

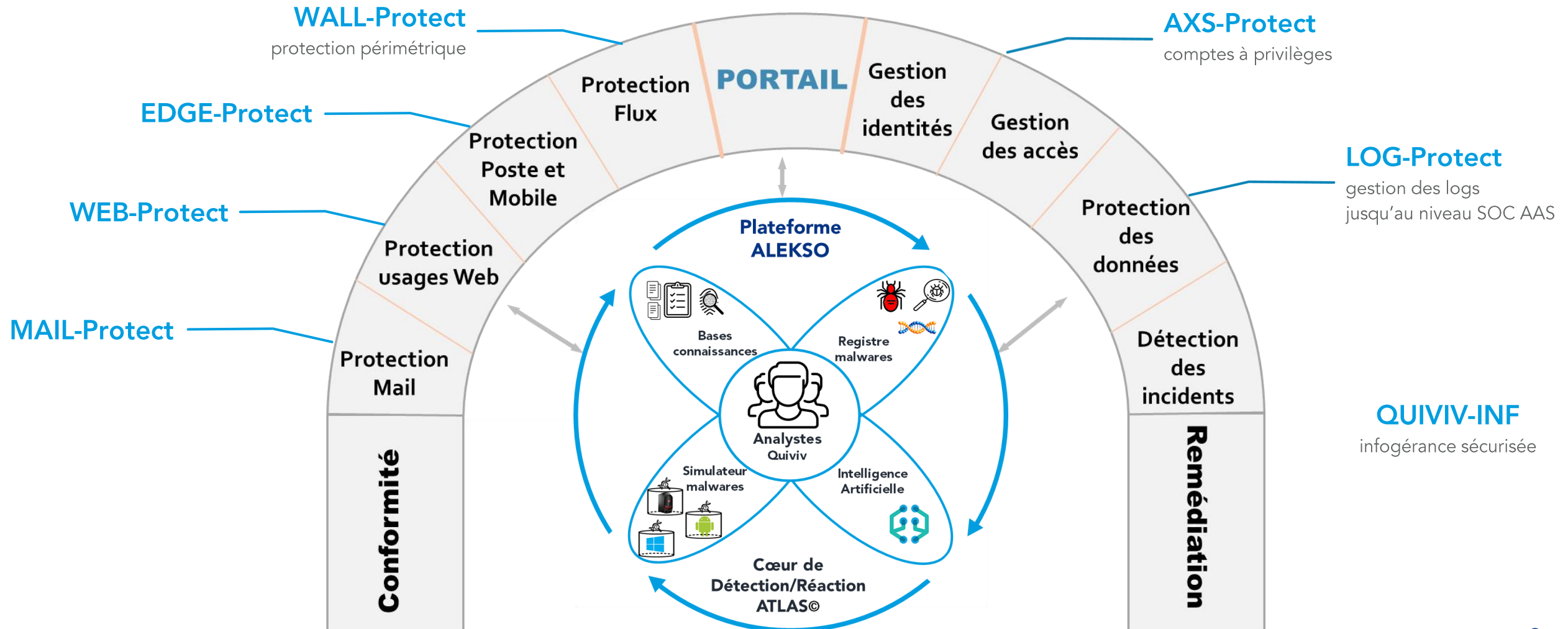


Catalogue de cybersécurité ALEKSO

Marché UGAP – SCC «Multi-Editeurs»

1.1 L'Offre de Service : QUIVIV

ALEKSO éditeur de Software Security-as-a-Service (SaaS)



02 QUIVIV-EDGE-Protect



ALEKSO

Simple as a service



2.1 EDGE-Protect : sécurisation des «endpoints» : PCs et Serveurs

■ Les objectifs, notre mission :

- Veiller au quotidien sur les signaux de sécurité
- S'assurer que les failles de sécurité système et applicatives sont comblées
- Veiller à l'intégrité et à l'évolution des outils de protection
- S'assurer que l'ensemble des machines connectées soient protégées
- Intervenir en cas d'incident de sécurité
- Faire face aux menaces et aux enjeux quotidiens de la gestion de la protection Endpoint

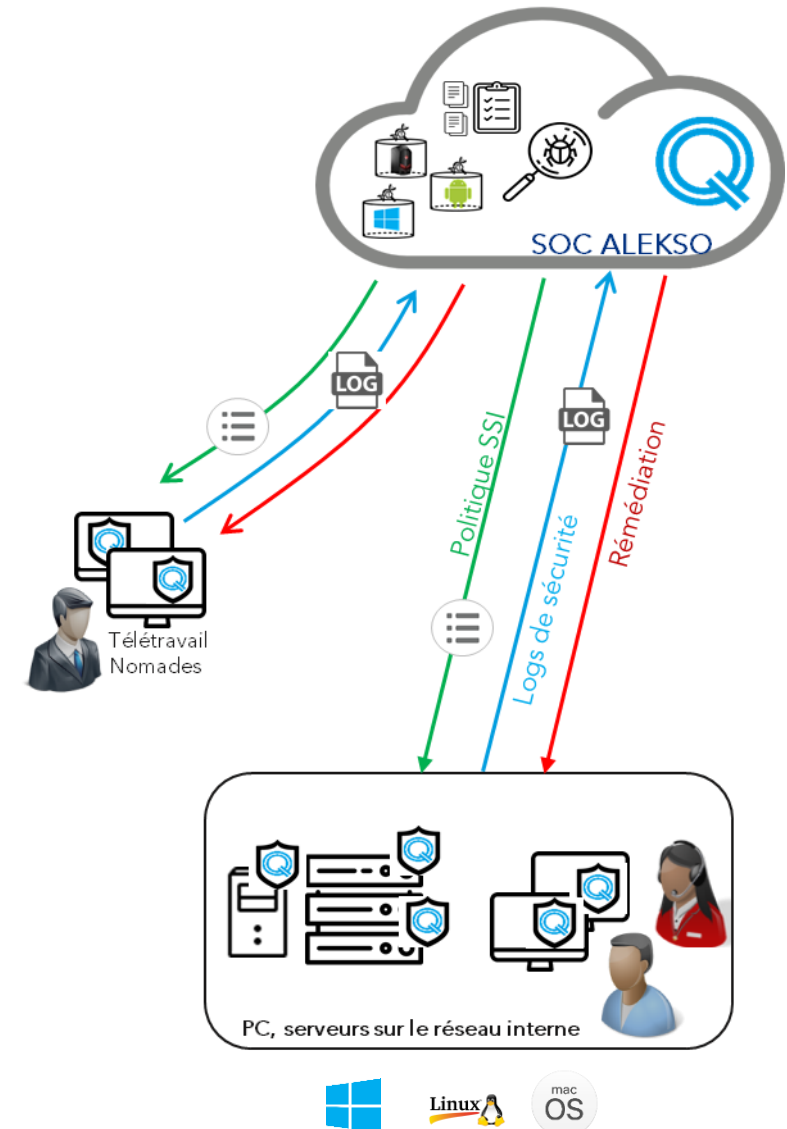
■ Les fonctions assurées :

- Antimalware EPP (Endpoint Protection Platform) efficace même en mode déconnecté
 - Antimalware EDR (Endpoint Detection & Response) efficace même en mode déconnecté
 - Endpoint IDS/IPS (Intrusion Detection & Prevention System)
 - Audit de vulnérabilités
 - Outils Forensic : collecte de preuves, analyse post-infection
 - Solution RMM (Remote Monitoring & Management)
 - Gestion des alertes rétrospectives et support à la remédiation
 - Archivage des logs de sécurité sur 12 mois
 - Applicable aux nomades (télétravail) et à tous les dispositifs « end-point »
-
- Solution développée et hébergée en France sur les infrastructures ALEKSO
 - Interface unique de pilotage et de gestion des événements

Inclus : Cœur de détection ATLAS : socle technologique avancé

- ✓ 14 moteurs anti-virus
- ✓ Base de réputation Editeurs sécurité
- ✓ Filtres de réputation / Sandbox
- ✓ Multimoteurs : antivirus, sandboxes, anti-APT
- ✓ Intelligence artificielle et technologies propriétaires
- ✓ Plateforme enrichie par les IOC Quiviv

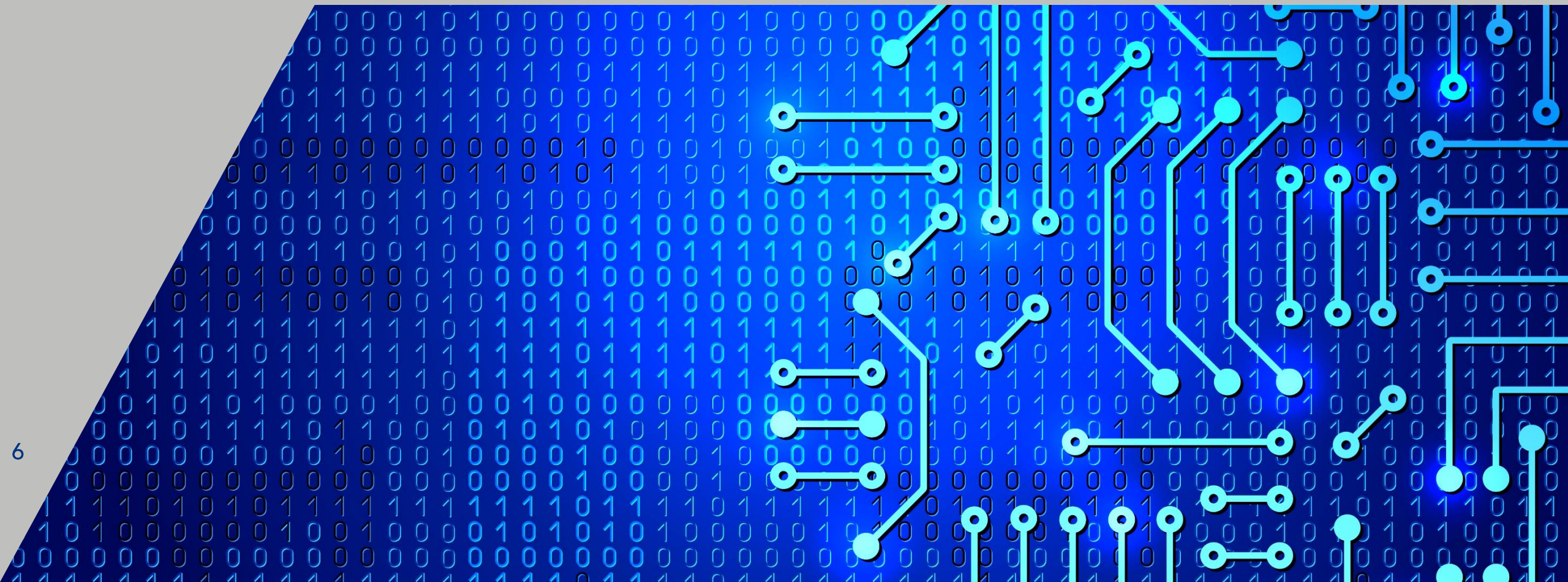
NB : Le niveau de service EDGE-Protect peut varier sur les serveurs en fonction des caractéristiques et contraintes de production



2.2 EDGE-Protect : fonctions et services par niveau de licence

EDGE-Protect	Advance	Complete
Produits		
Prise de main à distance : Remotely	X	X
EPP : Cylance Protect	X	X
EDR : Cylance Optics	X	X
EndPoint HIDS/HIPS : Wazuh/Sysmon	X	X
Détection en profondeur : Cœur ATLAS	X	X
XDR : Plateforme Quiviv	X	X
Audit de vulnérabilités (Maintien en sécurité Windows & Linux) : Wazuh		X
Threat Intelligence ATLAS		X
Collecte de tous les logs et alertes du "endpoint" et mise en corrélation : SIEM		X
Services		
Paramétrage des solutions dédié au Client	X	X
Service de surveillance et de remédiation - Gestion des alertes XDR	X	X
Paramétrage des solutions dédié au Client	X	X
Health Check : monitoring du Service	X	X
Accès à ATLAS "on-demand"	X	X
Support technique Administrateurs	X	X
Support technique Utilisateurs finaux	X	X
Assistance à la gestion de crise	X	X
Audit de vulnérabilités (Maintien en sécurité Windows & Linux) : Wazuh		X
SOC - Détection globale d'incidents		X
SOC - Réponse aux incidents de sécurité (SIR)		X

03 QUIVIV-LOG-Protect



3.1 LOG-Protect : XDR-SIEM-SOC

■ Les objectifs, notre mission :

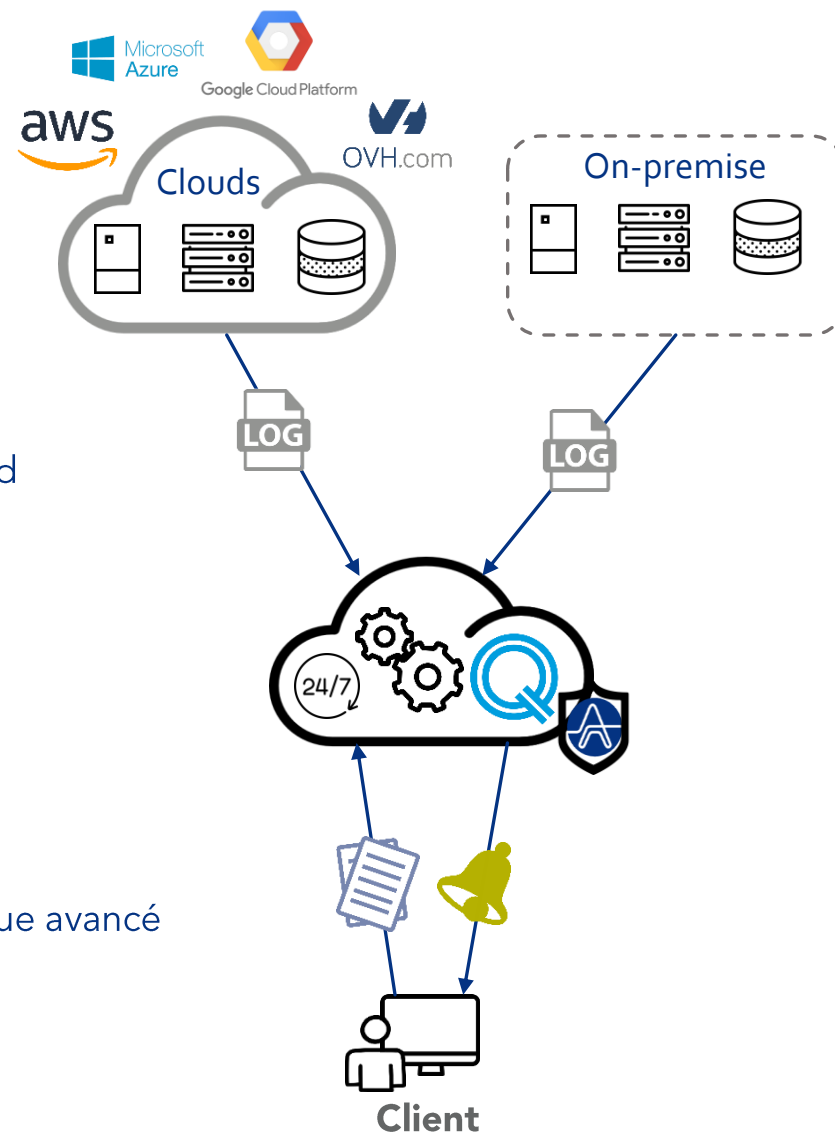
- Collecter et stocker les événements de sécurité et archiver les preuves
- Normaliser, enrichir et rendre disponibles les événements de sécurité
- Disposer des éléments d'analyse et remédiation
- Analyser les événements de sécurité
- Identifier les alertes et les incidents de sécurité
- Traiter et remédier aux incidents de sécurité
- Répondre aux enjeux réglementaires et obligations légales des organisations

■ Les fonctions assurées :

- Collecte des événements de sécurité de tous les composants « On Premise » et Cloud
- Normalisation, enrichissement (parsing) et stockage des événements de sécurité
- Analyse par corrélation d'événements et détection des alertes de sécurité
- Archivage légal d'un an glissant (chaînes froide, tiède et chaude)
- Remédiation sur incidents de sécurité
- Solution développée et hébergée en France sur les infrastructures ALEKSO
- Interface unique de pilotage et de gestion des événements

Inclus : Cœur de détection ATLAS : socle technologique avancé

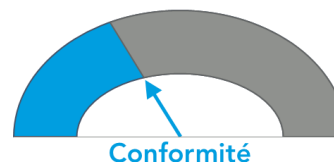
- ✓ Temps réel
- ✓ Horodatage des événements
- ✓ Collecte directe par tunnel mTLS ou VPN
- ✓ Collecte indirecte avec un collecteur relais
- ✓ Stockage big data 14 moteurs anti-virus
- ✓ Intelligence artificielle et technologies propriétaires
- ✓ Plateforme enrichie par les IOC Quiviv



3.2 LOG-Protect : niveaux de service (SOC aaS)

LOG-Protect *Compliance*

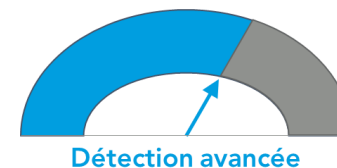
- Collecte des événements de sécurité
- Normalisation, enrichissement des événements de sécurité
- Analyse automatisée des événements de sécurité
- Détection automatique des alertes de sécurité
- Fourniture de rapports d'alertes de sécurité
- Tableau de bords de conformité



LOG-Protect *XDR*

« Compliance » +

- Analyse des alertes par des experts en H24/7 (sur astreinte)
- Remédiation sur alertes
- Aide à la remédiation sur incident de sécurité
- Aide à la gouvernance SSI



LOG-Protect *Complete*

« XDR » +

- Détection d'incidents de sécurité en temps réel
- Gestion des incidents de sécurité
- Intégration de la Threat Intelligence dans les analyses
- Remédiation sur incident de sécurité
- Remédiation avec délégation sur les dispositifs de sécurité
- Rapports d'analyse sur incidents



- *Compliance*
- *XDR*
- *Complete*

04 QUIVIV-MAIL-Protect



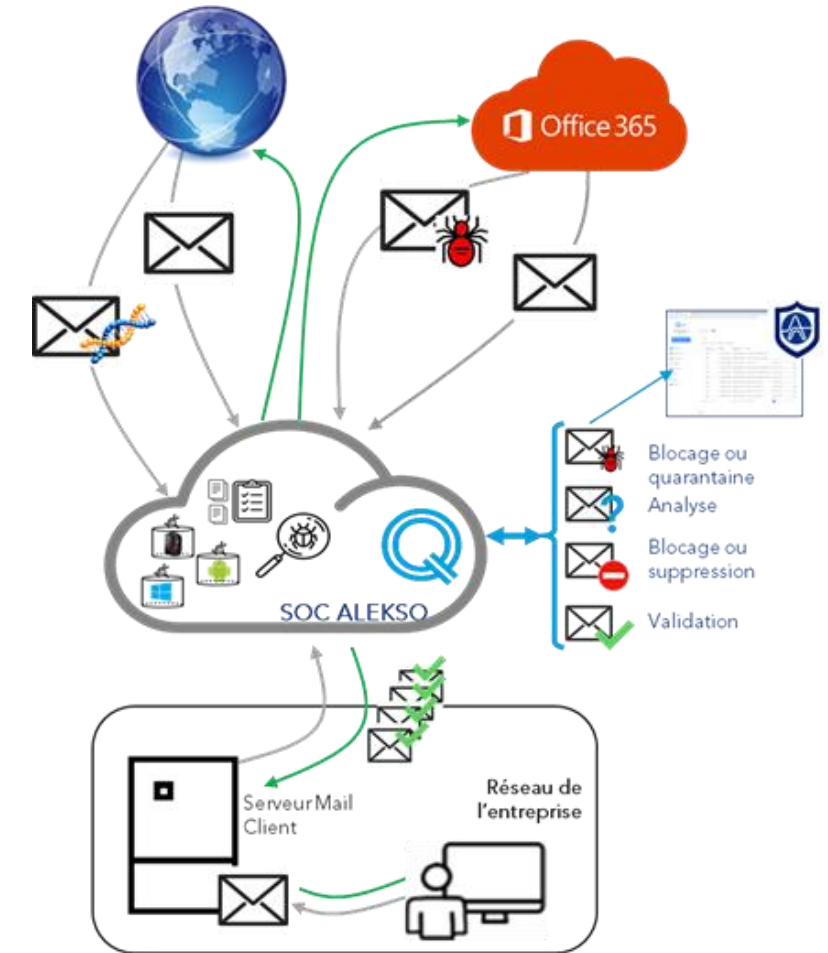
4.1 MAIL-Protect : sécurisation des mails entrants/sortants

▪ Les objectifs, notre mission :

- Menaces : malware, spam, phishing, arnaque au président, ...
- Actualité : ransomware / cryptolocker

▪ Les fonctions assurées :

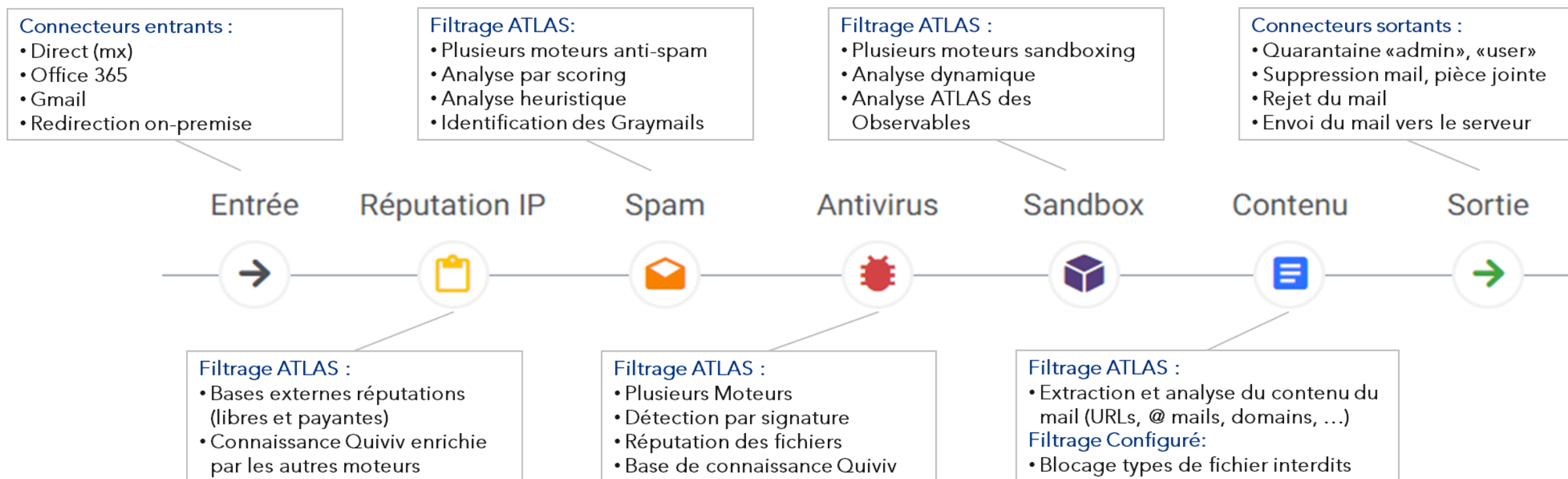
- **14 moteurs anti-virus** : signatures et exploits, réputation fichiers, tests et réputation des URL, réécriture des URL
- Protection des mails entrants ET sortants, y compris O365
- **Antispam** : RBL, signatures, analyse heuristique, image spam, nouveaux domaines
- **Gestion des « black lists »** des émetteurs malveillants
- Définition des politiques de **mise en quarantaine**, distribution, blocage, ...
- **Archivage des logs de sécurité sur 12 mois**
- **Service d'analyse et de threat intelligence**
 - ✓ Analyse comportementale
 - ✓ Gestion des alertes rétrospectives
 - ✓ Support à la remédiation pour la DSI
- Solution développée et hébergée en France sur les infrastructures ALEKSO
- Interface unique de pilotage et de gestion des événements



Inclus : Cœur de détection ATLAS : socle technologique avancé

- ✓ 14 moteurs anti-virus
- ✓ Base de réputation Editeurs sécurité
- ✓ Filtres de réputation / Sandbox
- ✓ Multimoteurs : antivirus, sandboxes, anti-APT
- ✓ Intelligence artificielle et technologies propriétaires
- ✓ Plateforme enrichie par les IOC Quiviv

4.2 MAIL-Protect : schéma de fonctionnement



05 QUIVIV-WEB-Protect



5.1 WEB-Protect : protection et filtrage de la navigation Internet

■ Les objectifs, notre mission :

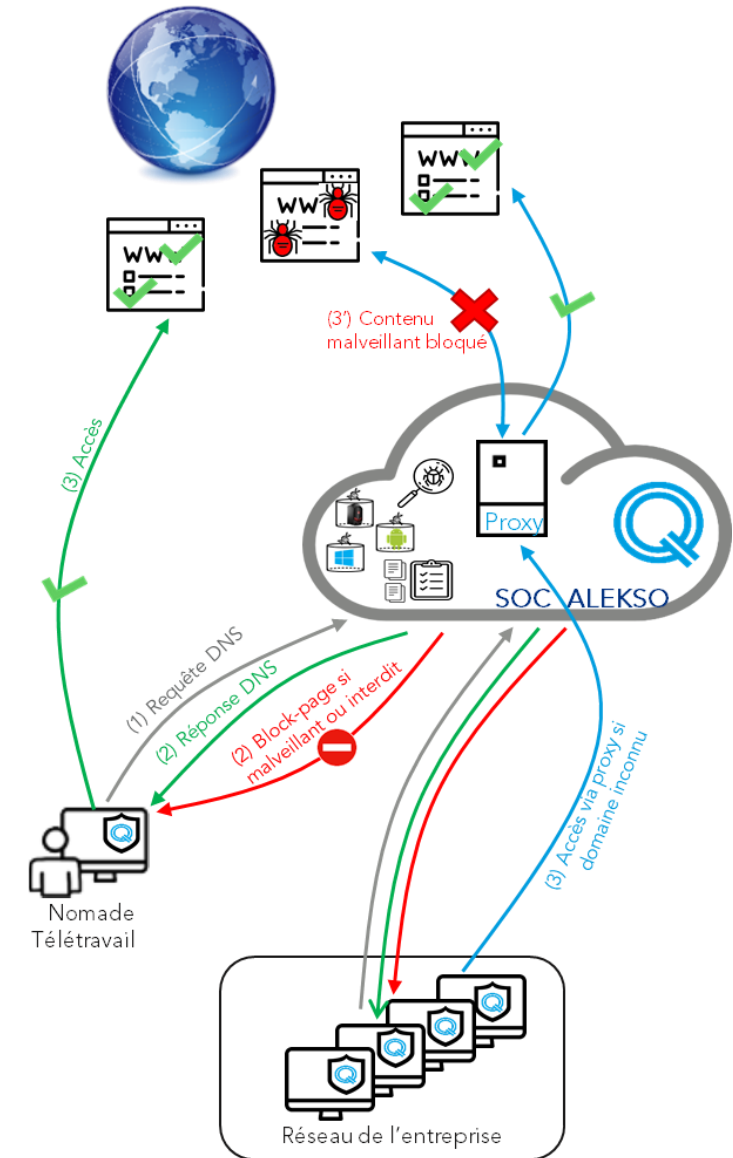
- Filtrage par catégorie d'url, gestion de l'utilisation non conforme
- Malware, protection contre l'exploitation des failles navigateurs
- Respect de la loi, Sécurité positive

■ Les fonctions assurées :

- Solution de filtrage conditionnel
 - Filtrage proactif : blocage avant d'atteindre la destination
 - Catégorisation efficace à plus de 99% (plus de 60 millions d'URL)
 - Pas d'interception des flux (si navigation autorisée ou interdite ou selon politique Client)
 - Inspection des flux SSL possible (équipement spécialisé et validation par le Client)
 - Traçabilité de la navigation
 - Archivage des logs de sécurité sur 12 mois
 - Gestion des alertes rétrospectives et support à la remédiation
 - Applicable aux nomades et à tous les dispositifs « end-point »
-
- Solution développée et hébergée en France sur les infrastructures ALEKSO
 - Interface unique de pilotage et de gestions des événements

Inclus : Cœur de détection ATLAS : socle technologique avancé

- ✓ 14 moteurs anti-virus
- ✓ Base de réputation Editeurs sécurité
- ✓ Filtres de réputation / Sandbox
- ✓ Multimoteurs : antivirus, sandboxes, anti-APT
- ✓ Intelligence artificielle et technologies propriétaires
- ✓ Plateforme enrichie par les IOC Quiviv



06 QUIVIV-WALL-Protect



6.1 WALL-Protect : protection périmétrique des flux

■ Les objectifs, notre mission :

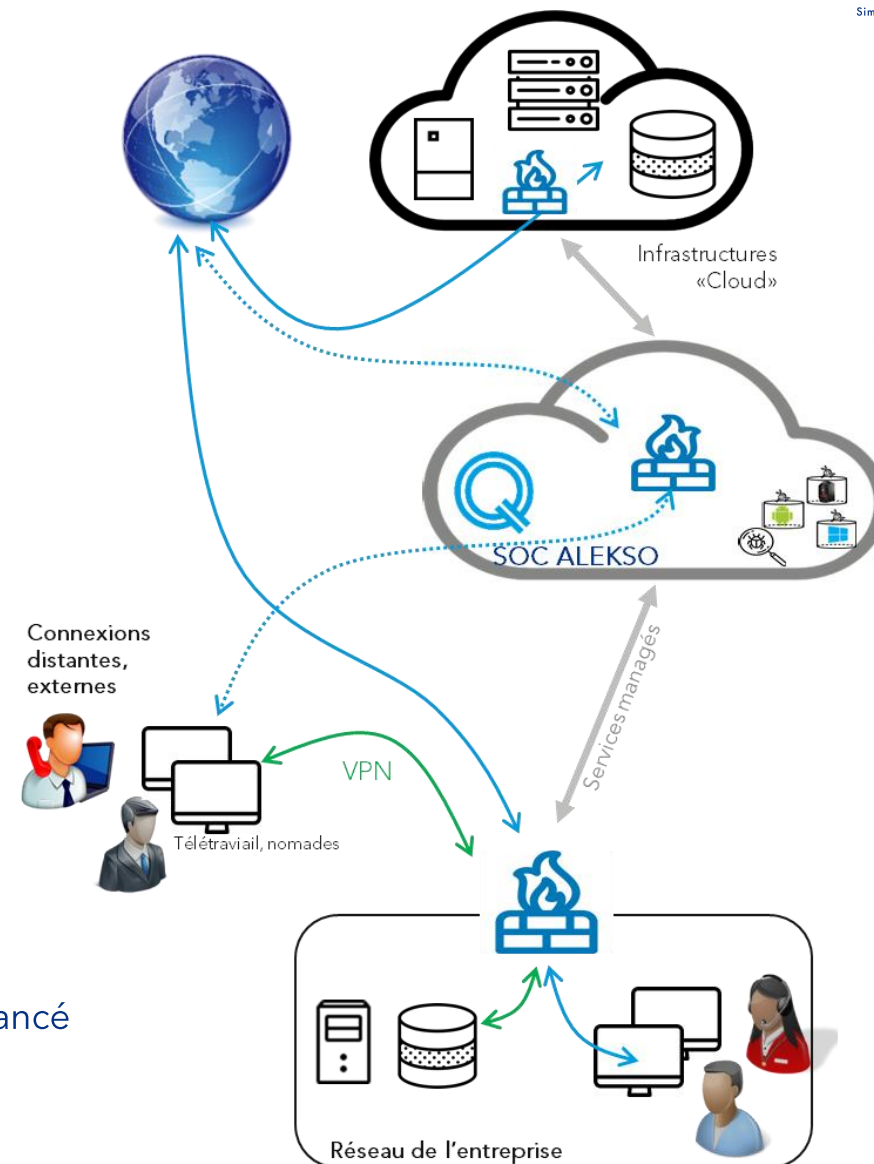
- Menaces : Intrusion, destruction, malware, vol de données...
- Actualité : Mining ...

■ Les fonctions assurées :

- Protection des réseaux « On Premise » et/ou cloud
 - Protection des accès
 - Analyse des flux
 - Chiffrement des flux : gestion des accès nomades
 - Gestion des VPN intersites
 - Traçabilité totale des actions et des accès
 - Gestion du SDWAN
 - Wifi sécurisé
 - Archivage des logs de sécurité sur 12 mois
-
- Solution développée et hébergée en France sur les infrastructures ALEKSO
 - Interface unique de pilotage et de gestions des événements

Inclus : Cœur de détection ATLAS : socle technologique avancé

- ✓ 14 moteurs anti-virus
- ✓ Base de réputation Editeurs sécurité
- ✓ Filtres de réputation / Sandbox
- ✓ Multimoteurs : antivirus, sandboxes, anti-APT
- ✓ Intelligence artificielle et technologies propriétaires
- ✓ Plateforme enrichie par les IOC Quiviv



07 QUIVIV-AXS-Protect



7.1 AXS-Protect : gestion des comptes « à privilèges »

■ Les objectifs, notre mission :

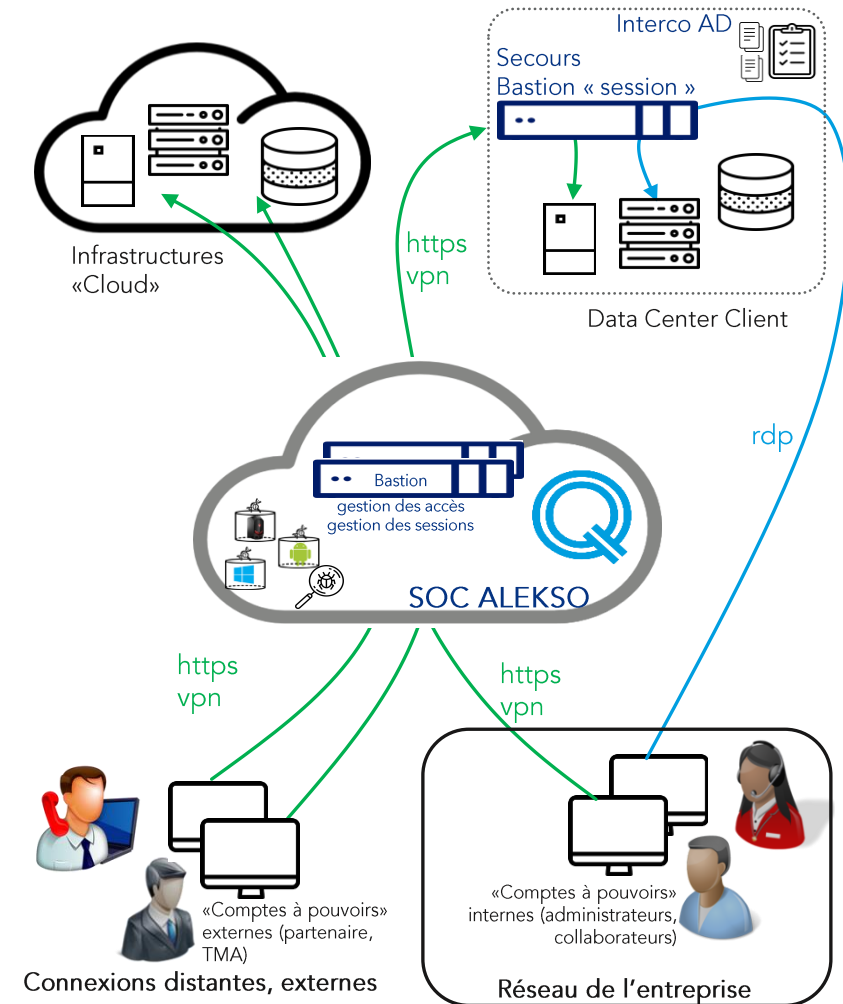
- Sécuriser les accès à vos infrastructures
- Gérer les accès et tracer les actions
- Gérer et maintenir la politique de comptes à privilèges

■ Les fonctions assurées :

- Contrôle des autorisations des « comptes à privilèges » avant connexion
- Protection des accès « On Premise » et cloud
- Sécurisation par rupture protocolaire
- Simplification de la gestion des mots de passe et des identités
- Traçabilité totale des actions et des accès
- Accès unique indépendant du positionnement des machines cibles
- Service d'analyse et de threat intelligence
 - ✓ Gestion des alertes rétrospectives
 - ✓ Support à la remédiation pour la DSI
- Solution développée et hébergée en France sur les infrastructures ALEKSO
- Interface unique de pilotage et de gestions des événements

Inclus : Cœur de détection ATLAS : socle technologique avancé

- ✓ 14 moteurs anti-virus
- ✓ Base de réputation Editeurs sécurité
- ✓ Filtres de réputation / Sandbox
- ✓ Multimoteurs : antivirus, sandboxes, anti-APT
- ✓ Intelligence artificielle et technologies propriétaires
- ✓ Plateforme enrichie par les IOC Quiviv





Contact : commercial@alekso.fr
Tél. : 09 85 60 02 00

