
HAFS
Distributeur à valeur ajoutée
VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES
EXPERTISE
Des solutions adaptées à chaque environnement
CONFIANCE
Un partenaire fiable à vos côtés
PERFORMANCE
Des infrastructures sécurisées et évolutives
SUPPORT
Un accompagnement technique de qualité
HAFS
Distributeur à valeur ajoutée
Des solutions IT innovantes pour un monde connecté et sécurisé
WIRELESS RADIO
Connectivité sans fil haute performance
RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés
VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives
CYBERSECURITY
Protéger vos données et vos systèmes
VIDÉO PROTECTION
Solutions de vidéosurveillance intellligentes
HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité
SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION

SECURE CHANNEL ACTIVE

Présentation Globale

NUCLEON SECURITY PORTFOLIO 2026

Plateforme **Nucleon**

Couverture complète : Prévention, Détection, Investigation & Réponse

Solution Engineering Team



CONFIDENTIEL

Nucleon carte d'identité

Nucleon en chiffre

+ 250

Clients

Tout secteurs & tailles confondus

+ 50%

Croissance des effectifs

Équipes R&D, Q\A, Sales, Presales, RH

3 M€

Levée de fonds en 2025

Réalisée par NewFund Capital

5

Portefeuilles produits

EDR | XDR | ScorX | Atom AI | Malprob

2

Implantation dans le monde

France & Maroc

Roadmap – approche souveraine

Certification CSPN | ANSSI

Prévu pour fin 2026



NUCLEON

AHEAD OF CYBER THREATS

Distinction & références

01

Prix

Best Cybersecurity Innovation Award at Gitex



02

Programme

Programme d'accélération du campus Cyber (la Défense)

CYBER BOOSTER

03

Performance

Nucleon a obtenu la meilleure note AAA pour la détection de l'EDR et de Malprob (98,8 %)

WEST COAST LABS Validated

SCALE360 POWERED BY IFZA

Éditeur référencé UGAP-SCC

UGAP

HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

THALES

Ce qu'en pense nos clients

Eurex

"Our financial operations benefit from smarter correlation and adaptive threat prevention."

CISO

Fortiche

"In production and creative environments, Nucleon EDR provides seamless protection without disrupting workflow."

HEAD OF IT

Agma

"We finally have real contextual insight into what's happening on our endpoints."

DSI

Bobbypills

"For animation studios like ours, Nucleon EDR ensures creative freedom while maintaining data integrity."

CTO

> 97 %

Taux de rétention client

Nucleon se distingue par un taux de fidélisation client élevé, reflet de la performance et de la valeur apportée par notre plateforme.

Nucleon carte d'identité

Nos challenges

Failing Legacy Systems

- Environ 86 % des attaques de malwares en 2025 utilisent des variantes personnalisées qui échappent à la détection antivirus traditionnelle basée sur la signature
- Cette tendance rend les systèmes de défense hérités de plus en plus inefficaces face aux menaces modernes

01

Blind Spots in Monitoring

- 45 à 55 % de l'activité des endpoints n'apparaît jamais dans les journaux d'événements (Gartner, 2023).
- Cela signifie que près de la moitié des activités suspectes sont invisibles pour les équipes SOC, les risques restent cachés jusqu'à ce que les attaquants frappent.

02

Teams chasing noise

- Les analystes consacrent 50 %+ de leur temps aux faux positifs (Ponemon 2024)
- Cela signifie des temps d'enquête plus longs, des coûts en hausse et de réelles menaces qui passent à travers

03

Analyse des Menaces 2026

Contexte Cyber 2026

Défis Opérationnels Critiques

Explosion Volumétrique Malware

560k nouveaux échantillons malveillants par jour. Les signatures traditionnelles sont obsolètes face à cette masse.

Fatigue Analytique SOC

Surcharge d'alertes et faux positifs élevés. Les équipes sont noyées, augmentant le risque d'ignorer une vraie menace.

MTTR Trop Élevé

Le temps moyen de réponse reste critique, laissant aux attaquants une fenêtre d'action trop large.

Nouveaux Samples

560k

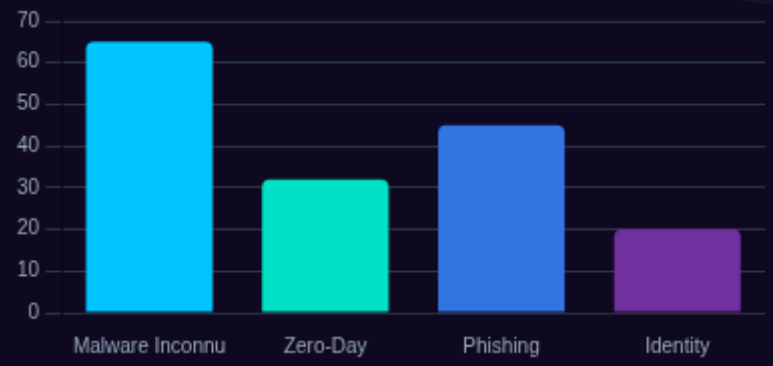
Malwares / Jour

Vulnérabilités

32%

Exploits Zero/One-Day

Répartition des Vecteurs d'Attaque



>4h

Temps moyen de détection sans automatisation

Source: Rapport Menaces Cyber 2026 & Statistiques SOC Globales

Portfolio Unifié

Approche Plateforme

Nucleon EDR

Protection Endpoint

Comportemental
Zero Trust
Remédiation

Prévention

Nucleon XDR

Corrélation & SIEM

Multi-sources
Chaînes d'attaque
Contexte étendu

Détection

Nucleon Malprob

File Intelligence IA

IA Prédictive
Multi-formats
API-First

Analyse

Nucleon ATOM AI

Automatisation SOC

Agents AI
Workflows DAG
Orchestration

Réponse

Nucleon ScorX

Risk Scoring

Priorisation
Contexte Métier
Réduction Bruit

Pilotage

Unified
Platform

5
Produits Intégrés

Zero
Trust Behavior

Full
Cycle Ops

Protection Endpoint

Nucleon EDR Overview

NUCLEON EDR

Performance & Légèreté

Architecture ultra-optimisée avec une empreinte système minimale : **CPU < 1%** et consommation mémoire **~100 Mo**. Invisible pour l'utilisateur.

Sécurité Zero Trust

Application de politiques comportementales strictes. Validation continue de chaque processus et blocage par défaut des comportements déviants.

Tamper Protection & Rollback

Agent blindé contre la désactivation malveillante. Capacité de **rollback** instantané pour restaurer les fichiers chiffrés ou altérés.



Architecture & Détection

Architecture Nucleon EDR

ENDPOINT PROTECTION



Composants Clés

- Agent Léger (<1% CPU)
- Zero Trust Policy
- Rollback Playbook

OS Supportés

WINDOWS · LINUX · MACOS · SERVER

Capacités Opérationnelles

Investigation & Réponse

NUCLEON EDR

Investigation

Timeline Complète

Visualisation chronologique de tous les événements système (fichiers, registre, réseau) pour reconstituer l'historique précis de l'attaque.

Forensics

Investigation

Arbre de Processus

Graphique interactif des processus parents/enfants montrant l'injection de code, les commandes CMD/PowerShell et la persistance.

Analyse

Investigation

Recherche IOC

Chasse aux menaces en temps réel sur l'ensemble du parc via hash, IP, domaine ou patterns comportementaux complexes.

Hunting

Réponse

Isolement & Kill

Coupe instantanée du réseau (sauf canal EDR) et arrêt forcé des processus malveillants pour stopper la propagation latérale.

Immédiat

Réponse

Quarantaine & Nettoyage

Suppression sécurisée des fichiers malveillants, clés de registre persistantes et tâches planifiées associées à l'attaque.

Remédiation

Réponse

Rollback & Scripts

Restauration des fichiers chiffrés (VSS) et exécution de scripts de réponse personnalisés à distance sur les endpoints affectés.

Restauration

Extended Detection & Response

Nucleon XDR Overview

NUCLEON Security

Visibilité Unifiée 360°

Agrège et normalise les données de télémétrie provenant des endpoints, du réseau, du cloud, des applications SaaS et des identités en une vue unique cohérente.

Moteur Sigma & Corrélation

Utilise des règles de détection standardisées (Sigma) et des algorithmes de corrélation avancés pour reconstituer automatiquement les chaînes d'attaque complexes multi-vecteurs.

Réduction du Bruit

Transforme des milliers d'événements bruts et d'alertes isolées en un nombre réduit d'incidents qualifiés et priorisés, diminuant drastiquement la fatigue des analystes.



Architecture & Pipeline

Pipeline Nucleon XDR

CORRELATION ENGINE

1. Collecte & Ingestion

Collecteurs
Syslog, API, Agents

Normalisation
Format unifié JSON

Enrichissement
GeoIP, Asset Info

2. Indexation & Tags

Indexation
Fast Retrieval

Sigma Tagging
Règles Détection

Politique Rétention
7J HOT / 1 AN COLD

3. Moteur Corrélation

Requête Unique | Temporelle
Event Count | Static Match

CTI / Threat Intel
Feeds IP, Hash, URL

IOC Matching
Temps réel vs Historique

4. Alerte & Réponse

Alertes Unifiées
Priorisation par Risque

Orchestration
EDR, SOAR, ITSM

Playbooks
Actions Automatisées

Flux Données · Intelligence · Action

Technologies Clés: SIGMA · ELASTIC · MITRE ATT&CK

Investigation & Réponse

Investigation XDR & Réponse Orchestrée

NUCLEON XDR

Investigation

Détails d'Alerte Enrichis

Contexte MITRE ATT&CK complet, mapping tactiques/techniques, sévérité dynamique et score de risque unifié.

Automatique

Investigation

Pivot Multi-Sources

Exploration croisée immédiate : IP, Hash, User, Machine à travers EDR, Cloud, Réseau et Identité.

Guidé Manuel

Réponse

Isolation Endpoint

Mise en quarantaine réseau instantanée des actifs compromis via l'agent EDR, maintien canal remédiation.

Automatique Manuel

Réponse

Blocage IP / Domaine

Blacklisting automatique d'IOCs sur les firewalls, proxys et passerelles web pour couper les C2.

Automatique Guidé

Écosystème

Gestion d'Incidents

Création et sync de tickets dans ITSM (ServiceNow, Jira) avec contexte complet pour le suivi SOC.

Automatique

Écosystème

100+ Connecteurs API

Intégration bidirectionnelle native avec SIEM, SOAR, EDR tiers, IdP et outils réseau.

Automatique Manuel

Intelligence Artificielle de Détection

MALPROB Overview

NUCLEON Security

IA Prédictive Statique

Moteur de détection avancé utilisant l'apprentissage automatique pour analyser la structure des fichiers sans exécution, identifiant les menaces avant qu'elles ne s'activent.

Multi-Formats Supportés

Analyse exhaustive couvrant une large gamme de types de fichiers : exécutables (PE, ELF, Mach-O), documents (PDF, Office), scripts, archives et paquets mobiles (APK).

Complémentarité Stratégique

Agit en synergie avec les signatures traditionnelles et le sandboxing dynamique, comblant les lacunes de détection pour une couverture Zero-Day optimale.

Formats Analysés

PE / ELF

PDF / Office

APK / Mach-O

ZIP / RAR

PowerShell

JavaScript

Intégration API

Intégration fluide dans les workflows existants (SOAR, EDR, Gateways) pour une analyse automatisée et scalable.

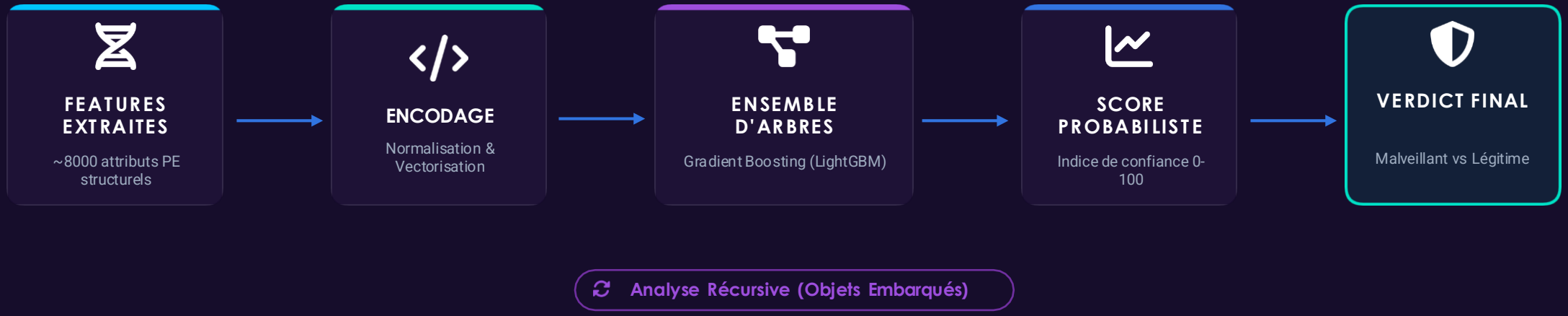
Modes d'Analyse

Supporte l'analyse ponctuelle à la demande ou en pipeline continu pour les flux de fichiers massifs.

Architecture & Intelligence Artificielle

Pipeline ML MALPROB

STATIC ANALYSIS



Avantages Clés

- Haute Performance
- Features Hétérogènes
- Interprétabilité

Spécifications ML

SCALABLE · MILLIONS SAMPLES · NON-GÉNÉRATIF

Performance Opérationnelle

Précision & Performance

Avantages Techniques

Couverture Variants Inconnus

Détection proactive des menaces zero-day grâce à l'analyse structurelle ML, sans signatures.

Débit Élevé (Statique)

Analyse ultra-rapide sans exécution dynamique, permettant de traiter des volumes massifs.

Intégration API & Web

Automatisation fluide dans les workflows SOC existants via connecteurs standards.

WCL AAA

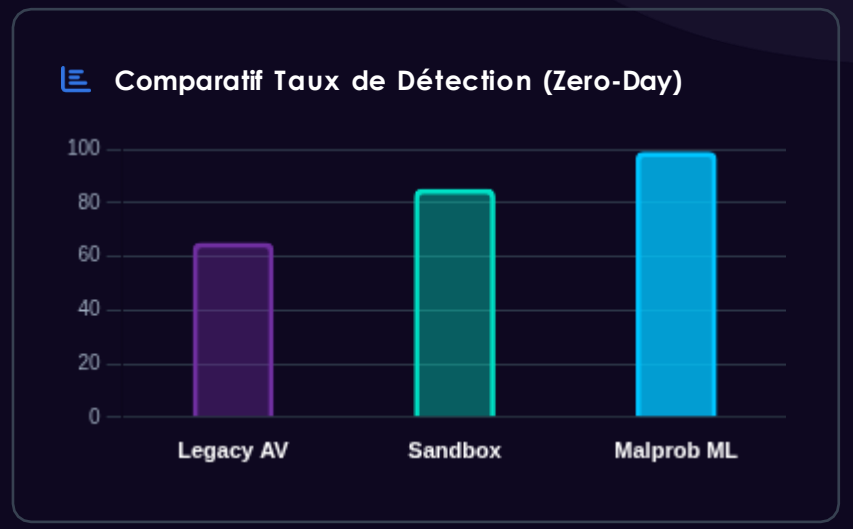
98.8%

Précision de Détection

Efficacité

< 50ms

Temps d'Analyse Moyen



8000+

Features extraites par fichier

Source: West Coast Labs Report 2025 & Internal Benchmarks

Plateforme d'Automatisation SOC

Qu'est-ce qu'ATOM AI ?



Agents IA Spécialisés

Des entités autonomes qui analysent les données, prennent des décisions intelligentes et exécutent des actions ciblées.

Orchestration Workflows

Architecture DAG (Directed Acyclic Graph) visuelle pour chaîner les agents et créer des pipelines d'automatisation complexes.

Performance SOC

Réduction drastique de la charge manuelle et amélioration significative des indicateurs MTTD/MTTR.

Architecture Enterprise

Multi-tenant avec isolation complète par entité, parfaitement alignée avec la Stack Nucleon existante.

NUCLEON STACK

Focus Endpoint + XDR

Latence Ultra-Faible

Contexte Data Riche

AUTOMATISATION & ORCHESTRATION

Agents AI & Workflows

ATOM AI

Éditeur Visuel - Workflow

Créez des flux d'automatisation complexes via une intuitive : triggers, agents IA, connecteurs, conditions logiques et actions de réponse.

Connecteurs OpenAPI

Intégration avec plus de 200 APIs de sécurité (EDR, SIEM, IAM, Cloud) et support des connecteurs custom OpenAPI pour une interopérabilité totale.

Validation Intelligente

Vérification en temps réel de la cohérence des workflows, simulation d'exécution et débogage pas-à-pas pour garantir la fiabilité des processus critiques.

Gouvernance & Traçabilité

Versioning & Contrôle
Historique complet des modifications, rollback instantané et gestion des branches de workflow.

Contrôle d'Accès RBAC
Gestion granulaire des permissions par rôle, équipe ou tenant pour sécuriser l'accès aux automatisations sensibles.

Tracking de Tokens & Coûts
Suivi précis de la consommation des modèles IA et attribution des coûts par workflow ou département.

Audit Trail

Compliance

ATOM AI Intelligence

Chat Assistant & Orchestration

ATOM AI

Interface NL Console

Création intuitive de workflows et de règles de détection via langage naturel, sans codage complexe.

Requêtage Multi-Sources

Interrogation unifiée de l'EDR, XDR pour obtenir des résumés actionnables et des rapports consolidés.

Rapports Automatisés

Génération instantanée de rapports d'incident détaillés et de synthèses exécutives basés sur l'analyse contextuelle.

Flux d'Orchestration Intelligent

Commande Langage Naturel
"Bloquer IP et isoler hôte infecté"

↓

Orchestration Multi-Outils
EDR / XDR / SIEM / ITSM

↓

Validations Humaines
Approbation avant action critique

Réponse Coordonnée & Rapide

Risk Management & Prioritization

ScorX Overview

NUCLEON ScorX

Scoring Contextualisé

Analyse dynamique des entités (utilisateurs, machines) et des alertes en tenant compte de leur historique comportemental et de leur environnement.

Criticité Métier & Exposition

Intègre la valeur des actifs (VIP, serveurs critiques) et leur exposition (internet facing, vulnérabilités) pour ajuster le niveau de risque réel.

Focus sur l'Impact Réel

Oriente l'attention du SOC vers les menaces qui comptent vraiment, réduisant drastiquement le bruit et la fatigue d'alerte.



Priorisation Intelligente
Filtrage du bruit et mise en avant des signaux forts

Risk Scoring Dynamique
Calcul en temps réel basé sur multi-facteurs

Focus Analytique
Investigation ciblée sur les menaces critiques

Priorisation & Risk Scoring

ScorX Enrichissement

NUCLEON SCORX

Enrichissement

Contexte Actif

Enrichissement automatique avec la criticité métier (VIP, Prod, R&D), localisation et rôle de l'actif pour pondérer le risque.

Automatique | CMDB

Enrichissement

Identité Utilisateur

Corrélation avec l'annuaire (AD/Azure AD) pour identifier les privilèges, groupes sensibles et anomalies comportementales.

Automatique | IAM

Contexte

Contexte Métier

Intégration des processus critiques et impact business potentiel pour transformer une alerte technique en risque métier.

Business Impact

Threat Intel

Enrichissement IOC

Qualification temps réel des hash, IP, domaines via CTI et Malprob pour confirmer la malveillance et réduire les faux positifs.

Temps Réel

Analyse

Corrélation Multi-Facteurs

Agrégation de signaux faibles et contextuels pour calculer un score de risque précis et éliminer le bruit opérationnel.

Réduction FP

Action

Triage Priorisé

Export vers XDR/SIEM des incidents à haute probabilité d'impact pour focaliser l'attention des analystes SOC.

Orchestration

ROI & Valeur Métier

Bénéfices Globaux Nucleon

NUCLEON SECURITY

01

Couverture Cycle Complet

De la prévention à la restauration.

- Prévention-first (EDR)
- Détection avancée
- Réponse & Rollback

02

Visibilité & Corrélation

Vision transverse multi-sources.

- Endpoint, Cloud, Réseau
- Chaînes d'attaque XDR
- Contexte enrichi

03

Automatisation Réponses

Réponse incident accélérée par l'IA.

- Workflows ATOM AI
- Playbooks dynamiques
- Orchestration SOC

04

Performance Opérationnelle

Gains d'efficacité mesurables.

- -50% MTTR (Réponse)
- -70% Tâches manuelles
- Réduction Faux Positifs

05

Déploiement Souverain

Flexibilité et conformité totale.

- Cloud / On-premise
- Air-gapped (Isolé)
- Souveraineté donnée

5 Produits Unifiés	-50% Temps Réponse	-70% Charge Analyste	100% Conforme Souverain

Architecture & Déploiement

Écosystème Intégré NUCLEON

INFRA SECURE

Sources & Télémétrie

M365 / Graph
SharePoint, OneDrive, Exchange

Nucleon EDR
Telemetry & Behavioral Events

SIEM / SOAR
Logs & Alert Ingestion

ITSM
ServiceNow, Jira

NUCLEON PLATFORM

MALPROB
File Intelligence & Malware Analysis

NUCLEON XDR
Corrélation & Contextualisation

ATOM AI
Orchestration & Agentic Automation

SaaS / Cloud | On-Premise | Air-Gapped

Réponses Automatisées

Containment
Isolation Endpoint, Blocage IP

Remédiation
Quarantaine fichier, Rollback

Notification & Audit
Alerte SOC, Ticket enrichi, Audit Logs

Gouvernance & Sécurité

Multi-Tenant RBAC | Logs & Audit Trail | Souveraineté des Données

APIs Bidirectionnelles

REST API | JSON/CSV

Plan d'Action

Next Steps & Contact

NUCLEON Roadmap

1

Ateliers Techniques

Sessions dédiées Architecture & Intégrations pour cadrer les besoins.

Cadrage & Scope

2

Plan POC & KPIs

Définition du calendrier de test et des critères de succès mesurables.

Critères Succès

3

Planning & Gouvernance

Validation des rôles, jalons de déploiement et accès RBAC.

Validation

4

Contact SE Team

Accès direct à l'équipe Solution Engineering Nucleon Security.

Support Direct

Prêt à sécuriser votre environnement ?

Alexandre.SEBIRE@nucleon-security.com | Équipe Solution Engineering

Démarre le projet →



Département Commercial

HAFS

Distributeur à valeur ajoutée

Vous accompagne

HAFS NETWORKS WCA

+225 07 89 82 56 49 / +225 07 59 05 85 82

sales-ci@hafs-networks.com

HAFS NETWORKS FRANCE

+33 (0)7 49 92 62 57 / +33(0)9 73 89 20 39

sales@hafs-networks.com

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone Networks | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY V vade | CyberShield

RUCKUS Networks | Ruijie Reyee | RAY | Wiflyx Woofi. Smart. Seamless | SEARCHINFORM Risk and Compliance Management | MOBOTIX | EXTRAVIS Analyse Automatisée Réponse XDR | HAFS MediVision