STORMSHIELD

ENDPOINT SECURITY

# EVOLUTION

Augmentez le niveau de protection de vos postes de travail avec une solution EDR proactive


## Déploiement

ON-PREM ET SAAS

## API REST

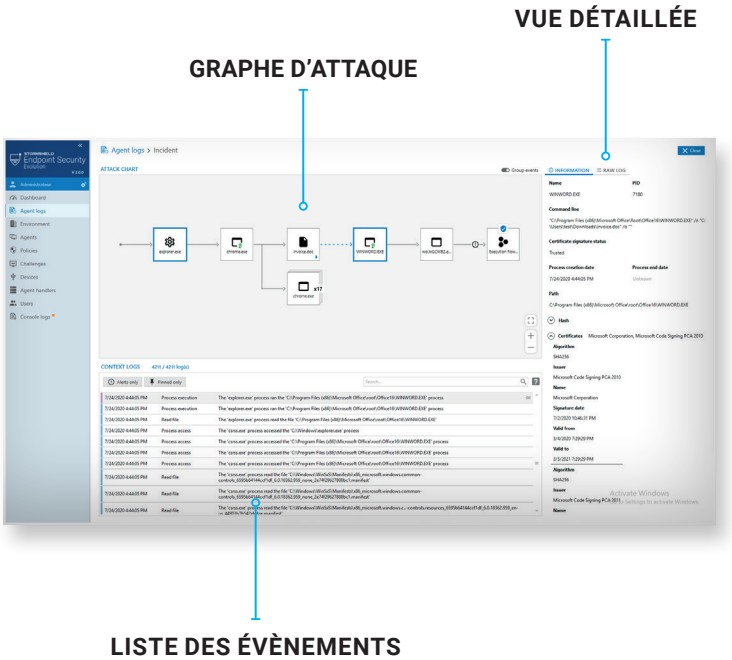
INTÉGRATION DANS L'ÉCOSYSTÈME

## Ultra personnalisable

PARAMÈTRES DE SÉCURITÉ AJUSTABLES

## Autonome

PROTECTION DES ENVIRONNEMENTS DÉCONNECTÉS




## Protection optimale avec notre solution EDR

Stormshield Endpoint Security Evolution est la solution de protection des terminaux et serveurs de nouvelle génération. Basé sur une technologie d'analyse sans signature, l'agent détecte des attaques et menaces et répond de manière appropriée.

### Sécurité proactive

- Attaque bloquée en temps réel
- Analyse et rémédiation prédéfinies et personnalisables
- Graphe d'attaque et Threat Hunting (IoC, règles Yara, etc.)

### Analyse comportementale

- Protection sans signature contre les attaques 0-day
- Combat les techniques d'exploitation des vulnérabilités
- Protection anti-ransomware

### Protection contextuelle

- La politique de sécurité s'adapte dynamiquement à l'environnement même hors connexion
- Politiques personnalisables par groupe d'utilisateurs
- Politiques de sécurité par défaut et actualisation par les équipes de sécurité Stormshield Customer Security Lab

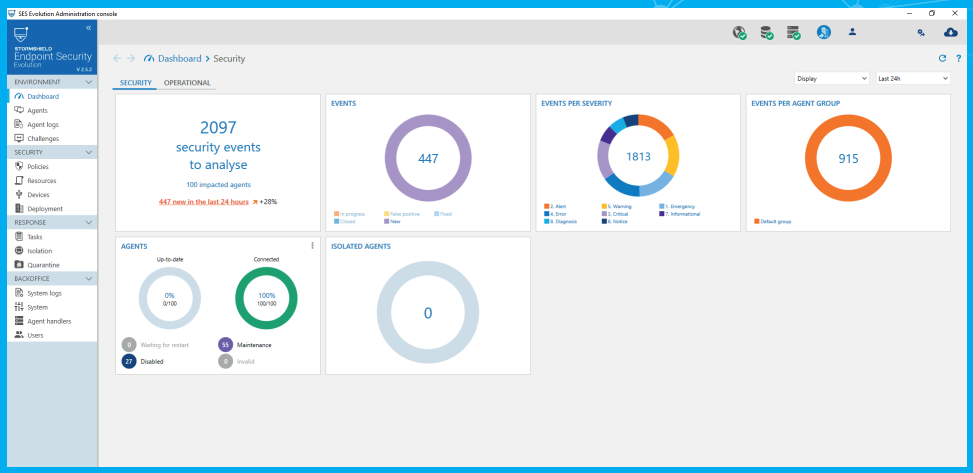
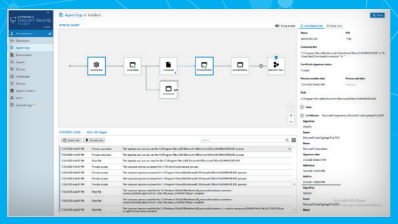
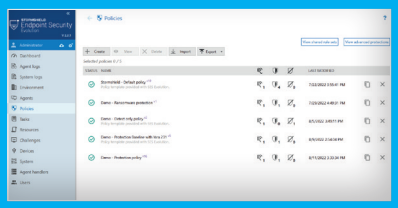



Tableau de bord



Vue détaillée du graphe d'attaque



Vue de la politique de sécurité

# FONCTIONNALITÉS

**Protection 0-Day contre les menaces connues et inconnues**

**Techniques d'attaques détectées**

- Corruption mémoire (buffer overflow, heap spray)
- Elévation de privilèges (privilege escalation, token stealing)
- Vol d'informations sensibles (keylogging, accès aux processus)
- Process Hollowing et ses variantes
- Injection de code (application hooking)
- Protection contre les attaques de type *fileless*

**Protection contre les ransomwares**

- Identification de processus de chiffrement malveillant
- Restauration des fichiers chiffrés par un ransomware
- Windows Shadow Copy
- Politique de sauvegarde

**Protection sans signature**

**Remédiation personnalisable**

- Arrêt d'un processus
- Suppression d'un fichier
- Suppression ou modification d'une clé registre ou de sa valeur
- Utilisation de scripts PowerShell pour des actions sur mesure (arrêt et suppression d'un service etc.)
- Mise en quarantaine automatique de malwares
- Isolation des postes compromis

**Identification d'indicateurs de compromission (IoC)**

- Texte suspect (nom de fichier, d'hôte, d'objet, etc.)
- Informations réseau (adresses IP, URLs suspectes, DNS)
- Hash SHA1, SHA256, MD5 et SSDEEP
- Recherche manuelle, planifiée ou sur détection
- Protection contre le contournement des moyens de détection des EDR

**Contrôle des périphériques**

- Réseaux wifi • Clé USB • Bluetooth • Accès aux volumes disques • Connexions réseaux • Contrôle d'exécution

**Agent optimisé**

- Consommation mémoire
- Consommation CPU

**Politique de sécurité**

- Adaptation dynamique en fonction du contexte
- Jeux de règles d'analyse comportementale et de contrôle de périphériques fournis et maintenus par Stormshield
- Prise en charge des règles Yara

**Administration centralisée**

- Gestion de la politique par groupes d'agents
- Gestion des administrateurs par rôle
- Activation / désactivation des modules par groupes d'agents
- API REST pour une intégration avec des produits tiers
- Rapport d'activité avec des indicateurs MCS et MCO en format HTML
- Notification automatique des alertes de sécurité par email

# COMPATIBILITÉ

## AGENT

**Ressources**

CPU :
1 core 1Ghz (min.) - 2 cores 2GHz (recommandé)

RAM :
1 Go (min.) - 2 Go (recommandé)

Espace disque :
100 Mo (installation) - 200 Mo (données)

**Système d'exploitation**

Client :
Windows 7 SP1, 8.1, 10 et 11

Serveur :
Windows Server 2008 R2, 2012 R2, 2016, 2019 et 2022 (y compris version Core)

## ADMINISTRATION

Possibilité d'une gestion SaaS ou on premise

## POUR L'ADMINISTRATION ON PREMISE

**Backend**

CPU :
1 core 1GHz (min.) - 2 core 2Ghz (recommandé)

RAM :
1 Go (min.) - 2 Go (recommandé)

Espace disque :
100 Mo (installation) - 200 Mo (données)

Serveur :
Windows Server 2012 R2, 2016, 2019 et 2022 (y compris version Core)

**Gestionnaire d'agents**

CPU :
2 core 2Ghz (minimum)

RAM :
2 Go (minimum)

Espace disque :
200 Mo (installation) - 1 Go (données - minimum)

Client :
Windows 10 et 11

Serveur :
Windows Server 2008 R2, 2012 R2, 2016, 2019 et 2022 (y compris version Core)

Base de données :
SQL Serveur 2017 et ultérieur