NETWITNESS

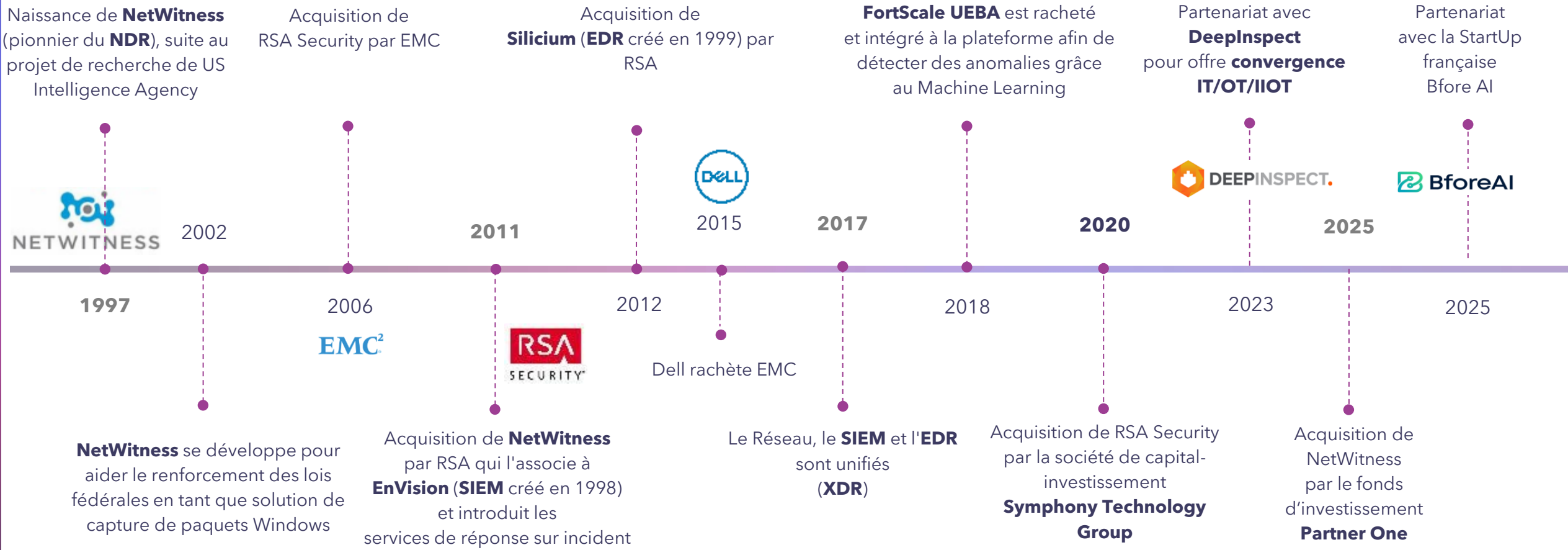
NetWitness

Une détection des menaces et réponse aux incidents à la hauteur de vos enjeux.

Qui nous sommes

… 30 d'expérience en détection de menaces et réponse aux incidents

Notre histoire & héritage



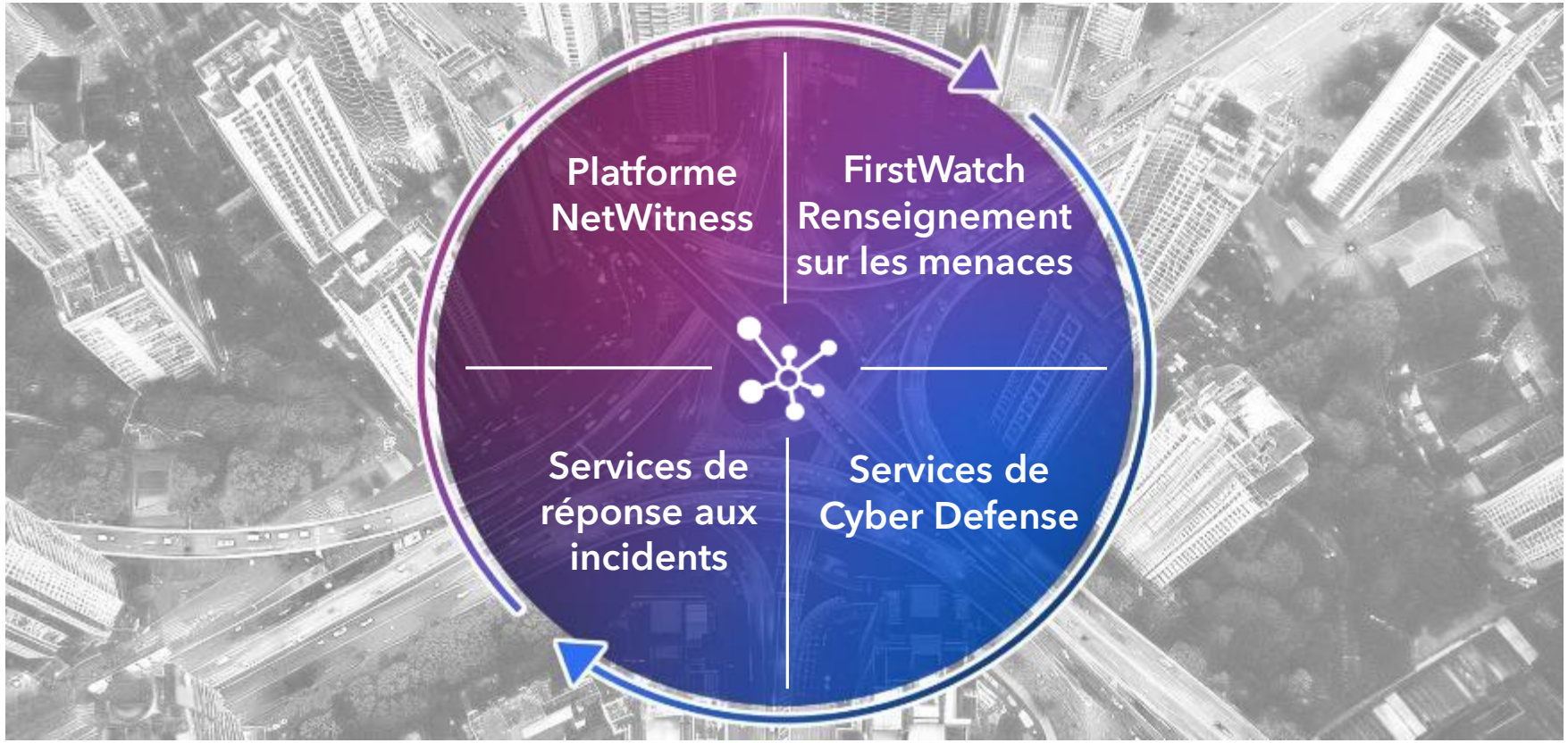
Un écosystème mondial pour servir plus de 600 clients

- Equipes présentes dans tous les continents (22 pays)
- Un écosystème composé de 272 revendeurs et/ou partenaires distributeurs présentes en 60 pays.
- Processus de gestion commerciale de la commande à l'encaissement, actionnable dans le monde entier
- Assistance et support aux clients 24/7. 95% de satisfaction clients grâce à notre programme CSM

- Des services d'intégration disponibles dans le monde entier avec des équipes de consultants locaux.
- Une équipe de réponse aux incidents mondialement reconnue
- Une large sélection de formateurs confirmés et de formations certifiantes à suivre en complète autonomie.
- Des services professionnels pour soutenir et assister vos équipes chargées de la sécurité du SI

Notre proposition de valeur

Renforcer la resilience de votre entreprise avec une détection rapide des menaces, une réponse efficace, et une gestion pro active des risques.



Nos services professionnels

Service de Cyber Défense

Améliorez votre capacité à détecter, enquêter et répondre aux menaces grâce à des audits proactifs et des formations

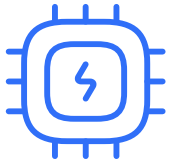
- Recevez un plan d'amélioration détaillé spécifique à votre organisation.
- Exploitez une expertise approfondie pour vous aider à concevoir et à développer votre SOC (Sécurity Operationnal Center).
- Améliorez les compétences de vos analystes grâce à des formations formelles et sur le terrain.

Services de réponse aux incidents

Trouvez rapidement la source d'une menace et remédiez-y en déployant l'équipe de réponse aux incidents de NetWitness

- Répondez rapidement avec une investigation approfondie sur les activités suspectes et les anomalies, sur les réseaux et les systèmes hôtes.
- Bénéficiez de l'expérience d'enquêteurs en cybersécurité ayant plus de vingt-cinq ans d'expérience dans la sécurité des réseaux.
- Passez en revue les activités suspectes identifiées sur le réseau, même sans motif préalable de suspicion d'activités malveillantes

NetWitness FirstWatch (Renseignement sur les menaces)

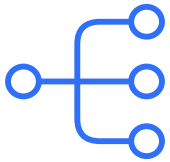


Données de renseignement de haute qualité

- Améliorez votre analyse avec des informations contextuelles de premier ordre.
- Réagissez rapidement aux menaces émergentes grâce à des informations en temps réel.
- Améliorez la prise de décision avec des données fiables qui réduisent les faux positifs et les faux négatifs.

Sources Uniques

- Obtenez une vue d'ensemble grâce à des résultats combinant les logs réseau, la télémétrie des endpoints et les feeds sur les menaces.
- Bénéficiez d'une intelligence centrée sur l'humain provenant des analystes, de l'OSINT et de la surveillance du dark web.



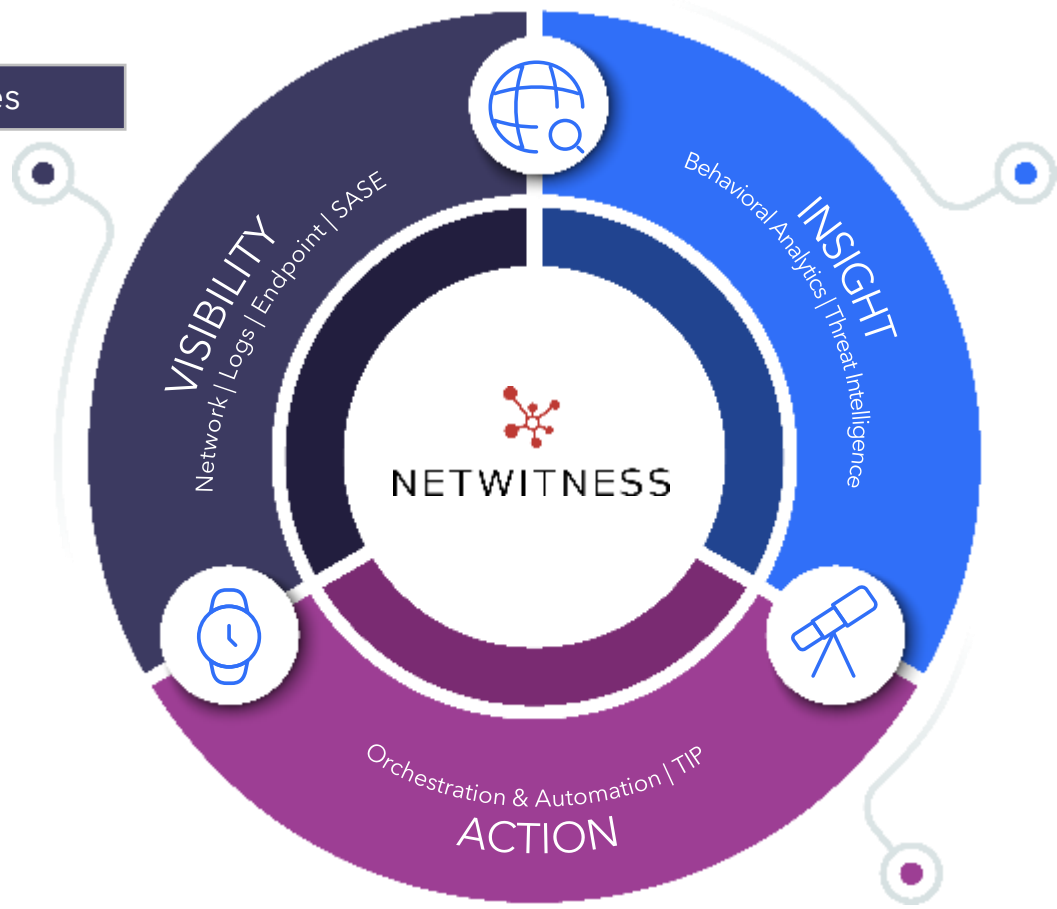
Enquêtes Rationalisées

- Réduisez le dwell time grâce à des algorithmes avancés qui détectent les menaces rapidement.
- Protégez votre environnement avec des renseignements sur les menaces, personnalisées.
- Identifiez les acteurs malveillants grâce à des analyses avancées corrélant des sources de données hétérogènes.

La plateforme TDR de NetWitness

Disposer de toutes les données

- Disposer de toutes les données (logs, paquets, netflow, endpoint logs, etc.) apporte une visibilité complète sur les activités du réseau et des systèmes. cela permet de mieux détecter les incidents en fournissant une image claire et détaillée des interactions, des comportements anormaux, et des signatures d'attaques potentielles.



Mener une analyse exhaustive

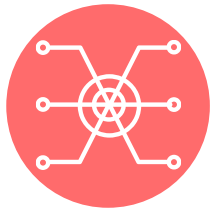
- Implémentation de méthodes déductives (règles statiques, pattern matching, etc.) et inductives (apprentissage automatique et analyse comportementale) pour mener une analyse exhaustive, détecter rapidement et efficacement toute menace et tout signe de compromission.

Définir des réponses automatisées et ciblées

- Contextualiser au mieux les menaces grâces à la Threat Intelligence.
- Définir des playbooks préconfigurés et personnalisables pour faciliter la collaboration entre toutes les parties prenantes et répondre au mieux aux incidents de sécurité.
- Accéder rapidement à de l'expertise de haut niveau disposant de processus et d'outils éprouvés.

La plateforme TDR de NetWitness (composants)

Une unique plateforme capable de détecter, et de répondre aux menaces dans l'ensemble de vos environnements



NETWORK

SIEM

ENDPOINT

AUTOMATION

INTELLIGENCE

Tout voir grâce à une visibilité complète du réseau

Détecter plus tôt les menaces, afin de limiter leur impact

Enquêter sur les menaces et y répondre rapidement et facilement

Démontrer la conformité aux normes de sécurité de manière efficace et efficiente

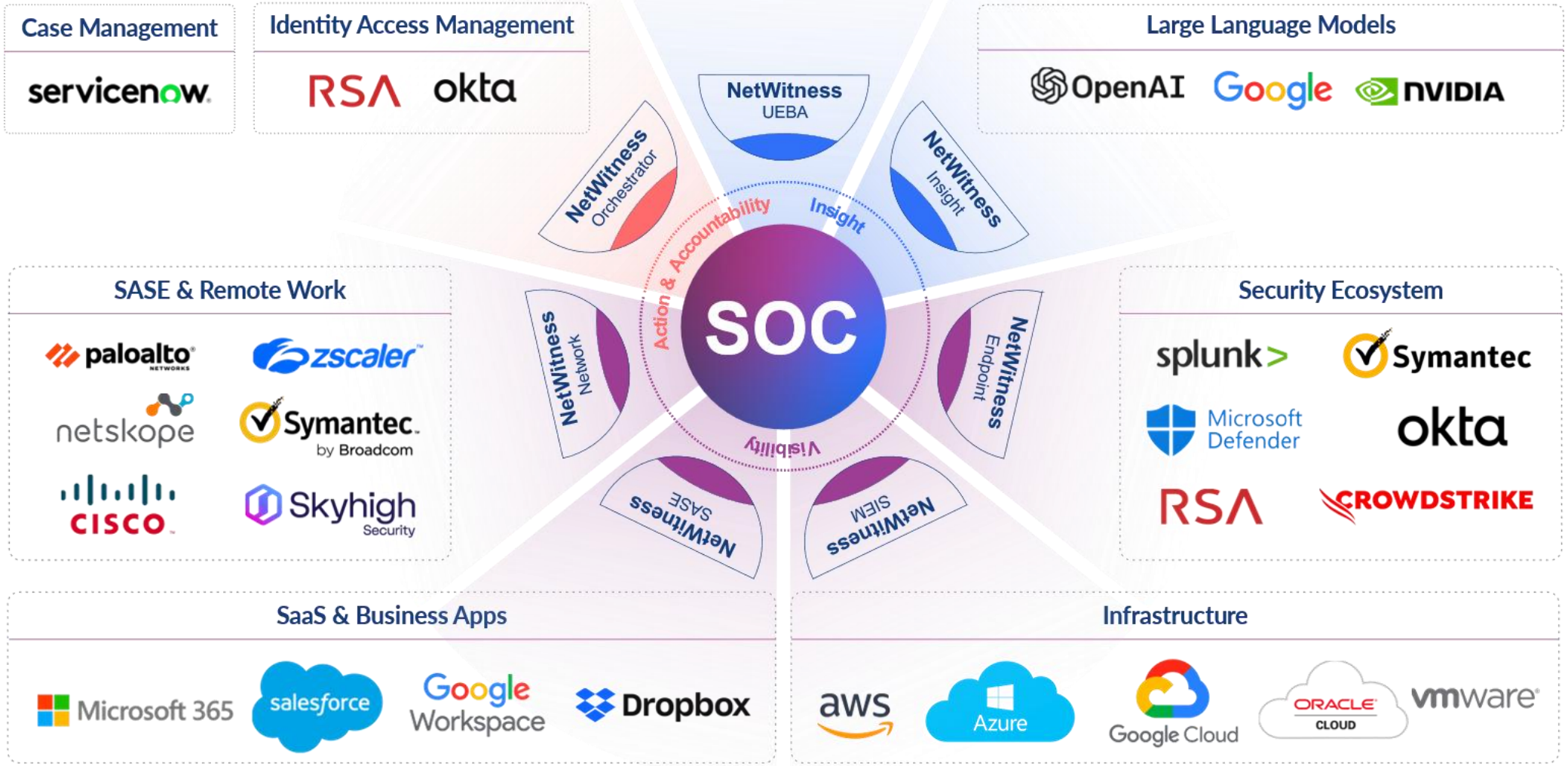
... Agile et modulaire afin de s'intégrer au mieux aux investissements technologiques déjà réalisés.

NETWITNESS

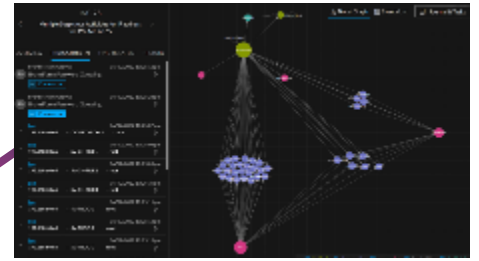
Annexe technique

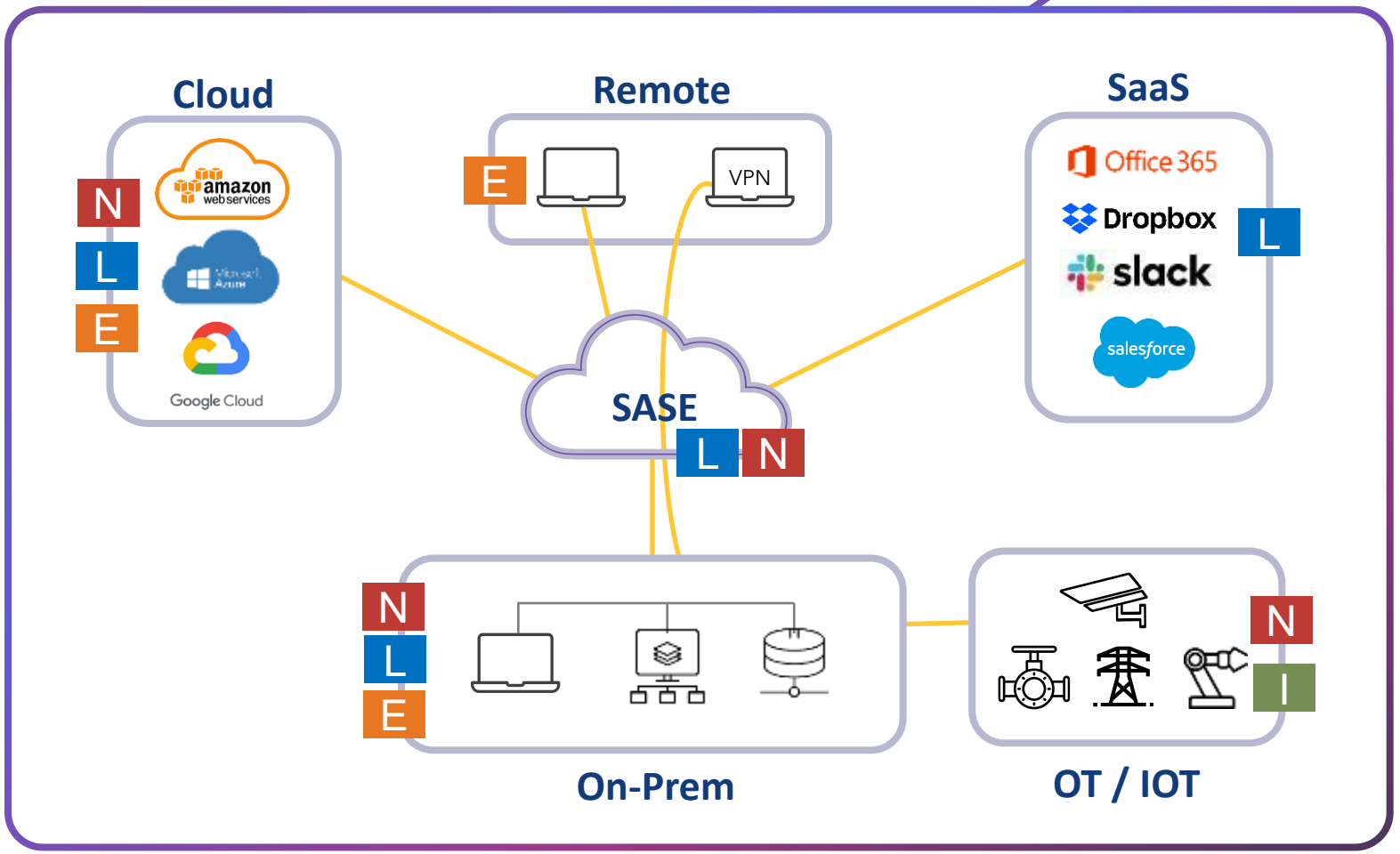
Une plateforme de détection des menaces et réponse aux incidents complète, un seul modèle de données, une détection des menaces inégalée et une réponse sur mesure.

Une intégration totale pour répondre aux enjeux du SOC



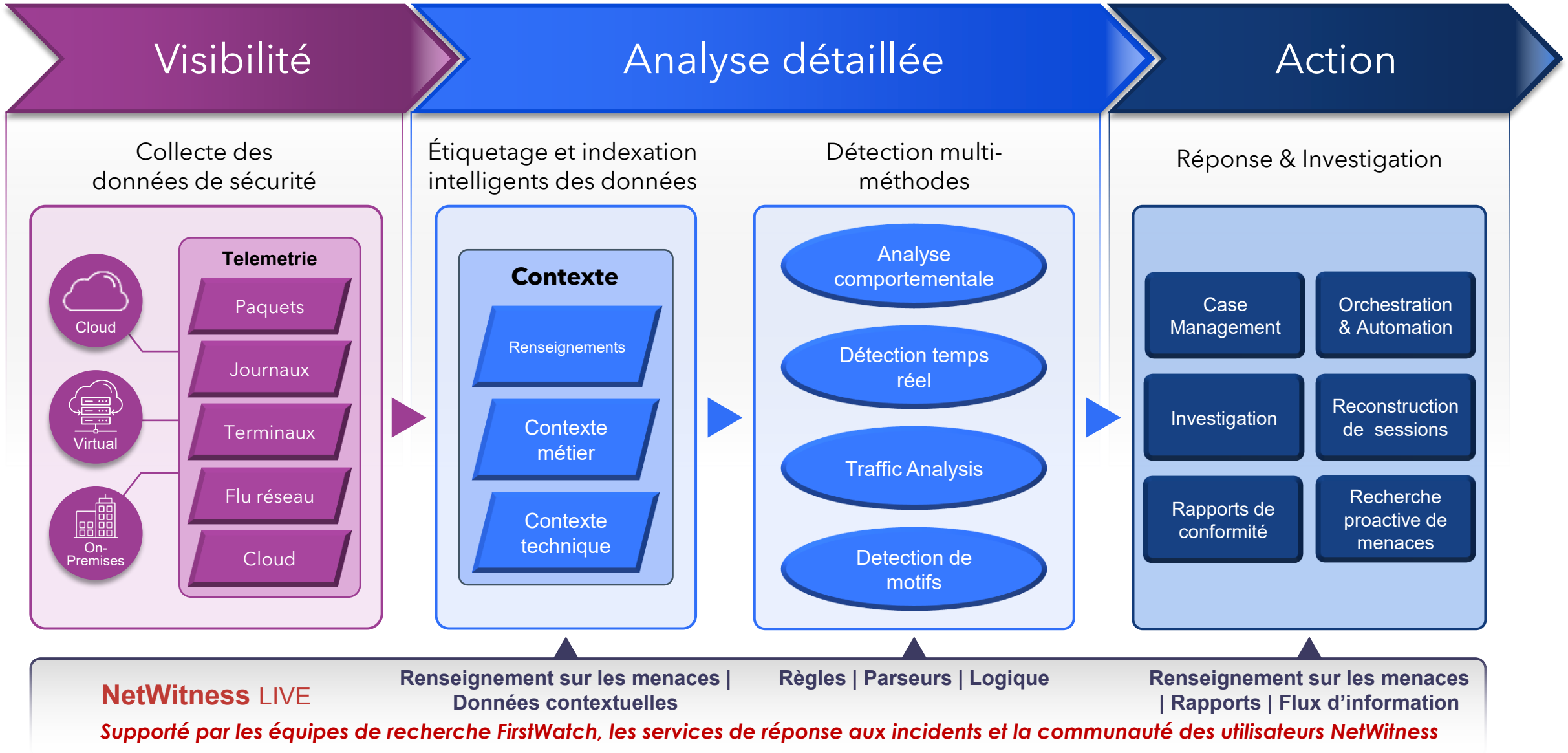
Une visibilité globale, partout



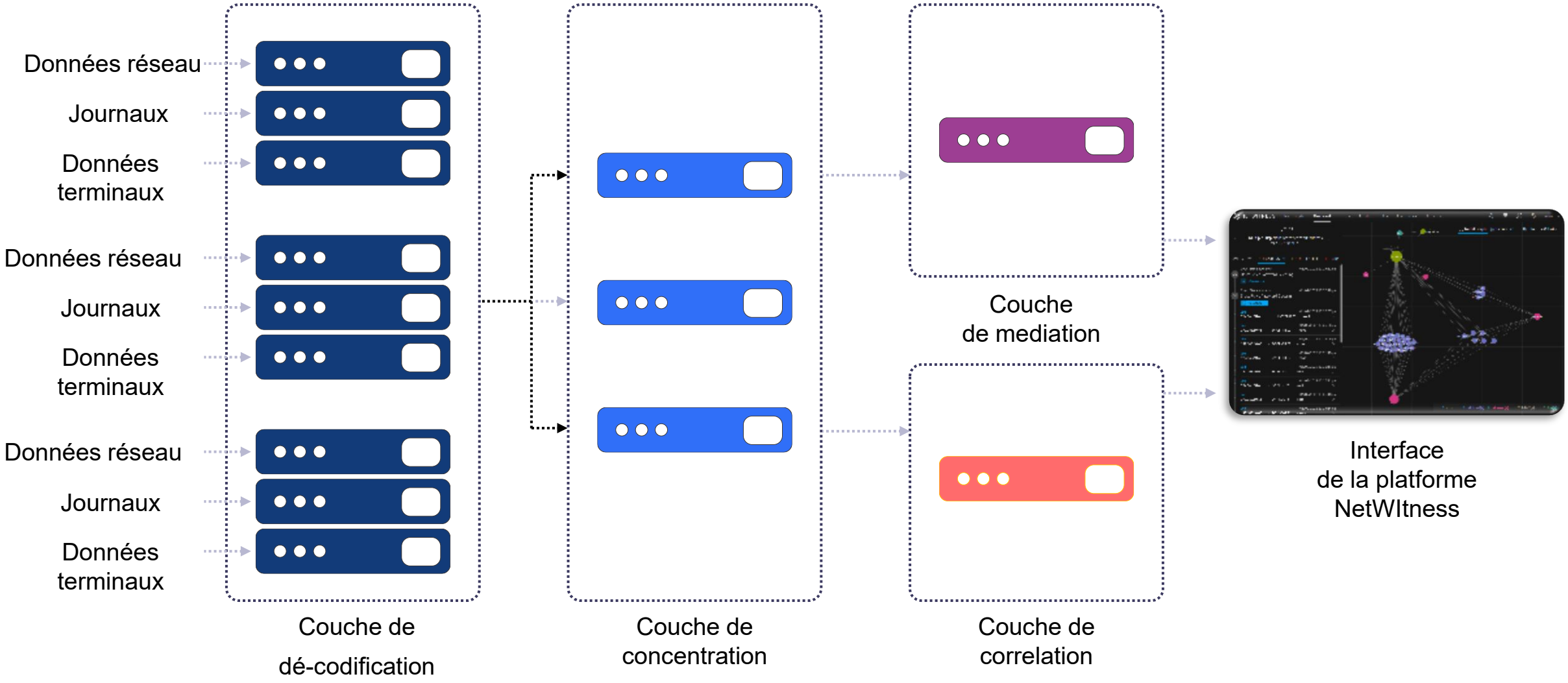


L Logs / SIEM
N Network / NDR
E Endpoint / EDR
I IOT / OT

Architecture fonctionnelle



Une architecture flexible et scalable



Architecture – Les composants

Composant	Description
Decoder	Capture et stocke les données brutes. Les décodeurs sont spécifiques aux logs ou au réseau (paquets). Créer des métadonnées à partir de la capture de données brutes et les enrichir avec le contexte de sécurité et du business.
Concentrator	Stocke et indexe les métadonnées pour des requêtes rapides et la récupération de la capture de données brutes.
Broker	Facilite les requêtes à travers un déploiement multi-site.
ESA	Moteur de corrélation et d'analyse en temps réel des logs, du réseau (paquets), des endpoints et de NetFlow.
Archiver	Conservation à long terme et compression des données.
NetWitness Server	Interface utilisateur Web et serveur de gestion, qui sert d'interface utilisateur principale.

NETWITNESS

Unissons nos forces!

Merci !

Frank CAROSI
Country Business Development Lead
+33 6 79 56 05 49
frank.carosi@netwitness.com

Jérôme PASCAL
Senior Sales Engineer France
+33 6 32 40 27 72
jerome.pascal@netwitness.com