



Zero Trust Endpoint Security



Antoine BOTTE
CTO - Cofondateur



Septembre 2025

Nucleon Security



Fondée en 2019

+100 Clients in 3 continents

+30 Collaborateurs

Europe / Afrique

Produits :

EDR

MDR

Malprob

XDR

ScorX

Zero Trust

NIST SP-800-207



Aucun utilisateur, appareil ou application n'est automatiquement **digne de confiance**. Chaque accès doit être **vérifié et autorisé** en permanence



**Orienté users / assets /
ressources**

Contrôle continue des
identités et authentification



**Surveiller et contrôler
dynamiquement**

Chaque accès est contrôlé et
autorisé en fonctions de critères
stricts



Moindre privilège

Permet une réduction de la
surface d'attaque

Endpoint Detection & Response



Comportements

- Heuristics
- Sigma rules
- TTP matching
- IOC
- Runtime memory scan
- AI

Fichiers

- Signatures
- Yara
- IOC
- Sandboxing
- AI

Réponse

- Isolation réseau
- Kill process
- Forensic / collecte
- Remediation / Rollback

Principalement basé sur des artefacts malveillants connus,
difficile de détecter de nouvelles menaces

Dans le choix d'un EDR, le poids réel des technologies de détection est faible.

Transposer le Zero Trust sur l'EDR



EDR Standard

Dans le modèle ZTA, l'EDR est généralement considéré comme un outil de télémétrie, détection et de réponse

Vision Nucleon

- L'EDR intègre le modèle ZTA directement dans le workflow de contrôle comportemental sur le terminal.
- Pas de détection orientée sur les menaces connues.
- Aucune confiance, tout est contrôlé. Les programmes et applications ont le minimum d'accès possible.

➡ Comment chaque pilier du Zero Trust prend forme dans notre EDR

Subject

This is the “who” that is requesting access to a resource. This is the set of subjects (human and processes) of the enterprise or collaborators and a collection of subject attributes/privileges assigned ...

- SP 800 207

- ➔ Habituellement appliqué aux utilisateurs, le modèle ZTA s'étend aussi aux programmes.



Le « subject » du Zero Trust est une entité logicielle

Tout programme en exécution est traité comme un sujet à contrôler

Authentication



Appliqué aux « humains »

- Identité de référence :
login, email, UID
- Mot de passe / authentification forte
- MFA (token, SMS, app, biométrie...)
- Recommandations sur l'identité
numériques : **NIST SP 800-63**

Appliqué aux programmes :

- Nom, chemin
- Commande
- Signature numérique
- Hash

Moindre privilège

Une fois authentifiés, les utilisateurs n'ont pas accès aux ressources dont ils n'ont pas besoin.

Une équipe de développement n'a aucune raison d'accéder aux données de compatibilité de l'entreprise.

Même logique applicable aux programmes et processus.

Un lecteur vidéo, un VPN ou Teams n'ont pas à accéder aux environnements de développement ou de compatibilité.



PEP

- Policy Enforcement Point

Responsable de la capture et contrôle des requêtes d'accès d'un sujet vers une ressource.

Interception des accès :

- Proxy
- Firewall
- ACL NTFS



Legacy EDR : collecter de télémétrie afin de déclencher des alertes et/ou actions.

L'approche Zero Trust nécessite d'**intercepter les événements** générés par les processus et de les transmettre au « Policy Decision Point »

PDP

- Policy Decision Point

S'appuie sur une base de règles pour évaluer les demandes d'accès en fonction du sujet

Règles de sécurité :

- Proxy
- Firewall
- ACL NTFS

Règles dédiées pour chaque action système possible, pour Nucleon :

- Exécution
- Lecture
- Écriture
- Connexion réseau
- Accès à un processus

➔ Multi-Layer ZeroTrust



TA

- Trust Algorithm

Verdict final

Règles de sécurité correspondantes



Informations externes

Vérifier si l'hôte à partir duquel le sujet demande l'accès possède un EDR installé et actif

Utilisation du TA comme couche de détection supplémentaire

Le TA peut déclencher une analyse de fichier : [Malprob](#)

➔ Détecte les payloads malveillants, bloque l'accès



De l'ambition à l'opérationnalisation



Transformer cette vision **Zero Trust** en une réalité opérationnelle exploitable au quotidien

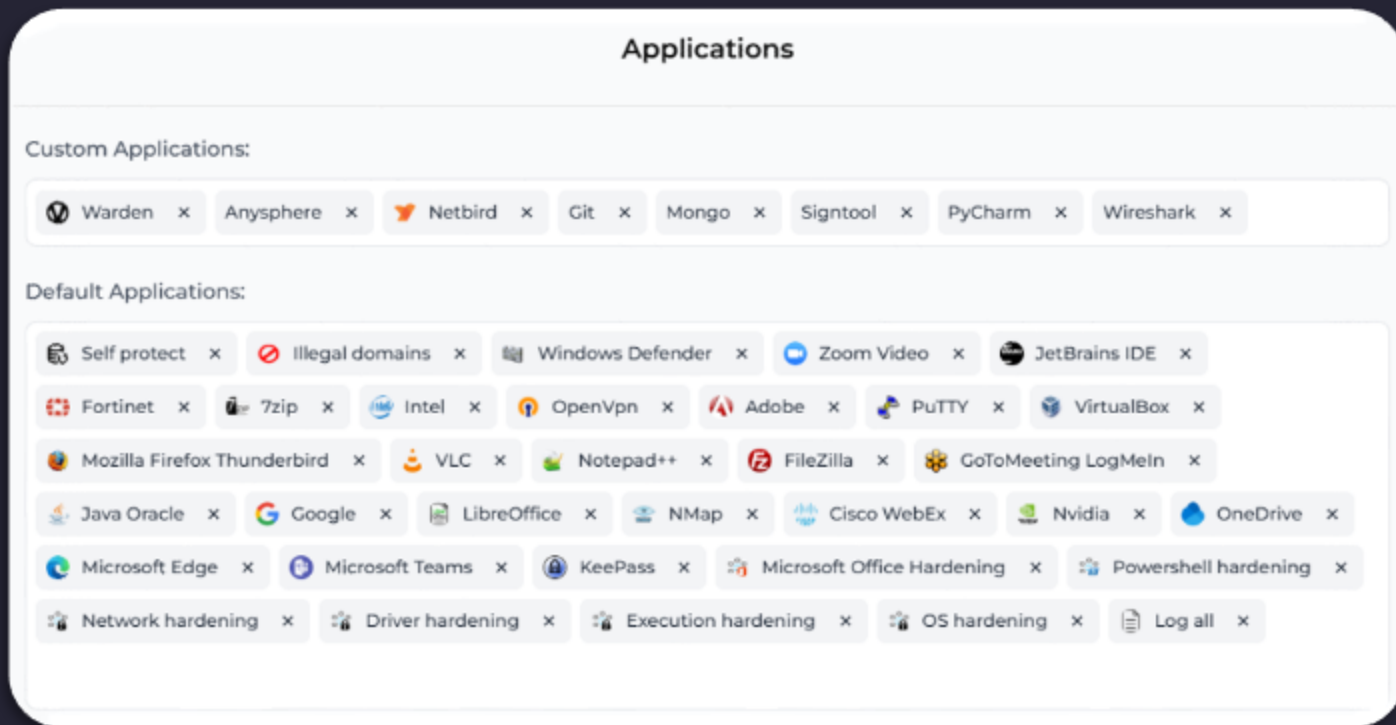


Socle de règles standard



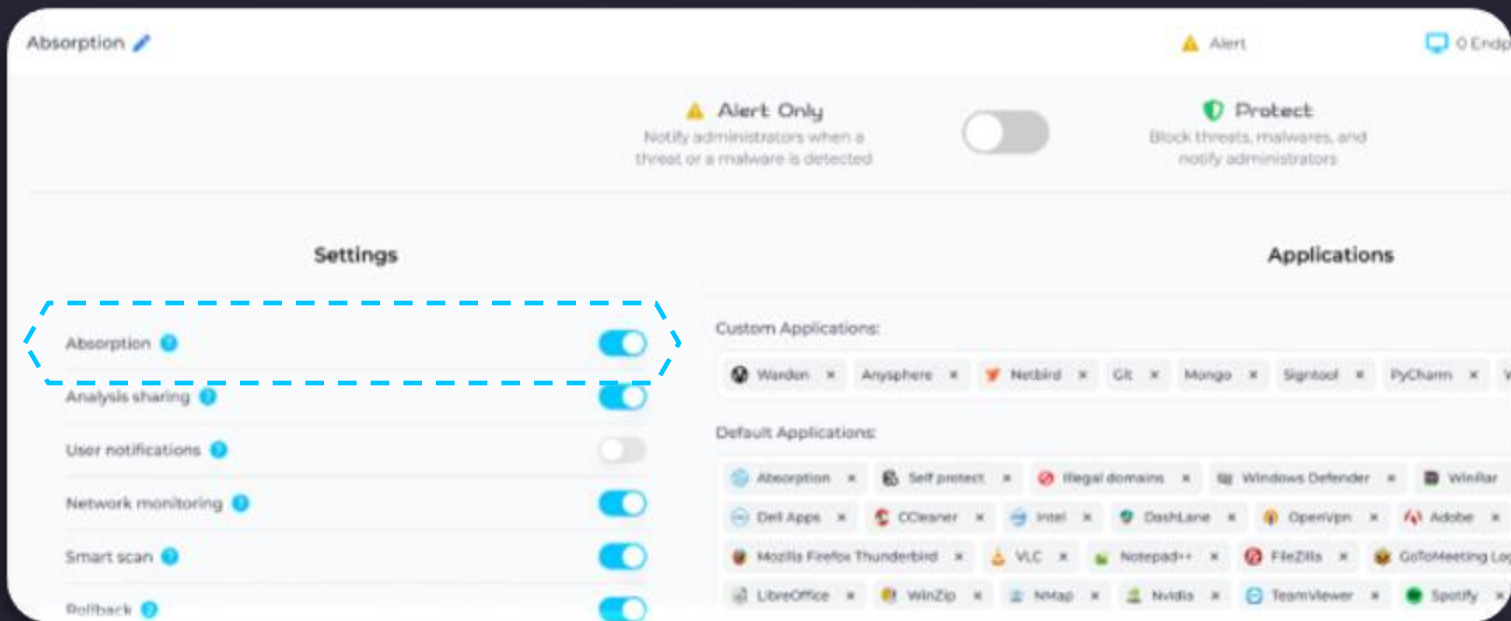
Applications

- Ensemble de règles ML-ZT
- 100+ Applications par défaut
- Durcissement natif
- Adaptées au contextes métiers
- 100% personnalisable
- PDP Efficace



Apprentissage

Les faux positifs sont une source d'enrichissement des règles, pas une raison de les désactiver



Signaux faibles

- Flexibilité et efficacité



Les signaux faibles offrent au TA une marge de manœuvre pour différencier l'innocent du suspect.

Any x Execute x Powershell x

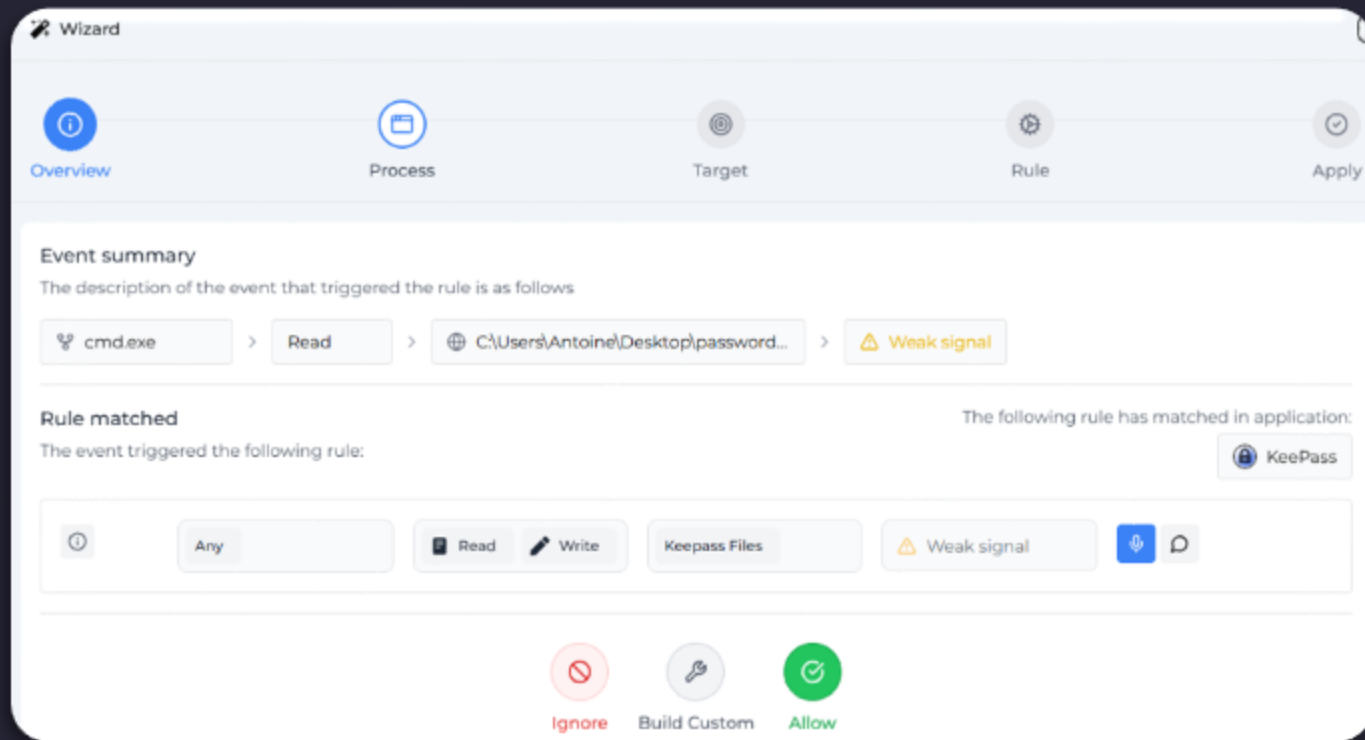
Weak signal

2 X Weak signal = Block

- Block
- Allow
- Analyze
- Ignore
- Weak signal ✓

Wizard

- Votre assistant Zero-Trust



- Création de règle à partir d'évènements
- Suggestion automatique de règle
- Gestion des signaux faibles

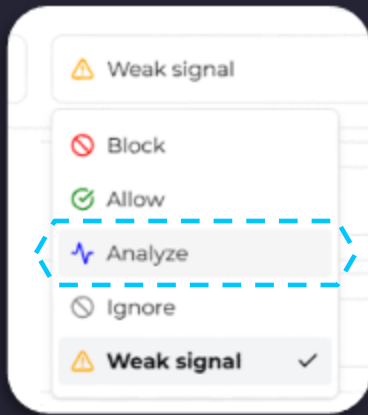
Héritage dynamique



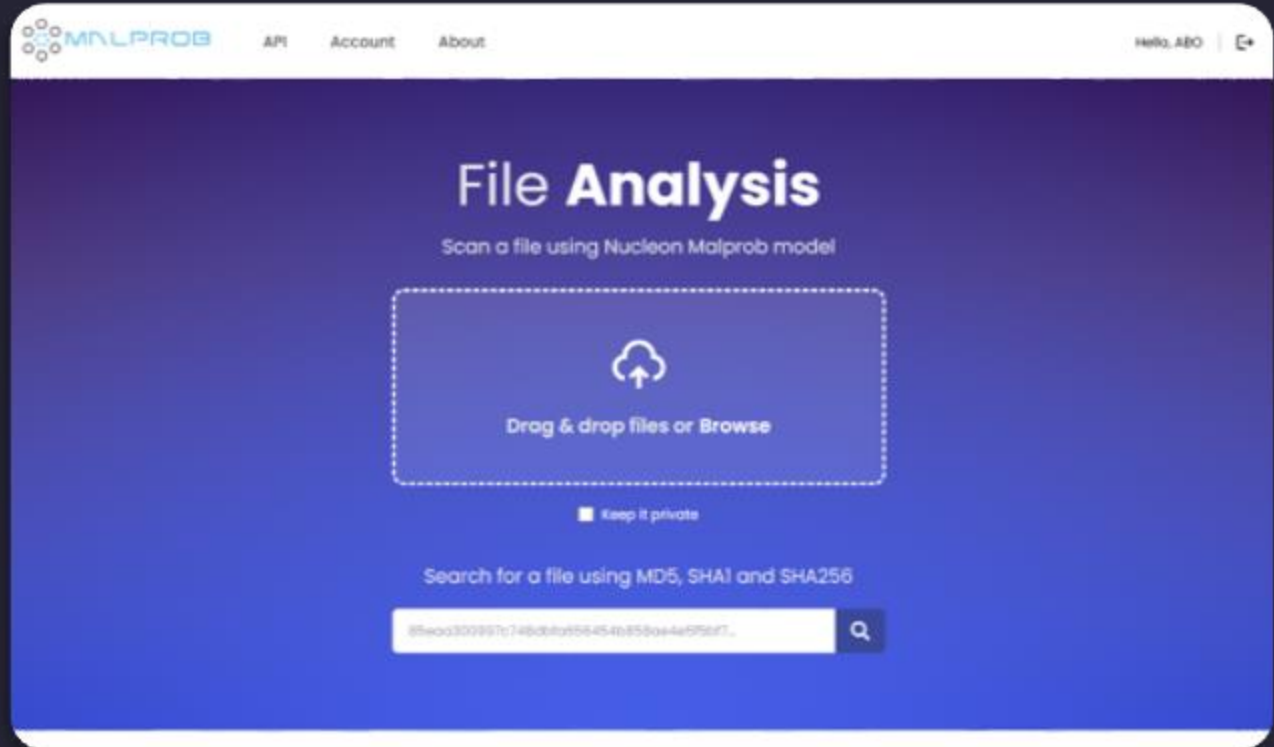
Contexte différent, règles différentes : l'option **Trusted** transmet les permissions dynamiquement.

Source	Type	Target	Action	Options
Visual Studio Code x	Network x	Github domains x npmjs.org domains x Python domains x docker.com domains x	Allow	  
Visual Studio Code x	Execute x	Python Signed x Powershell x Command line x Docker Signed x	Allow	    Trusted Trusted Write: Target will not be analyzed, Execute: Rule kept for child process

Décider avec l'appui de l'IA



- Renforcement du TA
- Analyse en profondeur de tout type de fichiers
- Sans signature
- API Ready



Atom AI



You
i want to block all execution for any source

AtomAI 05:42 PM

Rule Preview

⏸ Any ⚙ Execute Any ⛔ Block 🔍 ⚙ ⚙ ⚙ ⚙

Rule Analysis

Attribute	Details
Purpose	Block all execution attempts from any source
Action	Block
Scope	All execution attempts
Security Impact	Prevents unauthorized code execution, reducing the risk of malware and other types of attacks

Deployment Status

Status: Ready for immediate deployment - Schema validated

REMEMBER: This rule blocks all execution attempts from any source, which may impact legitimate system functionality. Use with caution and consider customizing the rule to only block specific sources or actions if necessary.

- Agent IA spécialisé
- Aide à la création de règles en langage naturel
- Propositions et explicabilité
- Investigations automatisées
- Interroge des services externes :

➡ Malprob

➡ ScorX

ScorX : étendre la vision Zero Trust



Une base unique qui compresse et unifie la connaissance des comportements systèmes.



Service d'extension des produits cyber

Interroger ScorX pour identifier instantanément la criticité d'un évènement système.



Explicabilité

Aide les analystes à comprendre, décider et agir plus vite.



Accélérateur de règles Zero Trust

Permet de proposer rapidement des règles standardisées.



MERCI

Antoine BOTTE - CTO

@ antoine.botte@nucleon-security.com