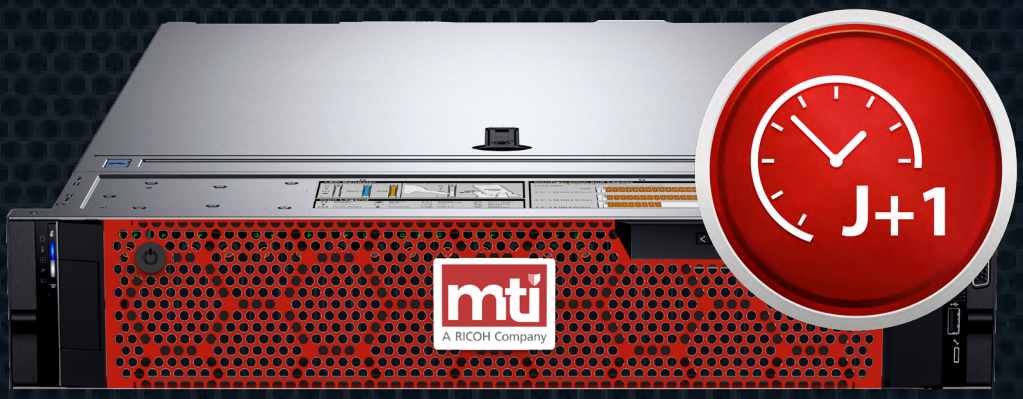
A RICOH Company

CLEAN ROOM MTI

Accélérez votre reprise d'activité après une cyberattaque



Powered by Dell Technologies

L’importance d’une infrastructure résiliente

La **résilience** d’une organisation se réfère à sa capacité à prévenir, limiter et se remettre de tout incident majeur. Ces incidents peuvent prendre différentes formes : panne de matériel, de réseau ou d’électricité, catastrophe naturelle, erreurs humaines ou logicielles...

Actuellement, c’est la notion de **cyber-résilience** qui prédomine, les incidents les plus courants étant liés à des cyberattaques (le plus souvent, des ransomwares ou des attaques DDoS).

Cette démarche est capitale pour les entreprises désireuses de garantir leur sécurité et d'assurer la continuité de leurs activités. Elle revêt une importance particulière pour les petites structures telles que les **PME ou les sites distants, qui sont souvent les plus vulnérables** - et de fait, les plus ciblées.

3 RAISONS DE CONSTRUIRE UNE STRATÉGIE DE CYBER-RÉSILIENCE EFFICACE :

1 PROTECTION INTÉGRALE DES DONNÉES

Protéger ses données est absolument crucial aujourd'hui, dans un monde où les cyber-menaces ne cessent de se multiplier et de se complexifier.

L’intégrité d'une entreprise et la pérénité de ses activités passent par la sauvegarde des données critiques, la préservation des systèmes et la sécurisation des infrastructures sensibles.

2 RÉDUCTION DES RISQUES FINANCIERS

La cyber-résilience est bien plus qu’une mesure de sécurité ; elle constitue également un impératif économique. Les risques financiers associés à la cybercriminalité sont en effet dévastateurs :

- **Coûts de remédiation très élevés** pour restaurer les systèmes, souvent en faisant appel à différents experts ;
- **Pertes significatives de revenus** dues aux interruptions des activités et au ralentissement des ventes ;
- **Amendes et sanctions financières** liées aux réglementations de plus en plus strictes en matière de protection des données.

3 PRÉSERVATION DE SA RÉPUTATION

Une cyberattaque engendre systématiquement une importante perte de confiance de ses clients ou partenaires. Adopter de bonnes pratiques de cyber-résilience permet également d'éviter ce type de préjudices.

Cela démontre également la capacité d'une entreprise à gérer les risques et à garantir la confidentialité de ses données, ce qui représente une base solide pour des relations commerciales durables.

La meilleure stratégie de défense : prendre conscience que le risque zéro n’existe pas

Les solutions de sécurité déployées par les oganisations (pares-feux, antivirus, mises à jour régulières, formations des salariés...) permettent évidemment de retarder ou de limiter les attaques. Cependant, aucune ne peut garantir une protection infaillible : les hackers finissent toujours par trouver un moyen de s’infiltrer.

La meilleure façon de se protéger consiste donc à se préparer au pire et à considérer qu’une cyberattaque est inévitable, par la mise en place d’une bonne stratégie de sauvegarde et de restauration de ses données. Ainsi, quand l’attaque survient, l’entreprise peut récupérer ses données et redémarrer son activité rapidement.

Protéger ses données de sauvegarde, oui... Mais ce n’est pas suffisant !

Beaucoup de directions informatiques se sentent prêtes à affronter une cyberattaque dès lors qu'elles sauvegardent leurs données et qu'elles protègent les copies (qui, elles aussi, sont devenues des cibles privilégiées).

Toutefois, elles négligent souvent la partie restauration, qui est pourtant primordiale ! En effet, après une attaque, l’infrastructure de production demeure indisponible pour plusieurs raisons :

- Nécessité de limiter la contamination et de déchiffer les données en cas de ransomware
- Mise sous scellés par les autorités
- Préservation en l’état obligatoire pour les analyses forensiques demandées par la justice
- Redémarrage impossible de certains matériels ayant subi des dommages physiques

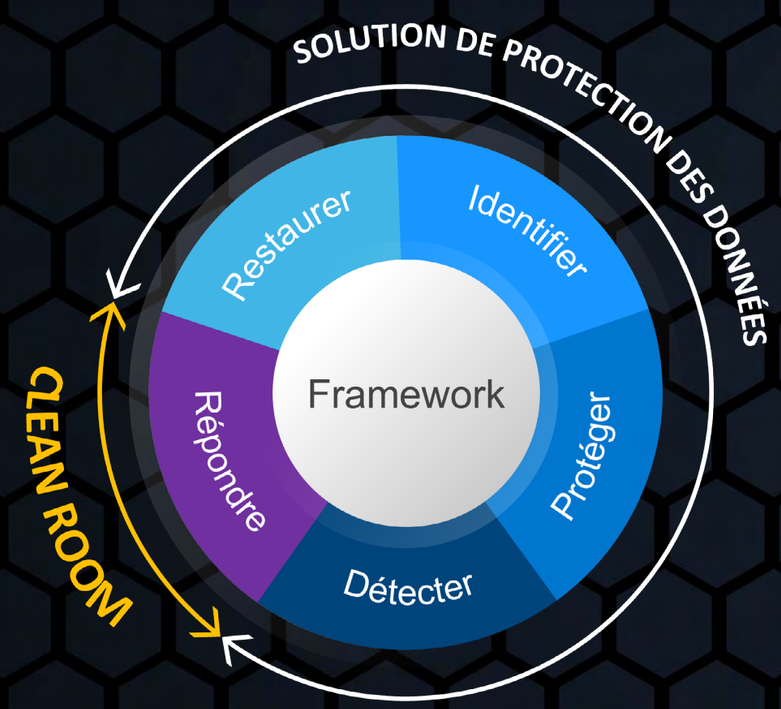
Il faut donc être préparé à entamer le processus de reprise d’activité sur une infrastructure vierge, qui puisse être disponible rapidement.

Assurer sa cyber-résilience grâce au service de Clean Room MTI

Une solution permettant de redémarrer son activité sans délai

Après une cyberattaque ou tout autre incident majeur, le service de Clean Room MTI offre la possibilité d'accéder très rapidement à un environnement isolé et propre, pour restaurer ses données.

Cette solution permet également d'effectuer des tests afin d'évaluer sa capacité de reprise. Cette démarche anticipative facilite une réaction plus rapide - et plus sereine - en cas de sinistre.



Le service de Clean Room MTI est une offre complémentaire aux solutions de protection des données. Elle constitue un élément essentiel de toute stratégie de cyber-résilience.

La Clean Room MTI a été développée en collaboration avec Dell Technologies et s'appuie sur des composants et des logiciels éprouvés, ainsi qu'une expertise poussée.

Chronologie d'une cyberattaque :

1. **Dernière sauvegarde**
2. Incident majeur / arrêt de la production

RPO*

INFRASTRUCTURE INDISPONIBLE

(Dommages physiques, enquête des autorités, limitation de la contamination, ...)

Attente évitée grâce au service de Clean Room MTI

RTO**

3. Nouvelle infrastructure saine
4. Restauration des données
5. **Reprise de l'activité**

Reprise d'activité **AVEC** Clean Room MTI :

Quelques jours

Reprise d'activité **SANS** Clean Room MTI :

1 mois au minimum

**Recovery Point Objective* ***Recovery Time Objective*

Détails de l’offre de service Clean Room MTI

Un service fourni sous forme d’assurance, avec une mise à disposition à la demande

Le service de Clean Room MTI se présente sous la forme d’une assurance. Après détection du sinistre, la solution peut être déployée à **J+1** sur site client, jusqu'à **120 jours consécutifs**. Elle offre la fourniture d’un environnement :

- VMware pré-intégré et entièrement contrôlé ;
- Indépendant des logiciels de sauvegarde ;
- Prêt à être utilisé.

Pour plus de flexibilité, nos clients ont la possibilité de prolonger la durée d’utilisation de la Clean Room MTI. Les coûts de prolongation sont définis contractuellement, ce qui assure un contrôle total sur le budget.

Nous proposons également des services supplémentaires en option, notamment la possibilité de tester la capacité de reprise de l’entreprise pendant une durée de 15 jours chaque année.

3 niveaux de service :

BRONZE

Couverture
20 VM

SILVER

Couverture
40 VM

GOLD

Couverture
80 VM

Configuration moyenne prise en compte par VM :
3 vCPU, 11 GB vRAM, 173 GB vDisk.

Les bénéfices du service de Clean Room MTI :

Notre solution est fiable et sécurisée ; elle simplifie grandement la gestion de sa reprise d’activité et permet d'optimiser ses coûts.

Associer les avantages du mode « as-a-service » et d’une solution sur site :

- Flexibilité ;
- Maîtrise de la connectivité et de l’accès aux données ;
- Utilisation des outils de l’entreprise ;
- Contrôle du temps d’indisponibilité de l’infrastructure de production ;
- Proximité des données de sauvegarde (rendant la restauration plus rapide) ;
- Maîtrise des coûts.

Bénéficier d’un environnement de reprise d’activité toujours prêt :

- Opérationnel et fonctionnel au bon moment (« DR Just in time ») ;
- Sain et totalement intègre ;
- Dans un état vierge et dépourvu de données préexistantes.

Réaliser des économies substancielles en évitant les dépenses liées :

- Au temps dédié à la gestion du maintien en conditions opérationnelles (mises à jour des firmwares, des pilotes et de l’environnement VMware) ;
- À la place requise au sein du Datacenter ;
- À la consommation électrique.

MTI France

Parc Claude Monet
3-5 allée de Giverny
78290 Croissy-sur-Seine

Standard :
+33 (0)1 30 09 52 00
FRinfo@mti.com

Abonnez-vous !

A RICOH Company