PROVEIT by rubycat DATASHEET

VISA DE SÉCURITÉ
Ref. 2023/05 - Validité 06/2026

Une politique de sécurité du SI inclut la **traçabilité** et le **contrôle des accès à privilèges**

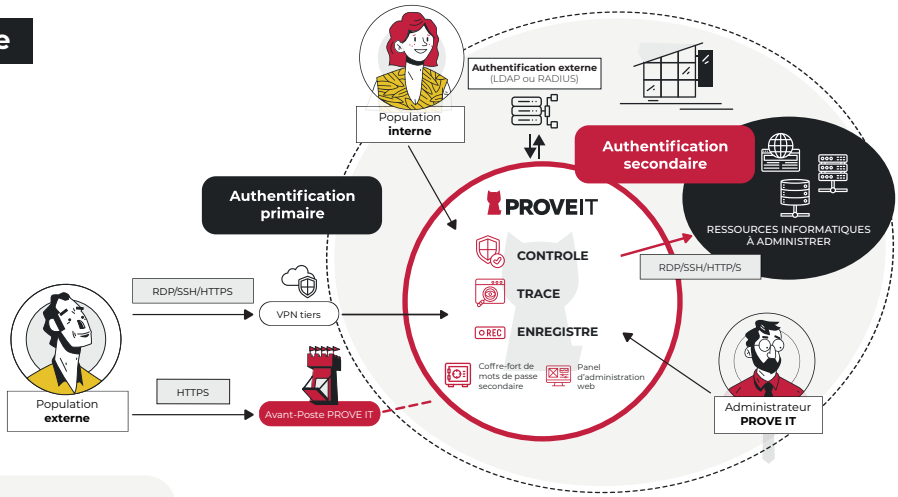
Vos équipements informatiques contiennent des **données** ou **applications sensibles** qu'il faut protéger pour garantir la continuité de votre activité, la pérennité de votre entreprise, mais aussi **la mise en conformité avec les normes et réglementations** (ISO 27001, RGPD, LPM, NIS 1 & 2...) et **recommandations ANSSI**.

« Un administrateur se distingue ainsi des autres utilisateurs par les droits et privilèges dont il a besoin pour mener à bien les actions d'administration qui relèvent de ses fonctions. »
(voir Guide de l'ANSSI relatif à l'administration sécurisée des SI reposant sur AD)

« Les actions d'administration imposent entre autres des exigences de traçabilité et de confidentialité. »
(voir Guide de l'ANSSI relatif à l'administration sécurisée des SI : R25 & Chapitre 13)

Schéma topologique - PAM All-In-One

- Exposition **maîtrisée et sécurisée** sur internet
- **Authentification centralisée** et **point d'accès unique** pour l'administration du SI
- Portail fédérateur pour une **gestion industrialisée** des **accès des utilisateurs à privilèges**
- Renforcement de la **sécurité des accès** avec notamment le **MFA** et **sécurisation des comptes à privilèges**
- Réduction du temps de **réponse à incidents**



Licensing

La **licence PROVE IT** est basée sur le **nombre maximum de sessions simultanées ouvertes** vers les ressources informatiques. Le nombre d'utilisateurs et de ressources déclarées est illimité.

Modes d'achat

Il y a **2 modes d'achat** disponibles :

- **Licence perpétuelle** + contrat de maintenance à souscrire
- **Souscription** : licence à durée déterminée avec contrat de maintenance inclus.

Partenaires & centrales d'achat

Pour vous accompagner, nous disposons d'un **réseau de partenaires intégrateurs certifiés**.

PROVE IT est disponible via différentes **centrales d'achat** *(CANUT, CAP TERRITOIRES, UGAP - marché multi-éditeurs, CAIH - marché S.A.L.O.H.M.E, RESAH Cybersécurité , SIPPEREC, HELPEVIA, UNICANCER).*

Certifications & labels

- Visa de Sécurité - CSPN par l'ANSSI depuis 2018 (Renouvellement en 2023 - Ref. 2023/05 - Validité juin 2026)
- Label France Cybersecurity
- Label Cybersecurity Made In Europe
- Utilisé par les armées françaises

Mise en conformité

PROVE IT est un élément fort de votre mise en conformité : NIS2 - ANSSI - RGPD - ISO 27001 - TISAX - LPM - HDS - CNIL - CRA - DORA - PCI-DSS...

Documentation et support

Un support éditeur dédié en France - Le contrat de maintenance intègre la mise à disposition des mises à jour mineures et majeures ainsi qu'une veille de vulnérabilité. Maintenance éditeur Rubycat : corrective, préventive, évolutive et réglementaire.
Documentation en anglais et en français disponible directement au sein de la solution.

PROVE IT SE DÉCLINE EN 3 GAMMES

	STANDARD	ADVANCED	CLUSTER
Authentification forte et centralisée	✓	✓	✓
Contrôle d'accès vers les ressources basées sur les rôles (RBAC)	✓	✓	✓
Journalisation des connexions internes, externes et des opérations d'administration	✓	✓	✓
Coffre-fort sécurisé pour la gestion des comptes sensibles	✓	✓	✓
Enregistrement et archivage des sessions	✓	✓	✓
Supervision en temps réel Re-visionnage pour analyse et action corrective	✓	✓	✓
Notifications avancées des évènements	✓	✓	✓
Politique de rétention configurable	✓	✓	✓
Segmentation par profil des droits d'administration : auditeurs / opérateurs / administrateurs	✗	✓	✓
API REST pour faciliter les opérations d'administration fréquentes	✗	✓	✓
Authentification via connecteur RADIUS	✗	✓	✓
Volumétrie supérieure ou égale à 50 sessions simultanées	✗	✗	✓
Résilience améliorée	✗	✗	✓
PRA assuré via une architecture actif/passif avec basculement manuel	Option	Option	Option

Caractéristiques techniques

POC

Licence d'évaluation gratuite sur demande

Environnement

VMWare ESXi 5+

Microsoft Hyper-V 2008+

QEMU/KVM/Nutanix/Proxmox

Livraison et déploiement

Appliance Virtuelle - Installation d'une image ISO basée sur Ubuntu 24.04 LTS qui embarque tous les composants PROVE IT

Hébergement Cloud - fourniture d'un fichier cloud-init

Fourniture de prérequis pour dimensionner la VM
Ex : 10 sessions = 4CPU, 4Go de RAM, 110Go d'espace de stockage pour 60j de rétention

Installation en moins d'une heure

Se positionne en rupture protocolaire, coupure des flux

Compatibilité sur environnement cloisonné d'internet

Sans agent / non invasive

Gestion sur plusieurs interfaces réseau possible

Disponible en version STANDALONE *(STANDARD / ADVANCED) ou CLUSTER*

Possibilité d'automatiser le provisionning en ligne de commande – ANSIBLE

Exposition internet sécurisée

Via VPN tiers

Via Avant-poste PROVE IT (frontal web HTTPS) : pas d'information sensible exposée sur Internet grâce à une architecture en diode, uniquement les flux authentifiés transitent de l'Avant-poste vers le Bastion

Utilitaires compatibles

Version minimale RDP : v8

Version minimale SSH : v2

Version minimale navigateur web : Chrome 103, Edge 103, Firefox 100

Exemples d'utilitaires compatibles (liste non-exhaustive)
- MRemote NG
- MobaXterm
- Putty
- Remmina
- Portails Web - tels que RDWeb (Microsoft)
- MSTSC

Sauvegarde et migration

Automatique en local sur la VM

Possibilité d'import / export des sauvegardes

Script de migration disponible pour passer des versions STANDARD et ADVANCED vers la version CLUSTER

Vie de solution

Mises à jour régulières disponibles
- Mineures : tous les 2 mois environ
- Majeures : tous les 24 mois environ

Documentations : guides d'administration, d'utilisateur et d'installation, notices d'intégration – incluses dans le WebAdmin – actualisées à chaque version

Nous consulter pour toute autre configuration

Fonctionnalités

Général

Modes d'authentification sur le bastion et vers les équipements cibles

Annuaire local (proveit - interne)

Annuaires compatibles : AD, AzureAD, OpenLDAP, LDAPS - Synchrone / Asynchrone

- Multi-facteurs : RADIUS via des solutions tierces (TrustBuilder/ STA / DUO / privacyIDEA / ...) pour tous les portails (en version ADVANCED)
- Multi-facteurs : WebAuthn intégré - authentification forte via passkey pour les portails web (compatible FIDO2, Windows Hello, smartphone, ...)

fail2ban intégré et paramétrable (nb de tentatives sur une durée)

Compatibilité Kerberos / Protected Users / Restricted Admin (RDP)

Mode d'authentification vers les cibles : (auth. secondaire)
- Propagation des identifiants primaires
- Utilisation des secrets du coffre-fort (clé SSH ou identifiant / mdp)
- LAPS 2015 pour les ressources RDP
- Saisie manuelle par l'utilisateur

Royaumes

Gestion de scénarios d'authentification multiples

Gestion des sessions : timeout inactivité, limitation du nombre de sessions par utilisateur - par royaume

Licence

Par palier de 5 sessions

Jeton de burst – possibilité de débloquer le nombre de sessions de la licence en 1 clic

Parcours utilisateur

Accès Kiosque – affichage des différentes ressources éligibles

Accès Direct (traçabilité préservée) :
- Connexion directe à la ressource identifiée
- Connexion M2M pour des accès sans intervention humaine

Accès Web : SSH / RDP / HTTPS

Cluster

Haute résilience

Répartition de charge – plus de 50 sessions

Hébergement sur le même LAN

Coffre-fort de mots de passe

Protégé via PASSPHRASE ou SECRET SHARING (partage de clés)

1 conteneur par secret

Chiffrement CHACHA20-POLY1305

API Admin (en version ADVANCED)

Automatisation des tâches d'administration fréquentes

Import en masse des ressources cibles (via template CSV)

Gestion des accès à privilèges - Gérer et maîtriser les accès à privilèges

Contrôle des accès (RBAC - Rôle Based Access Control)

Composé d'utilisateurs, de services et de filtres temporels

Filtre d'accès temporel : intervalle de date - date - fréquence - horaires

Politique d'accès activable / désactivable au clic

WebAdmin en HTTPS – administration de la plateforme

Version ADVANCED - segmentation par profil des droits d'administration PROVE IT

Contrôle de session

Enregistrement des actions désactivable

Dissuasion – message d'avertissement d'enregistrement – personnalisable

SSH :
- Autoriser X11, SCP, SFTP, PTY, SHELL, exécution de commandes, enregistrer les frappes clavier de la session SHELL
- Redirections de ports directs/inverses pour tout protocole non natif (ex : VNC,SQL, Telnet...)

RDP :
- Autoriser les redirections de disques, l'utilisation du presse-papier, les canaux dynamiques, du mode console
- NLA
- Forcer le mode Restricted Admin

HTTP/S : natif HTML5

Autre protocole : via un serveur de rebond ou via tunneling SSH

Portail web utilisateur

Supporte l'accès au service de type HTTPS, RDP et SSH

MFA via intégration RADIUS ou natif WebAuthn

Filtrage par IP

Traçage et blocage des accès suspicieux (robots et DDoS principalement)

Protection renforcée des utilisateurs légitimes (CSP, OCSP Stapling)

Chiffrement

Protocole de chiffrement SSH : aes256-ctr,aes192-ctr,aes128-ctr

Protocole de chiffrement RDP : TLSv1.2-1.3 / ECDHE-ECDSA-AES256-GCMSHA384: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCMSHA256: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHERSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA

Protocole de chiffrement HTTPS : TLSv1.2-1.3 / ECDHE-ECDSA-AES128-GCMSHA256: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCMSHA384: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305

Auditabilité - Visibilité sur les accès et actions réalisés

Journalisation / Traçabilité et visibilité temps-réel

Supervision d'une session utilisateur en temps réel

Clôture de sessions à la volée par l'administrateur PROVE IT

Recherche par nom de machine, protocole, date d'authentification...

Enregistrement des sessions SSH, RDP et HTTP/S

Visualisation depuis le navigateur ou téléchargement des enregistrements en local

Vidéo : en moyenne 1.5 Mo/minute/s ession active

Durée de rétention des enregistrements et journaux paramétrables

Logs

Utilisateur : authentification, autres événements...

Administrateur PROVE IT : authentification, actions effectuées sur le WebAdmin

Notifications via SMTP (mail) ou Syslog

Alerte avec configuration granulaire
Ex : connexion réussie d'un utilisateur à un service particulier

Alerte système – dépassement de seuil, nb de sessions, volumétrie de stockage...

SNMP

MIB Ubuntu

Document non contractuel v7.1a

rubycat control & trace

Editeur français de logiciels spécialisé dans la traçabilité et le contrôle d'accès au système d'information, RUBYCAT vous apporte son expertise en cybersécurité et expérience en sécurisation des accès pour vous aider à répondre de manière simple à une problématique majeure : le manque de visibilité sur les actions réalisées par les comptes à privilèges sur vos systèmes d'information.

RUBYCAT - Digital Park, 801 avenue des Champs Blancs, 35510 Cesson-Sévigné (Rennes)
Tél. : + 33 (0)2 99 30 21 11 – sales@rubycat.eu – www.rubycat.eu