LAZAR SOFT

Expert Partner ManageEngine

FICHE SOLUTION · GESTION UNIFIÉE DES TERMINAUX ET SÉCURITÉ (UEMS)

ManageEngine Endpoint Central

Gérez et sécurisez tous vos terminaux depuis une seule console.

Serveurs, postes de travail, portables, mobiles et tablettes : Endpoint Central automatise l'ensemble du cycle de vie de vos terminaux — déploiement, correctifs, inventaire, sécurité, prise en main à distance — dans une plateforme unique.

Windows · macOS · Linux · ChromeOS · iOS · Android

CINQ ÉDITIONS · SUR SITE OU CLOUD

Free · Professional · Enterprise · UEM · Security

Tarif éditeur **à partir de 795 €/an** pour 50 terminaux — détail complet en page 6.

26 M	31 000	190+	20	20 ans
TERMINAUX GÉRÉS DANS LE MONDE	PROFESSIONNELS IT UTILISATEURS	PAYS	LANGUES PRISES EN CHARGE	DE PRÉSENCE SUR LE MARCHÉ

LAZAR SOFT
Distributeur & intégrateur ManageEngine en France

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com

Un parc devenu multiple. Une console pour le reprendre en main.

Le défi d'aujourd'hui

La croissance rapide du nombre et de la diversité des terminaux utilisés en entreprise a redéfini les modes de fonctionnement — et ouvert la voie à de nouvelles formes de cyberattaques et de menaces internes. Face à des équipements aux formes et aux usages très différents, de plus en plus d'organisations recherchent un modèle de gestion unifiée des terminaux (UEM) : une plateforme logicielle unique pour administrer et sécuriser l'ensemble des équipements de l'entreprise — serveurs, postes fixes, portables, smartphones, tablettes et objets connectés.

SYSTÈMES PRIS EN CHARGE

Windows · macOS · Linux · ChromeOS · iOS · Android

MODES DE DÉPLOIEMENT

Sur site — ON-PREMISES

Cloud — HÉBERGÉ

La solution

Endpoint Central est une solution UEM qui permet de gérer et de sécuriser serveurs, postes de travail et terminaux mobiles depuis une console unique. Elle automatise l'intégralité du cycle de vie des terminaux, de bout en bout, pour aider les entreprises à réduire leurs coûts d'infrastructure IT, gagner en efficacité opérationnelle, améliorer la productivité, lutter contre les vulnérabilités du réseau et les menaces internes, prévenir les fuites de données et sécuriser les navigateurs de l'entreprise.

Utilisez Endpoint Central pour

- Automatiser les tâches courantes de gestion des terminaux.
- Standardiser les configurations des systèmes d'exploitation et des applications sur l'ensemble de votre réseau.
- Protéger les terminaux contre un large éventail de menaces.
- Résoudre les problèmes du quotidien.
- Auditer vos actifs informatiques.
- Mesurer et améliorer l'expérience numérique des utilisateurs (DEX).

Le périmètre couvert par la plateforme — 21 modules, une seule console

GÉRER LE PARC

- Gestion des correctifs
- Déploiement de logiciels
- Configurations
- Déploiement de systèmes d'exploitation
- Gestion des actifs informatiques
- Rapports
- Outils de support utilisateur

SÉCURISER LES POSTES

- Gestion des vulnérabilités
- Contrôle applicatif
- Gestion des privilèges sur les postes
- Contrôle des périphériques
- Sécurité des navigateurs

PROTÉGER LES DONNÉES

- Prévention des fuites de données
- Gestion de BitLocker
- Protection anti-ransomware
- Antivirus nouvelle génération

DÉPANNER ET GÉRER LES MOBILES

- Contrôle à distance
- Expérience utilisateur (DEX)
- Gestion des terminaux mobiles
- Gestion des applications mobiles
- Sécurité des terminaux mobiles

Le détail de chaque module figure aux pages 3 à 5.

Gérer le parc au quotidien

Gestion des correctifs

- Automatisez le déploiement des correctifs pour les systèmes d'exploitation Windows, Mac et Linux, ainsi que pour plus de 1 000 applications tierces.
- Détectez et déployez les correctifs manquants de façon proactive.
- Testez et approuvez les correctifs avant déploiement pour limiter les risques de sécurité.
- Déployez les correctifs critiques de type zero-day.
- Désactivez les mises à jour automatiques et refusez certains correctifs selon vos besoins.
- Obtenez des rapports sur l'état de santé et la vulnérabilité des systèmes.

Déploiement de logiciels

- Installez ou désinstallez des applications aux différents formats.
- Planifiez les déploiements logiciels et exécutez des actions avant et après installation.
- Laissez les utilisateurs installer eux-mêmes leurs logiciels via le portail en libre-service.
- Exploitez plus de 10 000 modèles prédéfinis pour déployer vos applications.
- Constituez un référentiel de paquets réutilisables autant de fois que nécessaire.
- Installez un logiciel sous une identité spécifique grâce à l'option « Exécuter en tant que ».

Configurations

- Standardisez les paramètres bureau, poste, application et sécurité à l'échelle de l'organisation grâce à des configurations de référence.
- Utilisez plus de 40 configurations pour les utilisateurs et les postes, ou créez vos propres modèles.
- Choisissez parmi plus de 180 scripts dans le référentiel de scripts.
- Restreignez l'usage des périphériques USB (imprimantes, lecteurs CD, supports amovibles, Bluetooth, modems…), au niveau utilisateur comme au niveau poste.
- Réduisez la consommation énergétique : schémas d'alimentation, extinction des postes inactifs, rapports de temps de fonctionnement.
- Configurez les stratégies de navigateur, de pare-feu et de sécurité ; contrôlez les accès aux fichiers, dossiers et à la base de registre via la gestion des permissions.
- Déclenchez des alertes sur l'expiration des mots de passe et l'espace disque système faible.

Déploiement de systèmes d'exploitation

- Capturez l'image d'un poste, allumé ou éteint, grâce aux techniques d'imagerie en ligne et hors ligne.
- Stockez ces images dans un référentiel centralisé et déployez les systèmes à la demande.
- Personnalisez les images capturées à l'aide de modèles de déploiement par métier ou par service.
- Déployez sans difficulté sur des matériels hétérogènes.
- Exécutez des actions post-déploiement : installation d'applications, configuration des postes, etc.

Gestion des actifs informatiques

- Suivez en temps réel l'ensemble du matériel et des logiciels de votre réseau.
- Assurez la conformité de vos licences logicielles.
- Bloquez les exécutables et désinstallez les logiciels interdits.
- Analysez les statistiques d'usage et réduisez les coûts liés aux logiciels inutilisés grâce au comptage d'utilisation.
- Recevez des notifications sur des événements précis : détection d'un nouveau logiciel, non-conformité par sous-licenciement, logiciel interdit.
- Disposez de plus de 20 rapports prédéfinis sur le matériel, les logiciels, l'inventaire et la conformité des licences.

Rapports

- Exploitez plus de 200 rapports Active Directory prêts à l'emploi sur les utilisateurs, les postes, les groupes, les unités d'organisation et les domaines.
- Réduisez la facture énergétique grâce à la gestion de l'alimentation et consultez les rapports de temps de fonctionnement.
- Obtenez le détail à jour des ouvertures de session utilisateur.
- Consultez les rapports de correctifs, de configurations et d'événements à des fins d'audit.

Outils de support utilisateur

- Supervisez et analysez les systèmes gérés à distance en consultant le détail des tâches et des processus en cours.
- Démarrez un poste à distance instantanément via Wake-on-LAN, ou planifiez les démarrages.
- Publiez des annonces à l'échelle de l'entreprise ou à destination des seuls techniciens.
- Planifiez la défragmentation, la vérification et le nettoyage des disques, en local comme à distance.

Sécuriser les postes et les données

Gestion des vulnérabilités

- Renforcez votre posture de sécurité grâce à une gestion intégrée des menaces et des vulnérabilités, avec détection et remédiation immédiates.
- Améliorez la sécurité en déployant des stratégies dédiées et en corrigeant les erreurs de configuration système.
- Appuyez-vous sur le partenariat exclusif de ManageEngine avec le Center for Internet Security (CIS) pour garantir la conformité aux référentiels CIS, sans oublier les autres : Cyber Essentials, ManageEngine, NIST et vos référentiels personnalisés.
- Repérez rapidement les vulnérabilités zero-day et déployez des scripts de contournement en attendant les correctifs.
- Auditez et éliminez les logiciels à haut risque — fins de vie, partage de bureau à distance, pair-à-pair — pour prévenir les fuites de données.
- Auditez les ports actifs pour détecter les anomalies dans le cadre de la gestion des vulnérabilités.

Contrôle applicatif

- Découvrez l'ensemble des applications et exécutables installés, et classez-les en approuvés ou non approuvés selon leur signature numérique.
- Bénéficiez d'une régulation souple, avec plusieurs modes pour établir efficacement un environnement Zero Trust.
- Facilitez le contrôle applicatif en permettant aux utilisateurs de demander l'accès à une application.
- Adoptez une approche Zero Trust en activant le mode strict, qui interdit automatiquement jusqu'aux applications non gérées.

Gestion des privilèges sur les postes

- Supprimez les droits d'administration superflus et exécutez les applications métier critiques avec des privilèges restreints, pour prévenir les attaques par élévation de privilèges ou compromission d'identifiants.
- Maintenez le modèle du moindre privilège sans nuire à la productivité, grâce à l'élévation de privilèges par application.
- Traitez les besoins ponctuels par un accès privilégié temporaire aux applications, révoqué automatiquement à l'échéance.

Contrôle des périphériques

- Régulez et restreignez efficacement plus de 15 types de périphériques depuis une console centralisée, avec détection automatique des ports actifs.
- Contrôlez l'accès aux fichiers et les transferts par rôle, avec limite de volume, pour protéger vos données critiques.
- Accordez un accès temporaire à des périphériques sur des postes précis, pour une durée définie.
- Anticipez les fuites en mettant en miroir, dans un emplacement sécurisé, les données consultées par les périphériques USB.
- Respectez les standards de conformité des équipements et exploitez des rapports d'audit détaillés.

Prévention des fuites de données

- Supervisez et encadrez les mouvements de données de l'entreprise depuis une console centralisée, pour contrer les attaques internes et les pertes de données.
- Analysez et classifiez les données critiques de l'entreprise selon les standards de conformité et de réglementation.
- Encadrez les tentatives de transfert par dépôt cloud, échange de courriels, impression et autres périphériques.
- Recevez des alertes instantanées en cas de tentative de violation de stratégie et traitez les faux positifs.

Sécurité des navigateurs

- Verrouillez les navigateurs de l'entreprise et durcissez leurs paramètres pour prévenir les attaques par le navigateur.
- Obtenez une vue d'ensemble des différents navigateurs utilisés sur le réseau.
- Appliquez des configurations de sécurité conformes aux référentiels STIG et CIS.
- Garantissez une navigation sûre en détectant et en supprimant les extensions malveillantes.
- Autorisez les sites approuvés et bloquez les applications web indésirables, au bénéfice de la productivité et de la sécurité.

Gestion de BitLocker

- Protégez les données des postes en automatisant le chiffrement de certains volumes ou du disque entier.
- Identifiez les postes équipés d'une puce TPM pour renforcer la sécurité par code PIN et phrase secrète.
- Récupérez les données grâce à la clé de récupération en cas de défaillance matérielle, et réinitialisez le mot de passe des postes retirés du réseau.
- Appliquez des stratégies de chiffrement et restez conforme aux cadres de protection des données tels que FISMA, HIPAA et PCI-DSS.

Protéger, assister et gérer la mobilité

Protection anti-ransomware

- Bénéficiez d'une protection réactive qui filtre les rançongiciels pour renforcer la sécurité des terminaux.
- Détectez instantanément toute tentative d'intrusion par rançongiciel grâce à une analyse comportementale multi-brevetée, assistée par apprentissage automatique.
- Disposez d'une analyse détaillée de toutes les tentatives d'intrusion.
- Restaurez vos données en un clic grâce au retour arrière intégré.

Antivirus nouvelle génération

- Détectez les logiciels malveillants en temps réel, avec l'assistance de l'IA, pour une protection face aux menaces en évolution constante.
- Menez une investigation d'incident complète, avec des rapports détaillés alignés sur les tactiques, techniques et procédures (TTP) du référentiel MITRE.
- Analysez en profondeur les méthodes d'attaque, les chemins empruntés et la chaîne d'exécution.
- Neutralisez rapidement les intrusions, protection contre les rançongiciels comprise.
- Traitez les menaces avec un impact minimal sur l'exploitation du réseau, au bénéfice de la continuité d'activité.
- Restaurez en un clic les fichiers compromis dans leur état d'origine.

Contrôle à distance

- Appuyez-vous sur une prise en main à distance sécurisée, conforme à différentes réglementations dont HIPAA et PCI DSS.
- Dépannez les postes distants en collaboration avec plusieurs intervenants.
- Profitez de la vidéo, de l'appel et du chat intégrés, ainsi que du transfert de fichiers entre machines.
- Enregistrez l'intégralité des sessions à des fins d'audit.
- Verrouillez le clavier et la souris de l'utilisateur et masquez son écran pour préserver la confidentialité pendant l'intervention.
- Bénéficiez du chiffrement AES 128 bits pendant les opérations de prise en main.

Expérience utilisateur (DEX)

- Collectez et analysez la télémétrie des terminaux : processeur, mémoire, carte graphique, disque, santé de la batterie, temps de démarrage, temps d'ouverture de session, plantages.
- Détectez en continu les premiers signes de gêne pour l'utilisateur : pics de processeur, saturation mémoire, incidents disque.
- Remontez à la cause racine en corrélant les baisses de performance avec le vieillissement du matériel ou les applications trop gourmandes.
- Hiérarchisez les alertes par gravité et corrigez en un clic, ou automatiquement, via une bibliothèque d'actions ou vos propres workflows.
- Notez et comparez terminaux et applications sur des critères de performance et de stabilité, pour suivre l'état du parc dans la durée.

Gestion des terminaux mobiles

- Automatisez l'enrôlement en masse et l'authentification des équipements personnels (BYOD) et professionnels.
- Maîtrisez les mises à jour de système d'exploitation et dépannez les mobiles à distance.
- Obtenez une visibilité complète sur le parc mobile grâce à des rapports prédéfinis et personnalisables.

Gestion des applications mobiles

- Créez votre propre catalogue d'applications d'entreprise, limité aux applications internes et commerciales approuvées par la DSI.
- Installez, mettez à jour et supprimez silencieusement les applications professionnelles, tout en gérant leurs licences et en préconfigurant leurs autorisations.
- Garantissez que les terminaux n'exécutent que des applications de confiance, bloquez les applications malveillantes ou vulnérables et empêchez la désinstallation des applications d'entreprise.

Sécurité des terminaux mobiles

- Configurez et appliquez les stratégies de sécurité de l'entreprise : Wi-Fi, VPN, messagerie et bien d'autres.
- Empêchez les accès non autorisés à la messagerie professionnelle et distribuez, stockez et consultez les contenus en toute sécurité.
- Imposez le chiffrement au niveau de l'appareil, cloisonnez les espaces personnel et professionnel sur les terminaux BYOD, et localisez, verrouillez ou effacez à distance un appareil égaré.

03 — ÉDITIONS ET TARIFS

Cinq éditions. On vous aide à choisir la vôtre.

ÉDITION	CE QUE COUVRE L'ÉDITION	À PARTIR DE
Free Pour évaluer sans limite de durée	Gestion complète jusqu'à 25 terminaux.	**0 €** 25 terminaux
Professional Parc sur un site unique (LAN)	Socle de gestion : correctifs, déploiement logiciel, inventaire, configurations, prise en main à distance.	**795 €** par an · 50 terminaux
Enterprise Parc réparti sur plusieurs sites (WAN)	**Tout Professional**, plus le portail en libre-service, les correctifs pilotes et drivers, les mises à jour antivirus et les sessions distantes sur mobile.	**945 €** par an · 50 terminaux
UEM Gestion unifiée de tous les terminaux	**Tout Enterprise**, plus la gestion des portables Windows et macOS par MDM, le déploiement d'OS et les fonctions avancées de mobilité.	**1 095 €** par an · 50 terminaux
Security Gestion unifiée + sécurité des terminaux intégrée	**Tout UEM**, plus les vulnérabilités, le contrôle applicatif, le contrôle des périphériques, la DLP, la sécurité des navigateurs et BitLocker.	**1 695 €** par an · 50 postes de travail

Failover

à partir de 1 195 €

Secure Gateway Server

à partir de 345 €

Prise en charge multilingue

à partir de 345 €

Tarifs publics éditeur, édition **On-Premises**, abonnement annuel, 1 technicien inclus — source : ManageEngine, matrice de comparaison des éditions Endpoint Central, consultée le 13/08/2026. Prix indicatifs et non contractuels : le montant applicable dépend du volume de terminaux, du nombre de techniciens, de la durée d'engagement, du mode de déploiement (les tarifs Cloud diffèrent) et des composants additionnels retenus. Devis personnalisé LAZAR SOFT sur demande.

Contactez-nous.

Une question ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com