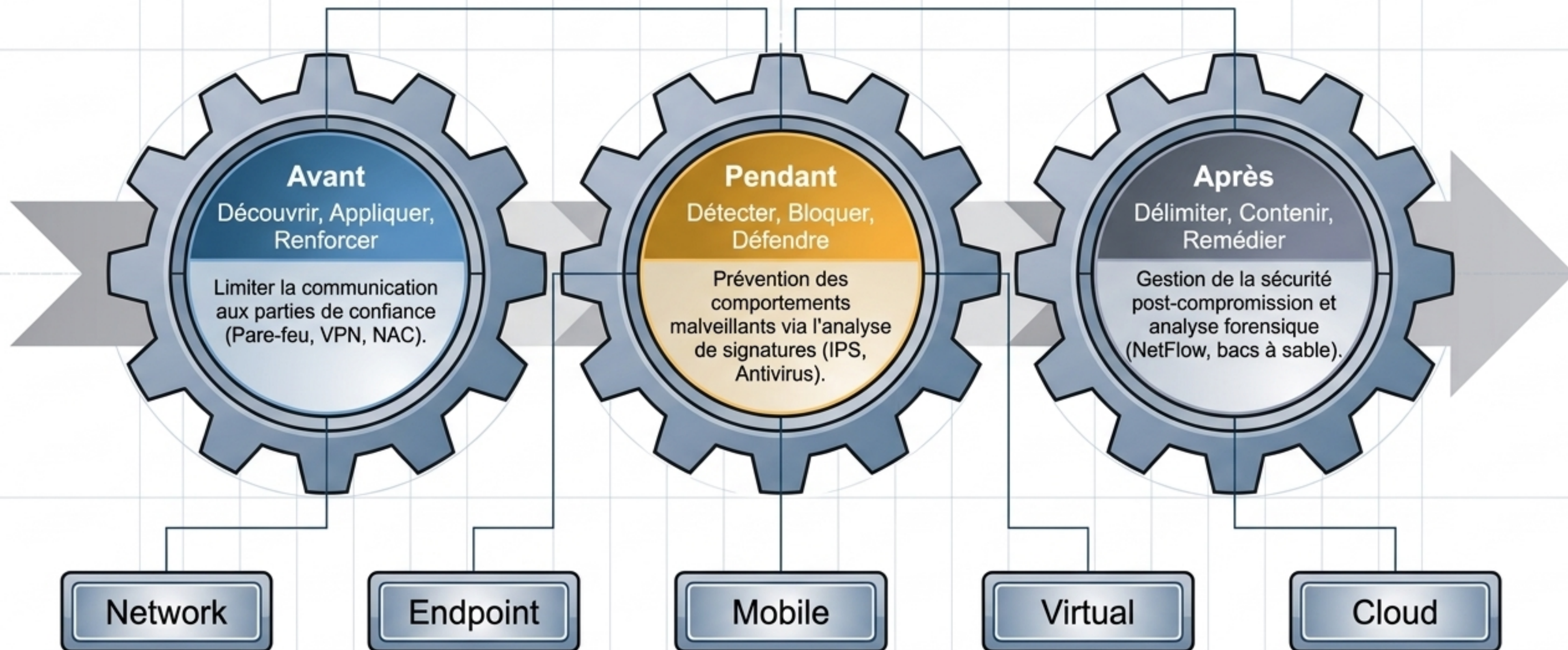


Capacités d'analyse forensique de Cisco : Architecture de la cybersécurité globale

« Tout produit qui nécessite un manuel d'utilisation
est défectueux. » — Elon Musk

La stratégie de défense BDA :

Le modèle de la chaîne d'attaque



Cisco Firepower : Le cœur de l'investigation réseau

Impact 1 (Rouge Cramoisi) :
Intervention immédiate requise
(Exploitation active)

Impact 2 (Orange) : Comportement
suspect méritant un examen

Impact 3 (Jaune) : Événement
potentiel (ex: port fermé ciblé)

Impact 4 (Bleu/Gris) : Hôte connu,
comportement acceptable

Impact 0 (Blanc) : Événement hors du
réseau profilé

Résumé du Tableau de Bord

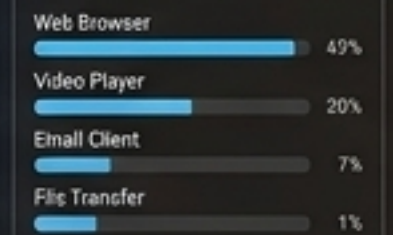
Unique Applications over Time



Top Web Applications Seen



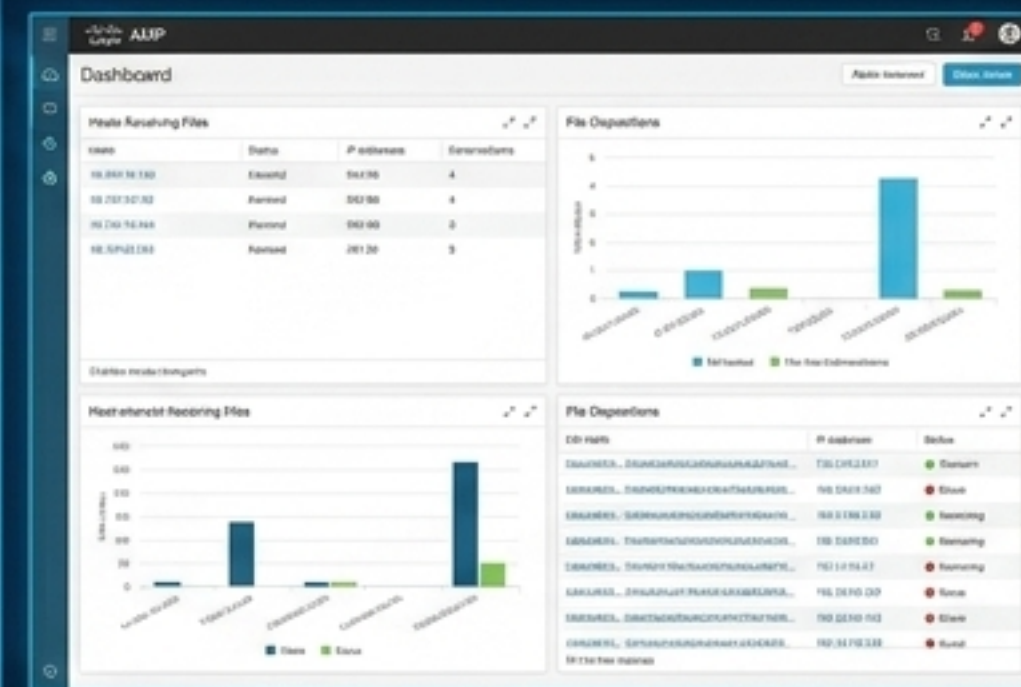
Top Client Applications Seen



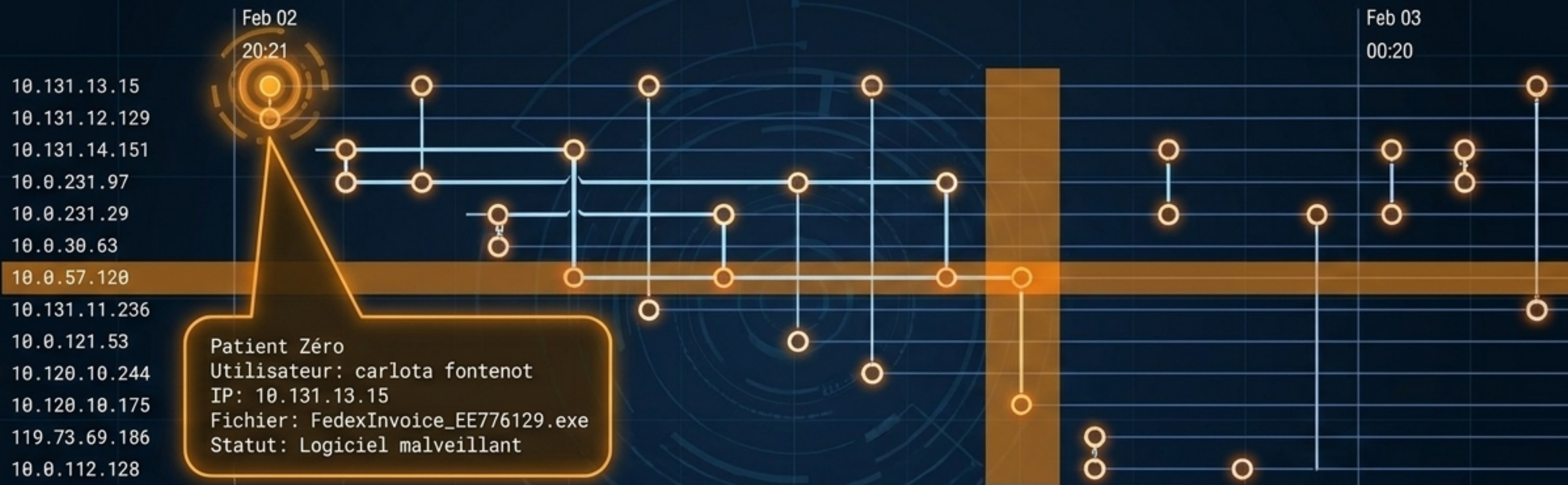
Fusionnant le pare-feu ASA et la technologie Sourcefire, Firepower offre une visibilité totale sur les ports, protocoles et applications, avec un système de classification par impact pour le triage forensique.

Cisco AMP : Le suivi rétrospectif des menaces

Le flux comportemental



Chronologie forensique : Traquer le « Patient Zéro »



Lors d'une intrusion, ne formatez pas immédiatement la machine. AMP cartographie la propagation latérale pour identifier le point d'entrée exact. Une facture FedEx ne devrait jamais être un exécutable (.exe).

Le maillon manquant : Réseau vs Poste de travail (Endpoint)

AMP for Network (Sur Firepower)



- **Avantage** : Bloque les fichiers en transit.
- **Limitation** : Perte de visibilité si l'hôte quitte le réseau. Impossible de supprimer le fichier du terminal.

Feedback Loop

Remontée des valeurs CVE :
Firepower ajuste automatiquement ses paramètres IPS pour activer les signatures bloquant ces failles spécifiques.

AMP for Endpoints (Agent léger)



- **Avantage** : Analyse continue sur l'hôte, même hors du réseau d'entreprise.
- **Capacité clé** : Détection et remontée des vulnérabilités locales.

☐	CVE-2013-0889	8.5	HIGH
☐	CVE-2013-5907	10.0	CRITICAL
☐	CVE-2014-0428	10.0	CRITICAL
☐	CVE-2018-1234	8.5	HIGH
☐	CVE-2018-1234	8.5	HIGH

Cisco Threat Grid : La chambre forte forensique (Sandboxing)



Lorsqu'un artefact suspect n'est pas reconnu par les signatures standard, Threat Grid l'isole pour le forcer à révéler sa vraie nature, documentant chaque action pour les enquêteurs.

Indicateurs comportementaux et renseignement global (Talos)

- [+] Potential TOR Connection (Severity: 100)
- [+] Ransomware Backup Deletion Detected (Severity: 100)
- [+] Shadow Copy Deletion Detected (Severity: 100)
- [+] Process Modified Desktop Wallpaper (Severity: 100)

Intégration Cisco Talos :

L'équipe de recherche observe le plus grand volume d'échantillons au monde. Une menace détectée dans votre environnement a probablement déjà été analysée ailleurs. Threat Grid alimente le reste de l'écosystème grâce à l'analyse de ces données massives.

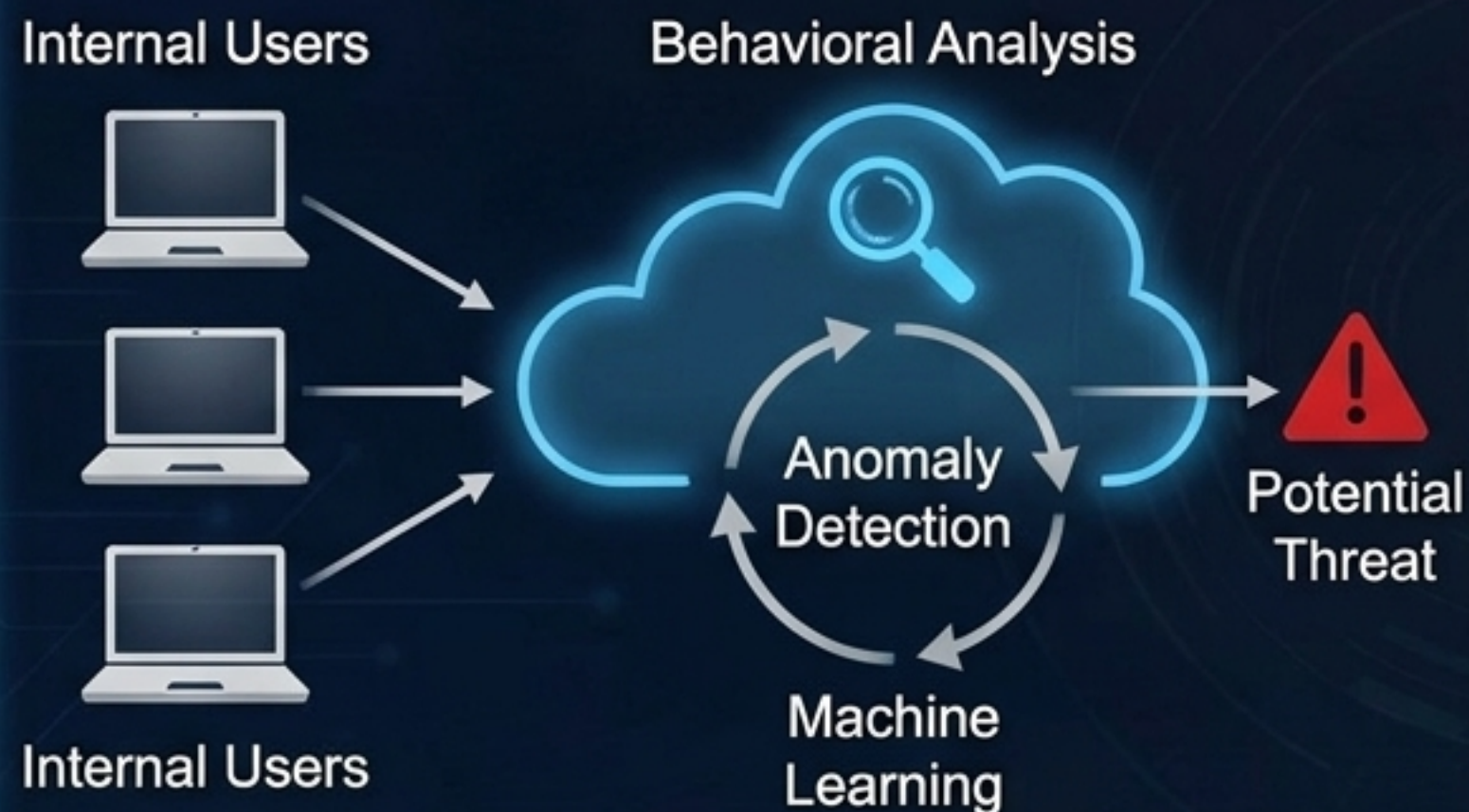
Matrice de déploiement : Pare-feu, Proxy ou Hybride ?

	Cisco Firepower	Cisco WSA (Web)	Cisco Meraki MX
Architecture	Pare-feu applicatif	Proxy Web (Internet uniquement)	Hybride (Matériel géré dans le Cloud)
Visibilité du trafic	Transit Internet + Mouvement latéral interne	Internet uniquement (Idéal pour DLP)	Géré par le Cloud (Idéal multisites)
Niveau de contrôle IPS	Contrôle total (Règles granulaires)	Options via CTA et antivirus tiers	Basique (Ensembles de règles généraux)

Conclusion : Sécurité maximale = Firepower. Performances utilisateur web = WSA.
Simplicité/Évolutivité multisite = Meraki.

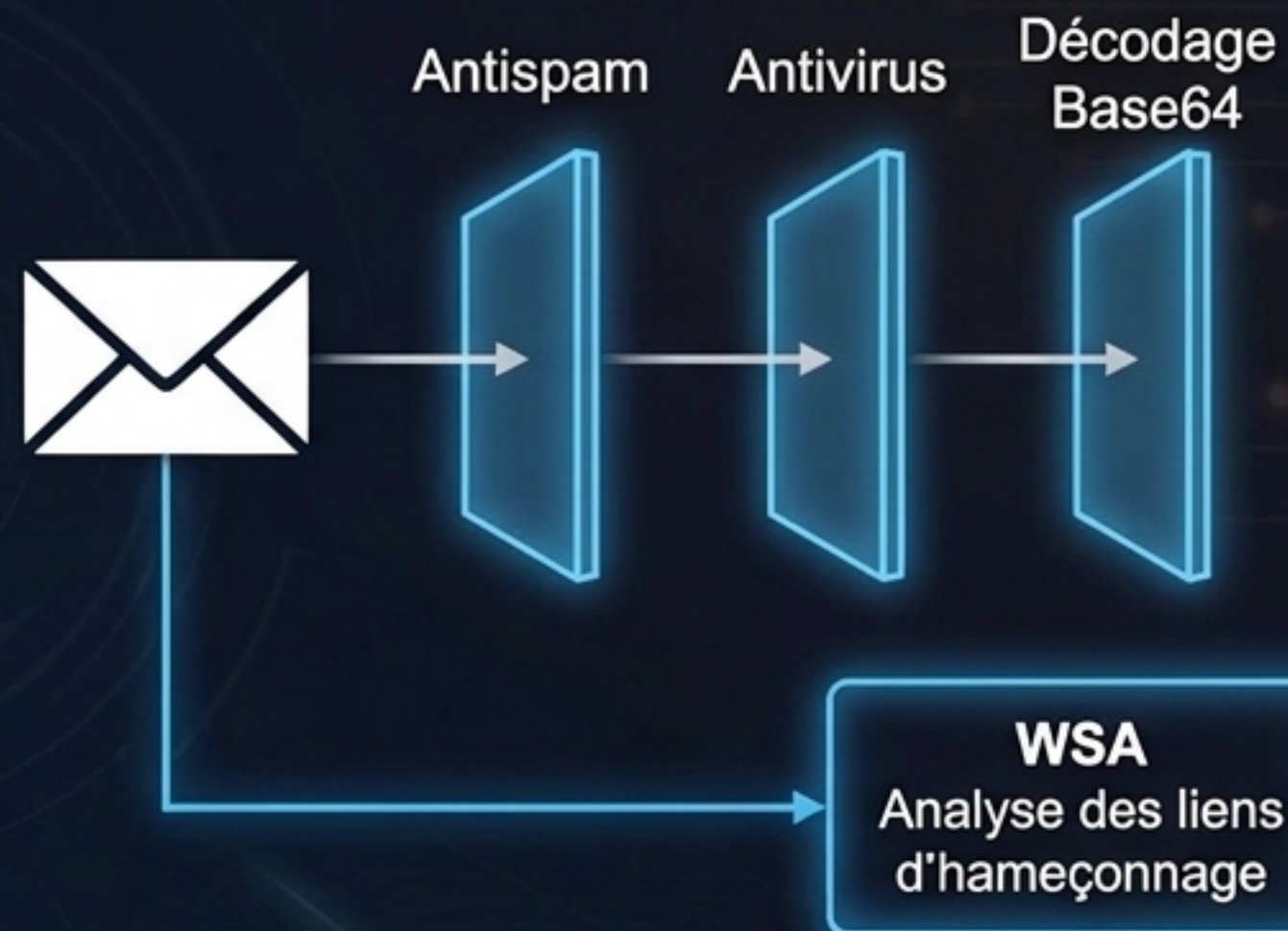
Détecter les menaces internes (CTA) & Sécuriser les courriels (ESA)

Cisco CTA (Cognitive Threat Analytics)



Détecte les menaces internes (Botnets, exfiltration) via l'apprentissage automatique dans le trafic Web anormal. 90% des menaces internes transitent par Internet.

Cisco ESA (Email Security Appliance)

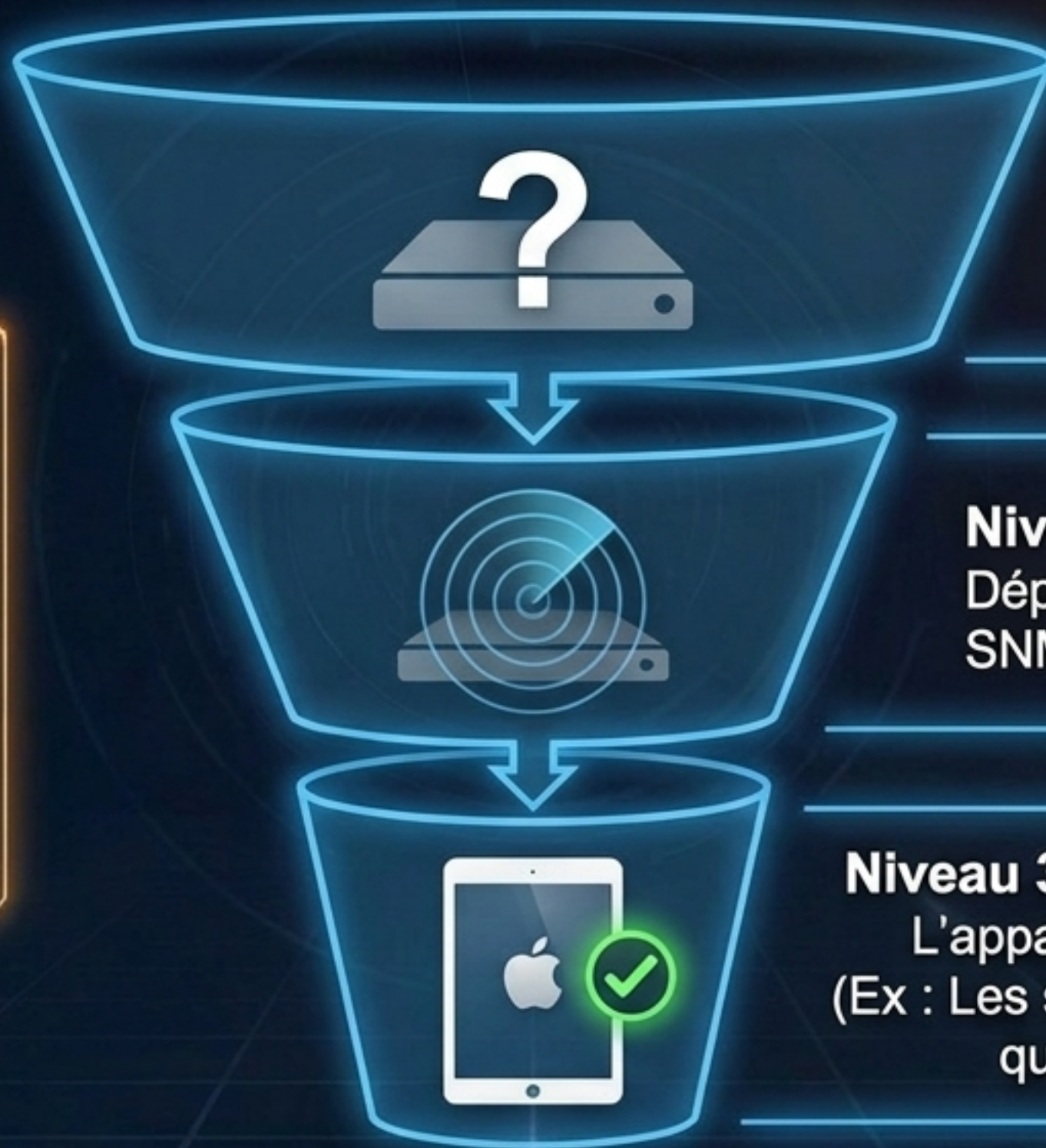


Sécurise le vecteur d'entrée le plus ciblé. Intègre l'analyse des URL via WSA pour empêcher les utilisateurs de cliquer sur des factures falsifiées.

Cisco ISE : L'entonnoir de profilage actif

Connaître son réseau est la règle d'or d'un SOC.

ISE automatise le contrôle d'accès au-delà des adresses MAC falsifiables.



Niveau 1 : Appareil inconnu
Connexion au réseau
(Filaire, VPN, WiFi).

Niveau 2 : Sondes actives
Déploiement de capteurs (DHCP, SNMP, HTTP, DNS, RADIUS).

Niveau 3 : Catégorisation dynamique
L'appareil est formellement identifié
(Ex : Les sondes DHCP et DNS confirment qu'il s'agit d'un iPad Apple).

La posture de sécurité (Cisco ISE) : Au-delà de l'adresse MAC



Avertissement : L'approche traditionnelle basée sur l'adresse MAC est obsolète car elle est trop facilement falsifiable. La vérification de la posture valide l'état réel et sécurisé du périphérique avant l'octroi de l'accès.

Synthèse : L'écosystème forensique unifié



Points clés des opérations forensiques

Visibilité Intégrale (Le Radar)



De l'authentification active (ISE) à la surveillance des ports (Firepower) en passant par les vecteurs spécialisés (WSA/ESA), l'écosystème élimine les zones d'ombre.

Capacité Rétrospective (La Machine à remonter le temps)



AMP ne se contente pas de bloquer ; il cartographie le réseau, trouve le « Patient Zéro » par hachage et trace la trajectoire de l'infection dans le temps.

Automatisation du Renseignement (Le Cerveau)



La chambre forte Threat Grid isole, force l'exécution et génère des indicateurs, alimentant Talos pour protéger instantanément le reste de l'architecture.

