DITEL Cyber Protection

La cybersécurité simplifiée pour protéger votre entreprise

Éditeur de la solution

DITEL

Solution de cybersécurité destinée aux entreprises, collectivités, commerces, industries et prestataires informatiques.

Sommaire

---

1. Présentation de la solution

DITEL Cyber Protection est une solution de cybersécurité conçue pour assurer la protection des entreprises contre les menaces informatiques modernes :

- ransomwares ;
- virus et malwares ;
- intrusions réseau ;
- comportements suspects ;
- vols de données ;
- interruptions d'activité.

La plateforme combine plusieurs technologies de sécurité afin d'offrir une protection globale simple à utiliser et compréhensible par les dirigeants comme par les équipes techniques.

La solution s'articule autour de trois composants complémentaires :

- un agent de protection des postes et serveurs ;
- une sonde de surveillance réseau ;
- une console centralisée de supervision.

---

2. Pourquoi protéger son entreprise ?

Les cyberattaques représentent aujourd'hui un risque majeur pour les entreprises de toutes tailles.

Une attaque peut provoquer :

- l'arrêt complet de l'activité ;
- le chiffrement des fichiers ;
- la perte de données stratégiques ;
- des coûts importants de remise en service ;
- une atteinte à l'image de l'entreprise ;
- des conséquences juridiques liées aux données personnelles.

Les TPE et PME sont particulièrement ciblées car elles disposent rarement d'une équipe cybersécurité interne dédiée.

La protection du système informatique devient donc un enjeu stratégique pour garantir la continuité d'activité.

---

3. Architecture de la solution

DITEL Cyber Protection repose sur une architecture modulaire composée de trois niveaux de sécurité :

Composant	Fonction principale
Agent EDR	Protection des postes et serveurs
Sonde NDR	Surveillance réseau et détection d'intrusion
Console centralisée	Supervision et pilotage global

Cette approche permet d'obtenir une vision complète de l'environnement informatique de l'entreprise.

---

4. Protection des postes et serveurs (EDR)

Présentation

L'agent EDR (Endpoint Detection & Response) est installé sur les ordinateurs, serveurs et équipements stratégiques de l'entreprise.

Il assure une surveillance continue des systèmes afin d'identifier les comportements suspects ou malveillants.

Fonctions principales

Surveillance en temps réel

L'agent analyse en permanence :

- les processus actifs ;
- les comportements logiciels ;
- les accès fichiers ;
- les tentatives d'exécution suspectes ;
- les modifications critiques du système.

Protection anti-ransomware

La solution détecte les comportements caractéristiques des ransomwares :

- chiffrement massif de fichiers ;
- activité anormale sur les répertoires ;
- processus suspects ;
- propagation inhabituelle.

En cas de détection, des actions automatiques peuvent être déclenchées.

Contrôle de sécurité

L'agent vérifie également :

- l'état des mises à jour ;
- la configuration de sécurité ;
- les logiciels installés ;
- les services actifs ;
- les anomalies de configuration.

Bénéfices

- Protection automatisée des postes.
- Réduction du risque de compromission.
- Détection rapide des incidents.
- Meilleure visibilité sur le parc informatique.
- Surveillance continue 24h/24.

---

5. Surveillance réseau (NDR)

Présentation

La sonde NDR (Network Detection & Response) supervise le trafic réseau de l'entreprise.

Elle analyse les communications afin de détecter :

- les intrusions ;
- les comportements anormaux ;

- les équipements inconnus ;
- les connexions suspectes.

Fonctionnalités

Analyse du trafic réseau

La sonde surveille :

- les flux internes ;
- les connexions Internet ;
- les échanges entre équipements ;
- les comportements inhabituels.

Détection des intrusions

Le système identifie :

- les scans réseau ;
- les mouvements latéraux ;
- les connexions anormales ;
- les tentatives d’accès non autorisées.

Cartographie réseau

La solution permet de visualiser :

- les équipements connectés ;
- les segments réseau ;
- les flux de communication ;
- les équipements inconnus.

Bénéfices

- Vision globale du réseau.
- Détection rapide des comportements suspects.

- Identification des équipements non autorisés.
- Réduction des risques d’intrusion.

---

6. Console centralisée de supervision

Présentation

La console centralise toutes les informations de sécurité dans une interface unique.

Elle permet au dirigeant ou au responsable informatique de suivre l’état de sécurité de l’entreprise en temps réel.

Fonctions disponibles

Tableau de bord global

Affichage de :

- l’état général de sécurité ;
- les incidents détectés ;
- les équipements surveillés ;
- le niveau de risque global.

Gestion des alertes

Les alertes sont classées par priorité :

Niveau	Description
Critique	Risque immédiat nécessitant une action
Élevé	Activité suspecte importante
Moyen	Événement à surveiller
Faible	Information ou activité mineure

Actions rapides

Selon les droits utilisateurs, il est possible :

- d’isoler un poste ;

- de bloquer une menace ;
- de lancer une analyse ;
- de consulter l'historique d'un incident.

Bénéfices

- Interface simple et centralisée.
- Lecture rapide de l'état de sécurité.
- Réduction de la complexité technique.
- Pilotage simplifié des incidents.

---

7. Intelligence artificielle et détection avancée

Fonctionnement

La solution utilise des mécanismes d'analyse comportementale assistés par intelligence artificielle.

Le système observe les habitudes normales de fonctionnement de l'entreprise afin d'identifier les anomalies.

Capacités principales

- détection comportementale ;
- réduction des fausses alertes ;
- corrélation d'événements ;
- priorisation des incidents ;
- aide à l'analyse des menaces.

Bénéfices

- Détection plus rapide des comportements anormaux.
- Réduction du bruit d'alertes.
- Lecture plus claire des incidents.
- Assistance à la prise de décision.

---

8. Aide à la conformité et traçabilité

DITEL Cyber Protection facilite certaines démarches de sécurité et de conformité grâce à :

- la journalisation des événements ;
- les historiques d'activité ;
- les rapports de sécurité ;
- les journaux d'audit ;
- la traçabilité des actions.

La solution peut contribuer aux démarches de conformité RGPD et aux référentiels de sécurité, sans remplacer un audit juridique ou organisationnel complet.

---

9. Hébergement et souveraineté des données

Les données de supervision peuvent être hébergées en France afin de répondre aux besoins des entreprises sensibles à la souveraineté numérique.

Cette approche permet :

- une meilleure maîtrise des données ;
- une limitation des transferts internationaux ;
- une meilleure conformité contractuelle ;
- une confidentialité renforcée.

---

10. Déploiement et mise en service

Étape 1 — Installation

- Installation des agents EDR sur les postes et serveurs.
- Configuration de la sonde réseau.
- Création des accès à la console.

Étape 2 — Phase d'apprentissage

Pendant plusieurs jours, la solution observe l'activité normale de l'entreprise afin d'optimiser les mécanismes de détection.

Étape 3 — Protection active

Une fois l'apprentissage terminé :

- la surveillance devient active ;
- les alertes sont générées ;
- les rapports sont disponibles ;
- les mécanismes automatiques sont opérationnels.

---

11. Fonctionnement quotidien

La solution fonctionne en continu sans intervention quotidienne obligatoire.

Les utilisateurs accèdent à :

- un tableau de bord ;
- des alertes prioritaires ;
- des rapports automatiques ;
- des historiques de sécurité.

---

12. Alertes et gestion des incidents

Gestion intelligente des alertes

Les alertes importantes sont remontées automatiquement afin de limiter les fausses alarmes.

Chaque incident contient :

- le type de menace ;
- le niveau de criticité ;
- l'équipement concerné ;
- les actions recommandées.

Réaction rapide

Selon la configuration, la solution peut :

- isoler automatiquement un poste ;
- bloquer certaines communications ;
- suspendre un comportement suspect ;
- notifier les administrateurs.

---

13. Rapports et supervision

La solution génère des rapports permettant :

- le suivi de la sécurité ;
- l'analyse des incidents ;
- la préparation des audits ;
- la documentation des événements.

Les rapports peuvent inclure :

- les incidents détectés ;
- les postes protégés ;
- les statistiques réseau ;
- les alertes critiques ;
- les actions effectuées.

---

14. Secteurs d'activité concernés

DITEL Cyber Protection peut être utilisé dans de nombreux secteurs :

- commerce ;
- industrie ;
- e-commerce ;
- santé ;
- services ;
- collectivités ;
- formation ;

- cabinets professionnels ;
- MSP et infogérance.

---

15. Bénéfices pour l’entreprise

Sécurité renforcée

- Protection globale.
- Surveillance continue.
- Détection avancée.

Simplicité d’utilisation

- Interface claire.
- Alertes compréhensibles.
- Gestion centralisée.

Réduction des risques

- Diminution du risque d’interruption.
- Réduction des impacts financiers.
- Meilleure capacité de réaction.

Meilleure visibilité

- Vue centralisée de la sécurité.
- Rapports automatisés.
- Suivi des incidents.

---

16. Informations techniques

Élément	Description
Type de solution	Cybersécurité EDR + NDR

Élément	Description
Déploiement	Local / Cloud
Supervision	Console centralisée
Surveillance	Temps réel
Alertes	Automatiques
Hébergement	France (selon configuration)
Compatibilité	Postes et serveurs
Fonctionnement	24h/24 – 7j/7

---

17. Conclusion

DITEL Cyber Protection apporte une approche moderne et simplifiée de la cybersécurité pour les entreprises.

Grâce à la combinaison :

- de la protection des postes ;
- de la surveillance réseau ;
- de l'analyse intelligente ;
- de la supervision centralisée ;

la solution permet d'améliorer la visibilité, la détection et la réaction face aux menaces informatiques tout en restant accessible aux structures ne disposant pas d'expertise cybersécurité avancée.

Contact

www.ditel.fr

DITEL — Solutions logicielles et cybersécurité pour les entreprises.