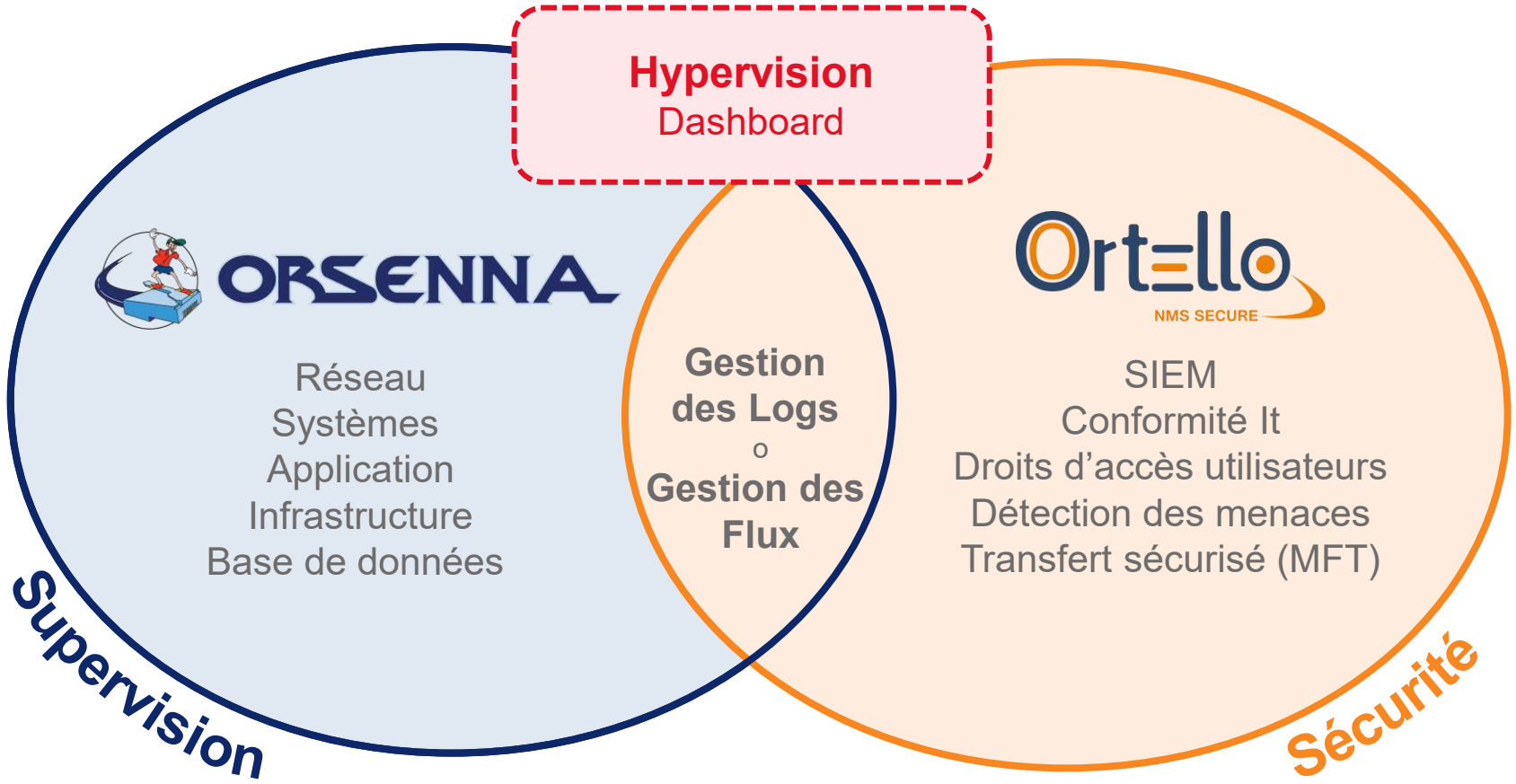
Intégrateur Spécialisé

Sécurité / Conformité IT

Une volonté d’expertise



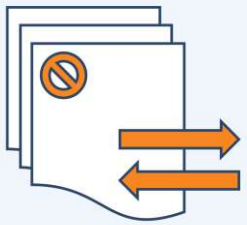
Nos partenaires majeurs

Gestion des droits d’accès utilisateurs

SolarWinds / Netwrix / Semperis …

Gestion des journaux d’évènements & SIEM

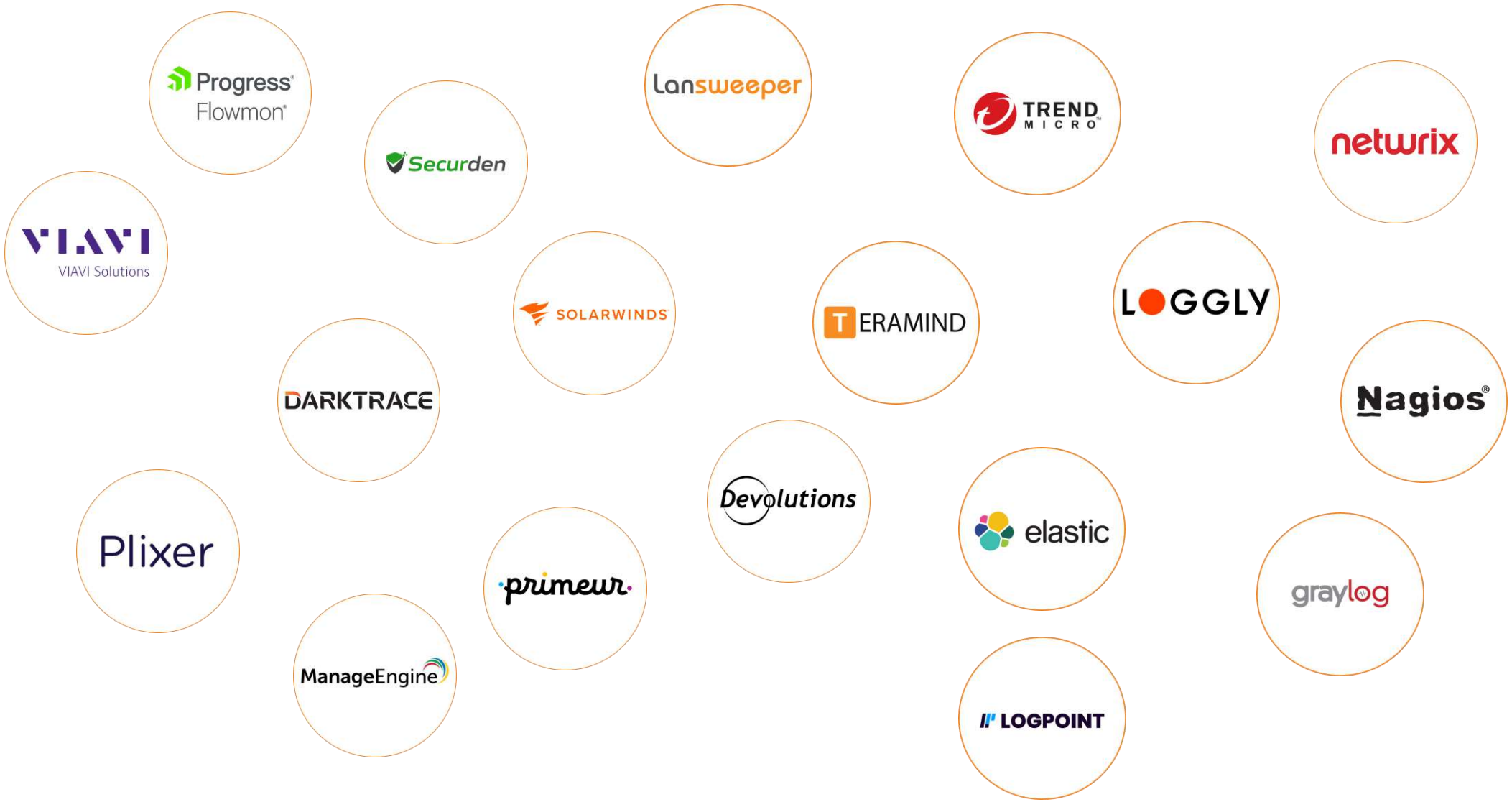
SolarWinds / Nagios / LogPoint …



Transfert de fichiers sécurisé (MFT)

Progress / Primeur / SolarWinds …

Nos principaux partenaires



Références | publiques & privées

SDIS

Education & Culture

Industrie

Commerce Distribution

Conseils & Services

Administrations Publiques

Secteur Santé

Médias / Presse

Télécom

Luxe

Mairie CD / CG

Energie

Banque Assurance

Chimie & Pharma.

Transport

Références concernant le Groupe Orsenna (Orsenna + Ortello)

Références | publiques & privées

Références concernant le Groupe Orsenna (Orsenna + Ortello)

Votre maturité sécurité

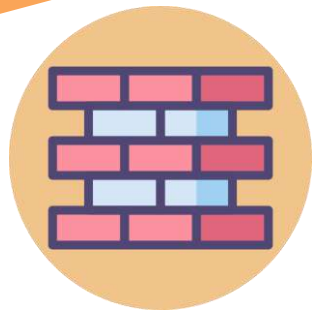
Budget \ Fonctionnalités \ Configuration / Prise en main

Audit

Outil simple pour réaliser une "photo" de l'état de mon IT, sur le sujet de l'AD par exemple

Analyse

Mise en œuvre de process et de solutions, de collecte et d'analyse de données, pour comprendre les menaces qui pèsent sur mon IT



Protection

Intégration de solutions avancées pouvant automatiser les réponses aux menaces, via l'utilisation efficiente de l'IA et du Machine Learning

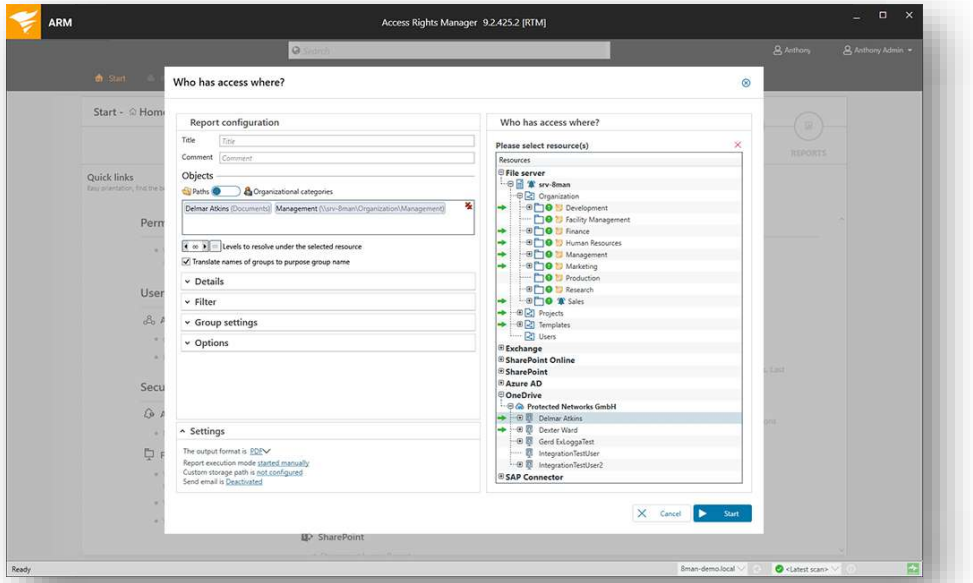
SOC

Mise en œuvre d'un SOC complet pour disposer d'une couverture sur l'ensemble des composants de mon IT

Notre offre « audit rapide de sécurité »

SolarWinds ARM-A

La solution regroupe l'essentiel des fonctionnalités « Audit » pour contribuer à garantir la sécurité et à démontrer la conformité à l'aide d'un logiciel d'audit AD, et peut simplifier les évaluations de sécurité en fournissant des informations précises sur les fichiers et dossiers spécifiques d'une organisation. compris



Purple Knight

Outil simple pour vous aider à découvrir les indicateurs d'exposition (IoE) et les indicateurs de compromission (IoC) dans votre environnement AD hybride.

Nous vous accompagnons dans la phase de votre audit, de la sélection des outils adéquats ou pour sa réalisation totale.

Notre approche sécurité par briques

01

Sécurisation des postes de travail

Le premier vecteur des attaques sont les postes de travail utilisateurs au bureau ou à distance.

02

SIEM & Logs

Analyse des logs pour identifier rapidement les incidents et les résoudre

03

Sécurisation de l'identité

Protection de l'Active Directory et de l'usurpation d'identité

04

Bastion

Protection des identifiants à privilèges [PAM] et Gestion des mots de passe

05

Protection de la donnée

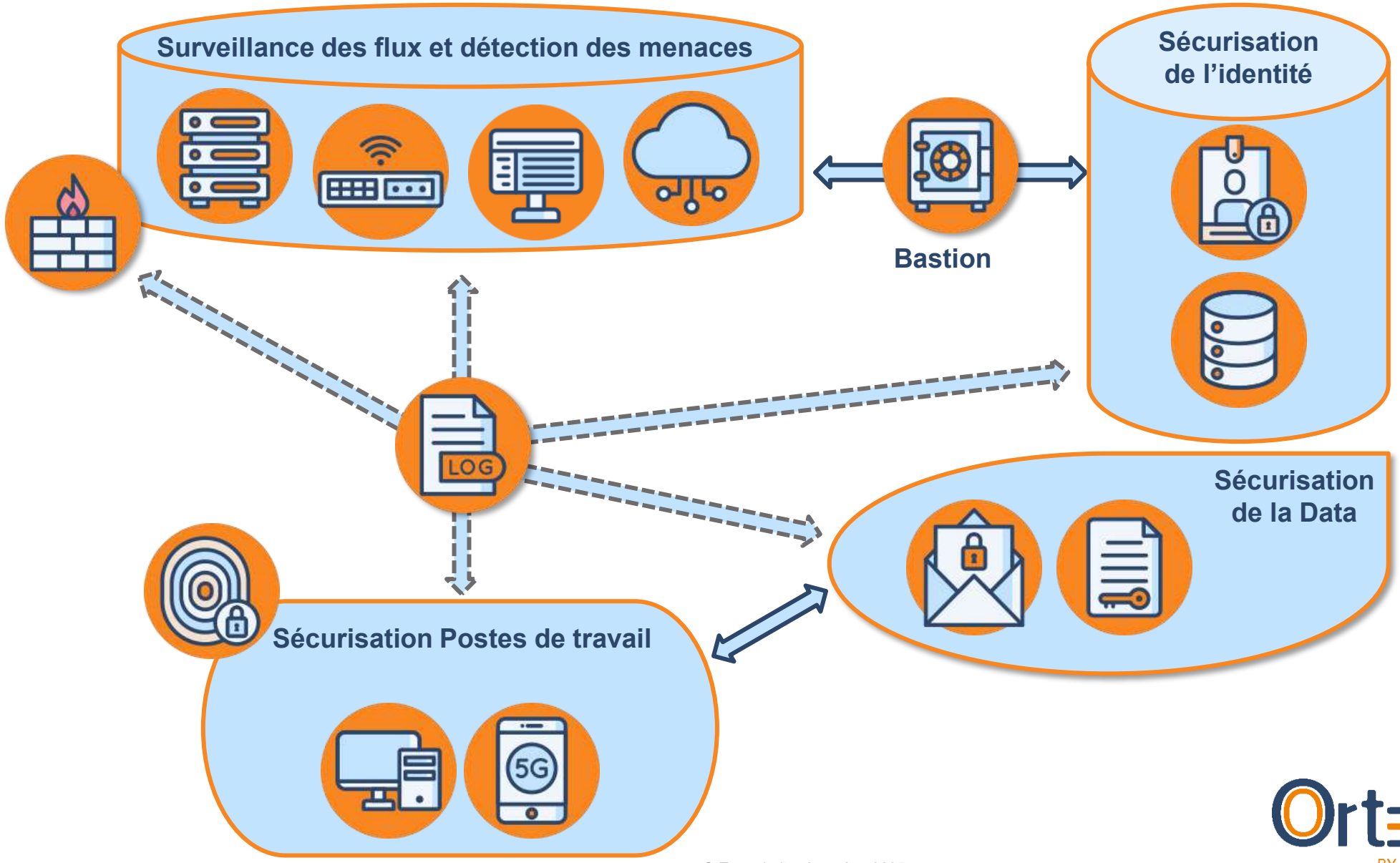
Sécurisation des échanges de données via des protocoles de sécurité + respect des normes (RGPD)

06

Détection des menaces

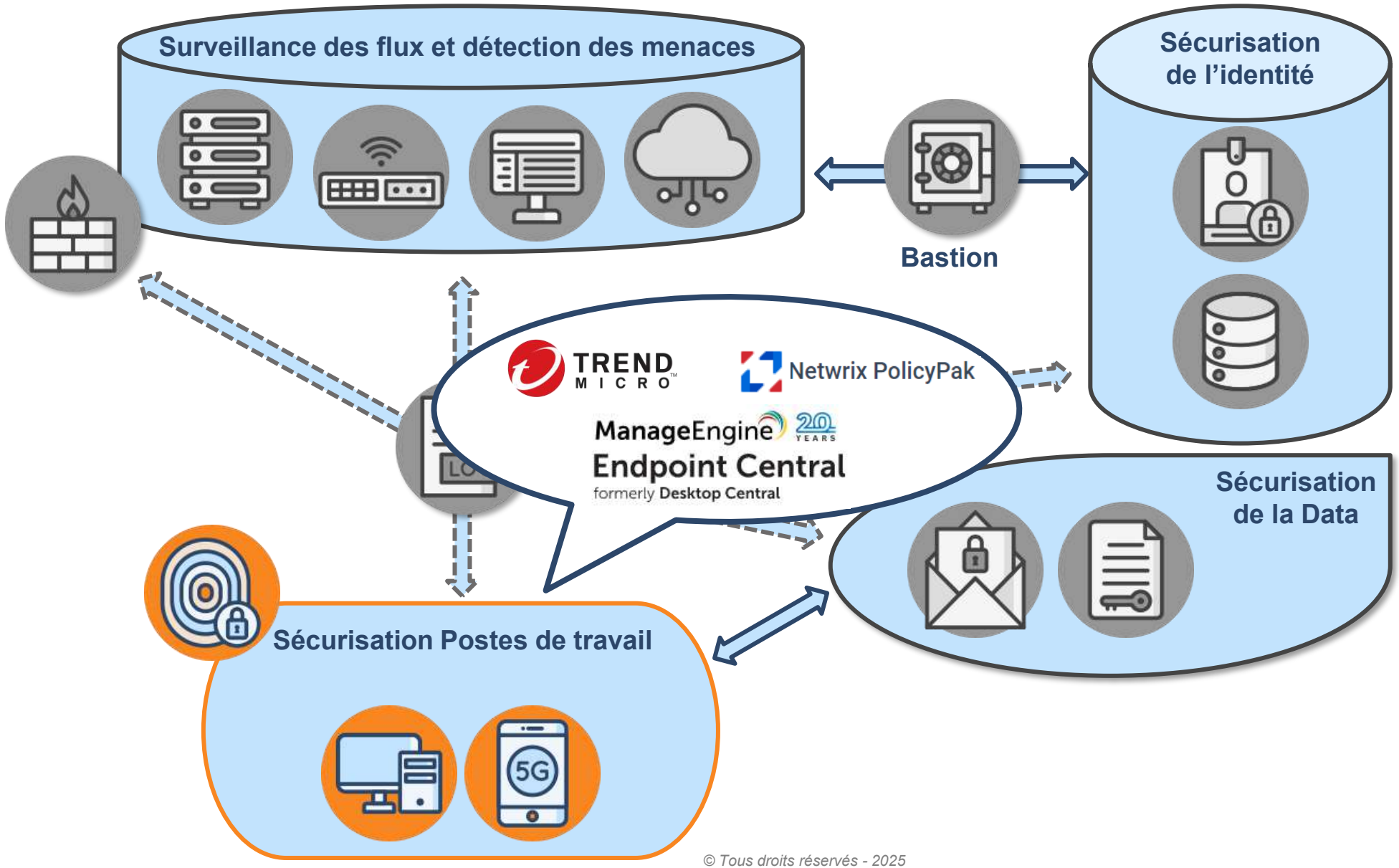
Analyse des flux réseau et détection des comportements anormaux pour éviter les attaques (malwares, ransomwares…)

Le cockpit de sécurité : une méthodologie du parcours de sécurité/conformité

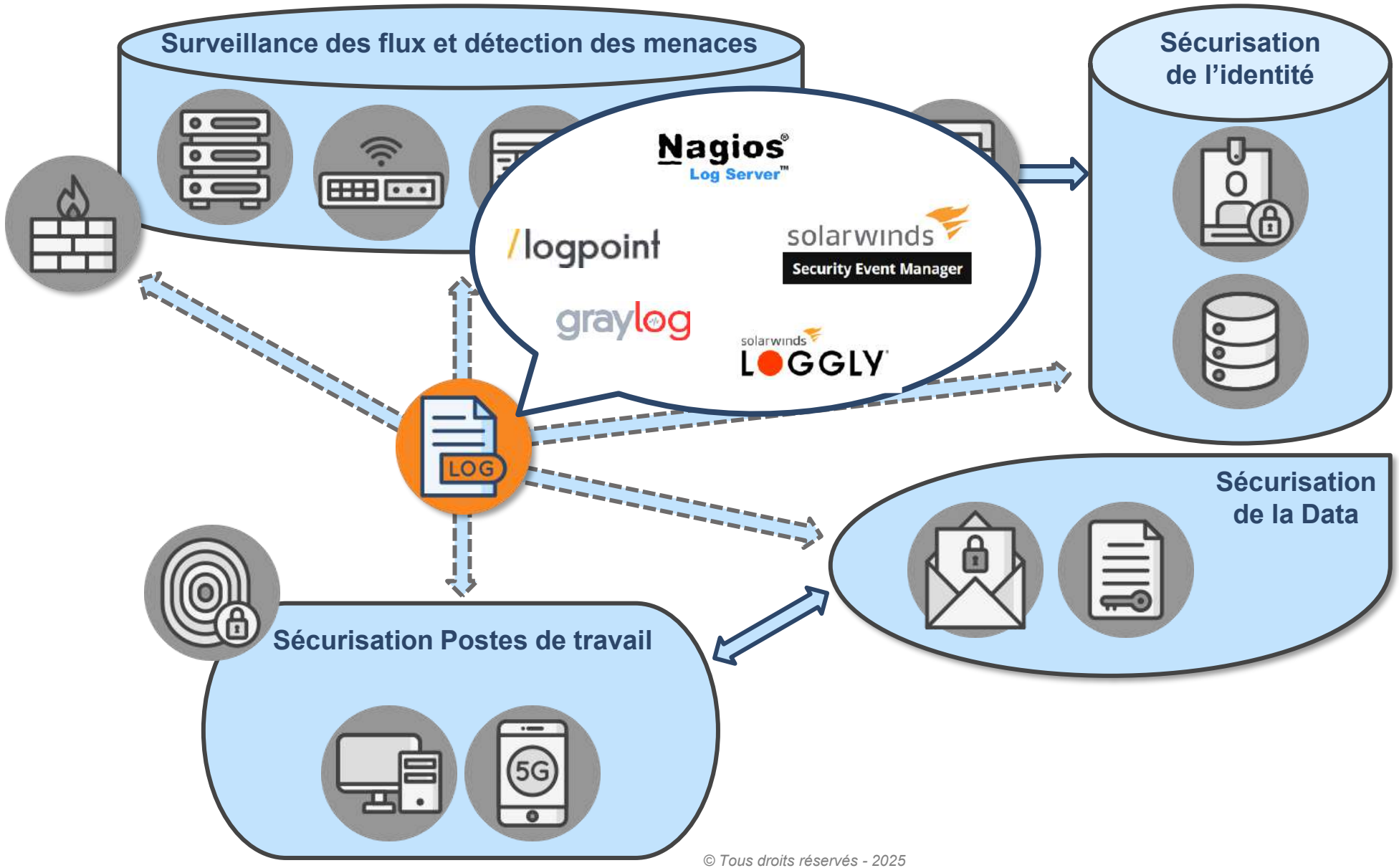


Ortello BY ORSENNA

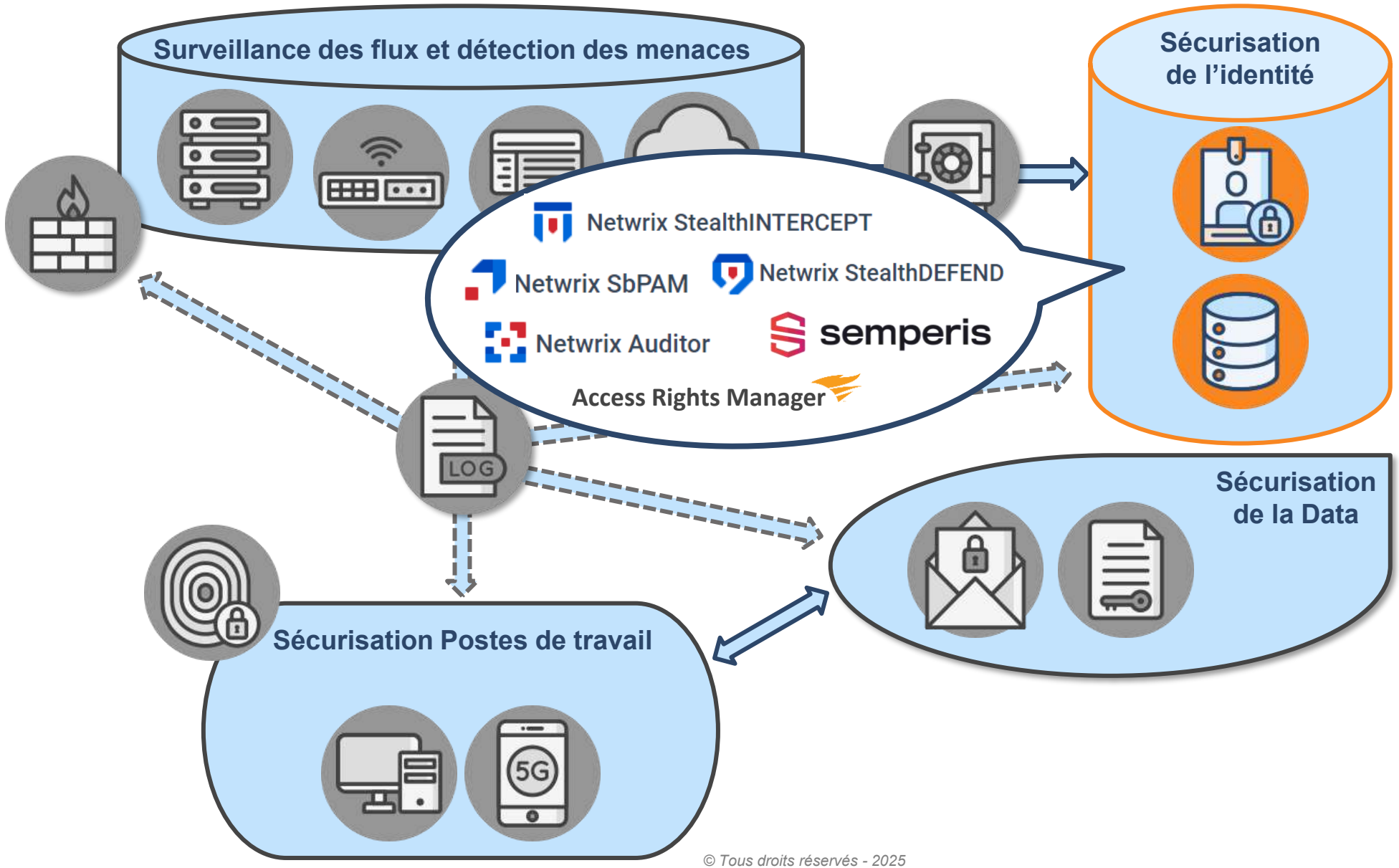
Le cockpit de sécurité



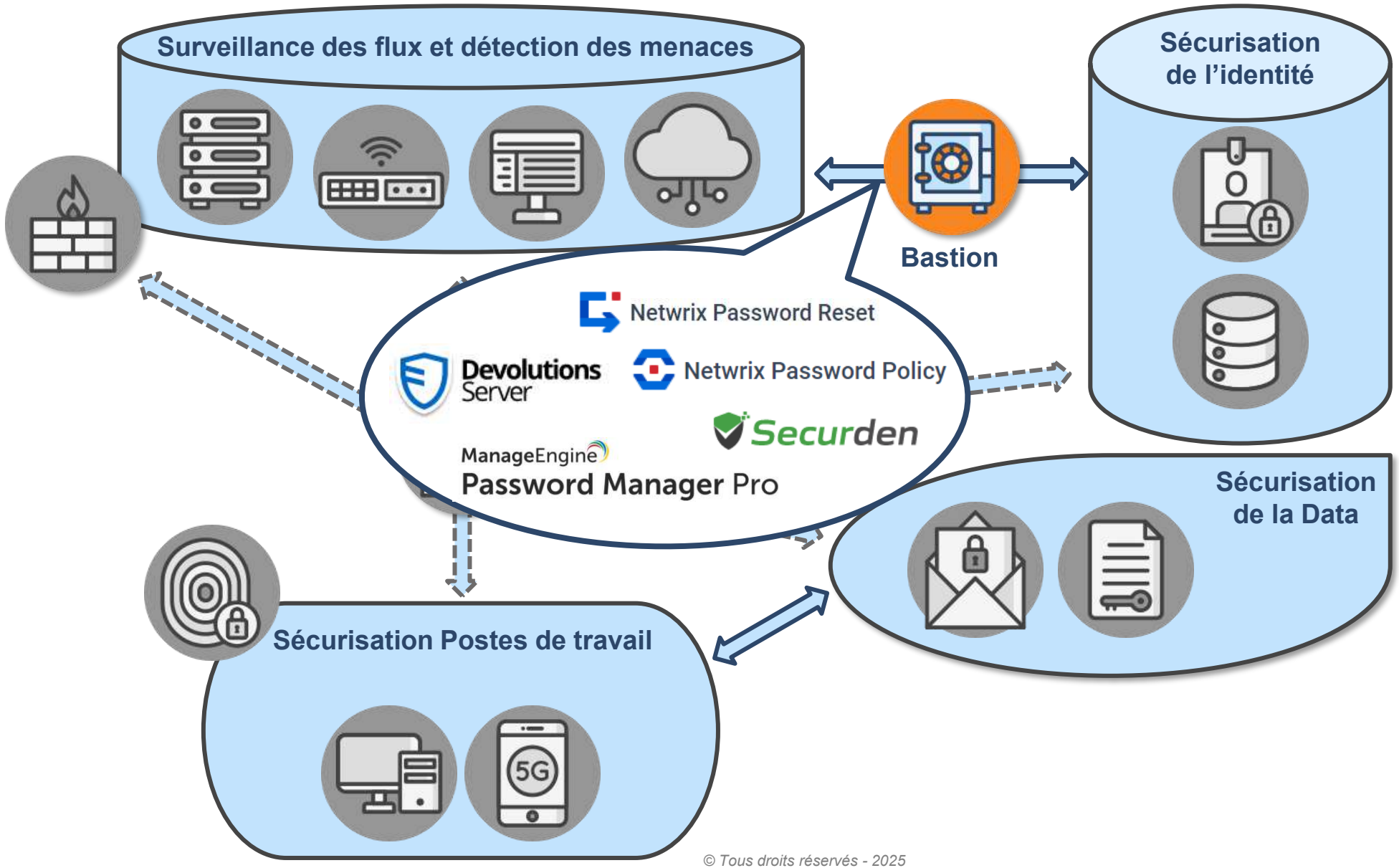
Le cockpit de sécurité



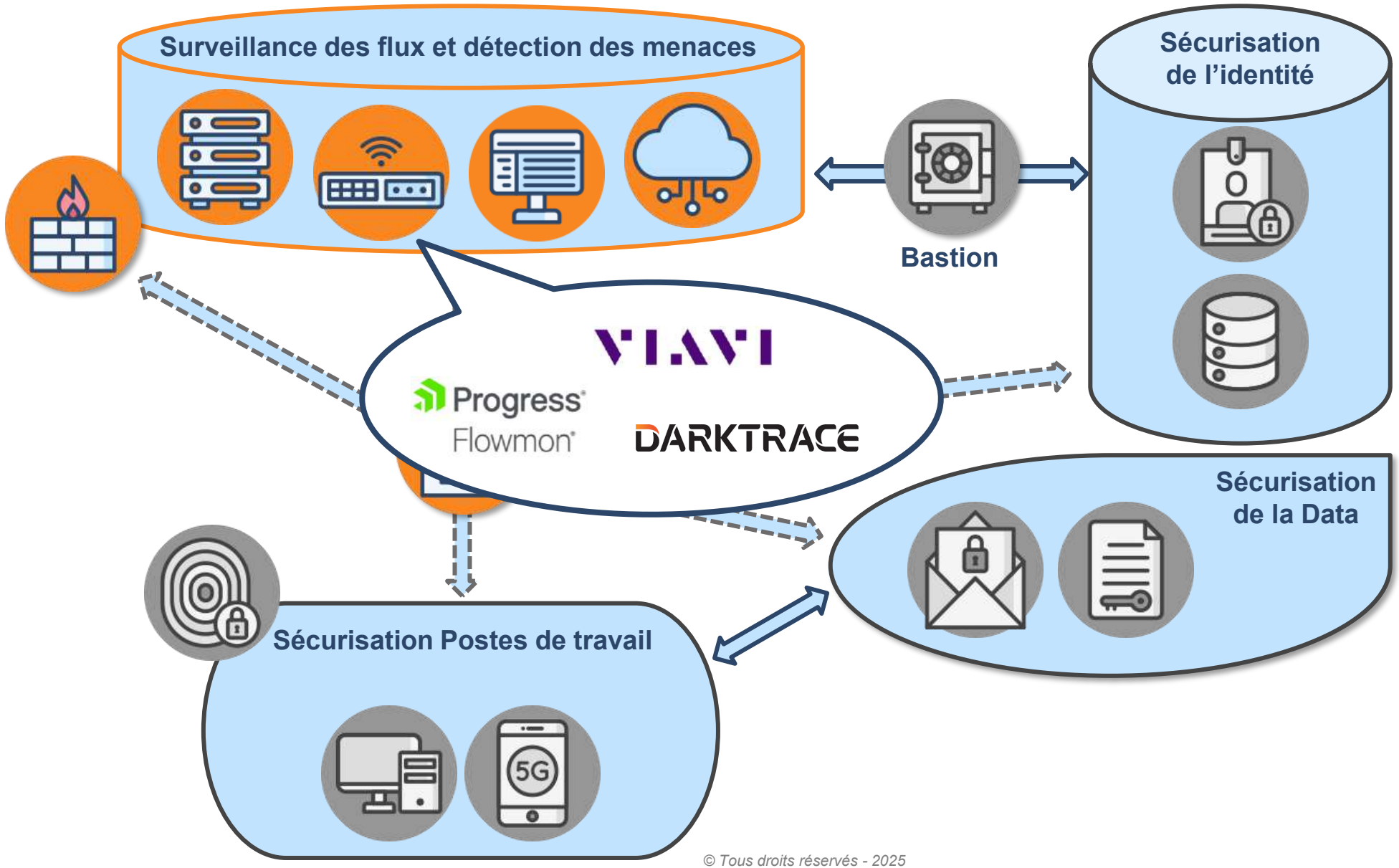
Le cockpit de sécurité



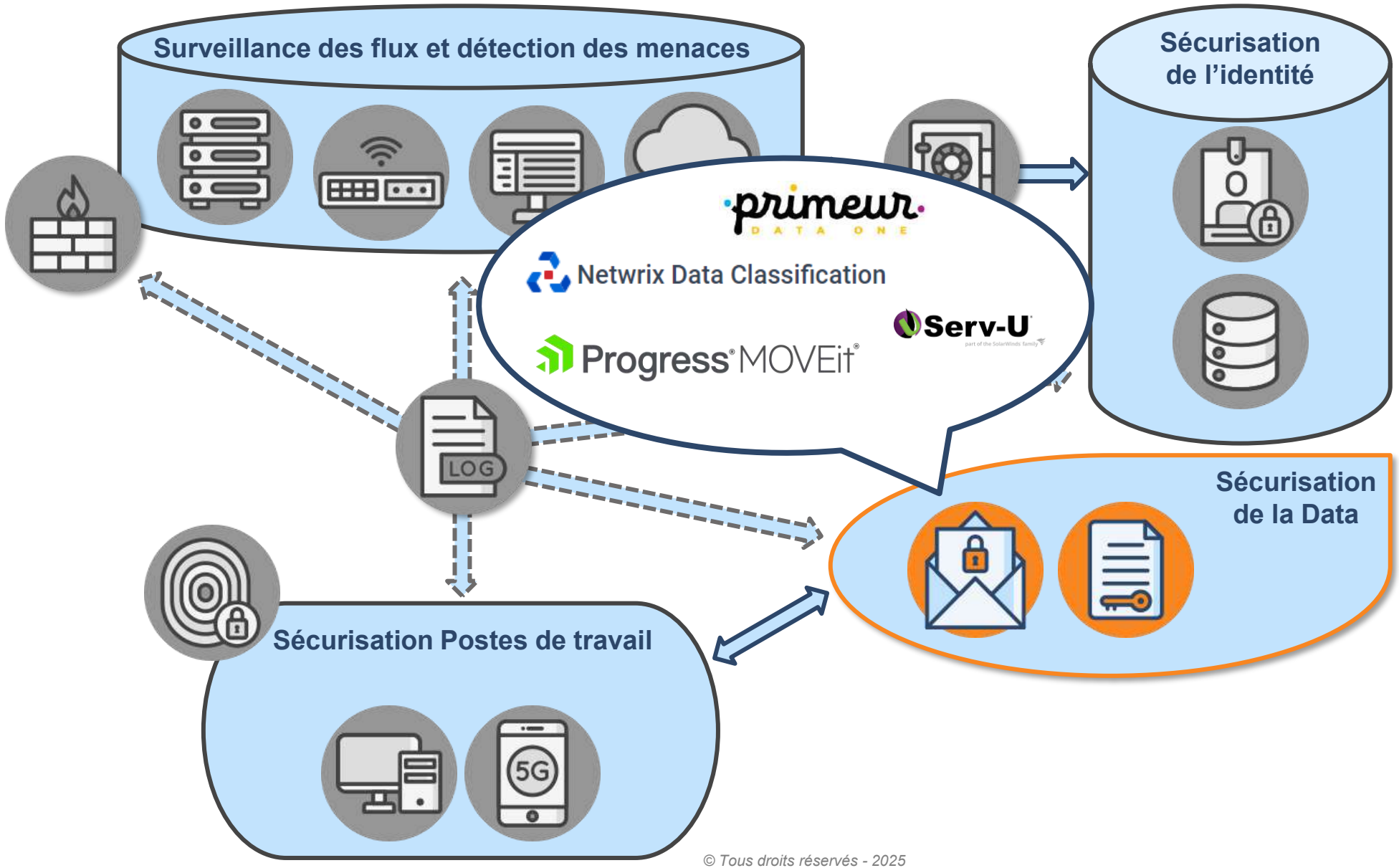
Le cockpit de sécurité



Le cockpit de sécurité



Le cockpit de sécurité



Recommandations de l'ANSSI

Nous prenons en compte les recommandations de l'ANSSI afin de vous proposer des solutions qui sécurisent vos systèmes informatiques.

Voici les principales lacunes relevées par l'ANSSI et nos solution pour les éviter :

Une politique de gestion des mots de passe insuffisante

- Securden Password Vault
- Devolutions Server
- ManageEngine Password Manager Pro
- Netwrix Password Reset
- Netwrix Password Policy

Une absence de séparation des usages entre utilisateur et administrateur des réseaux

- Netwrix Auditor
- Netwrix Privilege Secure
- SolarWinds ARM-A
- Netwrix PolicyPak

Un laxisme dans la gestion des droits d'accès

- Netwrix Privilege Secure
- Netwrix Auditor
- StealthDEFEND
- StealthINTERCEPT
- Semperis,
- Access Rights Manager

Une absence de surveillance des systèmes d'information

- Nagios Log Server
- Logpoint
- SolarWinds Security Event Manager
- Graylog,
- SolarWinds Loggly
- Suite ELK
- Kiwi Syslog

Une ouverture excessive d'accès externes incontrôlés au système d'information

- Teramind
- SolarWinds Access Rights Manager
- Netwrix Auditor
- Netwrix Privilege Secure
- Semperis

Poste de travail

Ces solutions de protection du système informatique vous aident à sécuriser votre environnement IT. Ces solutions complètes vous permet une visibilité globale pour la gestion de la sécurité pour tous les endpoints comme les ordinateurs de bureau, les serveurs et bien d'autres. Elles peuvent également s'occuper de la configuration des terminaux nomades ou sur site afin de diminuer les risques d'intrusions malveillantes.

Endpoint Central

Netwrix PolicyPak

TrendMicro

Lansweeper

SIEM & Logs

Les logs sont des journaux d'évènement qui servent à collecter des données utiles. Il est important pour la sécurité d'utiliser un système de gestion des logs afin d'identifier tout dysfonctionnement ou de comprendre les activités suspectes (logique SIEM). Les solutions de nos partenaires répondent ainsi à trois besoins courants : collecte, centralisation et analyse des logs.

SolarWinds Event Manager

Logpoint

Graylog

Suite ELK

Nagios Log Server

Loggly

Kiwi

Sécurisation de l’identité

La sécurisation de l’identité est importante et doit être nécessairement contrôlée pour éviter des intrusions malveillantes. Il est primordial que le bon accès soit accordé à la bonne personne pour éviter les abus d’accès privilégiés et le risque de vols de données. En effet, si les accès ne sont pas bien régulés il y a de très forts risques pour que ceux-ci soient piratés par des attaquants.

Netwrix StealthAudit

SolarWinds ARM et ARMA

Netwrix Auditor

Bastion

Il arrive souvent que les mots de passe soient la première faille de sécurité, bien souvent à cause de leurs simplicités. Ortello dispose de plusieurs solutions qui permettent de résoudre ce problème et de gérer les différents mots de passe avec plus d'efficacité et de conformité qu'une gestion manuelle.

Netwrix Privilege Secure

Devolutions Server

Securden PAM

Devolutions Password Hub

Securden Password vault

Détection des menaces

Les solutions NBA – Network Behavior Analysis – se classent dans notre catégorie « Analyses avancées des flux et détection d'incidents ». Les technologies NBA permettent d'analyser les flux réseau en temps réel et de manière rétrospective afin de remonter et d'identifier les sources d'attaques et les principales menaces.

VIAVI

Plixer/ Scrutinizer

Darktrace

Flowmon

StealthDefend

StealthIntercept

Data protection

Les données sont créées chaque jour et sont donc difficiles à gérer et à protéger correctement. Elles sont pourtant les informations recherchées lors des attaques, il est donc impératif de déterminer quelles données peuvent être sensibles, règlementées ou critiques pour l'organisation. Les solutions que nous proposons vous permettent de trouver les informations, d'identifier leur niveau de sensibilité et d'ainsi garder la maîtrise des données.

Primeur Data One

Netwrix Data Classification

MOVEit

WS_FTP Server

Serv-U MFT Server

Nous contacter

SE TENIR INFORMÉ

Nous organisons régulièrement des webinars sur nos différentes thématiques !

(+33) **01 34 93 35 35**

marketing@orsenna.fr

15, rue Croix Castel
78600 Maisons-Laffitte