PROVE IT by rubycat DATASHEET

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

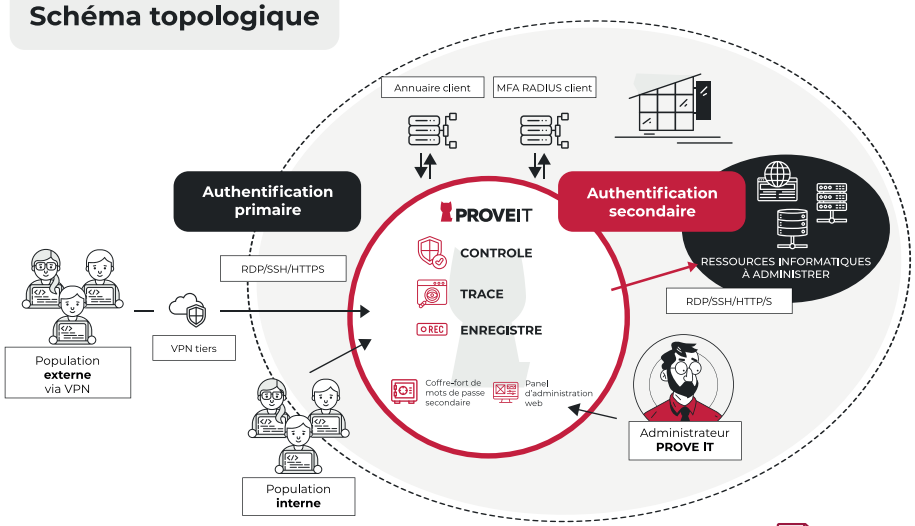
Une politique de sécurité du SI inclut la **traçabilité** et le **contrôle des accès à privilèges**

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



- **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**

	STANDARD	ADVANCED	CLUSTER
Contrôle des utilisateurs à privilèges et prestataires tiers	✓	✓	✓
Politique d'accès aux ressources critiques - RDP / SSH / HTTP/S	✓	✓	✓
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 PROVE IT : auditeurs / opérateurs / administrateurs	✗	✓	✓
API REST pour faciliter les opérations d'administration fréquentes	✗	✓	✓
Volumétrie supérieure ou égale à 50 sessions simultanées	✗	✗	✓
Résilience améliorée	✗	✗	✓

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.

PROVE IT se décline en 3 gammes : STANDARD - ADVANCED - CLUSTER

Mode d'achat

2 modes d'achat disponibles :
- Licence perpétuelle + contrat annuel de maintenance à souscrire en supplément.
- Souscription : licence à durée déterminée avec maintenance logicielle incluse.

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

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

Certifications et labels

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

Mise en conformité : réglementations - recommandations - normes

PROVE IT est un élément fort de votre mise en conformité :

RGPD - ISO 27001 - CNIL - ANSSI - HDS - NIS1 & NIS2 - TISAX - LPM - ...

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 disponible en anglais et en français dans la solution.

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 20.04 LTS qui embarque tous les composants PROVE IT
Fourniture de prérequis pour dimensionner la VM
- Ex : 10 sessions = 4CPU, 3Go RAM, 110Go d'espace stockage pour 60j de rétention
Installation en moins d'une heure
Se positionne en rupture protocolaire, coupure des flux
Compatibilité sur environnement cloisonné
Sans agent / non invasive
Disponible en version STANDALONE *(STANDARD / ADVANCED)* ou CLUSTER
Possibilité d'automatiser le provisionning en ligne de commande – ANSIBLE
Utilitaires compatibles (liste non-exhaustive)
MRemoteNG
MobaXterm
Putty
Portails Web – tels que RDWeb (Microsoft)
MSTSC
Version minimale RDP : v8
Version minimale SSH : v2
Version minimale navigateur web : Chrome 103, Edge 103, Firefox 100
Topologie
Se positionne derrière un VPN tiers pour les accès distants ou exposables directement sur internet
Gestion sur plusieurs interfaces réseau possible
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 mois environ
- Majeures : tous les 16 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 - interfaçage avec des solutions tierces en RADIUS (inWebo/STA/DUO/ LinOTP/...) + WebAuthn accès web
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 avec accès ouverts à l'utilisateur
Accès Direct (traçabilité préservée) :
- Connexion directe à la ressource identifiée
- Connexion M2M pour des accès sans intervention humaine
Cluster
Haute résilience
Répartition de charge – plus de 40 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 :
- NLA
- Autoriser les redirections de disques, l'utilisation du presse-papier, les canaux dynamiques, du mode console
- Forcer le mode Restricted Admin
HTTP/S natif HTML5
Tout autre protocole via serveur de rebond ou via tunneling SSH
Portail web
Supporte l'accès au service de type HTTPS, RDP et SSH
MFA via intégration RADIUS + 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-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-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-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305

Auditabilité - Visibilité sur les actions réalisées
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/session active
Durée de rétention des enregistrements et journaux paramétrables
Logs
Utilisateur : authentification, autres événements...
Administrateur PROVE IT : authentification, actions effectuées sur le WebAdmin
Notifications
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...
Notifications email
Via SMTP
Notifications syslog
Vers un concentrateur de logs externe – SIEM ou solution de supervision
SNMP
MIB Ubuntu

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 - Le Luthétium, 3 Square du Chêne Germain, 35 510 Cesson-Sévigné (Rennes)
Tél. : + 33 (0)2 99 30 21 11 – sales@rubycat.eu – www.rubycat.eu