



We are Lutessa,
We are refreshing.

LES BASTIONS
& LA GESTION DES COMPTES A PRIVILEGES

CLUSIR PACA – ESPACE RSSI / EURECOM
SOPHIA ANTIPOLIS

S.NAWROSKI

We are Lutessa
We are refreshing



Bâtisseur de carrière



30% de croissance annuelle



Déjà 75 Lutessiens en 4 ans

Entreprise d'Ingénierie et d'expertise spécialisée dans l'étude, l'intégration et la gestion des infrastructures critiques.

Spécialités



CONNECTIVITY

Réseaux performants et élastiques : LAN users, WLAN, MAN, Optimisation WAN, QoS, NAC,...

Nos spécialistes interviennent dans des contextes où la maîtrise des fondamentaux protocolaires est un facteur clé de réussite. Les infrastructures réseaux, sur lesquelles nous intervenons, doivent apporter une différenciation forte à nos clients.



CYBERSECURITY

Infrastructure de confiance, sécurité périmétrique, analyse de risques, audits, tests d'intrusion en boîte noire, blanche ou grise, investigations forensic, agrégation et corrélation de logs, mise en conformité,...

Notre domaine d'intervention réside dans la mise à disposition d'experts pour concevoir, mettre en oeuvre et maintenir les outils de sécurité de l'entreprise.



CLOUD

Infrastructures pour datacenters, hyperconvergence. Software Defined Network (SDN), Orchestration,...

Agnostiques aux technologies et passionnés, nos spécialistes conseillent, développent et opèrent les infrastructures qui permettent aux solutions Cloud (privées, hybrides) d'être efficaces.

SOMMAIRE

- Menaces & contraintes réglementaires
- les comptes à privilèges
- Les problématiques liées à ces comptes
- Le principe des bastions
- L'implémentation et les modes de fonctionnement
- Les impacts en terme d'organisation
- La conduite de projet
- Les solutions et produits du marché
- Un comparatif des solutions



INTRODUCTION

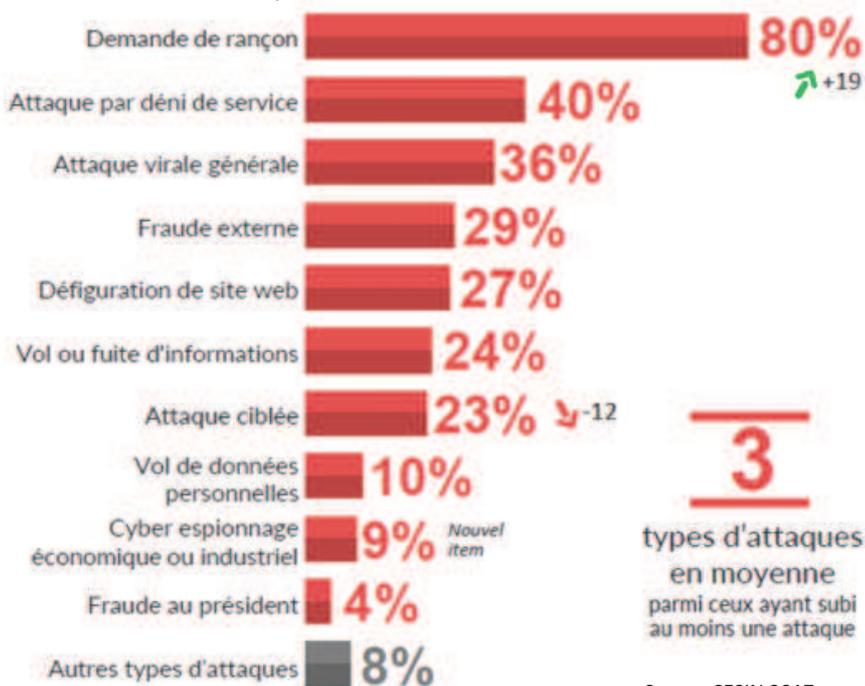
Cyberattaques, ransomwares, fuites d'information, loi de programmation militaire... les systèmes d'information, sont aujourd'hui au cœur de toutes les préoccupations.

L'augmentation de la surface d'attaque est soutenue par l'arrivée permanente de nouvelles technologies et de nouveaux usages.



Ces mutations affectent à la fois la gestion de l'entreprise, son management, son organisation mais aussi et surtout sa sécurité.

LES ATTAQUES SUBIES PAR LES ENTREPRISES



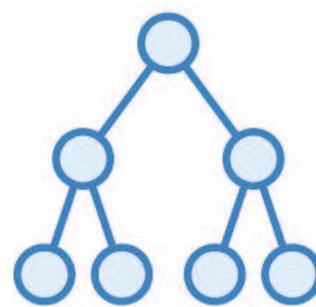
ACTUALITE : TOP 10
DES ATTAQUES

3

types d'attaques
en moyenne
parmi ceux ayant subi
au moins une attaque

Source CESIN 2017

MENACES : VECTEUR + METHODE



Vecteur

Humain (Facteur H)

Cible

Administrateurs

Objectif

L'accès total au SI

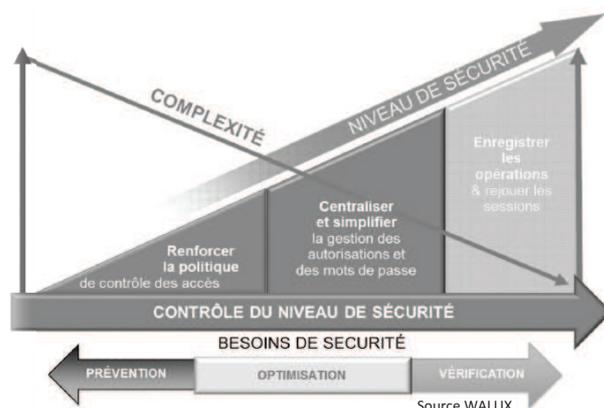
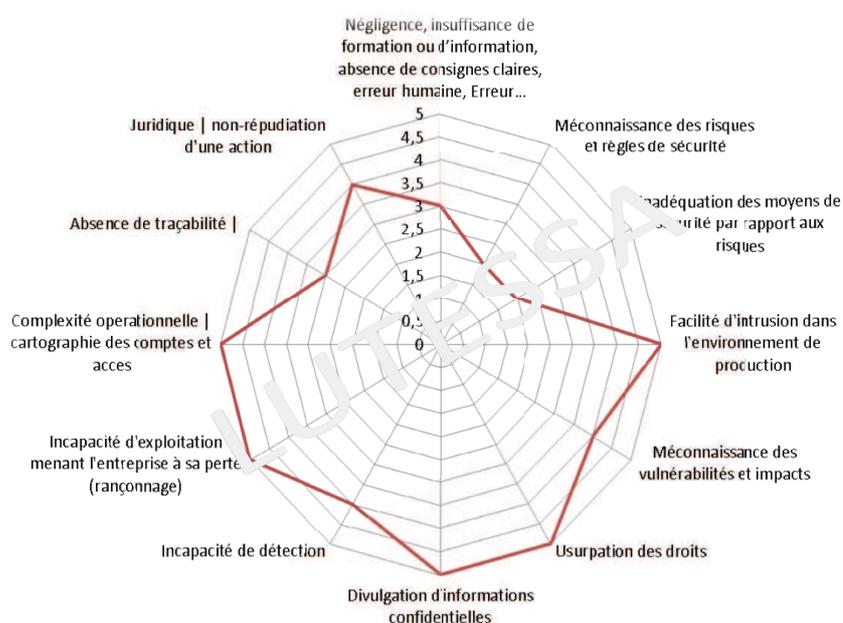
Moyens

- Phishing
- Hameçonnage
- Clef USB etc.....

- Elévation de privilèges
- Pass the hash
- Power Shell

- AD
- Réseaux | Zone de production
- Ressources critiques

LES RISQUES DU FACTEUR H



Les mutations technologiques, les nouveaux usages ainsi que le **facteur H**, font courir trois grandes natures de risques aux entreprises : des **risques opérationnels**, de **conformité** et de **sécurité**.

LES CONTRAINTES RÉGLEMENTAIRES



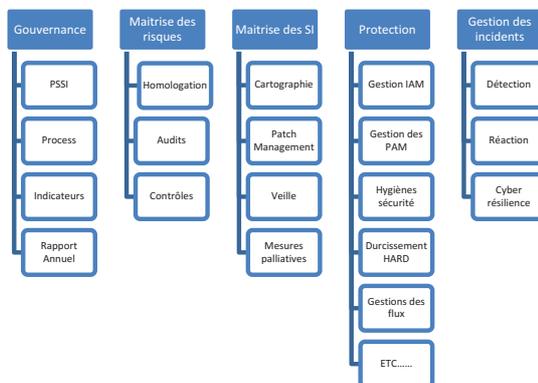
GDPR / RGPD

- Identifier les données les données personnelle
- Classifier et minimiser les données
- Définir les droits et politiques d'accès
- Contrôler, alerter et bloquer
- Déclarer, certifier et investiguer

DICT

=

Traçabilité
 Registre
 Politique PCPI
 IAM
 Authentification
 Habilitation
 Alerting
 Protection des données
 Chiffrement
 Stockage



=

Application des recommandations SGDN | IGI 1300 et RGS

Applications Web
 Architecture
 Cryptographie
 Dispositifs de vidéoprotection
 Externalisation
 Liaisons sans fil et mobilité
 Méthodologie
 Poste de travail et serveurs
 Réseaux
 Systèmes industriels
 Technologies sans contact

SYNTHESE

- Les cyber-menaces en 2017 sont en **forte augmentation**
- Ces menaces font courir trois grandes natures de risques aux entreprises:
 - ✓ **Risques opérationnels**
 - ✓ **Risques de conformité**
 - ✓ **Risques de sécurité**

- Le **facteur H** reste un important vecteur de propagation
- Les **comptes à privilèges** permettent la quête du Saint Graal pour les cyber attaquants
- Les **contraintes réglementaires** imposent la mise en place de moyens de **sécurisation** et de **traçabilité**

- Un des principaux challenges SSI : **La réduction de la surface d'exposition**

Le bastion s'avère un **bon moyen de réduction de la surface d'exposition**, en apportant également la **sécurisation des comptes à privilèges**.

QU'EST CE QU'UN COMPTE À PRIVILÈGES ?

Les comptes à privilèges, comme ceux des administrateurs, sont accompagnés d'ouvertures de flux et d'accès permettant de mener à bien les missions et tâches qui leur sont confiées.

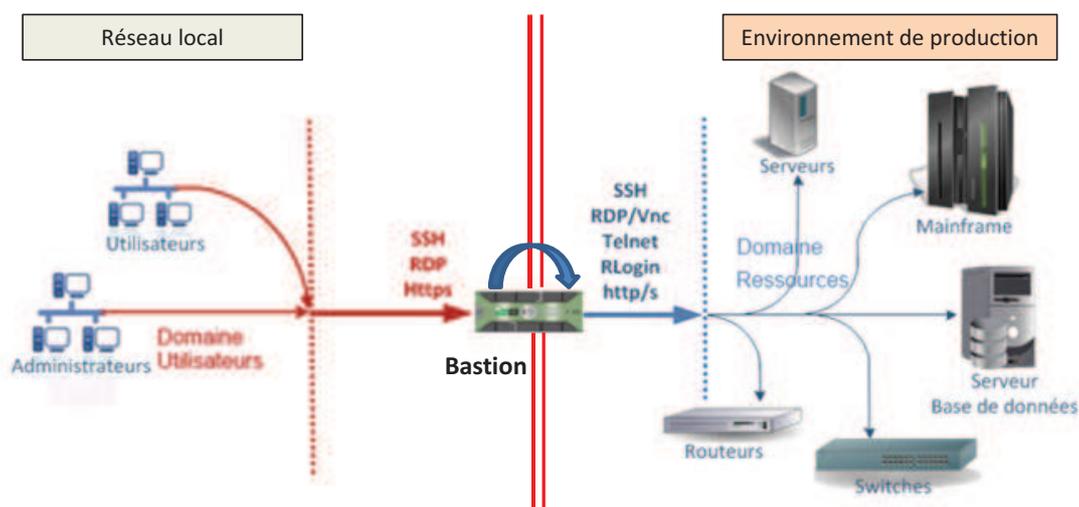
C'est pour cela que les comptes à privilèges sont souvent une cible de choix pour les hackers. Ils permettent un octroi de droits et la prise de contrôle de la quasi-totalité du patrimoine informationnel de l'entreprise avec facilité et rapidité.

- Comptes d'administration générique (root)
- Comptes à privilège personnel
- Comptes de service
- Comptes de développement
- Comptes d'applicatifs
- Comptes dit « d'urgence »

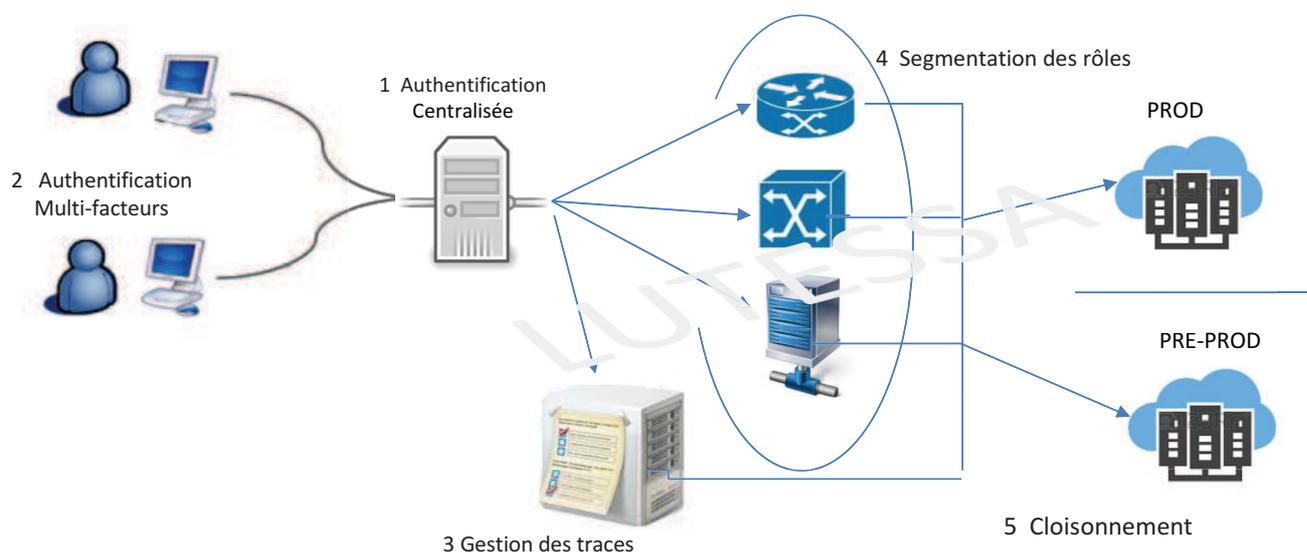


PRINCIPES ET FONCTIONNEMENT D'UN BASTION

- Un “bastion d’administration” est un **équipement** ou une **appliance software** permettant de **faire converger les accès et de segmenter les rôles** dans un système d’information au moyen d’une interface unique.
- Le bastion garantit une **rupture protocolaire** entre le poste d’administration et les serveurs distants.
- Les serveurs ne peuvent donc pas être joints directement depuis le poste d’un administrateur.

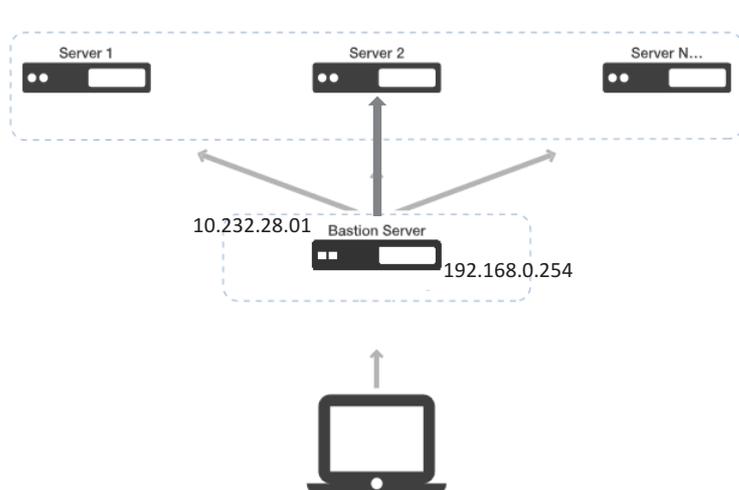


LES 5 AVANTAGES DE SECURITE D'UN BASTION



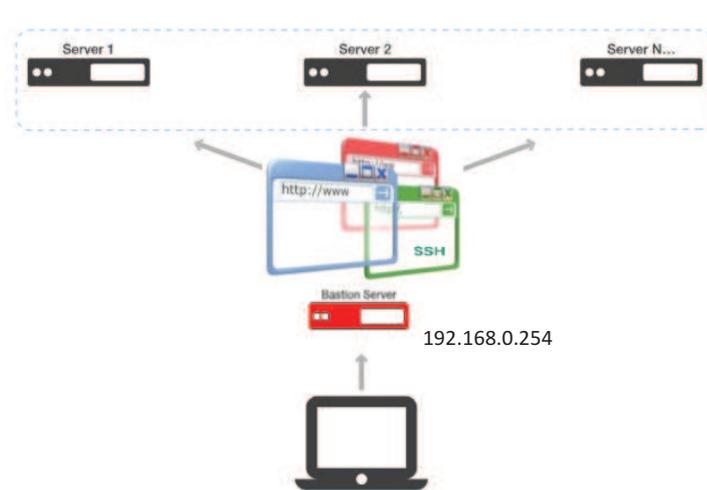
1. Authentification centralisée avec rupture protocolaire
2. Authentification multi-facteurs
3. Haute traçabilité (Log, enregistrement des sessions, SIEM...)
4. Segmentation des rôles et des pouvoirs
5. Cloisonnement des environnements

BASTION : DEUX MODES DE FONCTIONNEMENT



Le mode « **rooté** »:

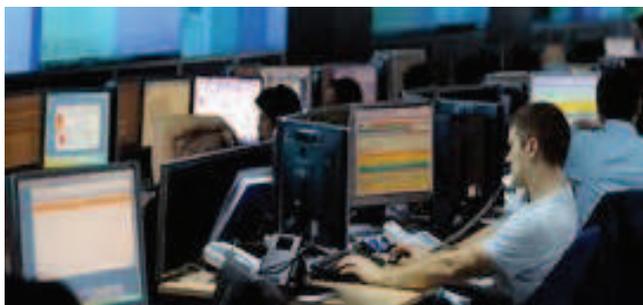
1. Les administrateurs utilisent les mêmes outils et clefs pour s'authentifier
2. La connexion s'établit auprès du bastion, qui initie alors une session sur le serveur de destination et réplique les commandes frappées par l'utilisateur
3. Toutes les fonctionnalités sont actives



Le mode « **Bastion** »:

1. Les administrateurs s'authentifient sur une interface unique
2. Leurs profils sont déjà configurés
3. Leurs rôles et leurs pouvoirs sont segmentés
4. Toutes les fonctionnalités sont actives.

FONCTIONS ATTENDUES



VISION OPÉRATIONNELLE

- Scalabilité
- Interopérabilité avec les outils de production
- Facilité d'administration
- Pas d'impact sur les méthodes de travail (prod)
- Workflow de demande d'accès (habilitations)
- Fonctions d'import /export
- Charte d'usage
- Validateurs ou modérateurs des demandes techniques d'accès



VISION DE SÉCURITÉ

- Haute disponibilité
- Cloisonnement
- Forte étanchéité
- Rupture protocolaire
- Authentification multi facteurs
- Management des comptes à privilèges
- Réduction de la surface d'attaque
- Visualisation en temps réel des sessions (rdp, ssh ...)
- Password Management
- Coffre-fort (AES256)
- Interopérabilité avec les outils internes de sécurité (HSM, SIEM, ..)
- Reporting et audit | enregistrement de sessions
- Chiffrement des sessions et des vidéos
- Analyse comportementale
- Backup



Intégration technique du bastion

La plupart des fournisseurs de **solutions de bastion** proposent des offres comprenant des composants complémentaires.

- IAM
- Coffre Fort
- Log Management
- etc..

Si l'intégration d'un équipement en coupure réseaux, comme le cas d'un bastion, reste un exercice facile pour la plupart des intégrateurs, il n'en va de pas de même concernant la gestion des comptes à privilèges.



Gouvernance des comptes à privilèges

Ces produits bien que complémentaires doivent être envisagés dans des projets bien distincts de l'intégration du bastion lui-même. Ils apportent un lot de questions pour le client:

- Ai-je la maîtrise des habilitations ?
- Possédons nous une cartographie des comptes à privilèges ?
- Contrôlons-nous la segmentation des rôles et des pouvoirs ?
- Puis-je révoquer des droits rapidement ?
- Puis-je retrouver les droits positionnés à un instant T ?
- Quel niveau de traçabilité avons-nous ?
- Avons-nous la capacité à lever et gérer les alertes ?

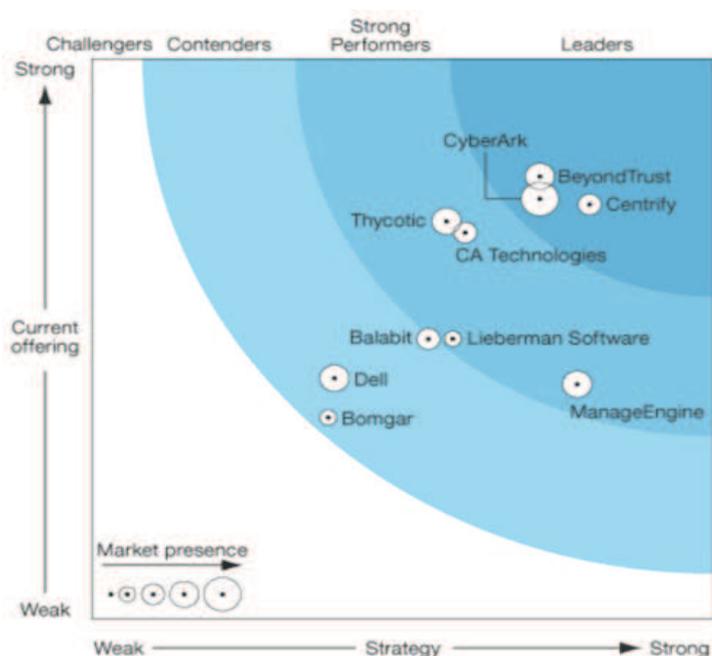
PRODUITS ET SOLUTIONS

Les acteurs du marché



MAGIC QUADRANT

➤ Les acteurs français absents



Gartner continue de constater une augmentation de l'intérêt pour les outils PAM.

Certains clients de Gartner ont indiqué qu'ils ont sélectionné un fournisseur en fonction de fonctionnalités spécifiques qu'ils finissent finalement par ne pas utiliser, ou d'acheter des modules supplémentaires sur "étagères".

Beaucoup de fournisseurs regroupent de nombreuses fonctionnalités dans leurs offres d'entrée de gamme; alors que d'autres fournisseurs ont divisé leurs offres en plusieurs éditions, en tant que modules distincts.

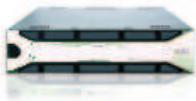
Wallix est un éditeur français de logiciels de sécurité informatique fondé en 2003. Il est spécialisé dans la sécurisation des systèmes d'information et la gestion des infrastructures critiques.

Wallix se positionne sur le marché de la sécurisation des comptes à privilèges (marché du PAM pour « Privileged Account Management »)

❖ Solution en trois modules:
| Session manger | Access manager | Password Manager

➤ Le produit correspondant: ADMINBASTION

- Gestion et gouvernance des comptes à privilèges
- Paramétrage contextualisé
- Visualisation en temps réel des activités
- Enregistrement des sessions
- Collecte des métadonnées et export vers un SIEM possible
- Stockage des mots de passe dans un VAULT interne
- Gestion avancée des mots de passe et clés SSH
- Console web d'administration des architectures distribuées



WALLIX
TRACE, AUDIT & TRUST



En tant que société informatique, WALLIX est membre de Clusif, d'Hexatrust, de BPI France Excellence.

Référentiel : Certification de sécurité de premier niveau
Commanditaire(s) : Wallix
Centre d'évaluation : OPPIDA

Leur produit à été certifié CSPN dans la catégorie « Identification, certification et contrôle d'accès » par l'agence national de la sécurité des systèmes d'information le 25/11/2013



Solution française de sécurisation des accès externes au SI, certifiée CSPN (Certification de Sécurité de Premier Niveau) par l'ANSSI



FSTEC

Systancia est un éditeur français de logiciels de virtualisation des postes de travail et des applications, et de sécurité des accès externes. La société a été créée en 1998, et dispose de 3 Centres de R&D.

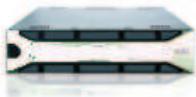
Elle acquiert en 2013 la société française **IPdiva**, éditeur dans la sécurisation, le contrôle et la traçabilité d'accès en mode applicatif VPN SSL.

❖ Solution en deux modules: |Serveur de médiation| Bastion

➤ Le produit correspondant: Ipdiva Safe

Fonctionnalités clés :

- Mobilité et télé-services par IP/Internet.
- Accès distant sécurisé (VPN SSL)
- Portail de contrôle d'identifiants.
- Fonctionnalités Reverse Proxy.
- Contrôle de conformité
- Contrôle d'intégrité (poste habilité / antivirus /).
- Traçabilité des accès.
- Enregistrement de sessions **IPdiva safe**.
- Interopérabilité avec l'interface **Nagios**.
- Coffre-fort SSOX (stockage chiffré)
- Authentification TLS



Référentiel : Certification de sécurité de premier niveau
Commanditaire(s) : Systancia
Centre d'évaluation : Amossys

Leur produit à été certifié CSPN dans la catégorie « Identification, authentification et contrôle d'accès » par l'agence national de la sécurité des systèmes d'information le 19/05/2016



Solution française de sécurisation des accès externes au SI, certifiée **CSPN** (Certification de Sécurité de Premier Niveau) par l'**ANSSI**

CYBERARK

CyberArk a été fondé en Israël en 1999. CyberArk a mis au point une plate-forme modulaire de technologie performante faisant appel à la solution de sécurité la plus complète pour les comptes à privilèges. Chaque produit peut être géré individuellement ou de manière collective, de sorte à obtenir une solution cohésive et complète.

Leur offre est composée de plusieurs modules:

Shared Technology Platform | Enterprise Password Vault | SSH Key Manager | Privileged Session Manager | Privileged Threat Analytics | Application Identity Manager | On-Demand Privileges Manager | Endpoint Privilege Manager

➤ Le produit correspondant: Privileged Session Manager



- Gestion et contrôle des mots de passe des comptes à privilèges
- Protection et gestion des clés SSH
- Supervision et enregistrement des sessions
- Isolation des sessions et contrôle des accès
- Application de privilèges minimaux
- Protection des informations d'identification des applications
- Analyse et détection des menaces
- Protection des fichiers sensibles



Référentiel : Certification de sécurité de premier niveau
Commanditaire(s) : Systancia
Centre d'évaluation : Amossys

Leur produit à été certifié CECC (critère commun) par EWA-Canada en 2015



Centre de la sécurité des télécommunications

© Gouvernement du Canada
Centre de la sécurité des télécommunications, 2015



BOMGAR

Bomgar est délivre des solutions d'accès sécurisé au service des entreprises. L'API Bomgar vous permet d'intégrer, en toute transparence, la gestion des accès privilégiés avec vos processus SIEM existants (gestion d'identités, des modifications et des événements).

Intégration avec les solutions ITSM et les systèmes de gestion de modifications. Gestion des autorisations et authentications avec AD, LDAPS, RADIUS, Kerberos

BOMGARTM
ENTERPRISE REMOTE SUPPORT



Bomgar fut acquis en juin 2016 par Thoma Bravo, un fond d'investissement privé.

- Pas de certification sécurité

➤ Le produit correspondant: **Privileged Access**



- Accès sécurisés à distance
- Recherche des données informatiques de session
- Contrôle d'accès au cloud
- Défense en profondeur
- Autorisation et notification
- Applis mobiles sécurisées
- Enregistrements vidéo
- Audit
- Accès web avancé
- Coffre Fort

Produits complémentaires



Password Vault



Remote Support

BEYONDTRUST

BeyondTrust (anciennement Symark) est une société américaine qui développe, et commercialise des produits de gestion d'identité et de gestion de vulnérabilités. BeyondTrust a été fondé en 2006.

Solution agent + serveur, se compose essentiellement d'un outil de PAM et modules d'audits

➤ Le produit correspondant: PowerBroker Privileged Access

- Accès sécurisés à distance
- Autorisation et notification
- Gestion des mots de passe
- SSO
- Enregistrements vidéo
- scalabilité
- Audit
- Dashboard d'alertes
- Coffre Fort



 BeyondTrust™



Le Laboratoire de test de Critères communs de Leidos (anciennement SAIC) a mené les tests de PowerBroker pour Unix et Linux et le National Information Assurance Partnership (NIAP), l'autorité d'approbation des États-Unis, a accordé le certificat Common Criteria qui est entré en vigueur au mois d'août 2016.

Leur produit à été certifié **CECC** (critère commun) par la National Security Agency and National Institute of Standards and Technology (NIST).



BALABIT

Balabit IT Security, fondée en 2000, à Budapest en Hongrie, est une entreprise de sécurité spécialisée dans le développement de systèmes de sécurité informatique et de services connexes utilisant l'apprentissage par machine pour sécuriser les comptes à privilèges.



- Catégorie : Identification, authentification et contrôle d'accès
- Référentiel : Certification de sécurité de premier niveau
- Commanditaire(s) : Balabit
- Centre d'évaluation : Oppida

❖ Solution en trois modules: | Access manager | Password Vault | Report Manager

➤ Le produit correspondant: Shell Control Box

Fonctionnalités clés :

- Gestion et gouvernance des comptes à privilèges
- Paramétrage contextualisé
- Visualisation en temps réel des activités
- Enregistrement des sessions
- Collecte des métadonnées et export SIEM possible
- Stockage des mots de passe dans un VAULT interne
- Gestion avancée des mots de passe et clés SSH



Leur produit a été certifié CSPN dans la catégorie « Identification, certification et contrôle d'accès » par l'agence nationale de la sécurité des systèmes d'information ANSSI-CSPN-2016/07



Solution française de sécurisation des accès externes au SI, certifiée CSPN (Certification de Sécurité de Premier Niveau) par l'ANSSI

CONCLUSION

❖ En conclusion, les solutions permettent:

- ✓ une meilleure auditabilité et le suivi des comptes à privilèges
- ✓ D'augmenter la capacité de surveillance des activités et traçabilité d'accès aux ressources critiques.
- ✓ De circonscrire l'utilisation des comptes partagés
- ✓ De segmenter les rôles et les pouvoirs.
- ✓ De faciliter la rotation du cycle de vie des mots de passe
- ✓ De garantir la sécurité et l'étanchéité du SI

De fait, elles concourent à la couverture des trois familles de risques citées:

- **Risques opérationnels,**
- **Risques de conformité**
- **Risques de sécurité.**



Les offres proposées par les éditeurs ne sont pas équivalentes

- Certaines solutions ne sont pas durcies et nécessitent l'installation d'un OS
- Il existe deux modes de fonctionnement : « **rooté** » ou « **bastion** ».
- Les deux modes ne sont pas incompatibles et peuvent répondre à des besoins différents.
- Certaines solutions nécessitent parfois un agent sur les postes.
- Les offres sont composées de modules complémentaires ... (attention à l'organisation nécessaire et au prix)
- Il est recommandé d'aborder le projet de bastion en douceur avec les modules de base.
- Il est recommandé de segmenter le projet d'intégration de celui de la gestion des comptes à privilèges




Lutessa