiance**
- **Résilience**
- **Invisibilité!**

snowpack | Quelques références publiques ...



CYBER INTELLIGENCE & COMMUNITIES

Plateforme française intégrée de renseignement sur les cybermenaces





brightnet

DNS sécurisé Zéro knowledge & invisibilité pour les PME et les autorités publiques

*DOH filtering
Cybersecurity service*

*Zero-Knowledge
layer*

*Network Infra.*



SPHINX

Confidentialité de données
(Lutte Contre le Blanchiment et le Financement du Terrorisme)

*Application & Data
level privacy*

*Zero-Knowledge
layer*



CYBAS

Evaluation & renforcement des capacités opérationnelles de cyberdéfense



En savoir plus :

- <https://www.lemondeinformatique.fr/actualites/lire-avec-scred-thales-veut-mutualiser-le-renseignement-cyber-en-france-90091.html>
- https://www.youtube.com/watch?v=mpjP_h7B0tzk

En savoir plus :

https://www.linkedin.com/posts/altrativ_brightnet-france2030-activity-7050092285555826688-rBYK?utm_source=share&utm_medium=member_desktop

En savoir plus :

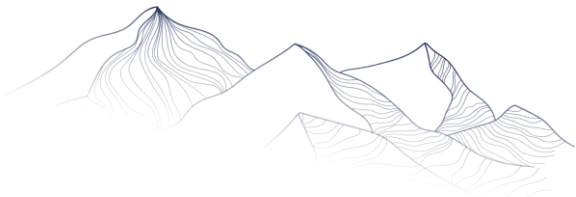
- <https://acpr.banque-france.fr/tech-sprint-acpr-sur-la-mutualisation-confidentielle-de-donnees>

Partenaires (intégration technologique)





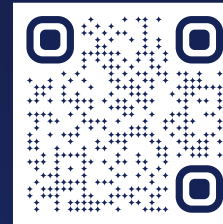
#Innovation	• Spin-of du CEA, un des plus grands centres de recherche européen • Technologie brevetée, développée depuis 2017 and lancée en 2023 • 2024 : Grand prix du Forum in Cyber et Prix du jury des Assises			
#Différentiation	• 1^{ère} solution globale et ergonomique d'invisibilité sur Internet • Absence de tiers de confiance			
#Réponses #concrètes	• Solutions adaptées à toutes les entreprises dans tous les secteurs • Protection des utilisateurs, Conformité réglementaire (NIS2 ...), Cyber assurance, Sécurité de la chaîne d'approvisionnement,			
#Dynamique	• Visibilité ↗ • Roadmap ↗	• Adoption ↗ • Channel ↗	• Equipes ↗ • Pipe ↗	



Pour vivre heureux, vivons cachés !^{*}

Ne nous faites pas confiance,
Testez-nous !

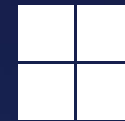
WWW.SNOWPACK.EU



Download!



Linux



Windows



Android



iOS
macOS



SDK
API

^{*} « Le Grillon »,
Jean-Pierre Claris de FLORIAN,
1755 - 1794