



**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



# Sangfor Athena Security Operations

---



## Cybermenaces 2026 : pourquoi vos défenses traditionnelles ne suffisent plus

- Sécuriser l'entreprise face aux attaques modernes
- Approche EDR + XDR
- Solutions de Sangfor Technologies

## Tendances majeures :

- Explosion des ransomwares
- Attaques sans fichier (fileless)
- Utilisation de l'IA par les cybercriminels
- Attaques multi-vecteurs (endpoint, réseau, cloud)

## Conséquence :

Les outils traditionnels ne détectent pas ces attaques à temps.

## Solutions classiques :

- Antivirus
- Firewall classique
- SIEM isolé

## Limites :

- Détection basée sur signatures
- Peu de visibilité sur les comportements
- Analyse fragmentée
- Réponse lente et manuelle

# 01 C'est quoi l' EPP de sangfor?

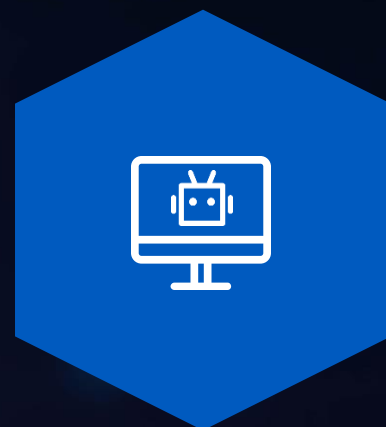


# What is Sangfor Athena EPP Now?



## Modern EPP

Plateforme de protection des terminaux Solution multicouche intégrant des fonctionnalités de prévention et des fonctions avancées, notamment EDR et de gestion.



## NGAV

Antivirus nouvelle génération doté de fonctionnalités avancées telles que l'analyse comportementale et l'intelligence artificielle



## EDR

Détection et réponse aux incidents sur les terminaux Détecte les violations de données et y répond après leur survenue.



## Endpoint Mgmt.

Identifie et gère les actifs des terminaux, en assurant la visibilité, le contrôle et l'atténuation des risques.

Protection contre tous les types de ransomware grâce à des moteurs de détection statiques et dynamiques basés sur l'IA.

Détecte les processus suspects liés aux ransomwares et les bloque en seulement 3 secondes afin de garantir un impact minimal sur les actifs des utilisateurs.

Les indicateurs de compromission des ransomwares sont collectés sur plus de 12 millions d'appareils déployés avec Athena EPP, ce qui lui permet d'atteindre un taux de précision de détection de 99,83 %.

En plus des protections existantes contre les ransomwares, telles que les fichiers appâts et l'authentification à deux facteurs RDP, Athena EPP offre des fonctionnalités dynamiques de sauvegarde et de récupération de fichiers pour sécuriser et restaurer intégralement vos données en cas de chiffrement par ransomware.

# Sangfor Athena EPP Function Overview



**Modern  
EPP**

**Prevention and  
Protection  
(AV/NGAV)**

Bloquez et supprimez les processus et fichiers malveillants.

**Detection and  
Response  
(EDR)**

Enquêter sur les activités suspectes non bloquées et y remédier.

**Endpoint  
Management**

Gestion et reporting des systèmes de points de terminaison



**Sangfor  
Athena EPP**

- Découverte et inventaire des actifs
- Stratégie d'analyse flexible
- Surveillance et analyse en temps réel
- Collecte des données comportementales et des journaux des terminaux
- Protection contre les ransomwares et récupération des données
- Protection contre les attaques par force brute

- Moteurs de détection basés sur l'IA
- Détection des APT et analyse de la chaîne d'attaque
- Détection des webshells
- Cartographie MITRE ATT&CK
- Isolation des terminaux
- Fichiers d'appât pour ransomware
- Détection et mise en quarantaine des fichiers
- Détection et réponse coordonnées

- **Gestion sur site et SaaS**
- **Gestion des vulnérabilités**
- **Gestion des correctifs**
- **Contrôle des applications**
- **Assistance à distance**
- **Journalisation et rapports**
- **Gestion de base des terminaux**
- **Désinstallation automatique des antivirus tiers**

avec Athena NGFW et Athena Secops

## Endpoint Secure Protect Agent - Essential Edition (includes service)

- Essential Endpoint Secure Protect Agent for PC/Workstation/Linux/Mac/Server,
- Includes Vulnerability Management, Inventory Management, compliance check, USB Control, Engine Zero, Neural-X, Basic Ransomware Protection, Software and Security Updates, and 7x24 Support

## Endpoint Secure Protect Agent - Ultimate Edition (includes service)

- Ultimate Endpoint Secure Protect Agent for PC/Workstation/Linux/Mac/Server,
- Includes Vulnerability Management, Inventory Management, compliance check, USB Control, Engine Zero, Neural-X, Basic Ransomware Protection, based on Essential, **add-on Enhanced Ransomware Protection (Three seconds to kill Ransomware and data Backup), Advanced Threat Protection and Application Control**
- Software and Security Updates, and 7x24 Support.

## 02 C'est quoi l' XDR de sangfor?

## Qu'est-ce que le XDR ?

**XDR = Extended Detection & Response**

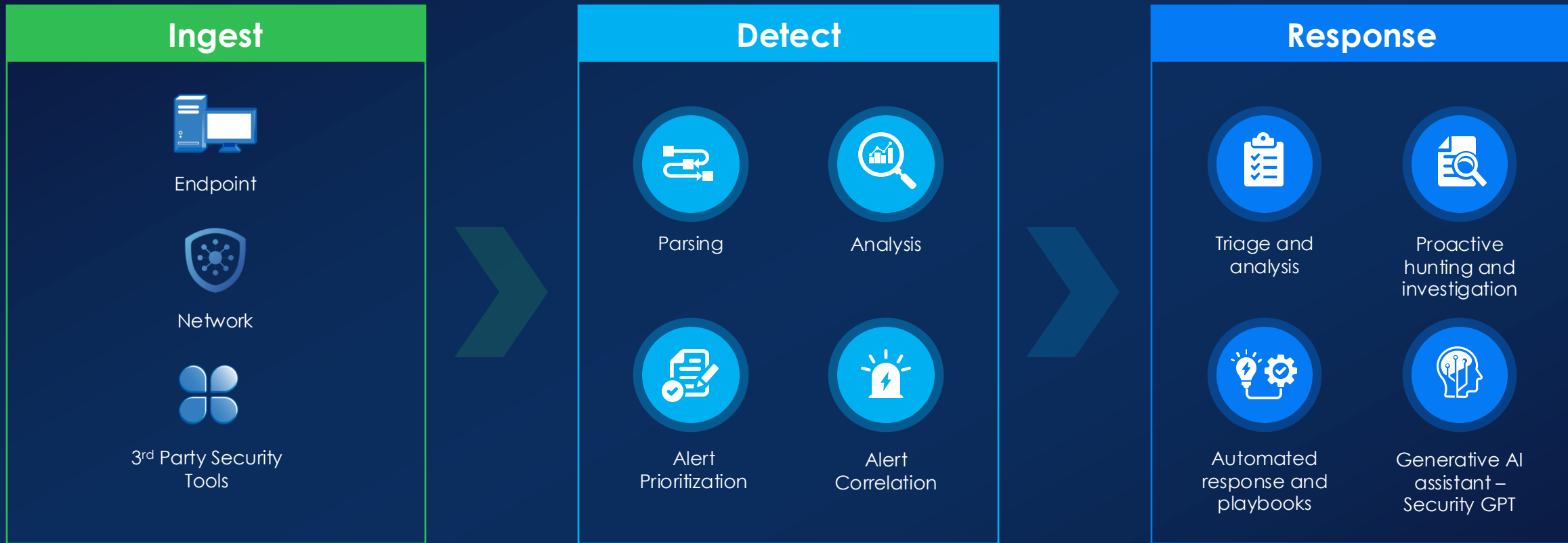
Le XDR corrèle les données provenant de :

- endpoints
- réseau
- serveurs
- cloud
- emails

## Avantages du XDR

Le XDR permet :

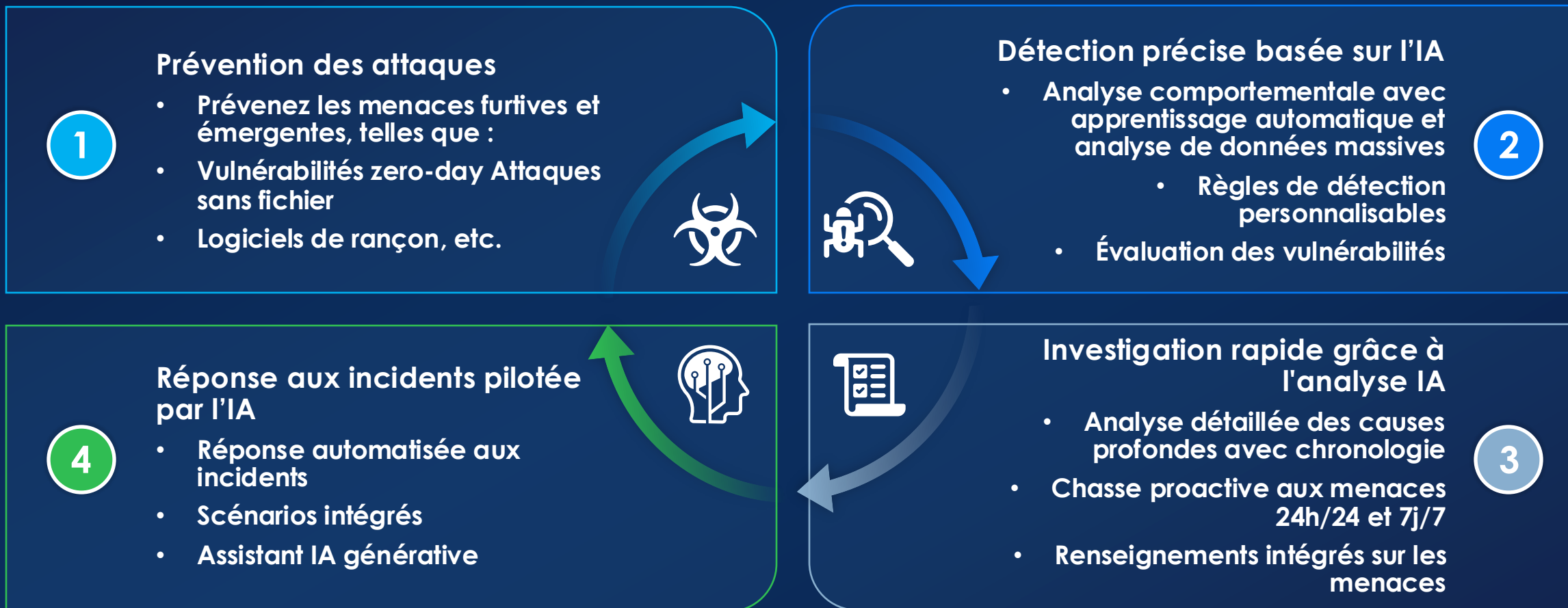
- **Visibilité globale** de la sécurité
- **Corrélation automatique des événements**
- Détection des **attaques complexes**
- Réduction du **temps d'investigation**



Collecte et ingestion de données télémétriques

Analyser et corréler les données pour détecter automatiquement les menaces cachées

Conseils pratiques pour améliorer les opérations de sécurité

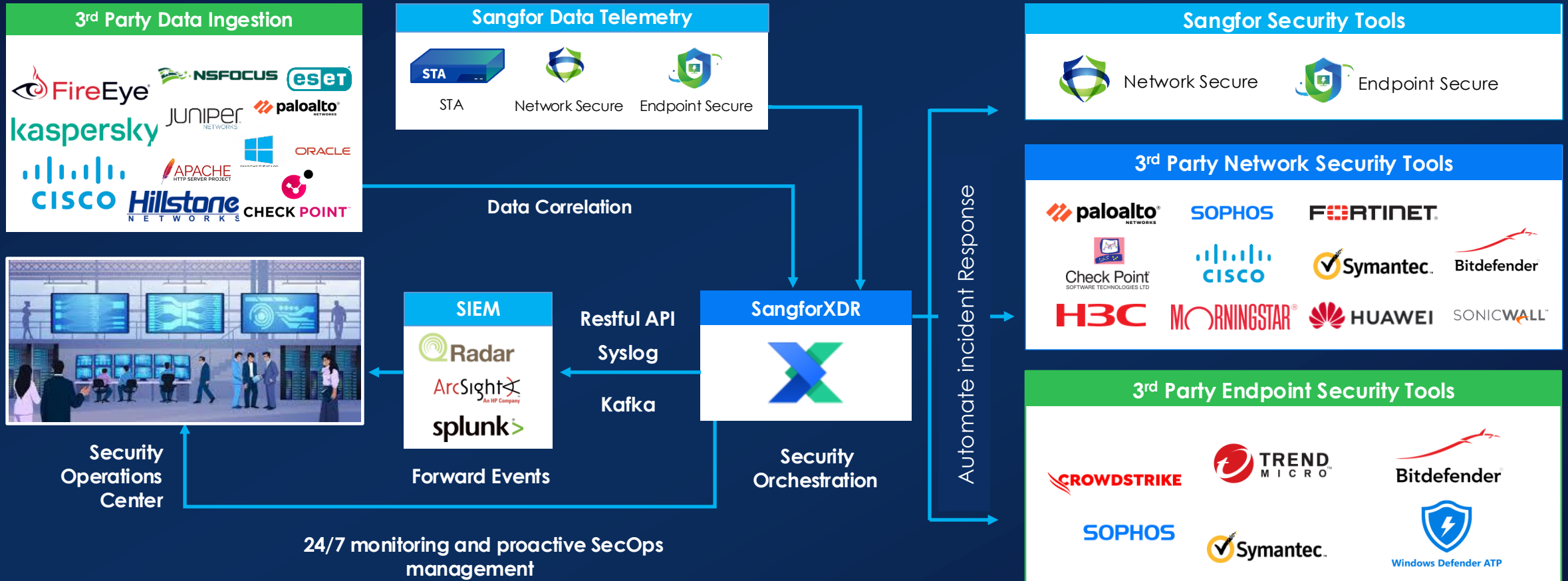




# Ce qu'il faut : une intégration transparente avec les outils de sécurité



Intégration entre Sangfor et les outils de sécurité tiers pour une visibilité accrue et un confinement rapide des menaces





## ALL-IN-ONE SECURITY PLATFORM

- Intègre les terminaux, le réseau, les outils tiers, SOAR, la gestion des tickets, les rapports.
- Offre une visibilité complète sur l'ensemble de l'infrastructure informatique.

## SIMPLIFY SEC OPS

- Réduisez le nombre d'alertes en corrélant et en analysant les données provenant de sources multiples.
- L'investigation et l'évaluation des menaces sont simplifiées et optimisées grâce à Security GPT.

## WIDER RANGE OF INTEGRATION

- Intégration transparente avec un large éventail d'outils de sécurité tiers
- Pour l'ingestion de données et les capacités de réponse aux incidents



## SCALABILITY & FLEXIBILITY

- Nous proposons des modèles sur site et SaaS.
- La souveraineté des données est préservée pour le modèle sur site, tandis que le SaaS offre une plus grande évolutivité.

## COST EFFECTIVE

- Tarification tout-en-un, sans frais cachés, réduisant le coût total de possession grâce à l'élimination du besoin de plusieurs outils de sécurité.
- Tarification simple et transparente.

## 03 EDR + XDR : la combinaison gagnante

Pourquoi combiner EDR et XDR

EDR

XDR

Protection **au niveau  
des endpoints**

**Vision globale** de la  
sécurité

## Cas de figure : attaque ransomware stoppée grâce à EDR + XDR

### Contexte

Une entreprise possède :

- 300 postes utilisateurs
- un serveur de fichiers
- un firewall
- un SOC interne

Les solutions déployées :

- EDR sur tous les endpoints**
- XDR pour corrélérer les événements réseau, endpoint et serveurs**

# Étape 1 — L'attaque initiale (Phishing)



Un employé reçoit un email contenant :

- une **facture PDF malveillante**
- un **lien vers un site compromis**

L'utilisateur télécharge un fichier qui exécute un **loader malware**.

## Ce que voit l'EDR

Sangfor Endpoint Secure détecte :

- création d'un **processus suspect**
  - exécution d'un script **PowerShell anormal**
  - connexion vers un **serveur C2**
- L'EDR génère **une alerte comportementale**

### Étape 2 — Tentative de communication avec le serveur de commande (C2)

Le malware essaie de contacter un serveur externe pour :

- télécharger un ransomware
- recevoir des instructions

#### Ce que voit le XDR

Sangfor Cyber Command corrèle :

- trafic réseau anormal
- domaine malveillant connu
- activité suspecte sur le poste

→ Le XDR confirme **une activité de type malware C2.**

L'attaquant tente ensuite :

- d'utiliser **des identifiants volés**
- de scanner le réseau
- d'accéder au **serveur de fichiers**

## Détection combinée

EDR détecte :

- utilisation anormale de **credential dumping**
- outil type **Mimikatz**

XDR détecte :

- plusieurs tentatives de connexion internes
- comportement similaire sur d'autres machines

→ Le XDR **reconstruit la chaîne d'attaque complète.**

Le malware tente de :

- chiffrer les fichiers
- désactiver les sauvegardes
- supprimer les logs

### Réaction automatique

EDR :

- bloque le processus
- isole le poste du réseau**

XDR :

- déclenche **une alerte critique SOC**
- bloque la communication avec le domaine malveillant
- identifie **les machines potentiellement affectées**

Grâce au XDR, l'équipe sécurité peut voir :

- **la timeline complète de l'attaque**
- la machine initiale compromise
- les tentatives de propagation

Le SOC peut :

- rechercher le hash du malware sur tous les endpoints
- vérifier si d'autres postes sont infectés
- appliquer des règles de blocage globales.

Sans EDR + XDR :

- ransomware déployé
- serveurs chiffrés
- arrêt de production

Avec EDR + XDR :

- ✓ infection contenue sur **1 seul poste**
- ✓ attaque stoppée avant le ransomware
- ✓ visibilité complète sur l'incident
- ✓ réponse rapide



Département Commercial  
WCA

 **HAFS**  
Distributeur à valeur ajoutée **WCA**

***Vous accompagne***



[www.hafs-networks.com](http://www.hafs-networks.com)  
Visitez notre site web



[sales-ci@hafs-networks.com](mailto:sales-ci@hafs-networks.com)  
Envoyez-nous un e-mail



(+225) 07 69 32 13 55  
Contact commercial 1



(+225) 07 59 05 85 82  
Contact commercial 2

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

