NUCLEON
AHEAD OF CYBER THREATS

NUCLEON EDR

Endpoint Detection & Response

Security teams encounter various obstacles while attempting to identify, analyze, and address sophisticated attacks. These difficulties consist of inadequate insight into essential control points, laborious scouring of extensive and heterogeneous data sources devoid of context and association, weariness from alerts due to inadequate signal-to-noise ratios, and the complexity of rapidly curtailing the attack, leading to interruptions in critical business operations, diminished efficiency, and heightened operating expenses.

Comprehensive approach to cyber threat protection

Nucleon Detection & Response provides protection for workstations and servers.

- Set up of successive protection layers to protect you at all levels during an attack
- Identification of weak points in your infrastructure and systems
- Blocking attacks and providing a range of tools for investigation.

Protection adapted to your critical activities and data

Nucleon Detection & Response absorbs your internal uses and identifies your critical data to protect.

- Absorption of behaviors and uses to adapt security mechanisms.
- Automatic creation of specific protection rules, against illegitimate access, leakage and blocking by ransomware.

1 Prevention

System and application hardening.

2 Detection

Identification of new malicious strains using artificial intelligence

3 Response

Easier incident response thanks to on-board tooling

4 Remediation

Return to a resilient state after an attack

ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Microsoft Virus Initiative

ABUSE.ch

Identification of malicious behavior

Zero-Trust policies ensure that attack techniques used by hackers are blocked. Sensitive scripts and administration tools are not allowed in order to block complex infection processes and fileless attacks.

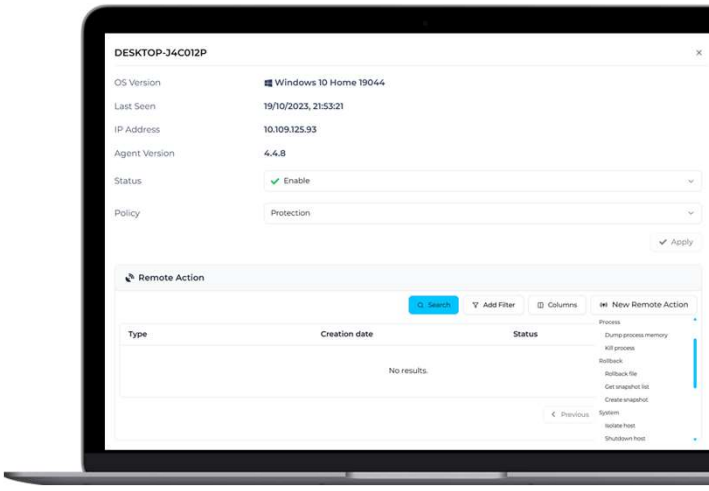
Network accesses are also restricted by policies to avoid abnormal accesses by abused softwares. For example, the Microsoft Office suite only has access to IPs and domains it needs to run and update.



Facilitated investigation

The centralized administration console provides all the tools to identify the source of a suspicious behavior. It is easy to understand the execution flow of a malware or even the one of a business software.

Remediation, isolation and Rollback



In case of data compromission by a malware, or simply by a user, data can be restored from the administration console. This feature always provides a last resort solution in case of a problem, and can be used natively without installing any additional components.

In case of detected suspicious behavior, the endpoint can be directly isolated from the network to prevent further damage. In addition, remediation also allows the machine to be cleaned automatically starting from the first action of the the attack.

Benefits

Comprehensive and simplified protection powerd by Zero-Trust

Real-time visibility of system and network activities

A sleek, lightweight agent that doesn't affect production and users' daily lives

Centralized console

Easy install

Cloud or On premise

Privacy

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 intelligentes

HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité

SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION



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 vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision