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

HAFS
Distributeur à valeur ajoutée

PortfolioSolutions

Hillstone NETWORKS

SANGFOR

SECPOINT®

HORNETSECURITY BY proofpoint.

SEARCHINFORM

NEOWAVE

Axidian

CyberShield

Synology®

MOBOTIX

RUCKUS NETWORKS

EXTRAVIS
Analyze • Automate • Accelerate

Wiflyx® TECHNOLOGY
Empowering Connectivity

HAFS MediaVision

Ruijie | Reyee

Site web : www.hafs-networks.com

France
sales@hafs-networks.com
+33 (0)6 51 10 87 49 / (0)9 74 98 52 96

Côte d'Ivoire
sales-ci@hafs-networks.com
+225 07 89 82 56 49 / +225 07 59 05 85 82

Thème
NIPS + NDR : Détection avancée & Prévention des intrusions par l'IA

Detect → Block → Remediation

Conformité PCI-DSS | OWASP Top 10 | ISO 27001

Agenda

- Problématique métier
- Proposition de valeur du NIPS Hillstone
- Proposition de valeur du NDR Hillstone
- Argumentaire de choix entre l’IPS et NG firewall + module IPS

1

Problématique métier

Les vulnérabilités à haut risque connaissent une croissance explosive

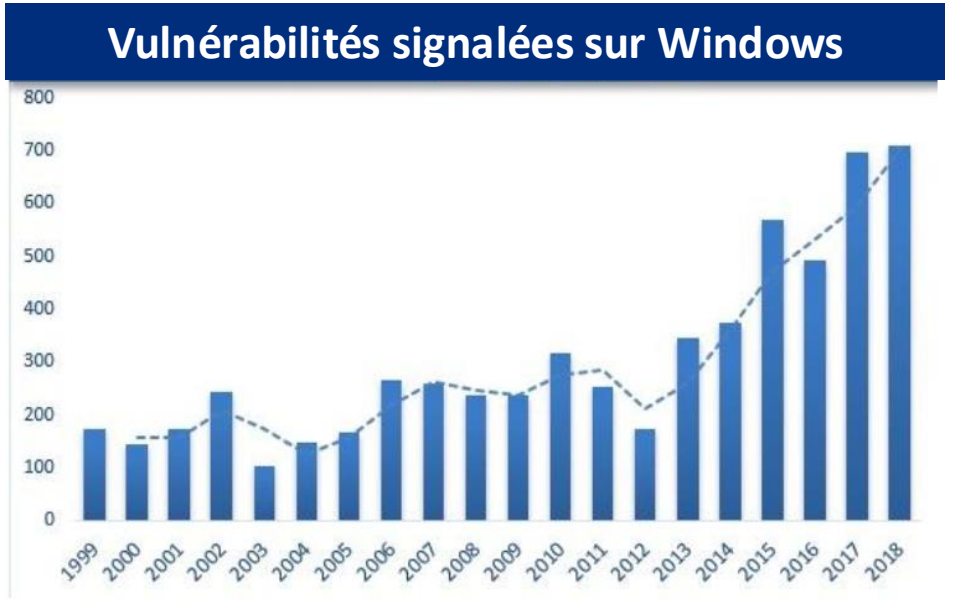
Faille Heartbleed

Vulnérabilité Bash Shellshock

Vulnérabilité de désérialisation Java

IIS 7 HTTP.sys

Vulnérabilité d'accès non autorisé à Redis



Le nombre de vulnérabilités signalées pour le système d'exploitation Windows connaît une croissance explosive

L’IPS est encore plus pertinent dans le paysage actuel de la sécurité réseau

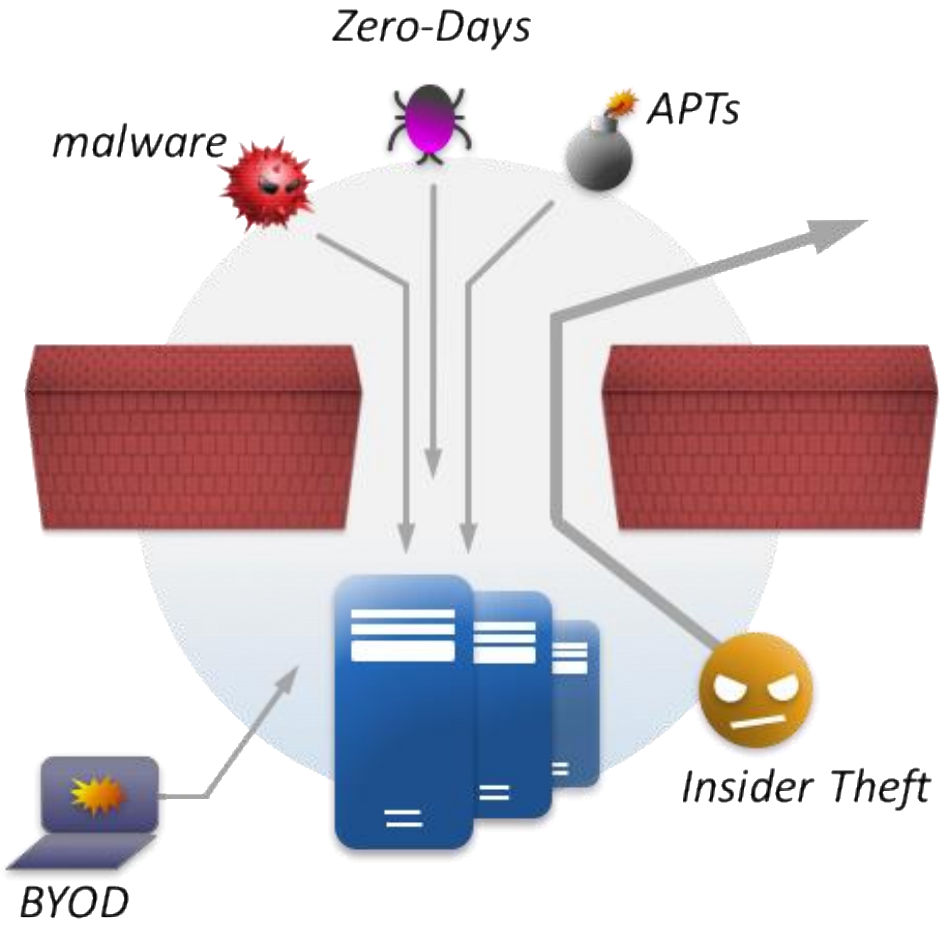
- IDPS dédié
- Défense en profondeur
- Niveaux de performance élevés avec un débit soutenu
- Pour la segmentation du réseau interne
- Solution IDPS d’un autre fournisseur

- 85 % des nouveaux IDPS autonomes seront déployés dans des centres de données (cloud ou sur site).
- Plus de 40 % des nouveaux déploiements d’IDPS ne se trouvent pas en périphérie. Gartner estime qu’à fin 2021, 80 % des nouveaux IDPS autonomes seront déployés pour des usages internes, contre environ 40 % en 2018

Guide du marché des systèmes de détection et de prévention des intrusions | 1er juillet 2019

Les solutions IPS autonomes sont idéales lorsque vous avez besoin d’un meilleur blocage et de meilleures performances

Les compromissions des réseaux internes se produisent à un rythme alarmant

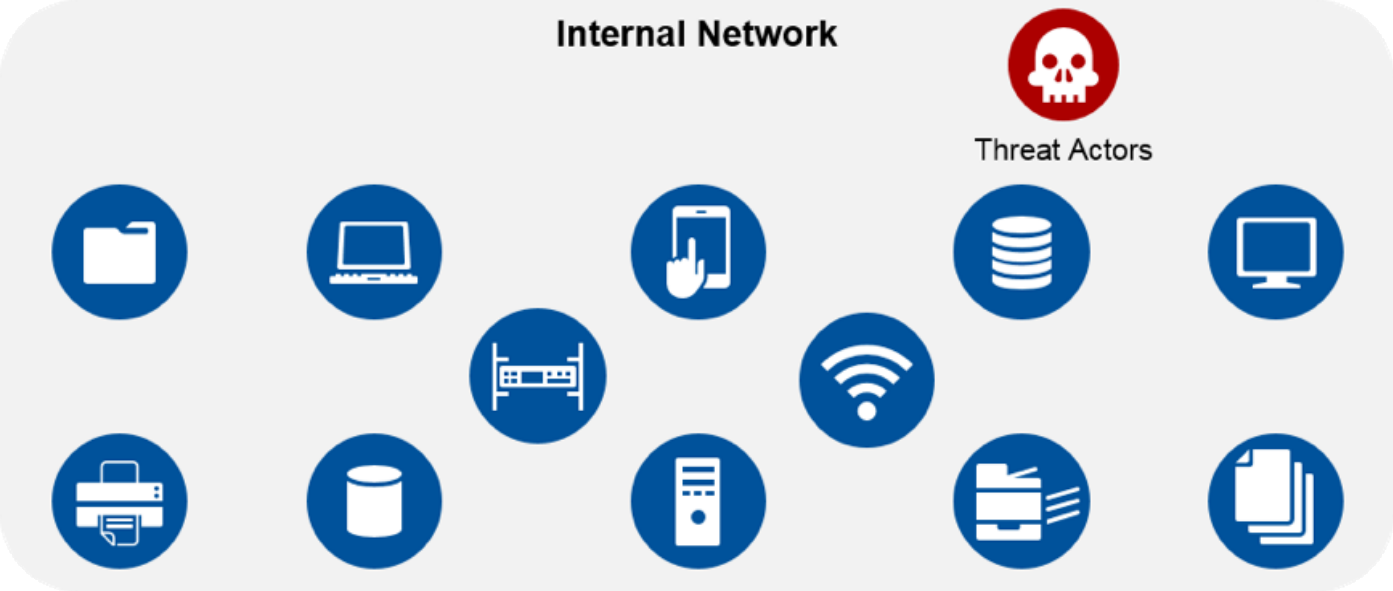


Les défenses traditionnelles basées sur les signatures ne peuvent arrêter que les anciennes attaques « amateurs »

De nouvelles **attaques sophistiquées** parviennent à pénétrer tous les réseaux.

« Dans 60 % des cas,les attaquants sont capables de compromettre une organisation en quelques minutes. » – Verizon 2015 DBIR

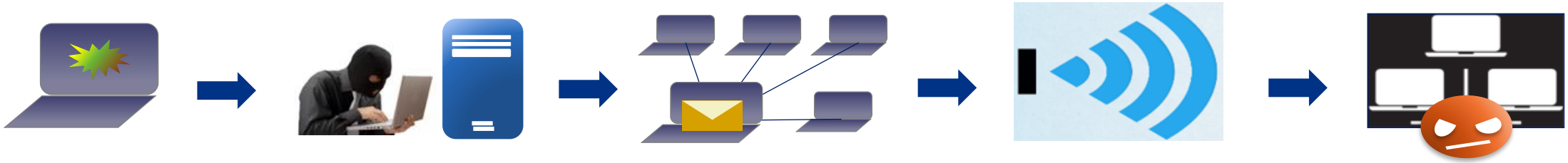
Les menaces se propagent facilement dans les réseaux internes plats…



« …quelle que soit leur motivation, si des adversaires parviennent à prendre pied sur votre réseau interne, ils peuvent se déplacer latéralement et accéder à tout ce qui s'y trouve. C'est l'une des principales raisons pour lesquelles les compromissions modernes sont si dévastatrices, tant par la quantité de données perdues que par le temps passé sur le réseau avant leur découverte. La détection et la prévention des mouvements latéraux sont donc devenues des domaines d'attention majeurs. »

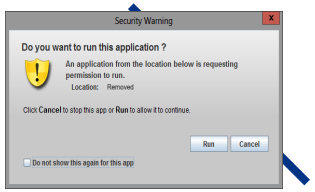
-Source : Gartner (septembre 2016)

Interrompt les serveurs critiques et la continuité d'activité



- Une attaque de phishing survient lorsque le personnel navigue sur Internet
- C&C
- Le pirate contrôle complètement l'hôte
- Un faux e-mail interne et sa pièce jointe propagent les dommages à l'intérieur du réseau
- Davantage d'hôtes sont
- L'hôte perd le contrôle
- Lance une attaque DDoS depuis l'intérieur
- Entraîne la défaillance des serveurs et du pare-feu
- Au final, le réseau et l'activité sont paralysés

Exfiltrer des données sensibles via un hôte compromis



- Une attaque de phishing survient lorsque le personnel navigue sur Internet
- Injecte des logiciels malveillants avec de fausses signatures antivirus ou des signatures expirées
- Le logiciel antivirus ne détecte pas le logiciel malveillant
- Le logiciel malveillant est exécuté
- C&C
- Télécharge un fichier PE
- Le pirate contrôle complètement l'hôte
- Le serveur de base de données est compromis via l'hôte compromis

Quand utiliser un IPS plutôt qu'un NGFW ?

Système de détection et de prévention des intrusions

- Lorsque l'on souhaite bénéficier d'une protection de pointe
- Lorsque différents membres du personnel gèrent l'IPS à partir des pare-feu
- Lorsqu'un débit élevé est requis
- Pour activer la segmentation du réseau sur certaines parties du réseau interne
- En tant que solution IDS sur certaines parties du réseau interne

Next-Generation Firewall

- Lorsqu'une vue d'ensemble des menaces réseau est nécessaire
- Lorsque les performances et le débit ne sont pas une priorité
- Lorsqu'une reconnaissance des applications est nécessaire (visibilité et contrôle du trafic)
- Lorsque la surveillance des logiciels malveillants est obligatoire
- Lorsque la reconnaissance de l'identité de l'utilisateur est nécessaire

Une histoire d'« innovation » continue

2006 — Fondée par des vétérans de NetScreen

2008 — L'un des premiers fournisseurs à lancer un pare-feu multicœur

2010 — L'une des premières plateformes de pare-feu 100G du secteur

2013 — Architecture de pare-feu entièrement distribuée 360G

2014 — Premier fournisseur à lancer un pare-feu basé sur l'IA

2015 — CloudHive, l'une des premières solutions à prendre en charge OpenStack et VMware

2016 — CloudEdge, premier NGFW virtuel prenant en charge les principaux clouds publics et la NFV

2017 — Solution NDR basée sur l'IA

2018 — Plateforme de pare-feu de centre de données 1T

2019 — Solution SD-WAN sécurisée

2021 — Solution XDR alimentée par l'IA

2022 — Solution CWPP : CloudArmour — ZTNA

2023 — Plateforme de pare-feu de centre de données 3,5T

Futur

Innovation de chipset propriétaire

- FPGA
- ASIC
- **SECoC**

AI

- Détection des menaces
- Renseignement sur les menaces
- Opérations de sécurité
- Services managés

IA dans la sécurité

Gestion, analyse et opérations de sécurité centralisées

Hillstone NETWORKS

iSource

HSM/vHSM

HSA/vHSA

CloudView

PROTECTION DE LA PÉRIPHÉRIE


NGFW


DCFW


NIPS

PROTECTION CLOUD

CloudArmour

CloudHive

CloudEdge

PRÉVENTION DES COMPROMISSIONS


BDS

vBDS

PROTECTION DES APPLICATIONS


ADC

vADC


WAF

vWAF

ZTNA

SD-WAN

XDR

NDR

CWPP

Micro-Segmentation

Gestion, analyse et opérations de sécurité centralisées

Hillstone NETWORKS

iSource

HSM/vHSM

HSA/vHSA

CloudView

PROTECTION DE LA PÉRIPHÉRIE


NGFW


DCFW


NIPS

PROTECTION CLOUD

CloudArmour

CloudHive

CloudEdge

PRÉVENTION DES COMPROMISSIONS


BDS

vBDS

PROTECTION DES APPLICATIONS


ADC

vADC


WAF

vWAF

ZTNA

SD-WAN

XDR

NDR

CWPP

Micro-Segmentation

2

Proposition de valeur du NIPS Hillstone

Hillstone NIPS – Un système complet de prévention des intrusions réseau

Nouvelle plateforme matérielle

01 Détection et défense complètes contre les menaces réseau

06 Déploiement facile avec une interruption minimale du réseau

05 Gestion simplifiée et centralisée pour une exploitation efficace de la sécurité

Protection avancée contre les menaces tout au long du cycle de vie de la menace 02

Meilleure compréhension grâce à des rapports riches et détaillés 03

Haute fiabilité pour garantir le fonctionnement fiable du réseau 04

Haute performance du trafic chiffré SSL

Capacité améliorée d'accélération matérielle du déchiffrement SSL

- Augmentation du trafic HTTPS
- Nouvelles méthodes d'attaque
- Exigences clés de sécurité

Les NIPS assurent une protection complète du trafic chiffré SSL grâce à un module intégré de chiffrement/déchiffrement

Coût réduit

Avec capacité d'accélération matérielle du déchiffrement SSL

Sécurité et visibilité

Permet la détection des systèmes, applications, logiciels malveillants et clients

Garantie d’un traitement massif

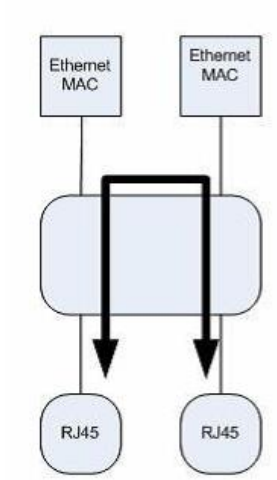
Débit élevé au niveau applicatif

01 Interface haute densité
Le S5500-IN est équipé de 8 ports GE (4 paires de contournement) + 16 ports SFP+ + 2 ports QSFP+ fixes d'entrée/sortie

02 La plupart des modèles prennent en charge un emplacement d'extension

03 Prise en charge du contournement matériel de l'interface optique/électrique

04 Espace de stockage intégré de grande capacité, extensible à la demande



Prise en charge complète du bypass, garantissant la continuité d’activité en déploiement en série

Détection contextuelle

Connaissance des utilisateurs

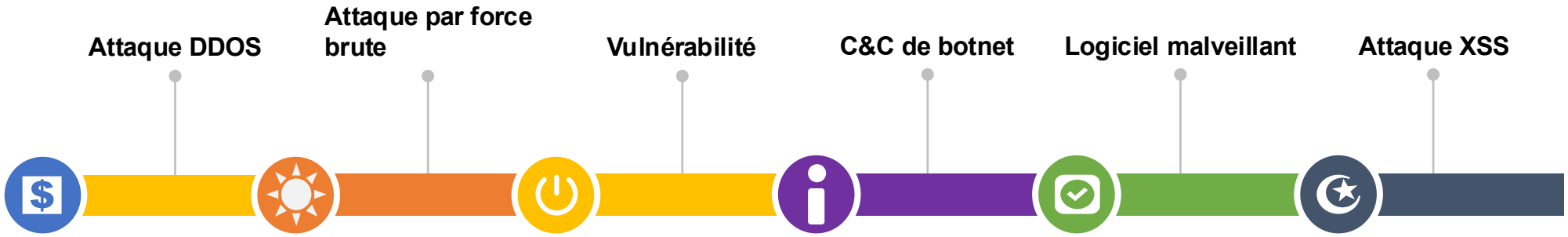
Identifie précisément les utilisateurs définis et non définis et analyse le trafic utilisateur ainsi que les connexions simultanées

Connaissance des applications

Identifie précisément plus de 3 000 applications réseau et des centaines d'applications mobiles/cloud, y compris les applications utilisant un trafic chiffré SSL

Connaissance des risques

Fournit des informations multidimensionnelles, notamment le niveau de risque, les vulnérabilités connues, la consommation importante de bande passante et le comportement de transfert de fichiers



Plus de 10 000 règles d'intrusion et une base de données de dizaines de millions de signatures de virus pour détecter et prévenir différents types d'attaques

Protection avancée contre les menaces tout au long du cycle de vie de la menace

Renseignement sur les menaces en temps réel : prévention proactive des menaces
L'IPS bloque l'exploitation des vulnérabilités
La réputation IP bloque l'accès des IP à risque aux serveurs
Le filtrage d'URL contrôle l'accès des utilisateurs aux sites spécifiés
L'antivirus empêche les utilisateurs de visiter des sites malveillants et de phishing
L'anti-spam classe et bloque les spams potentiels

L'antivirus réagit aux virus connus
Le sandbox cloud réagit aux virus inconnus

La prévention C&C des botnets bloque le canal de commande et détecte les bots présents sur l'intranet

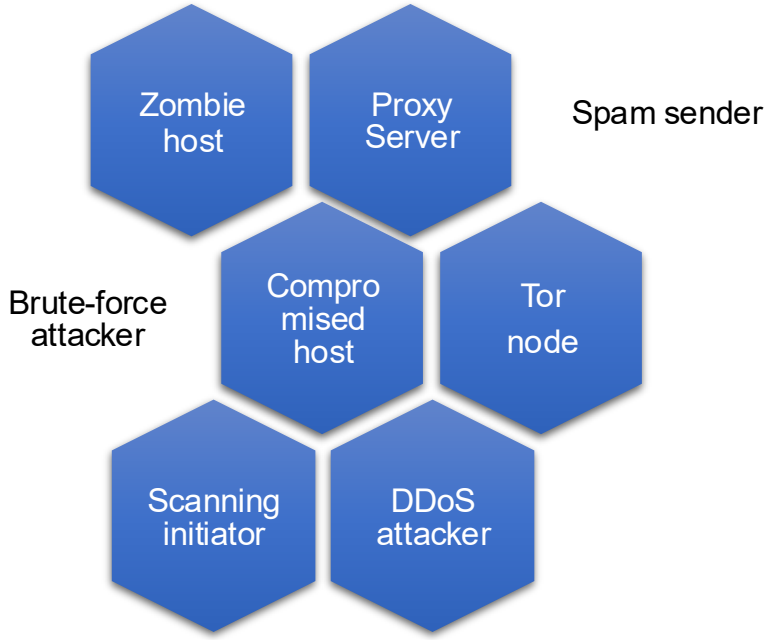
Avant compromission | **Compromission** | **Après compromission**

Prévention des intrusions | **IP Reputation** | **URL Filtering** | **Anti-spam** | **Antivirus** | Sandbox cloud | **Prévention C2 des botnets**

Fonctionne conjointement avec le NGFW Hillstone

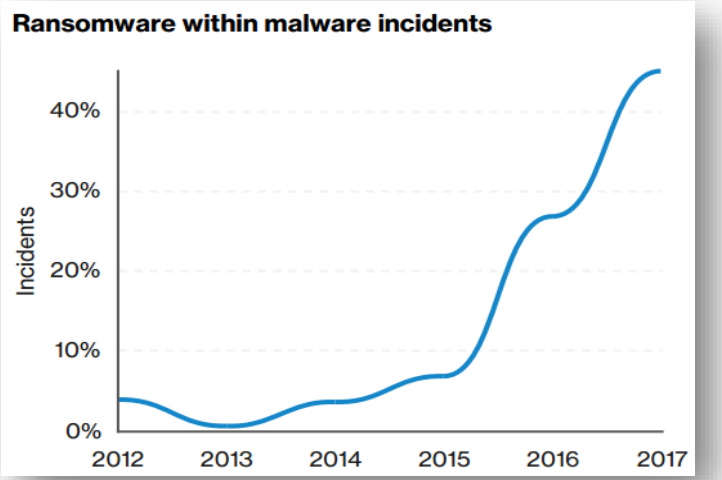
Réputation IP – Identification et blocage de plusieurs catégories d'IP à risque

- Renseignement sur les menaces IP : enregistre tous les journaux de trafic provenant d' IP à risque et bloque leur accès à l' intranet
- Identification de plusieurs risques IP : hôtes zombies, spammeurs, etc.
- Mise à jour des signatures de réputation IP toutes les heures pour disposer des dernières informations de renseignement sur les menaces IP



Service de filtrage des virus – détecte et bloque efficacement les ransomwares

- Moteur efficace de détection des flux : protection antivirus d’ un seul appareil jusqu’ à 24 Gbit/s
- Des dizaines de millions de signatures de virus : mise à jour quotidienne en temps réel pour détecter et bloquer efficacement tous les types de logiciels malveillants
- Protection efficace contre les ransomwares : détecte et bloque efficacement la propagation des logiciels malveillants et ransomwares, filtre et bloque les virus présents dans les fichiers transférés via le protocole SMB lors de la reprise après interruption



Les incidents liés aux ransomwares augmentent rapidement ; les mesures de protection contre les virus sont essentielles

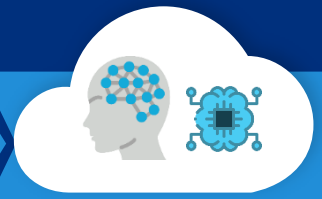
Sandbox cloud pour la détection et la prévention des fichiers malveillants

Static Analyse/ Pre-Processing

- Liste blanche d'URL, vérification de la signature des fichiers
- Échantillons suspects basés dans le cloud
- Requête MD5 pour analyser le comportement du fichier ; vérification et rapport

Analyse comportementale

- Simulation Windows/Android/macOS
- Analyse comportementale des processus de fichiers, des actions du registre et du comportement réseau
- Détection des techniques d'évasion



Renseignement cloud

- Identifie les fichiers malveillants
- Génère les journaux et rapports de menaces
- Partage les renseignements sur les menaces
- Bloque les menaces

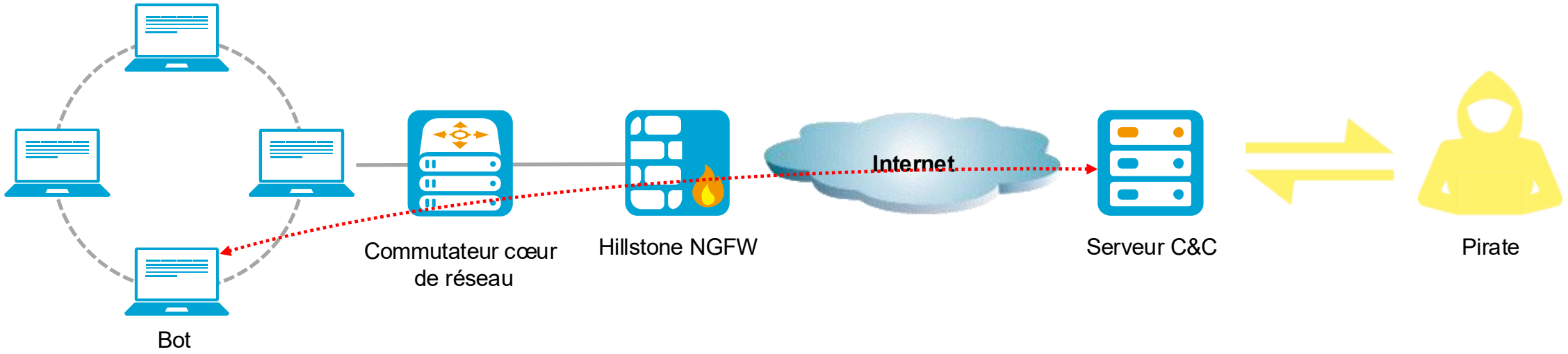
Fichiers malveillants

Rapports

Mise à jour des signatures

NIPS

Prévention complete des C&C de botnets



C2 Address Database

Détection des sinkholes DNS

DNS Tunnel Détection

Détection des domaines DGA

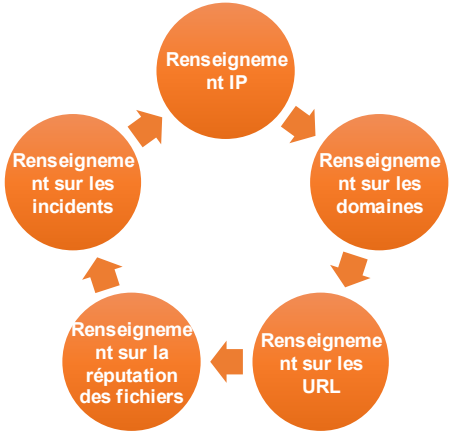
La technologie IA permet une protection intelligente et efficace contre les menaces

- **Détection du trafic chiffré**
  - Exploite l'IA pour analyser et détecter le trafic chiffré sans déchiffrement
  - Améliore l'efficacité et la précision de la détection des comportements anormaux dans le trafic chiffré
- **Anti-DDoS intelligent**
  - Configuration automatique du seuil de protection contre les floods grâce à l'établissement d'une référence basée sur le machine learning
  - Protection DDoS précise et efficace avec configuration automatisée

Détection des algorithmes de génération de domaines (DGA)

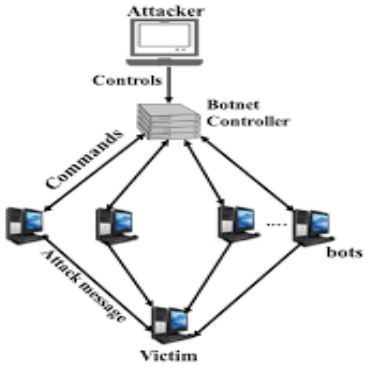
- Construit, entraîne et met à jour le modèle de détection en temps réel
- Assure une meilleure défense contre les menaces inconnues avec une efficacité accrue

Atténuation des menaces inconnues



Renseignements internes : FW, IPS, WAF, sandbox cloud, collecte de trafic, CloudView

Renseignements externes : renseignements métier, renseignements en sources ouvertes



Données riches de renseignement sur les menaces

Intégration de renseignements provenant de plusieurs sources

Atténuation des menaces fondée sur les renseignements

Prévention en amont

Avant l'attaque :
Les renseignements sur les menaces en temps réel sont activement transmis afin de prévenir les menaces en amont.

Activation continue

Pendant l'attaque :
Permet au dispositif de sécurité d'améliorer ses capacités de détection des menaces.

Réduction des menaces

Après l'attaque :
Grâce aux renseignements disponibles, le NIPS peut détecter les hôtes compromis et contribuer à atténuer la menace.

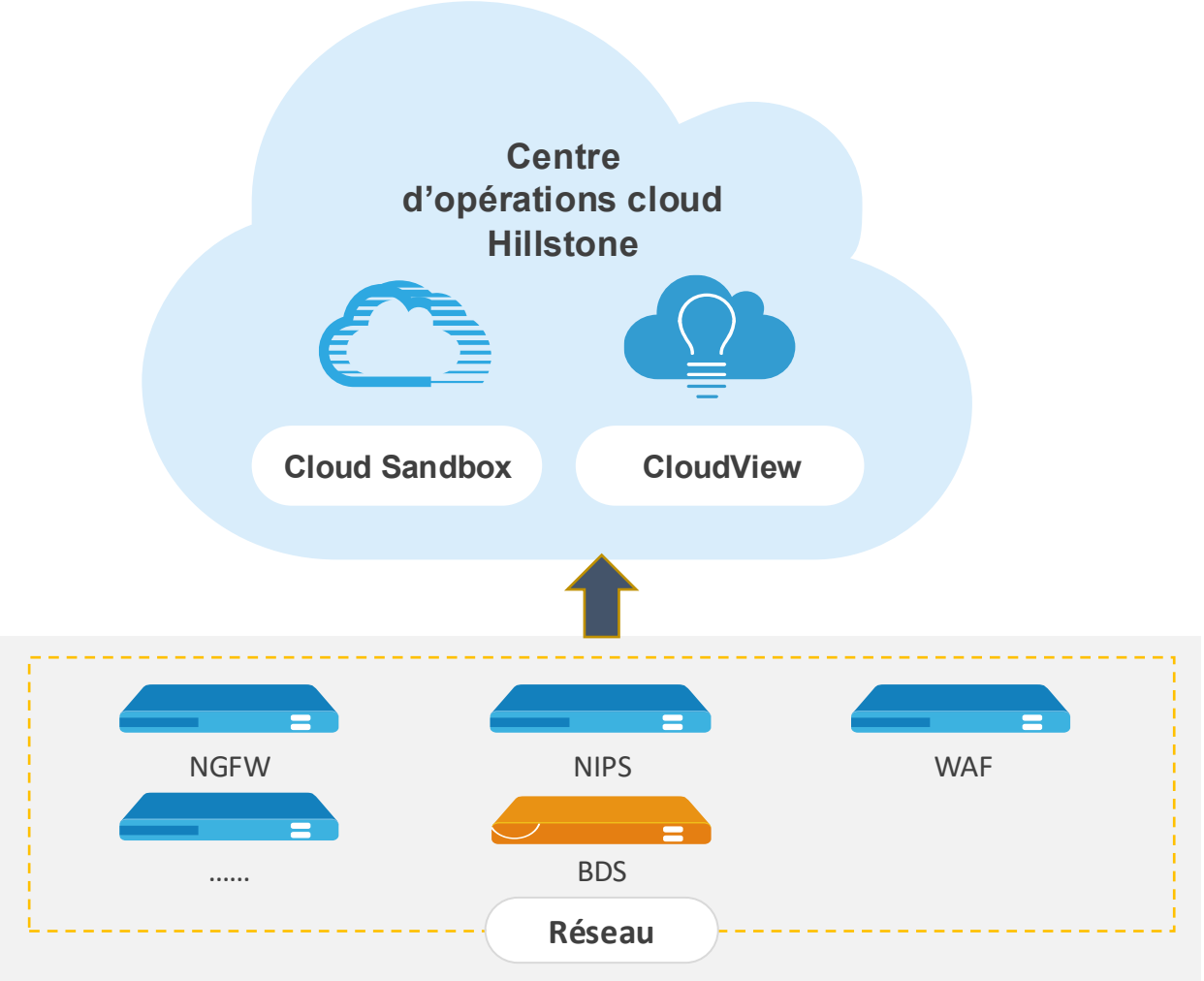
Interaction avec les renseignements basée sur le cloud

Prend en charge la liaison avec le pare-feu Hillstone, CloudView, HSM, HAS et iSource

01 **Surveillance des menaces en temps réel**

02 **Gestion des incidents**

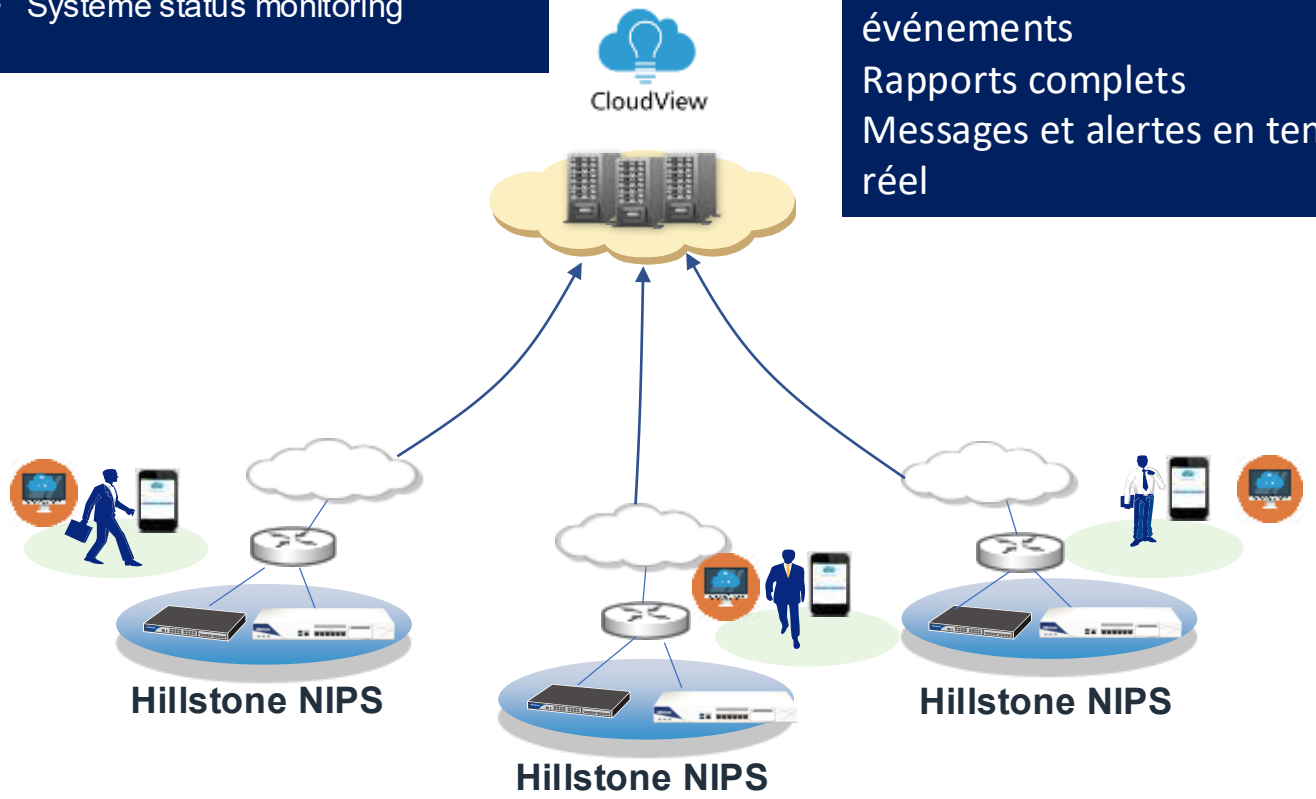
03 **Signature update**



Surveillance et analyse de sécurité basées sur le cloud

Centralized Menace Surveillance
- Menace monitoring
- Système status monitoring

Analyse et alertes de menaces
Journaux des menaces et événements
Rapports complets
Messages et alertes en temps réel



Real-time Monitoring

- 24/7 monitoring and alerts
- Threat analysis and reports
- Mobile/web access

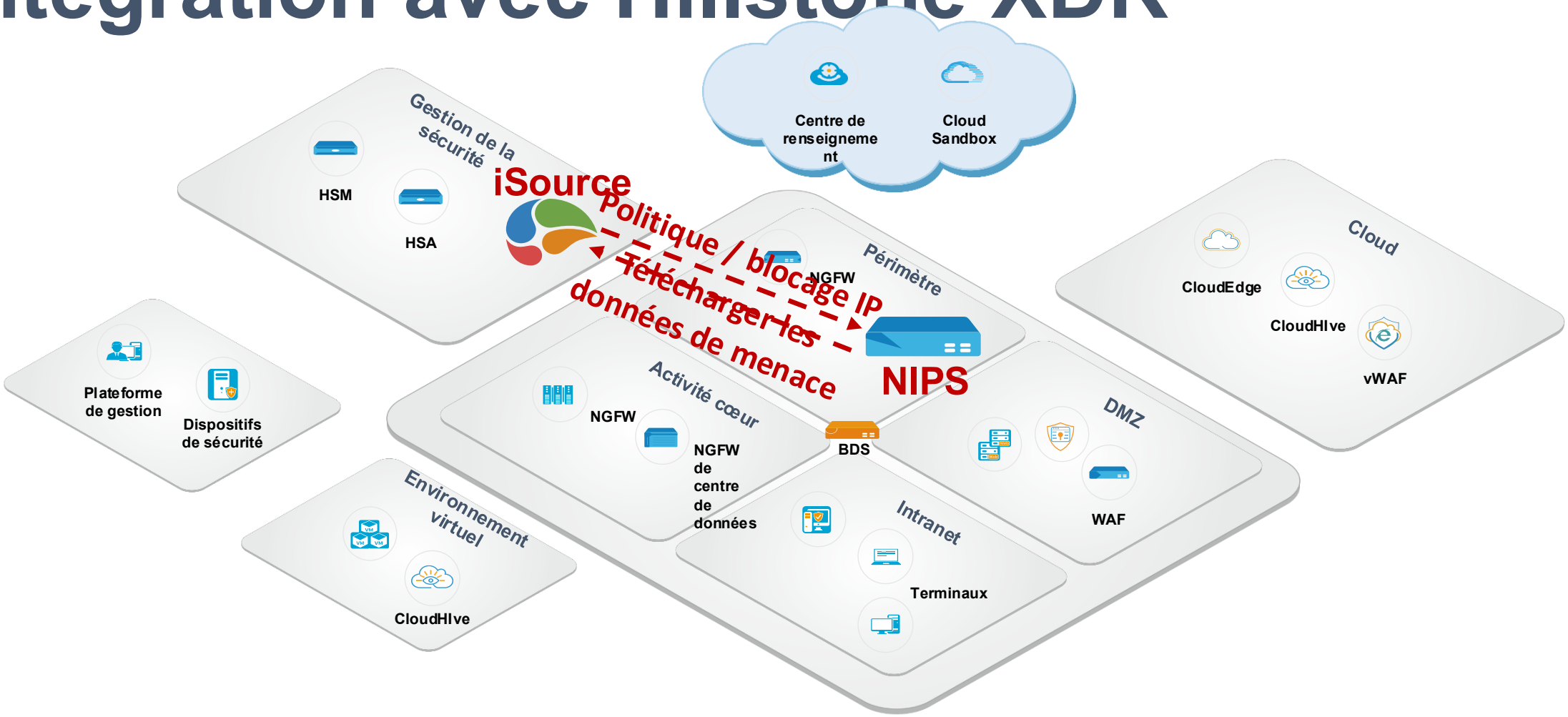
Ease of Deployment

- No deployment required
- No maintenance
- Easy and instant subscription

Low/Flexible Investment Options

- Free to initiate (Includes essential features)
- Pay to subscribe (For advanced features, Professional Version)
- Security as a Service (SaaS)

Intégration avec Hillstone XDR



Le NIPS envoie les données de menace (événement de menace / PCAP forensique) vers iSource, renforçant l'analyse corrélative des menaces

Meilleure compréhension grâce à des rapports riches et détaillés

Système de reporting IPS

Analyse du trafic réseau
État de santé du trafic

Évaluation des applications et des risques
État des applications et risques liés aux actifs critiques

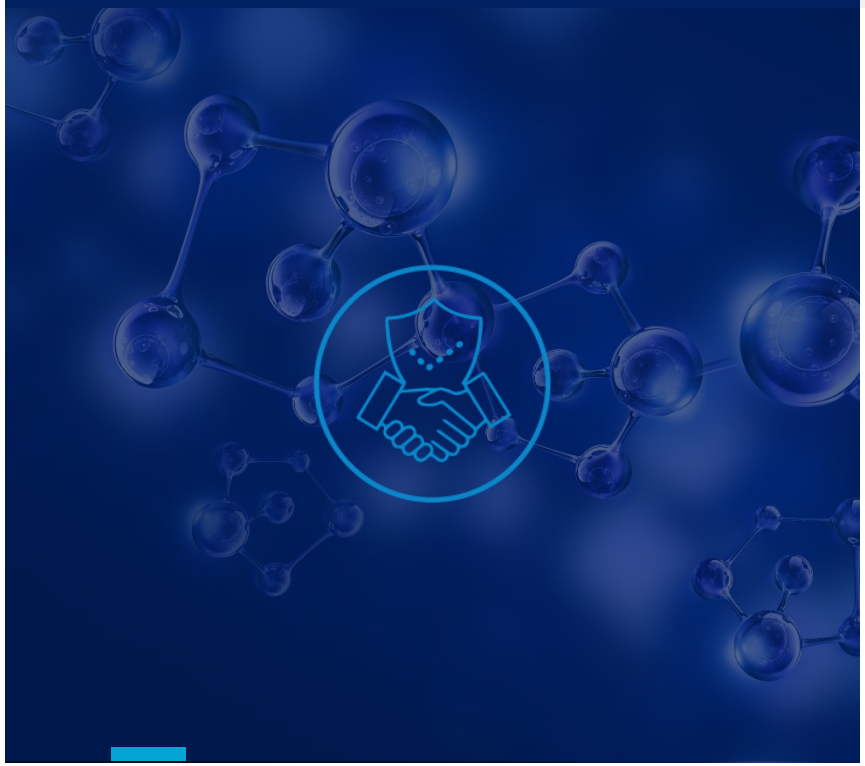
État de fonctionnement du système
Affichage du matériel système et des ressources informatiques

Vue d'ensemble des risques de sécurité
Affichage complet des risques de sécurité et de leur importance

Évaluation des menaces
Attaques et comportements anormaux

Rapports basés sur le profil utilisateur
Direction/C-level, responsables des applications, administrateurs de sécurité réseau

Haute fiabilité pour garantir le fonctionnement fiable du réseau



Système fiable
Système d'exploitation sûr et stable, Hillstone StoneOS

Réduit les défaillances matérielles grâce à des composants fiables.Disque dur stable.
Alimentation redondante

Dispositif stable avec surveillance en temps réel de son état.
Surveille l'utilisation du CPU/de la mémoire, les processus, l'état des ports réseau,les informations sur les menaces, etc.

High reliable networking
Supports AP / AA mode

Le déploiement en bypass garantit la continuité d'activité
Fournit des paires de bypass par défaut
Prend en charge l'extension des interfaces de bypass

Exploitation efficace de la sécurité : gestion intelligente des politiques

Déploiement automatisé des politiques utilisateur
Autorisation dynamique RADIUS
Applique automatiquement la politique utilisateur via un message CoA

Policy Redundancy Check
Discover redundant policies for deletion

Policy Analysis
Adjust the policies by observing the hit counts and hit trends

Policy Group
Efficient policy management based on business requirement

Aggregate Policy
A set of policies act as one single policy

Policy Assistant
Refine a general policy into detailed policy

Déploiement facile

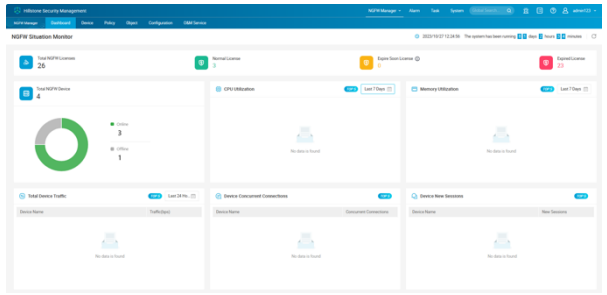
Lancement rapide de nouveaux services

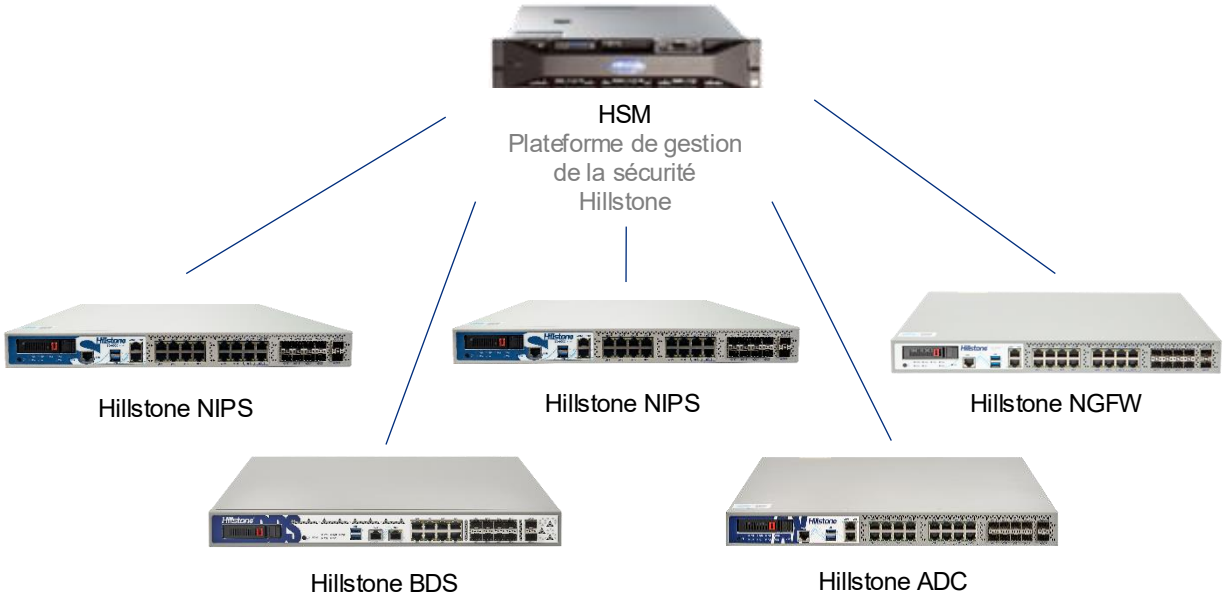
Ajustement dynamique des politiques

Efficacité accrue et réduction des coûts indirects

Exploitation efficace de la sécurité : plateforme de gestion simplifiée et centralisée

Interface de gestion intuitive





Le NIPS peut être géré par l'appliance matérielle HSM et l'appliance virtuelle vHSM

Prise en charge de l'enregistrement et de la gestion des appareils NIPS via HSM/vHSM

Prise en charge de la mise à niveau de l'image NIPS via HSM/vHSM

Prise en charge de la configuration, de la surveillance et du reporting NIPS, ainsi que de la mise à jour en ligne/hors ligne des signatures NIPS

Prise en charge de l'API RESTful

Déploiement facile avec une interruption minimale du réseau

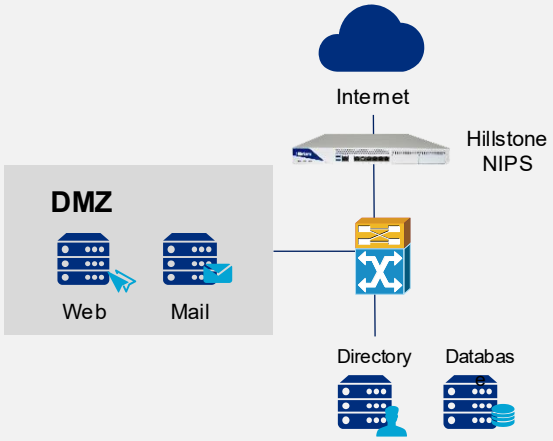
Plug-and-play with three easy steps:

- Connect the line
- Select the mode
- Bundle the policy as applicable

Minimum network disruption

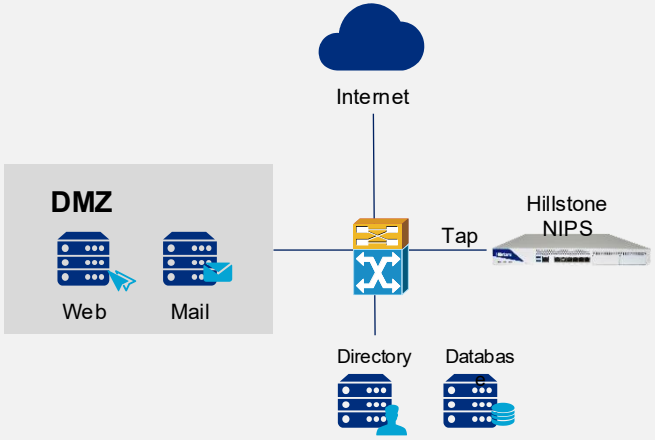
- No network topology change
- No network configuration needed
- No network traffic interruption

Prise en charge VSYS



Inline Mode: Blocking/monitoring

- Real time monitoring and blocking
- L2 transparent or L3 routing
- Two ports requirement



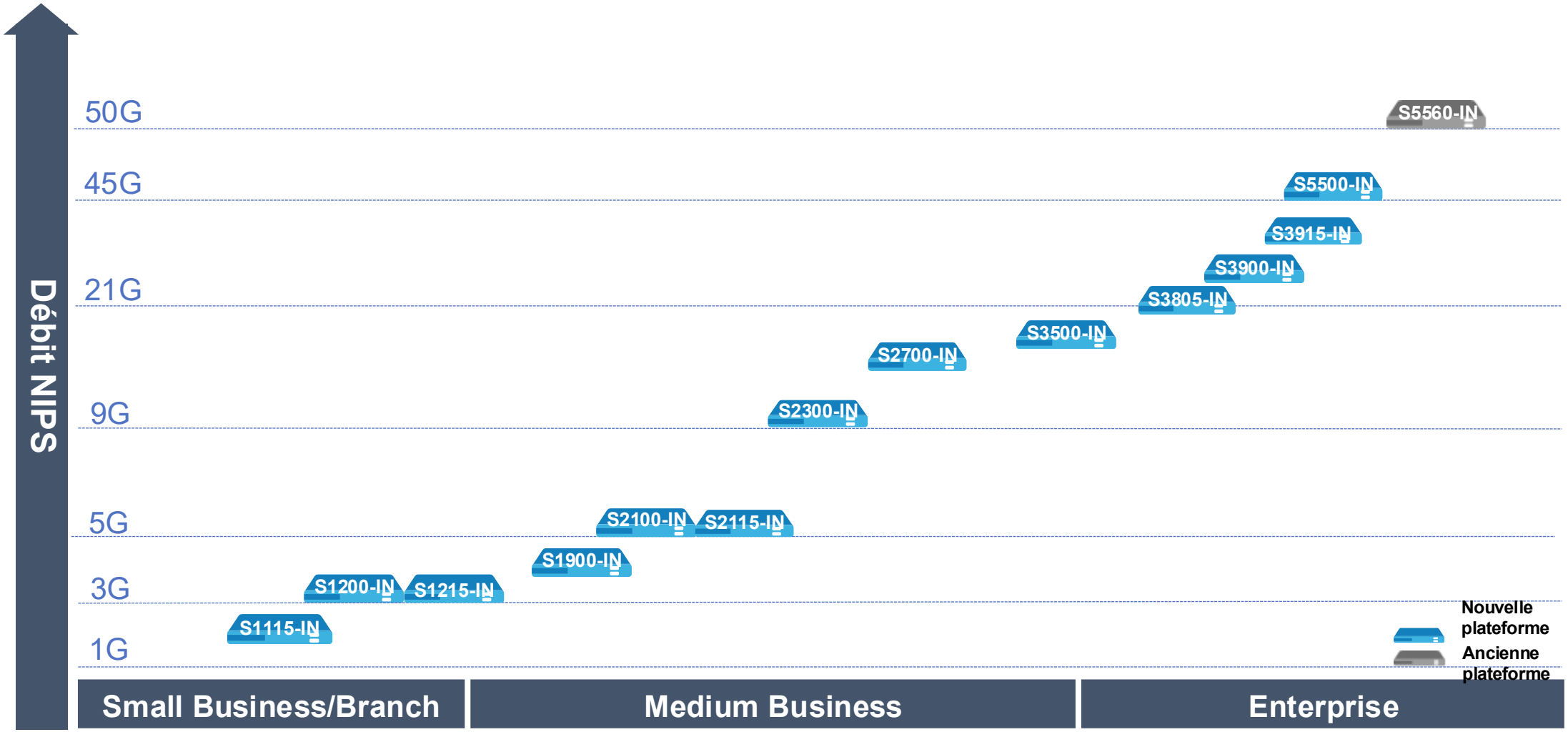
Passive Mode: Surveillance Only

Surveillance et alertes en temps réel
Mirroring/TAP
Un port requis

3

Portefeuille NIPS Hillstone

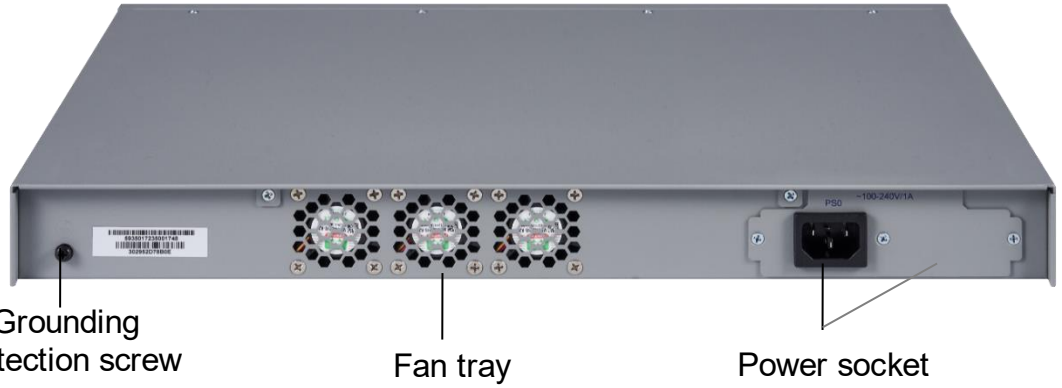
Portefeuille NIPS Hillstone



S1115

Vue avant

Vue arrière



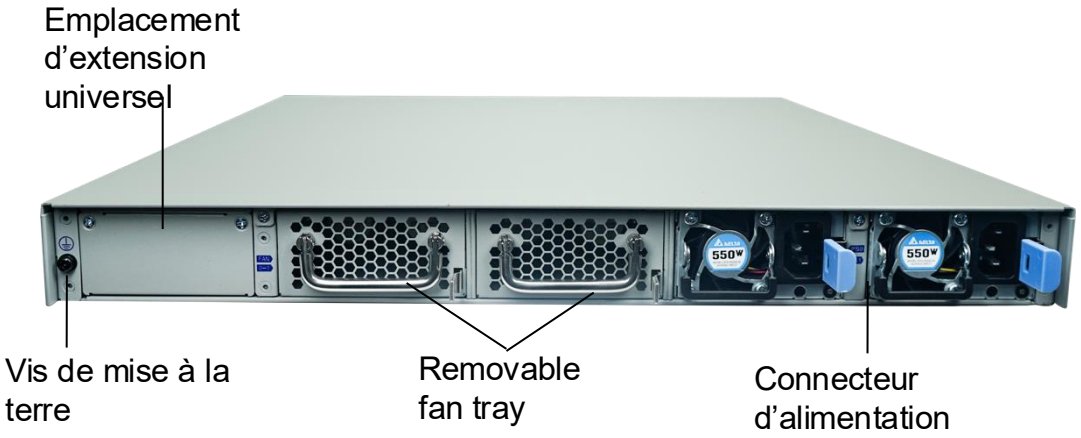
Model	S1115-IN
IPS throughput (HTTP)	2 Gbps
IPS throughput (realworld, IPS on)	1.5 Gbps
Maximum Concurrent Connections (TCP)	1.2 Million
New connections per second (HTTP)	30,000
Storage *	500 GB / 1 TB SSD
Form factor	1 U
Management Ports	2 x USB port, 1 × MGT port, 1 x Console port, 1 x HA
Fixed I/O Ports	8 × GE (including 2 pairs Bypass port), 8 × SFP
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-F-4SFP+-A-IN, IOC-S-F-8SFP+-A-IN, IOC-S-F-8GE-B-A-IN
Bypass Ports (Default / Max.)	4/12
Power Supply	AC: 100-240V 50 / 60 Hz
Maximum Power Consumption	60W 1 x AC power supply 2 x AC power supply

* Le stockage de 1 To pour le S1115-IN est disponible uniquement sur les appareils équipés de deux alimentations CA.

S5500

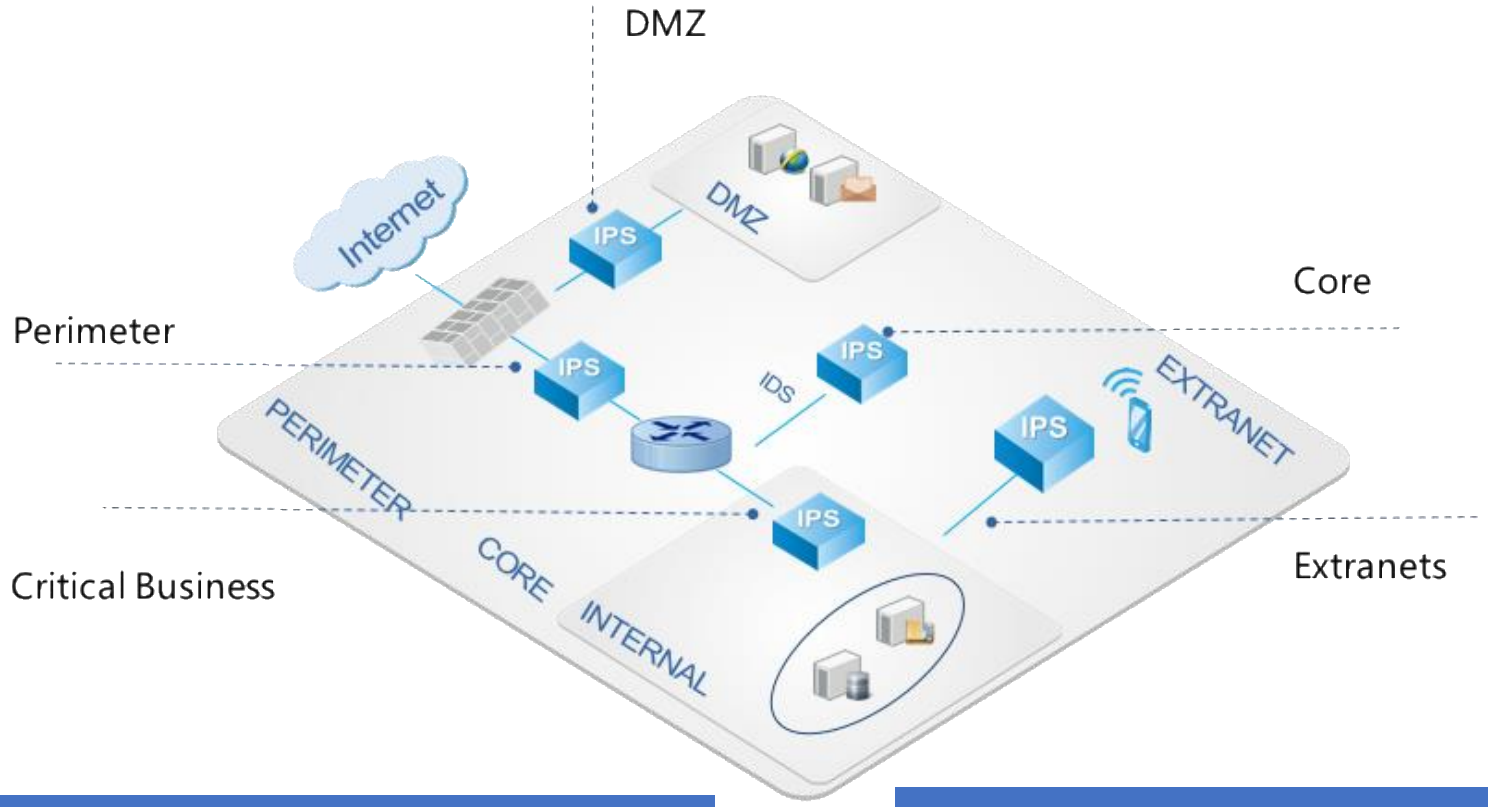
Vue avant

Vue arrière



Model	S5500-IN
IPS throughput (HTTP)	45 Gbps / 75 Gbps (with IOC-S-2QSFP+-A-IN)
IPS throughput (realworld, IPS on)	25 Gbps
Maximum Concurrent Connections (TCP)	24 Million
New connections per second (HTTP)	550,000
Storage	1 TB SSD
Form factor	1 U
Management Ports	2 x USB 3.0 Port , 1× Console Port, 1 x MGT Port, 1 x HA Port (SFP+)
Fixed I/O Ports	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN
Bypass Ports (Default / Max.)	8 / 8
Power Supply	DC: -36~ -72 V; AC 100-240 V 50 / 60 Hz
Maximum Power Consumption	320W 2 x AC power supply 2 x DC power supply

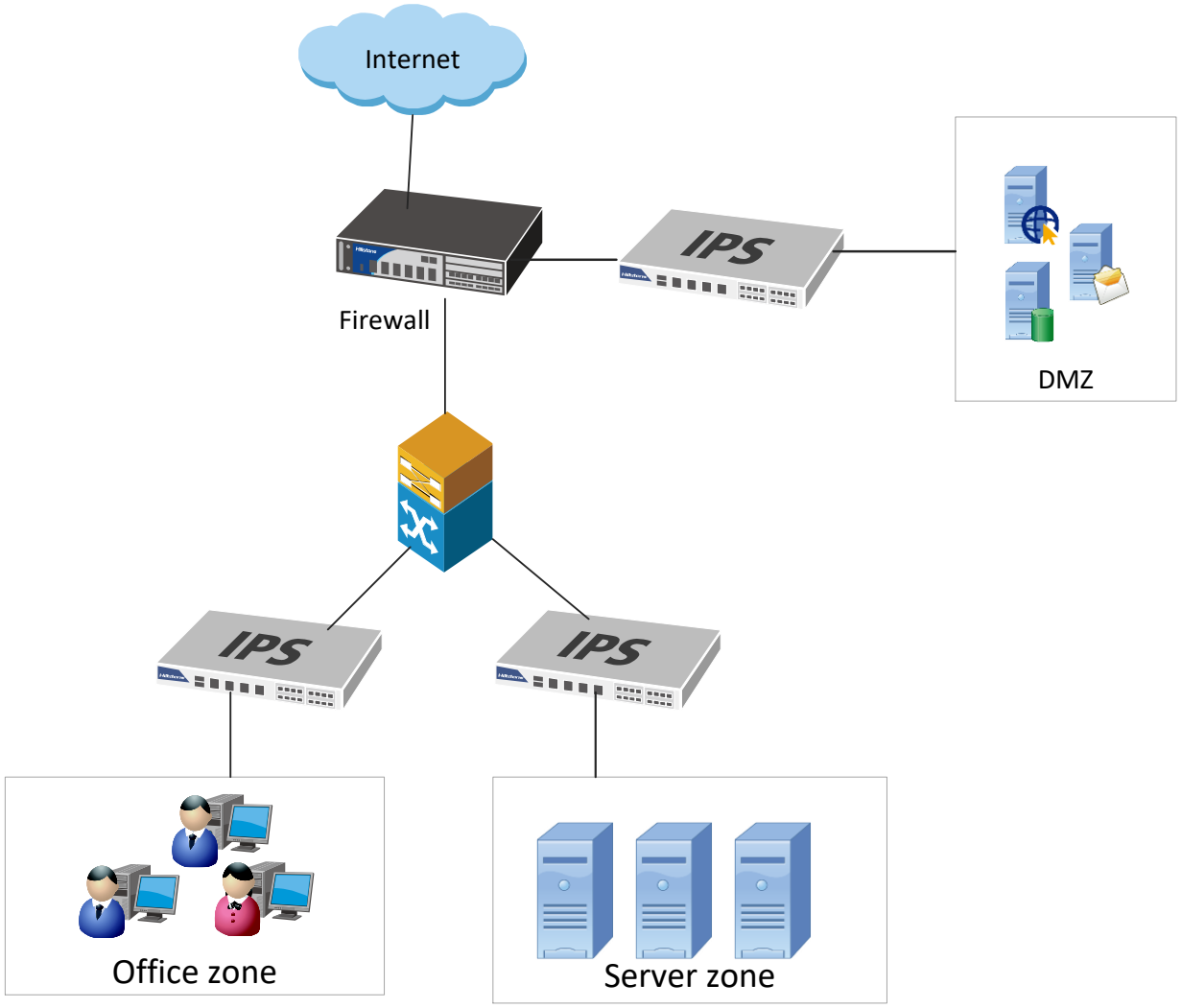
Scénarios de déploiement



Clients : administrations, secteurs financiers et entreprises ayant besoin d'une appliance IPS/IDS autonome pour une meilleure protection, la segmentation du réseau interne, la surveillance des menaces, etc.

Scénarios de déploiement : déploiement inline après le pare-feu périmétrique, segmentation DMZ/réseau interne/accès distant, mode TAP via le commutateur cœur ou le commutateur d'accès pour la surveillance/détection des menaces

Déploiement de la série S en entreprise



Requirements

- Protection against sophisticated attacks
- Insight into network environment

Solutions

- Strong defensive capabilities
- Deep visibility from L2 – L7
- Unknown threat detection
- Automated analysis and mitigation

Products

- S Series

Market

- Education
- Enterprises
- Government

Proposition de valeur du NDR Hillstone

Produit NDR BDS de Hillstone

Le produit NDR BDS de Hillstone détecte et répond aux menaces réseau avancées

Détection des menaces	Visibilité approfondie	Analyse forensique numérique	Réponse efficace
ABD/ATD/WEB	IOCs	Chaîne d'attaque	Actions administratives
NTA/Déception	Dashboards	MITRE ATT&CK	Liste noire / liste blanche
Menace Correlation	Risque/Menace/Trafic	Données forensiques détaillées	Blocage avec NGFW/NIPS
…	…	…	…

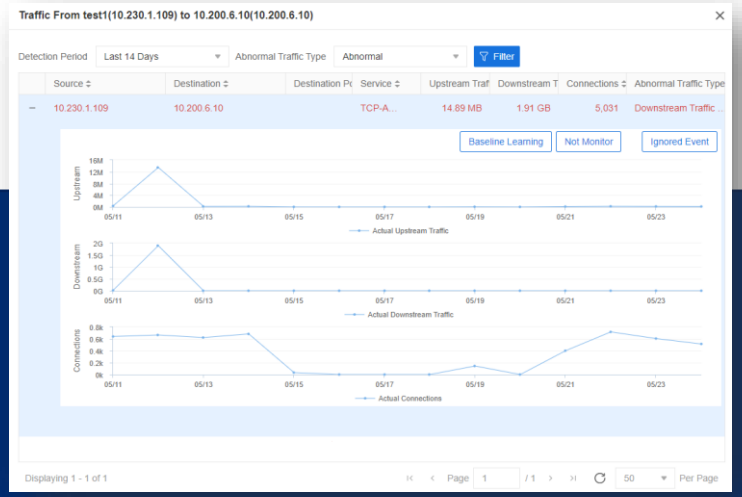
Analyse basée sur le machine learning des comportements anormaux

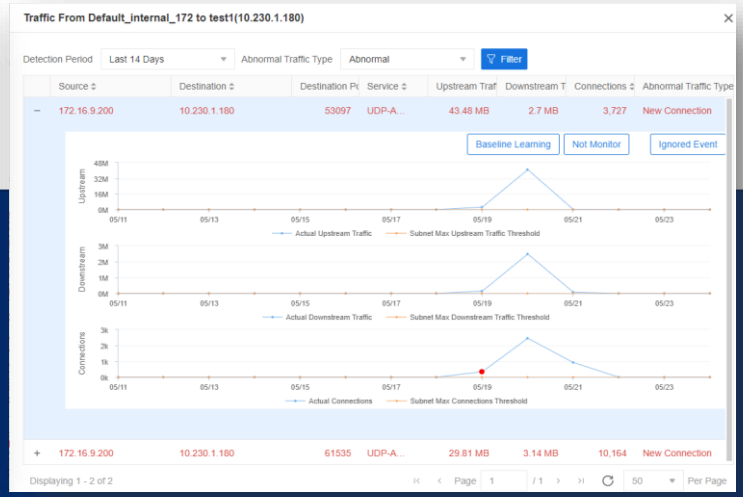
Apprend et établit une référence et un seuil pour le trafic normal

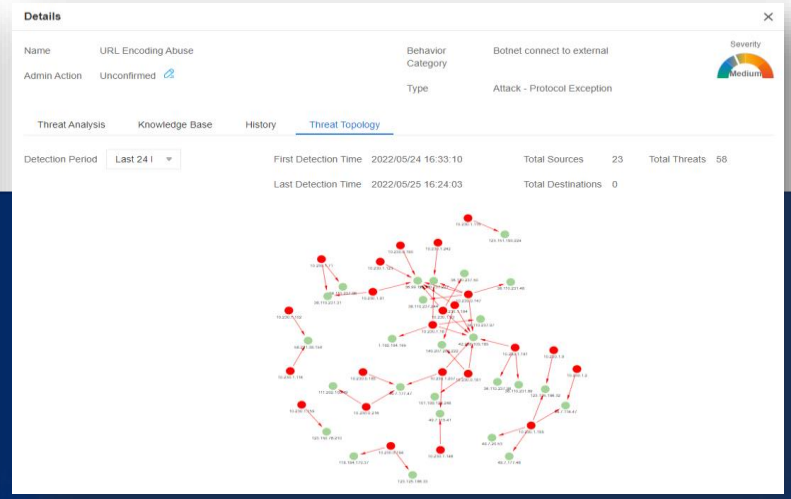
Détecte les tendances du trafic et identifie les comportements anormaux

Surveille le trafic normal et anormal de chaque serveur/hôte

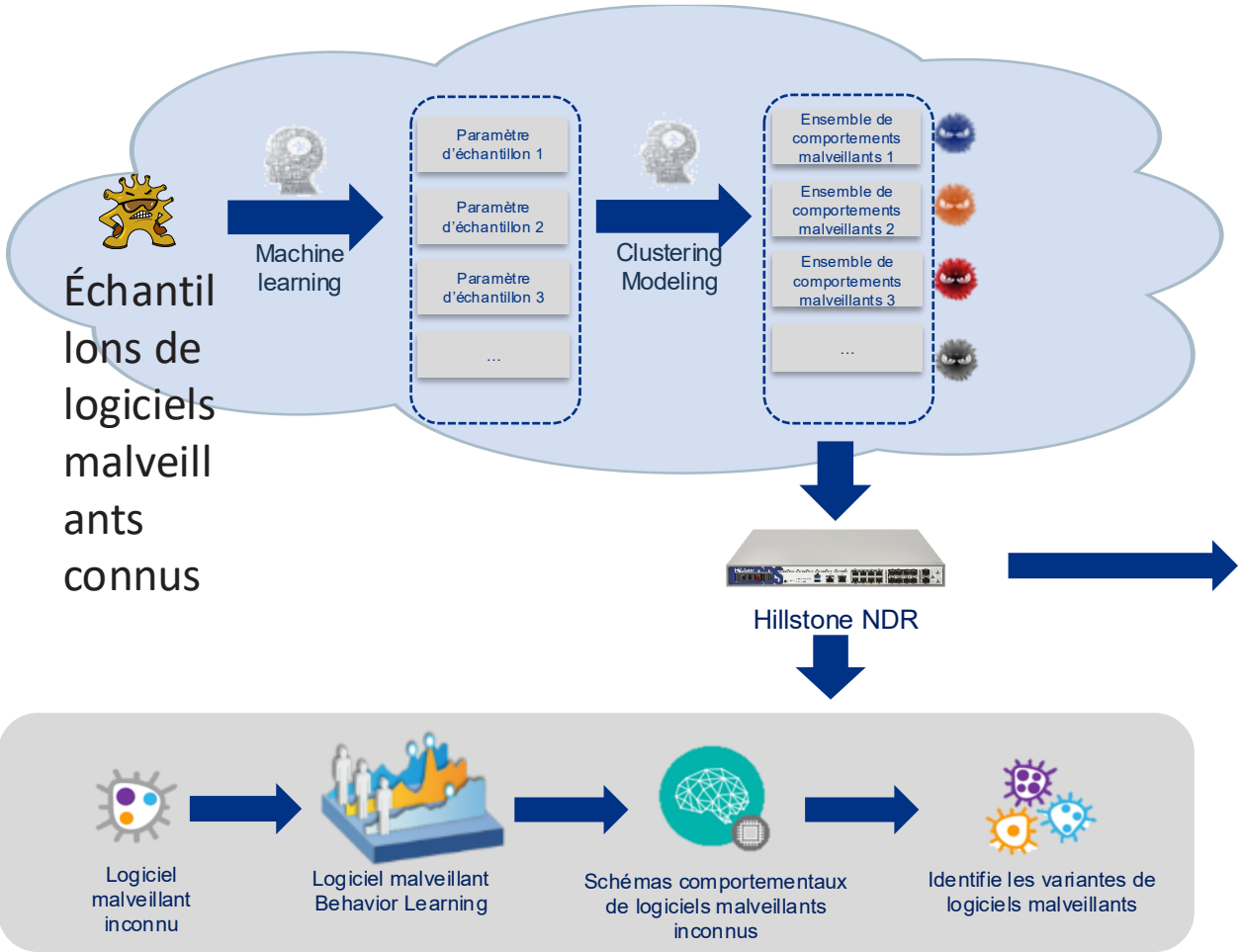
Analyse comportementale basée sur le machine learning pour les URL, l'UEBA, les corrélations de menaces, etc.

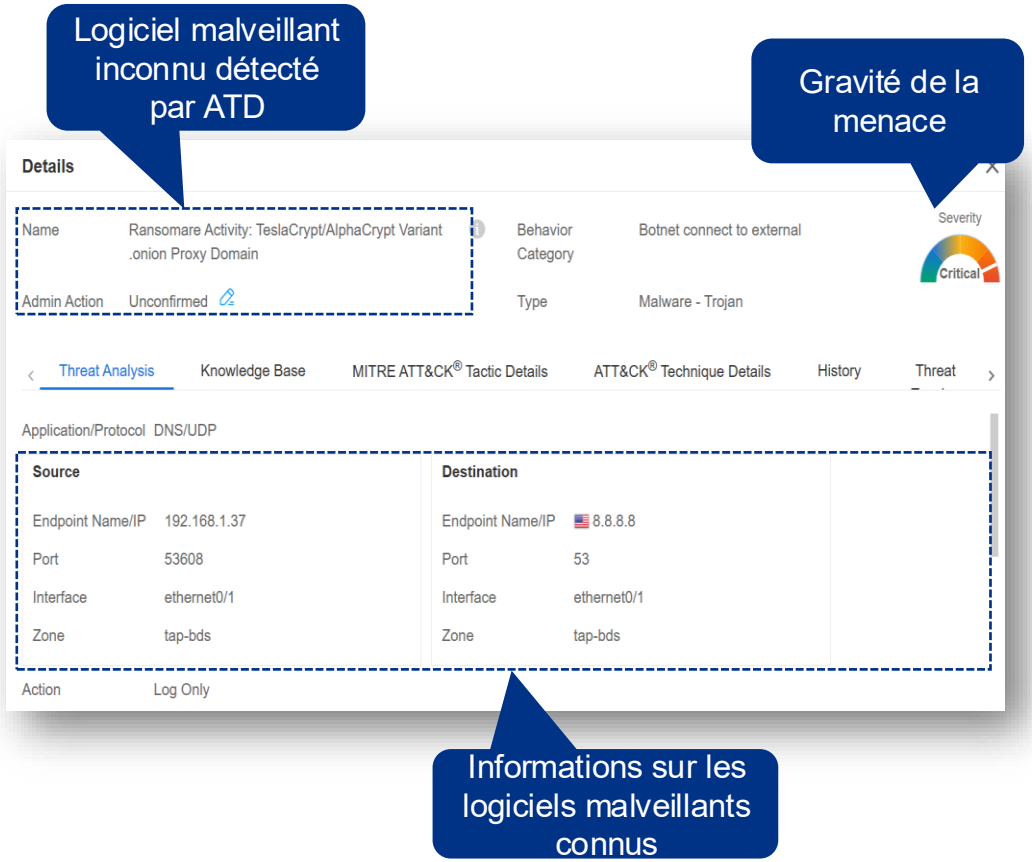






Détection : détection avancée des menaces (ATD)





Détection : détection des trafics chiffrés anormaux

Trafic chiffré

Hillstone NDR

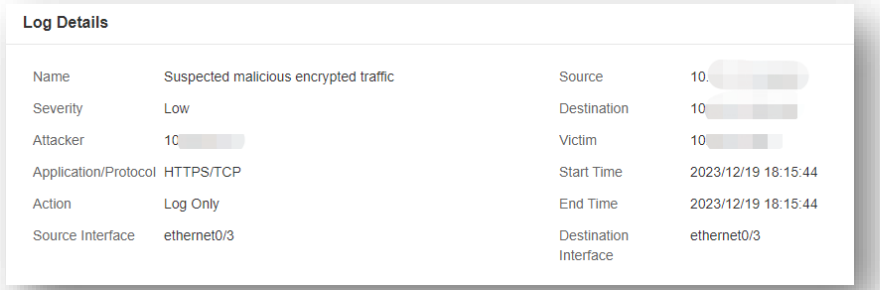
Extracting Signatures without Decryption

- Paramètre 1
- Paramètre 2
- Paramètre 3
- .....

Moteur de détection

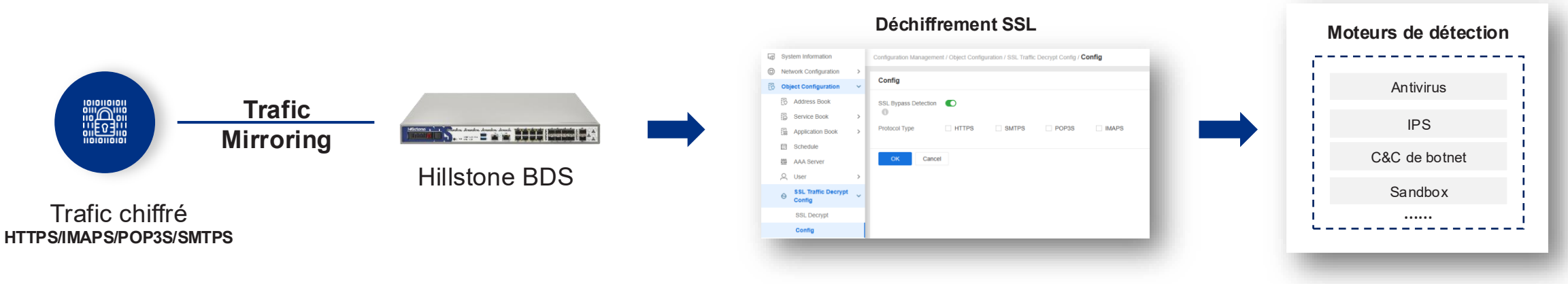
Moteur de détection alimenté par l'IA

Journalisation des verdicts malveillants



Exploite une technologie alimentée par l'IA pour détecter les trafics chiffrés anormaux sans déchiffrement

Détection : détection des menaces sur le trafic chiffré avec déchiffrement SSL en mode TAP



Détection complète des menaces sur le trafic chiffré avec déchiffrement SSL en mode TAP

Détection : détection des attaques WEB

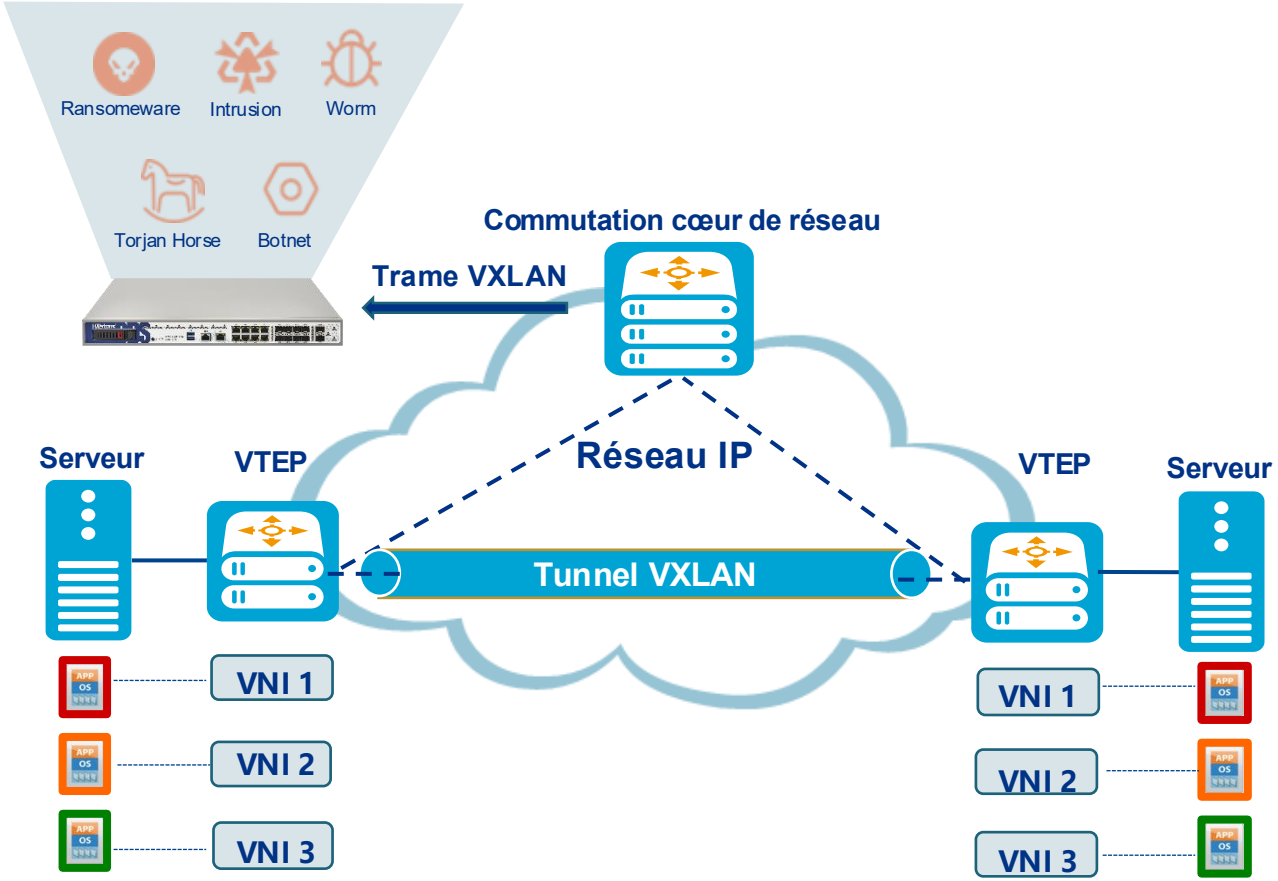
WAF rules
Utilizing OWASP ModSecurity Core Rule Set (CRS) 3.3

Detect and analyze threats for WEB servers and applications

Détection des attaques WEB

- DDoS Attack
- Attaque par injection
- Attaque intersite
- HTTP anormal
- Attaque exploitant une vulnérabilité particulière
- Fuite d'informations
- Logiciel malveillant
- Accès illégal aux ressources
- Scan réseau malveillant

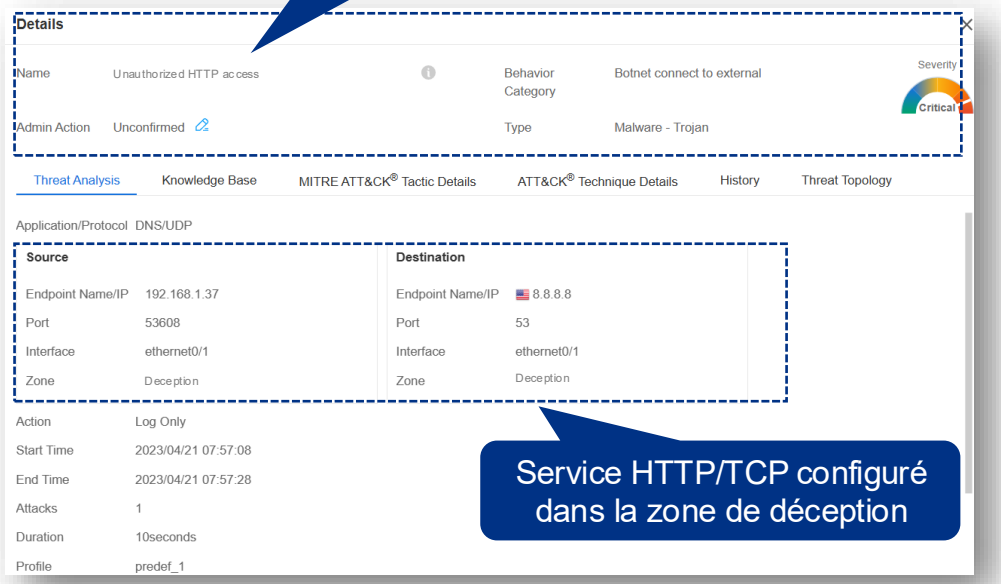
Détection: VxLAN Frame Détection



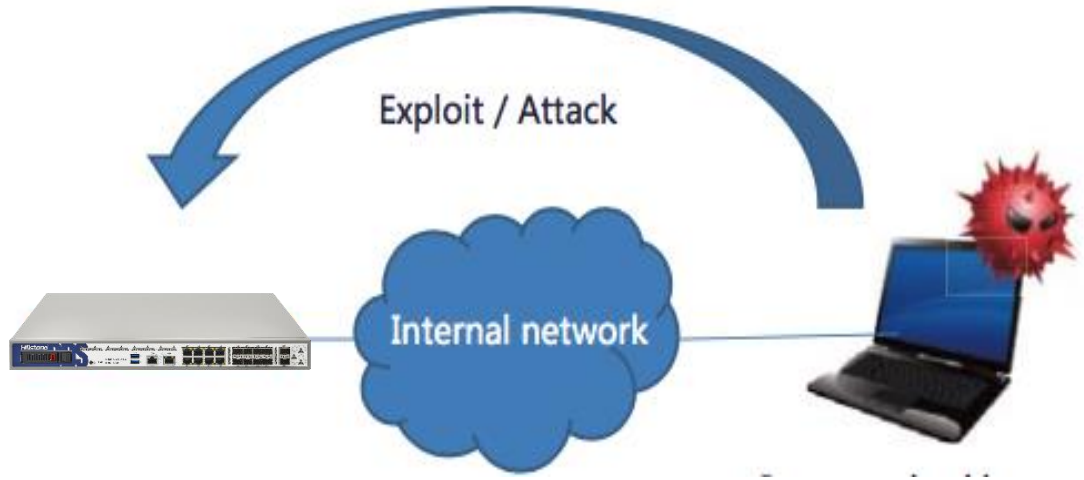
Détecte les trames VXLAN dont le port UDP de destination est 4789
NE détecte PAS le trafic non-VXLAN dont le port de destination est UDP 4789

Détection : technologie de déception

Accès HTTP non autorisé détecté par le moteur de déception



Service HTTP/TCP configuré dans la zone de déception



Simule des services dans une zone de déception ; lorsqu'un pirate accède à ces services, l'attaque est détectée

Détection : moteur de détection antivirus double

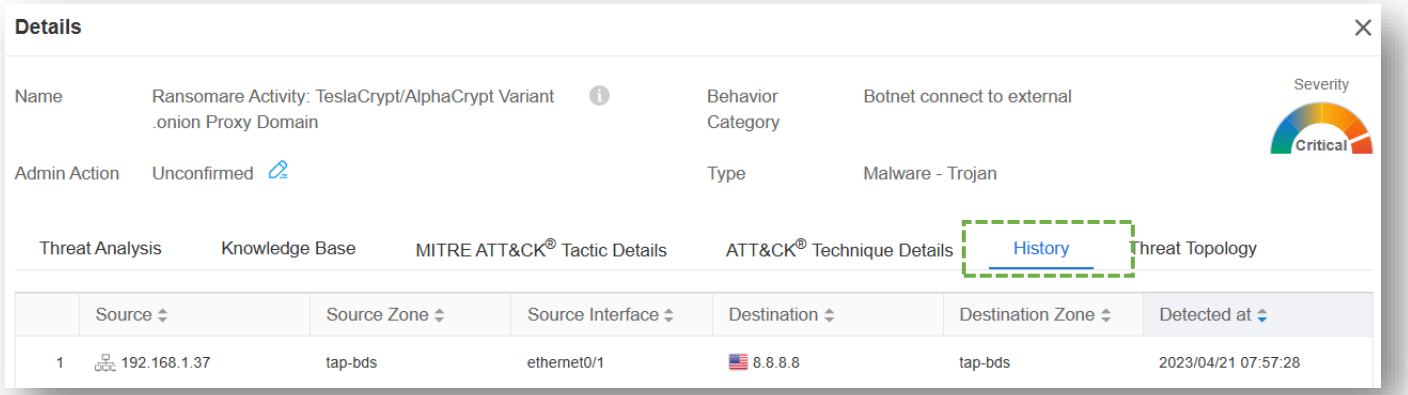
Détection basée sur le hash

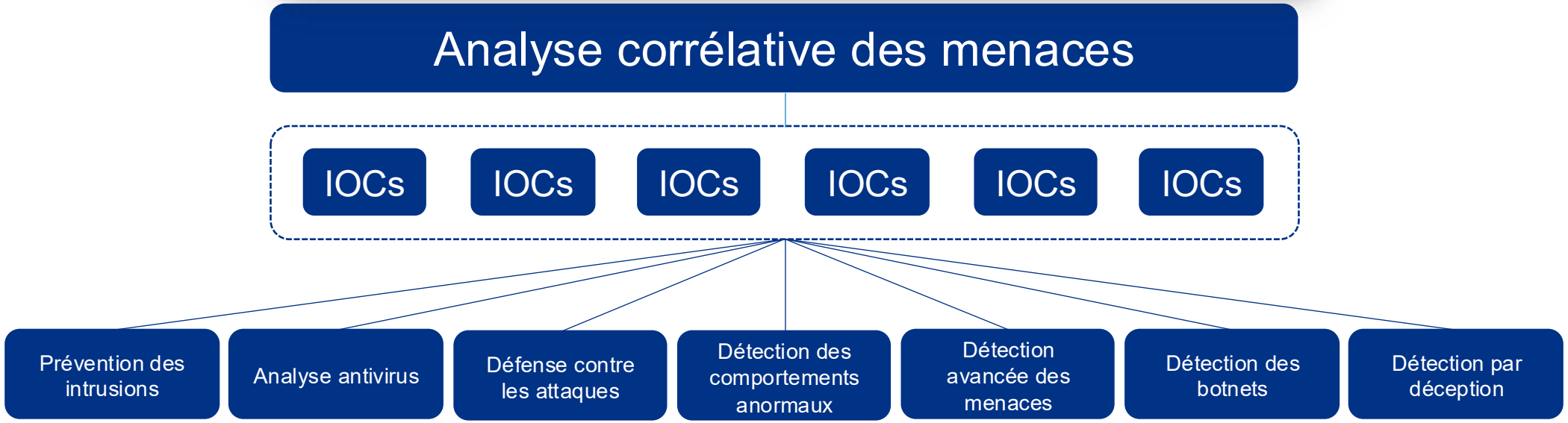
- Basée sur le hash MD5 du fichier
- Prend en charge tous les fichiers
- Cas d'usage : détection des virus connus

Détection alimentée par l'IA

- Analyse des caractéristiques des fichiers
- Prend en charge les fichiers PE/PDF/Office/ELF
- Cas d'usage : détection des virus inconnus/variantes

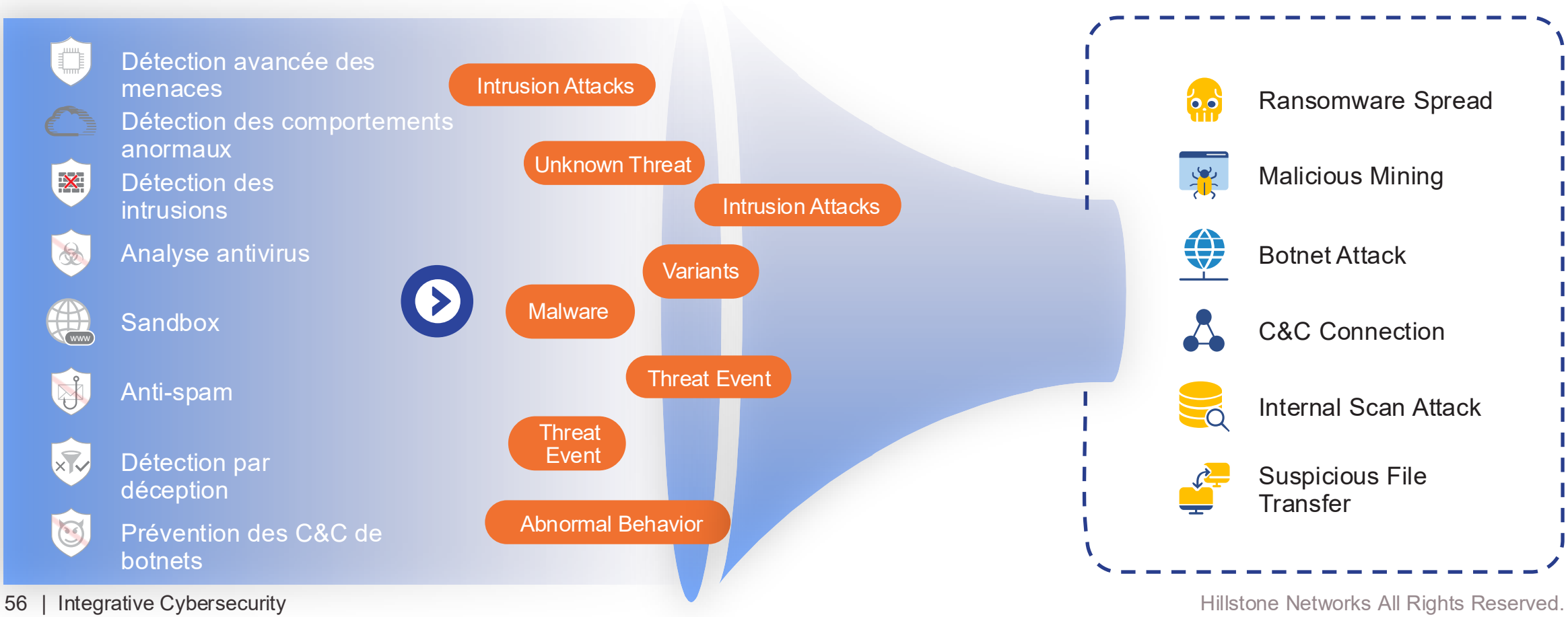
Détection : efficacité de détection et réduction des faux positifs





Visibilité : menaces associées aux indicateurs de compromission (IOC)

Les moteurs de détection des menaces détectent les événements de menace	Analyse corrélative des menaces	IOCs



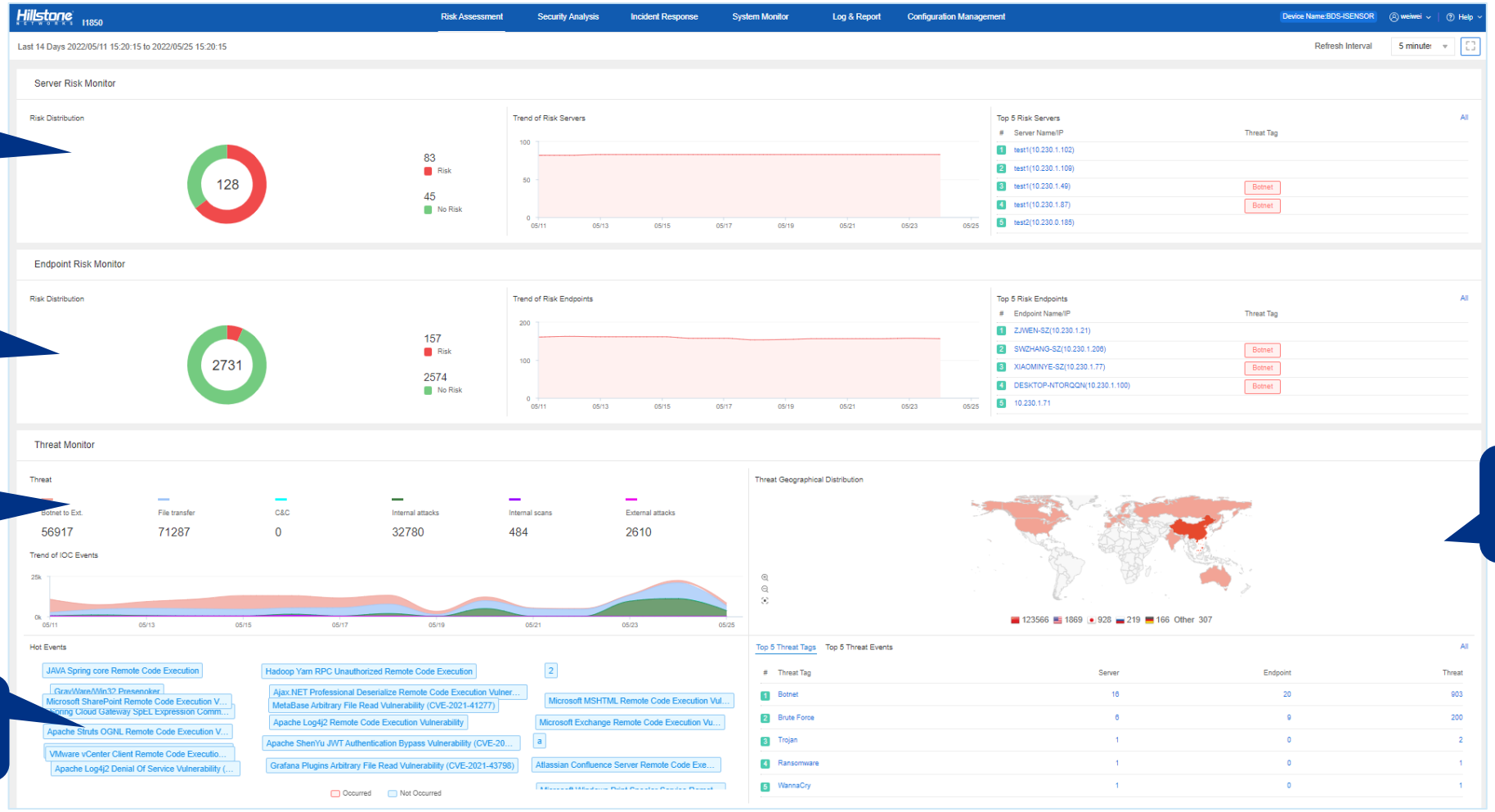
Visibilité : vue globale des menaces sur l'intranet

Vue d'ensemble des serveurs critiques et du niveau de risque

Vue d'ensemble des hôtes internes et du niveau de risque

Type de menace, statistiques, répartition historique, etc.

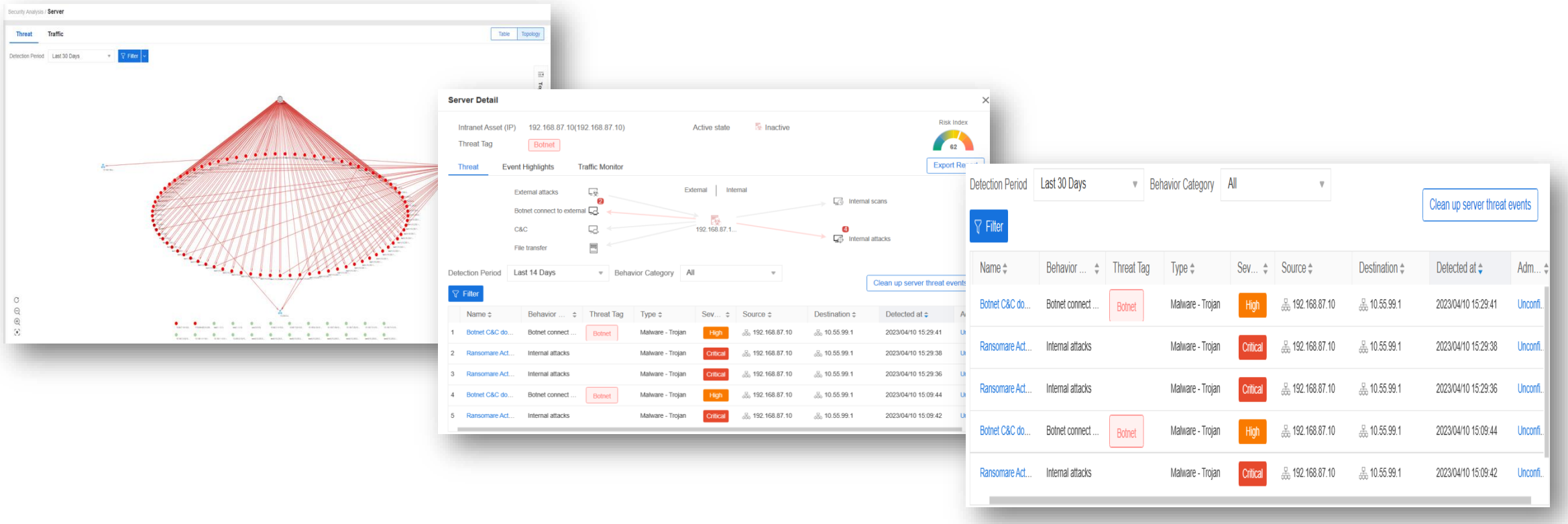
Événements critiques nécessitant une attention



Répartition géographique des menaces et principales menaces

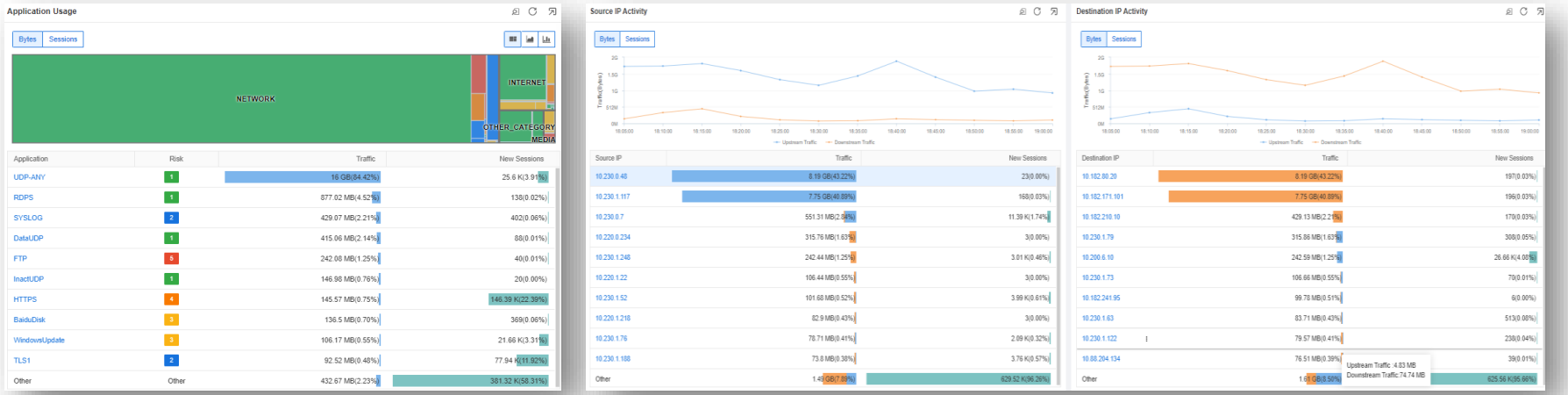
Visibilité : tableau de bord de surveillance des risques de l'intranet

Visibilité : surveillance des menaces sur les serveurs

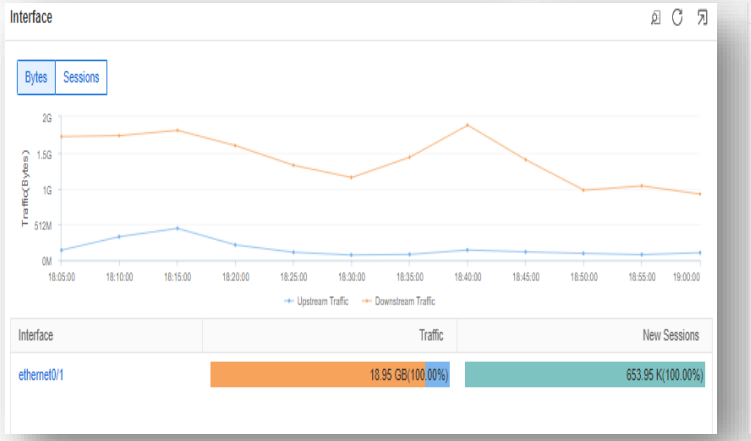


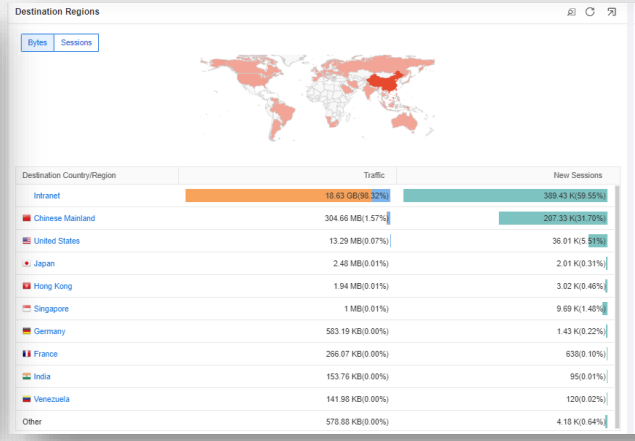
Topologie des menaces des serveurs intranet : direction des attaques, gravité, relations
Analyse des menaces pour chaque serveur : 6 types de chaînes d'attaque
Liste des événements de menace

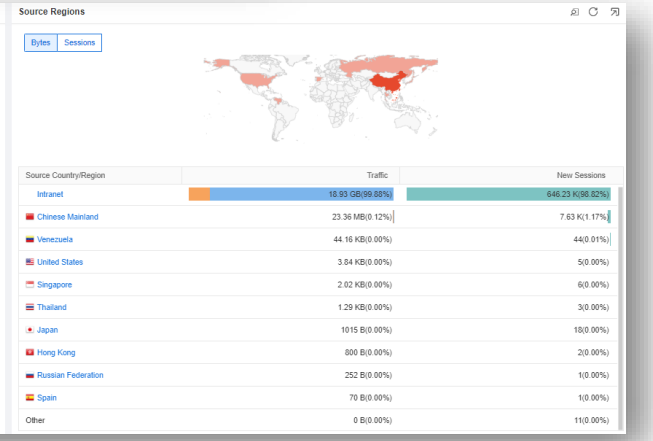
Visibilité : analyse des applications de l'intranet



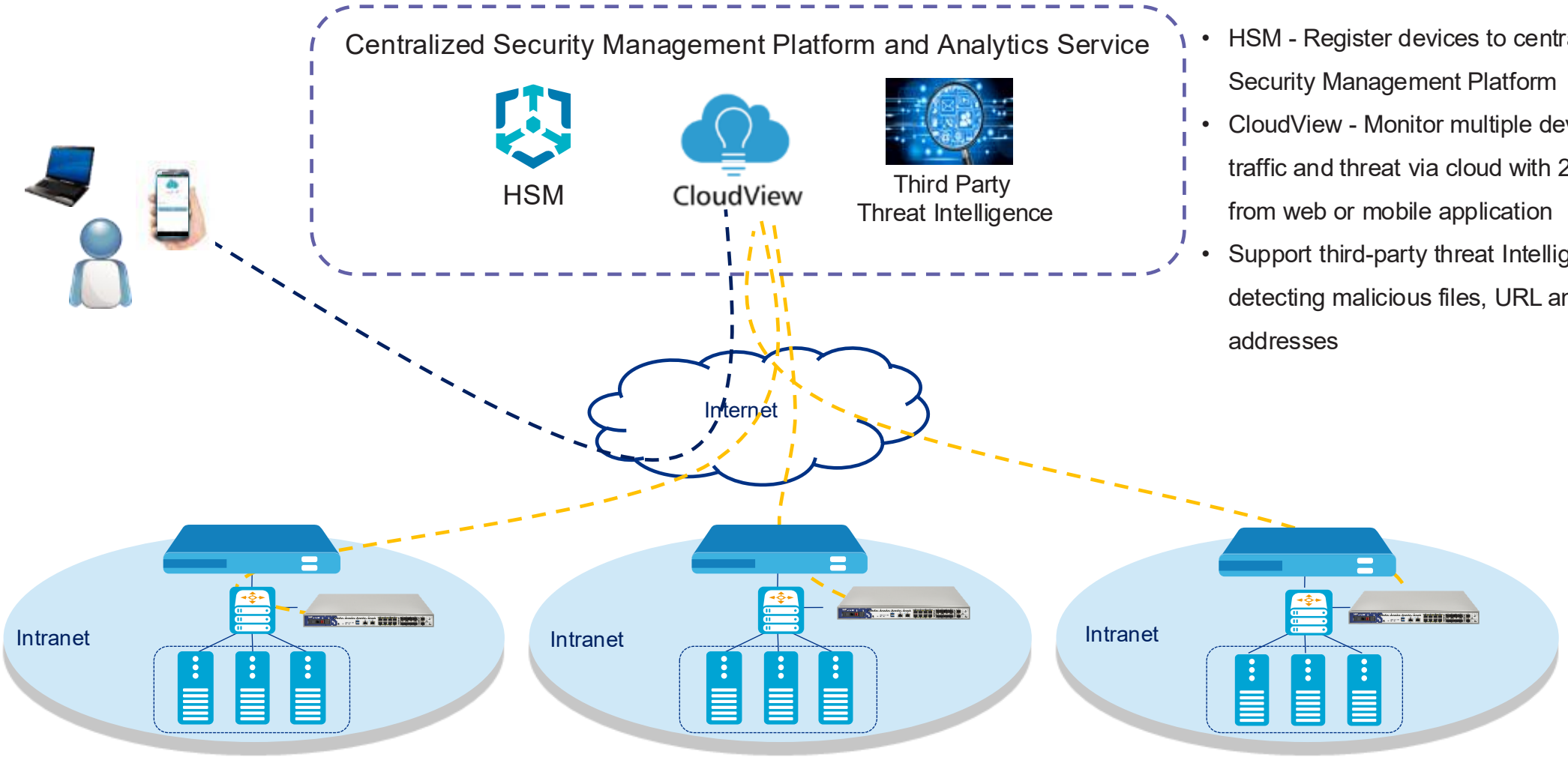
- Utilisation/classement des applications
- Classement du trafic IP source/destination
- Classement du trafic par interface
- Géolocalisation des menaces





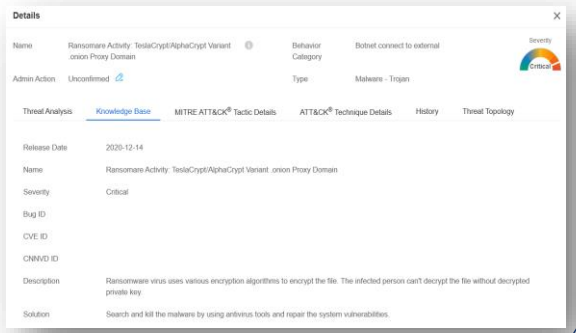


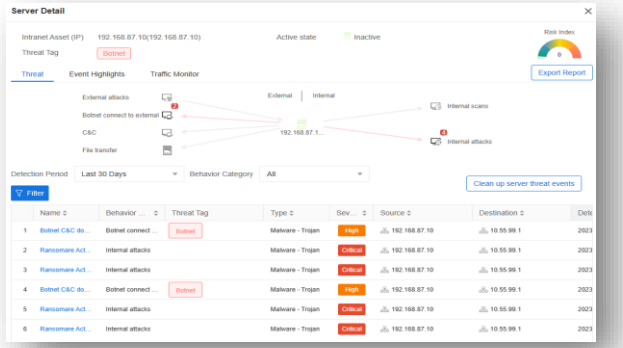
Visibilité : gestion centralisée de la sécurité



- HSM - Register devices to centralized Security Management Platform
- CloudView - Monitor multiple devices status, traffic and threat via cloud with 24/7 access from web or mobile application
- Support third-party threat Intelligence for detecting malicious files, URL and IP addresses

Analyse forensique numérique : des données forensiques riches permettent l'évaluation des risques



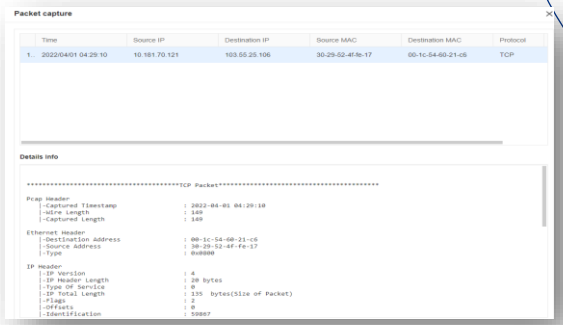


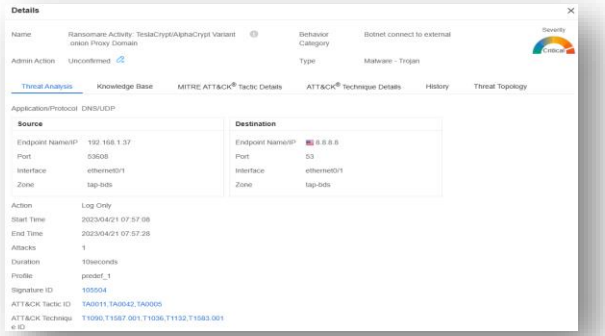
Restore the Attack Chain and Mapping to MITRE ATT&CK

Knowledge Base

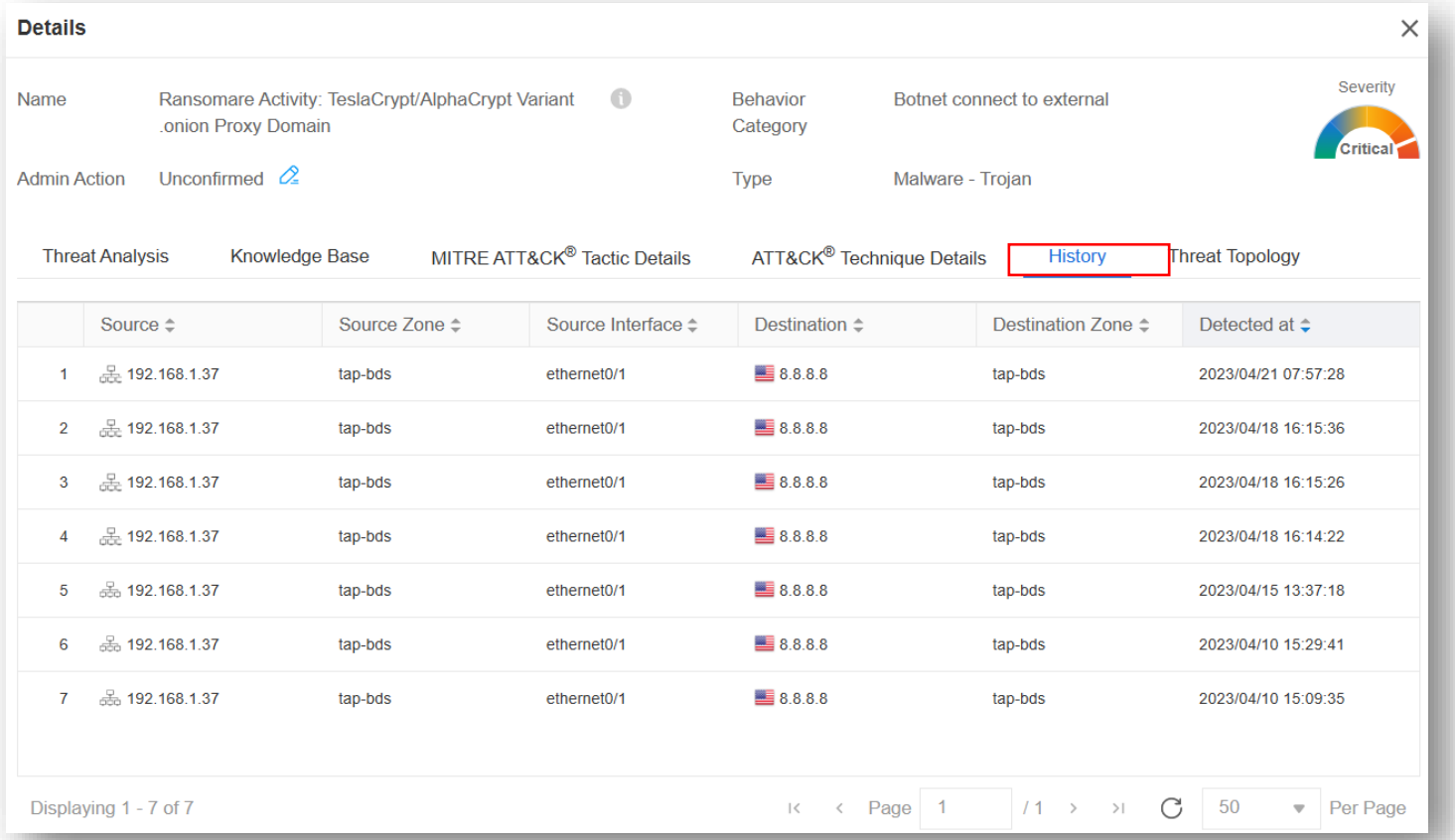
Threat Analysis

PCAP Forensics



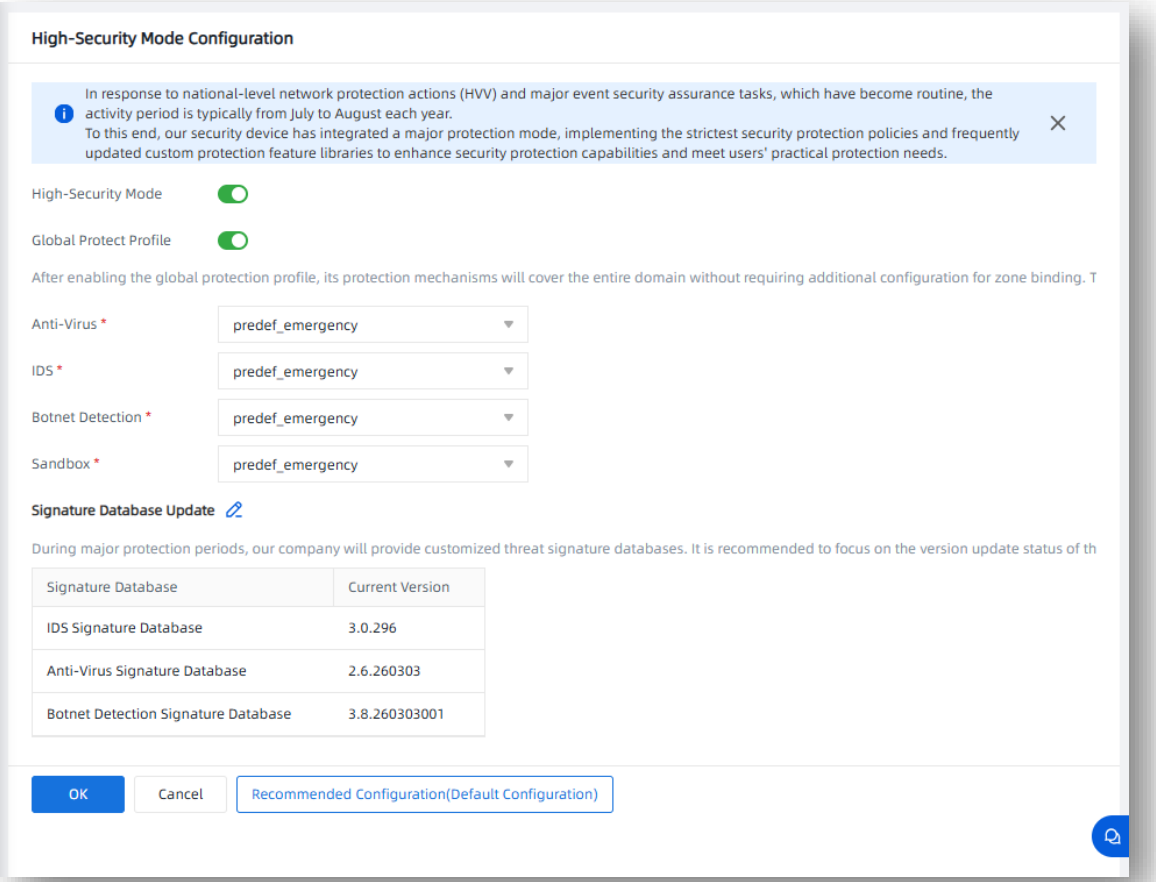


Analyse forensique numérique : détails du comportement des menaces



- Suivi des informations relatives aux événements de menace :
- Scan d'IP et de ports
- Craquage par force brute de services courants tels que FTP, LDAP et MySQL
- Réponse d'accès HTTP anormale
- Connexion C&C

Mode de protection critique pour HVV et les opérations de sécurité à enjeux élevés



Activation du mode en un clic

Applique instantanément un modèle global à tous les domaines de sécurité — aucune configuration par zone n'est nécessaire. Remplace tous les paramètres au niveau des domaines avec la priorité système la plus élevée.

Multi-Engine Simultaneous Hardening

Active simultanément quatre mécanismes de protection : antivirus, IDS, botnet et sandbox.

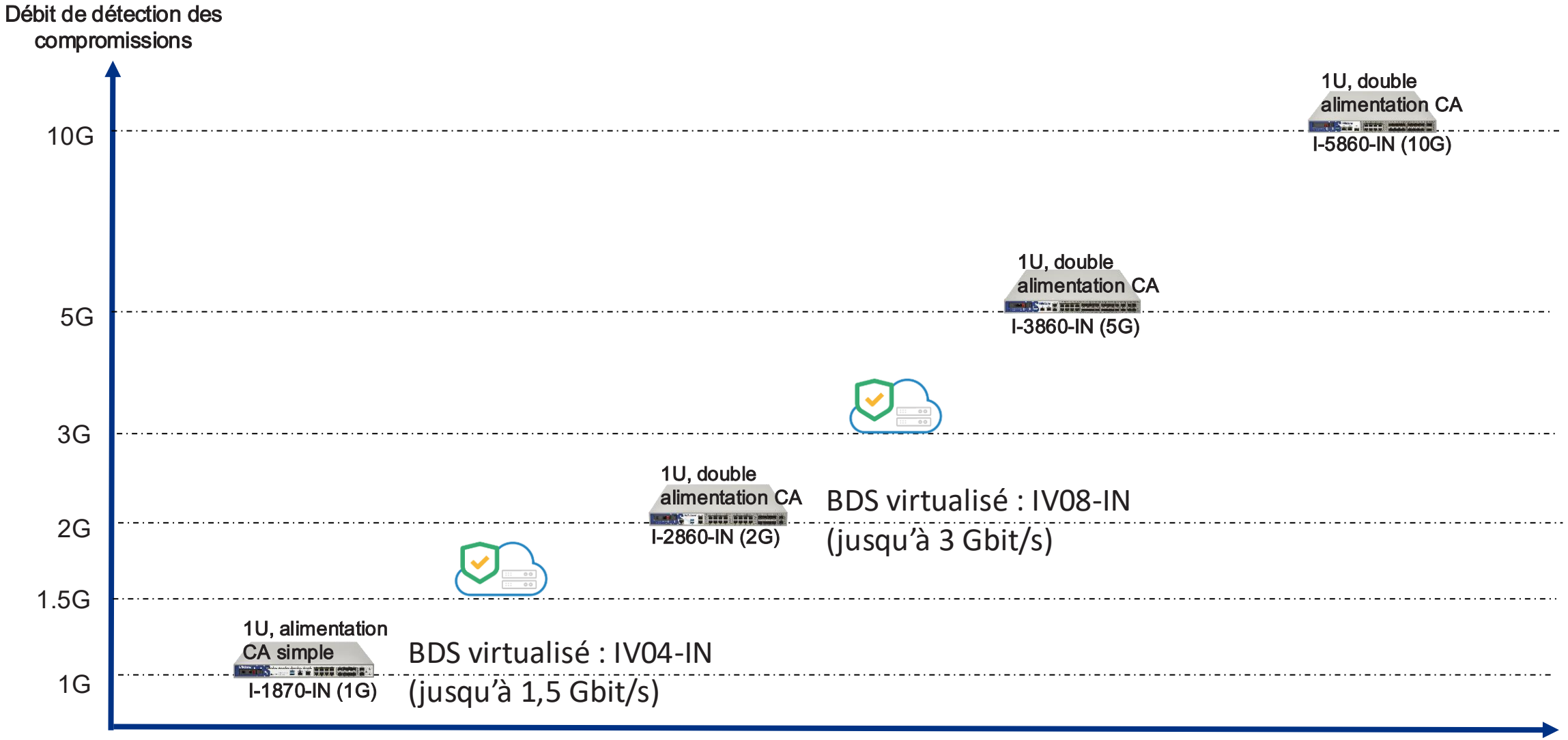
Emergency-Grade Detection Policies

Les quatre moteurs sont réglés par défaut sur le niveau « pré-urgence » — le niveau de politique le plus strict. Réglable sur « faible », « moyen » ou « élevé » pour plus de souplesse opérationnelle.

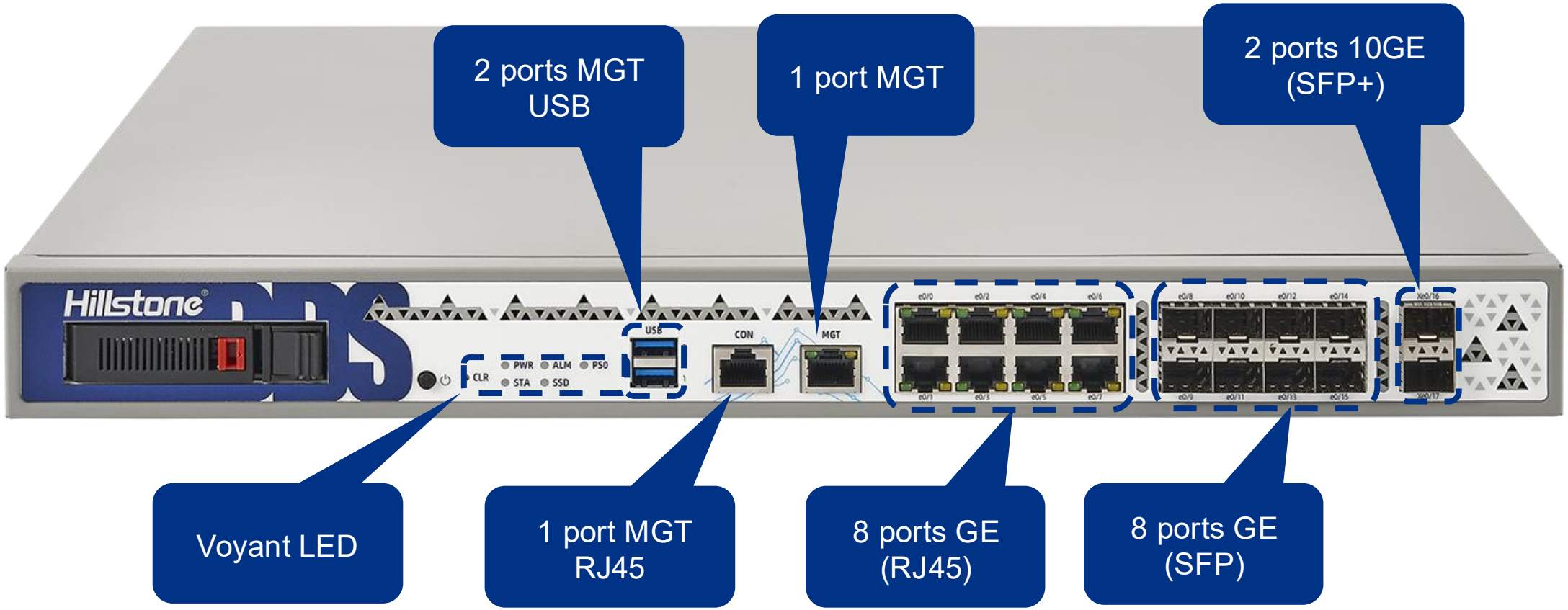
Cycle fermé : détection et réponse réseau

Portefeuille de produits NDR Hillstone

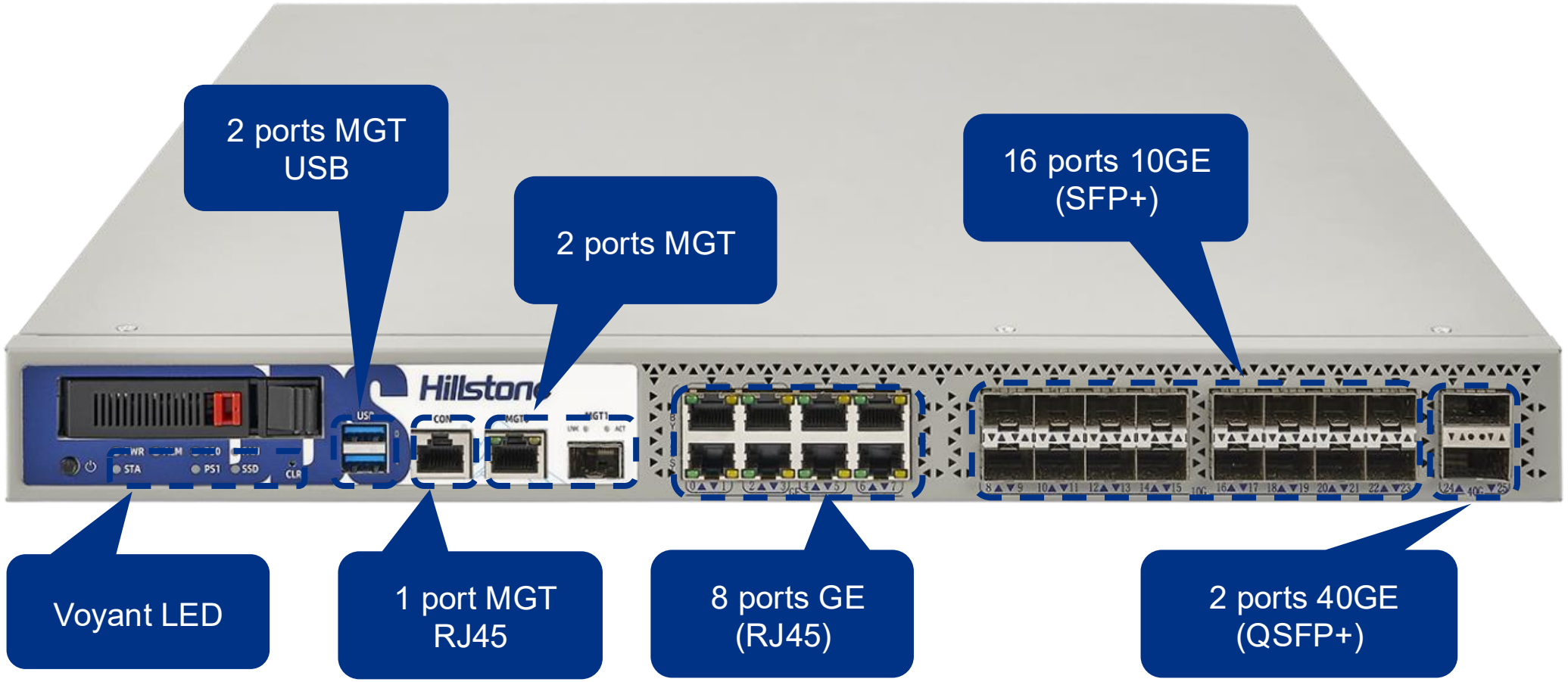
Portefeuille de produits NDR Hillstone



Spécifications matérielles de l’I-1870



Spécifications matérielles de l’I-5860



BDS

Item	Question
1. Network Size	**Number of endpoints and network devices:**
	Number of critical assest (list a critical servers, PCs, IoT devices, network devices, etc.):
	Complexity of the network (single location, distributed, etc.):
	Number of networks to be scanned:
	Number and type of interfaces needed to scan the scope:
2. Network Traffic Volume	Average and peak bandwidth usage:
	Anticipated growth in network traffic:
3. Types of Traffic to Monitor	Internal (east-west) traffic, external (north-south) traffic, or both:
	Specific protocols or applications of interest:
4. Threat Detection and Response Capabilities	Preferred detection techniques (signature-based, behavioral analysis, etc.):
	Need for automated response capabilities:
5. Compliance Requirements	Specific industry regulations to comply with (PCI DSS, HIPAA, GDPR, etc.):
	Reporting features required for compliance purposes:
6. Budget	Allocated budget for the NDR solution:
	Consideration of ongoing costs for maintenance, updates, subscriptions, etc. :
7. Integration with Existing Infrastructure	Need for integration with SIEM/XDR system:
	Integration requirements with other security tools or platforms:
8. Scalability and Performance	Scalability requirements as the network grows:
	Performance metrics essential for your environment (throughput, packet capture rate, etc.):
9. Deployment Preferences	Preferred deployment model (on-premises, cloud-based, hybrid):
	Specific requirements for deployment architecture and ease of implementation (TAP mode):
10. Security Objectives and Priorities	Types of threats or attack vectors of greater concern:
	Critical assets or data that need protection:
11. Time	Support time:
	Licensing time:
12. Special features/others	Special function (honeypots, EDR, etc.):
	Local storage:
	Any other requirement:

Nous pouvons dimensionner l'appareil approprié en fonction du nombre de terminaux et d'actifs critiques.

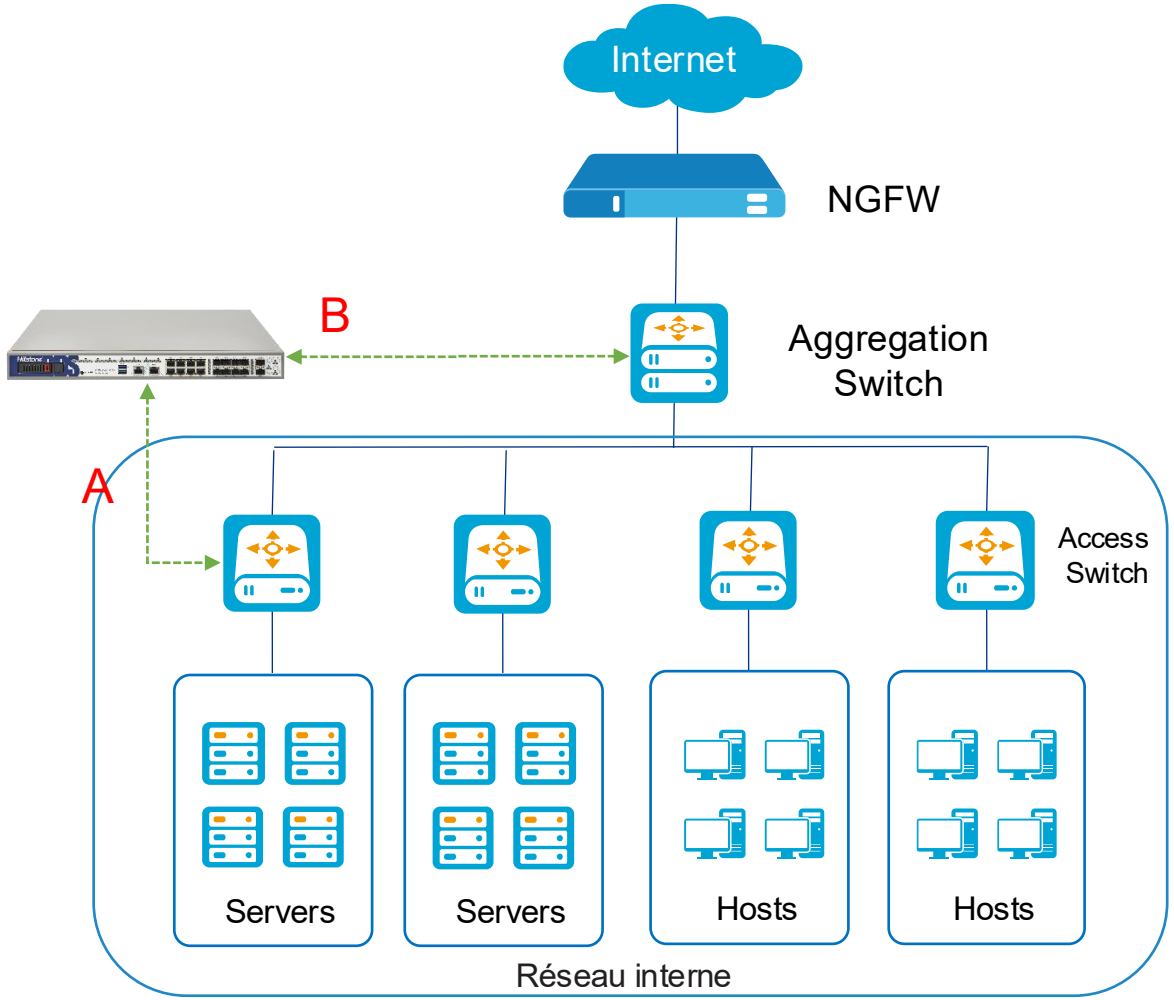
Exemple : une entreprise souhaite dimensionner un BDS et dispose de 2 000 terminaux et de 100 actifs critiques dans l'ensemble de l'entreprise. Nous pouvons suivre ce tableau et choisir notre modèle BDS.

Model	I1850/I1870/IV04	I2860/IV08	I3860	I5850/I5860
Critical assets	128	256	512	1024
Endpoints	5000	10000	20000	40000

En suivant cet exemple, nous pouvons choisir I1850/I2870 ou IV04 en mode virtuel.

Remarque : veillez à prendre en compte tous les détails, tels que le débit de prévention, les interfaces physiques, les fonctionnalités de sécurité, la haute disponibilité, etc. Si le projet dépasse 20 000 $, nous recommandons de travailler avec un spécialiste produit Hillstone.

Scénarios de déploiement NDR Hillstone – BDS et NGFW



Scénario A : commutateur d'accès connecté aux serveurs ou groupes de serveurs
Surveille le trafic entre les serveurs d'un même segment, les serveurs de segments différents, les serveurs et Internet, ainsi que les serveurs et les autres hôtes.

Scénario B : commutateur d'agrégation entre les commutateurs d'accès
Surveille le trafic entre les serveurs de segments différents, les serveurs et Internet, les serveurs et les autres hôtes, ainsi que les hôtes et Internet.

Scénario C : combinaison des scénarios ci-dessus

Réponse : atténuation des attaques avec les dispositifs de sécurité Hillstone et tiers

Hillstone NDR

Détecter et identifier la menace
Configurer la liaison avec le NGFW/NIPS Hillstone ou un NGFW tiers
Ajouter les attaques confirmées à la liste de blocage

Hillstone NIPS
Hillstone NGFW

NGFW tiers

Lier au NDR Hillstone
Synchroniser la liste de blocage depuis le NDR Hillstone
Bloquer les attaques

Threat Alarm Rule
Threat Event Allowlist
Mitigation
Linkage Device
Collapse

Linkage Device | Security Ecological Cooperation Device Blocking Configuration Template

New | Edit | Delete | Clone

Name	Type	Description
SangforAF-FH1600B	Predefined	This template is a command-line template for sending blocking commands to linked devices, applicable to Sang...
Huawei-USG6600E	Predefined	This template is a command-line template for sending blocking commands to linked devices, applicable to Hua...
Paloalto-PA8201	Predefined	This template is a command-line template for sending blocking commands to linked devices, applicable to Palo...
FortiGate-300E-v7.4.1	Predefined	This template is a command-line template for sending blocking commands to linked devices, applicable to Forti...

SÉCURITÉ RÉSEAU · HAFS NETWORKS CI

NIPS Hillstone vs NGFW + module IPS en cœur de réseau

Argumentaire technique, commercial et conformité ISO/CEI 27001

Le constat terrain

Sur le terrain, plusieurs concurrents déploient un NGFW avec module IPS activé directement au **cœur de réseau** — à l'endroit où circule le plus de trafic est-ouest (inter-VLAN, datacenter, sauvegardes) — plutôt qu'un IPS dédié.

C'est un choix pratique à vendre… mais risqué à opérer à cette échelle.

-30 à -60%

de débit réel constaté quand l'IPS est activé sur un NGFW multi-fonctions

Repère fabricants — débit "firewall only" vs débit avec inspection complète activée

Pourquoi ça casse en cœur de réseau

1

Trafic est-ouest massif

Le cœur agrège tout le trafic interne (inter-VLAN, stockage, sauvegardes) — des débits bien plus élevés et constants qu'en périmètre Internet.

2

Latence pénalisante

Le traitement multi-fonctions d'un NGFW ajoute une latence sensible pour le SAN, la VoIP interne et les applications métier.

3

Fonctions superflues activées

NAT, VPN, SSL inspection tournent au cœur sans utilité réelle, au détriment du débit disponible pour l'IPS.

4

Point de défaillance unique

Une surcharge ou une panne interrompt simultanément le firewalling ET l'inspection de tout le trafic interne.

5

Refonte d'architecture

Insérer un NGFW au cœur impose souvent un redesign, alors qu'un NIPS s'insère en TAP/SPAN sans impact sur l'existant.

Comparatif direct

Critère	NIPS dédié Hillstone	NGFW + IPS en cœur (concurrent)
Débit à pleine charge IPS	Optimal — moteur dédié	Dégradé — ressources partagées
Latence	Minimale	Plus élevée (multi-fonctions)
Visibilité trafic est-ouest	Complète (TAP/SPAN, inline)	Limitée — conçu pour le périmètre
Impact d'une panne/surcharge	Isolé (inspection seule)	Global (firewalling + inspection)
Insertion dans le réseau	Sans refonte d'architecture	Redesign souvent nécessaire
Fonctions actives au cœur	Inspection uniquement	NAT / VPN / SSL + inspection

Conformité ISO/CEI 27001 — Annexe A

Un NIPS dédié en cœur de réseau donne des preuves d'audit concrètes sur plusieurs contrôles clés

A.8.16

Activités de surveillance

Visibilité comportementale dédiée sur le trafic interne, sans dégrader la performance du firewall.

A.8.20

Sécurité des réseaux

Filtrage et journalisation du trafic renforcés par un moteur d'inspection indépendant en cœur de réseau.

A.8.21

Sécurité des services réseau

Exigences de sécurité appliquées en continu, sans dépendre des ressources déjà sollicitées du firewall périmétrique.

A.8.22

Cloisonnement des réseaux

Isolation des sous-réseaux critiques (datacenter, DMZ interne) confirmée par une inspection dédiée en cas d'incident.

Arguments commerciaux

- **Vente complémentaire, pas concurrente**

  Augmente le ticket moyen sans remettre en cause l'investissement NGFW déjà réalisé par le client.

- **Cible : clients déjà équipés d'un NGFW**

  Module IPS souvent désactivé ou sous-utilisé faute de capacité — cycle de vente court, pas de remplacement d'infra.

- **Argument conformité / audit**

  La séparation firewall / IPS est valorisable en audit ISO 27001, PCI-DSS ou BCEAO — un point facile à faire valoir.

- **Coût marginal vs remplacement complet**

  Un NIPS dédié coûte moins cher qu'un upgrade de gamme NGFW pour retrouver le débit perdu avec l'IPS activé.

Département Commercial

WCA

HAFS

Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

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

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

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