Solution Brief

Redéfinir la résilience cyber des établissements de santé

Guide du Domaine 2 du programme CaRE et de la continuité d'activité avec Veeam

La résilience numérique au cœur du secteur de la santé

Les établissements de santé et établissements médico-sociaux font face à des menaces numériques de plus en plus fréquentes et sophistiquées. Les attaques par rançongiciel ciblent désormais aussi bien les systèmes de production que les sauvegardes, mettant en péril la continuité des soins et la confiance des patients. Le Domaine 2 du programme CaRE vise à renforcer la capacité des établissements à prévenir, réagir et se relever après une cyberattaque, en structurant une stratégie de continuité et de reprise d'activité solide et sécurisée. Veeam accompagne les établissements de santé et établissements médico-sociaux dans la mise en œuvre de solutions de sauvegarde et de restauration en répondant aux objectifs du domaine 2 du programme CaRE, pour garantir la disponibilité et la résilience des données de santé.

Protection, sauvegarde et restauration des données au cœur de la résilience opérationnelle

Solution Brief

Les objectifs du Domaine 2 — Un cadre clair pour la résilience

Le Domaine 2 du programme CaRE s'articule autour de quatre axes fondamentaux pour consolider la continuité, la sauvegarde et la restauration des systèmes critiques des établissements de santé :

1. Gouvernance et gestion de crise (D2.O1)
2. Politique et plans de sauvegarde (D2.O2)
3. Sécurisation du système de sauvegarde (D2.O3)
4. Tests et validation (D2.O4)

Ces objectifs définissent une trajectoire claire vers une meilleure maîtrise des risques numériques et une reprise rapide des activités critiques en cas d'incident.

Le rôle de la direction et de la gouvernance

La direction générale, le RSSI et le DSI portent la responsabilité du pilotage de la continuité et de la résilience cyber. Leur engagement est essentiel pour structurer une gouvernance claire, suivre les indicateurs de sécurité et s'assurer de la conformité aux exigences du programme CaRE. Veeam soutient cette approche par des solutions de supervision, de reporting et d'audit automatisés favorisant la transparence et la prise de décision et par des services d'accompagnement.

Solution Brief

Focus sur les 4 axes du Domaine 2

1. Gouvernance et gestion de crise (D2.O1)

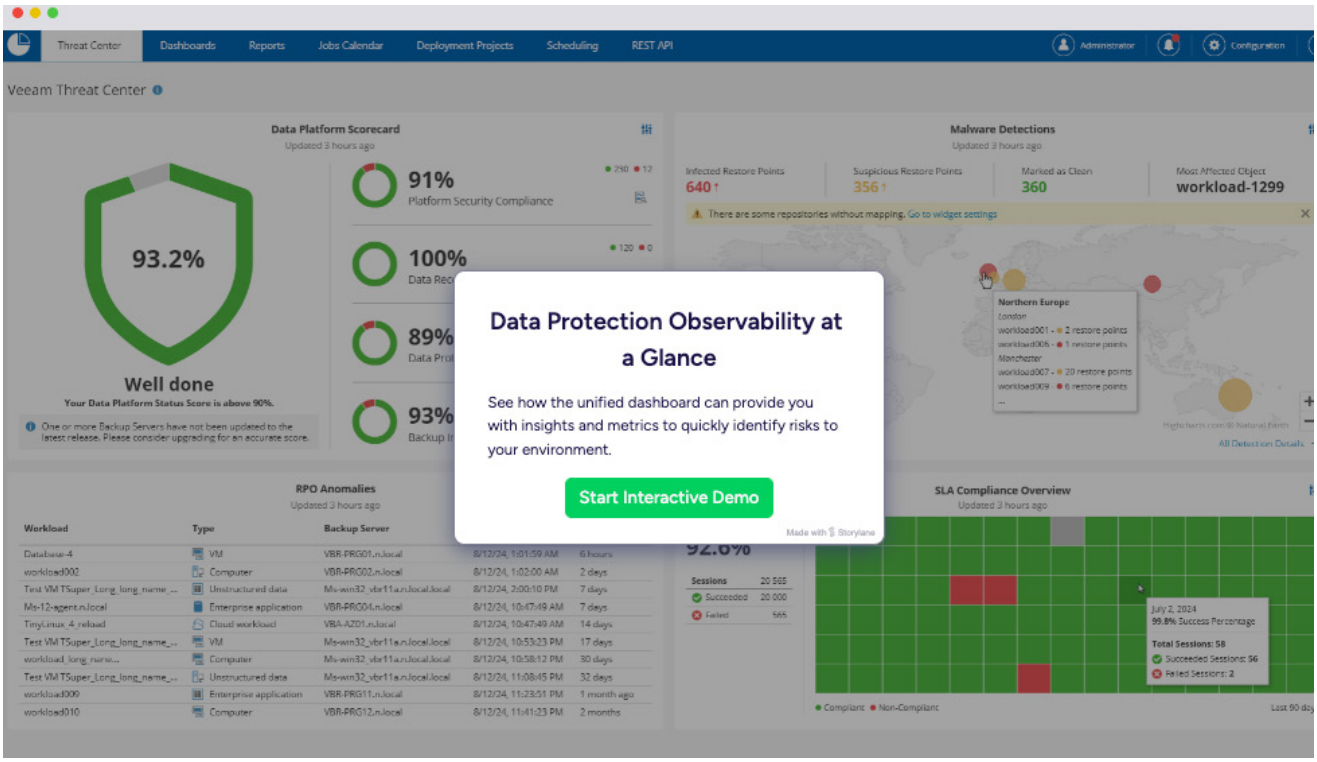
Les établissements doivent structurer leur gouvernance de continuité d'activité, définir des plans PCA/PRA, et réaliser des exercices terrain pour valider leur efficacité. Cette approche garantit la préparation et la réactivité face aux crises cyber.

Veeam soutient cette démarche par la supervision de la continuité d'activité, des outils de reporting, et des tests de restauration automatisés permettant de mesurer en permanence la résilience opérationnelle.

2. Politique et plans de sauvegarde (D2.O2)

L'objectif est de définir et maintenir à jour une politique de sauvegarde complète, couvrant l'ensemble des systèmes critiques, y compris les environnements SaaS. Les établissements doivent formaliser leurs plans de sauvegarde et de restauration pour garantir la cohérence et la traçabilité.

Veeam offre une gestion unifiée des politiques et plans de sauvegarde, avec une automatisation des processus et un suivi précis des opérations de restauration.



3. Sécurisation du système de sauvegarde (D2.O3)

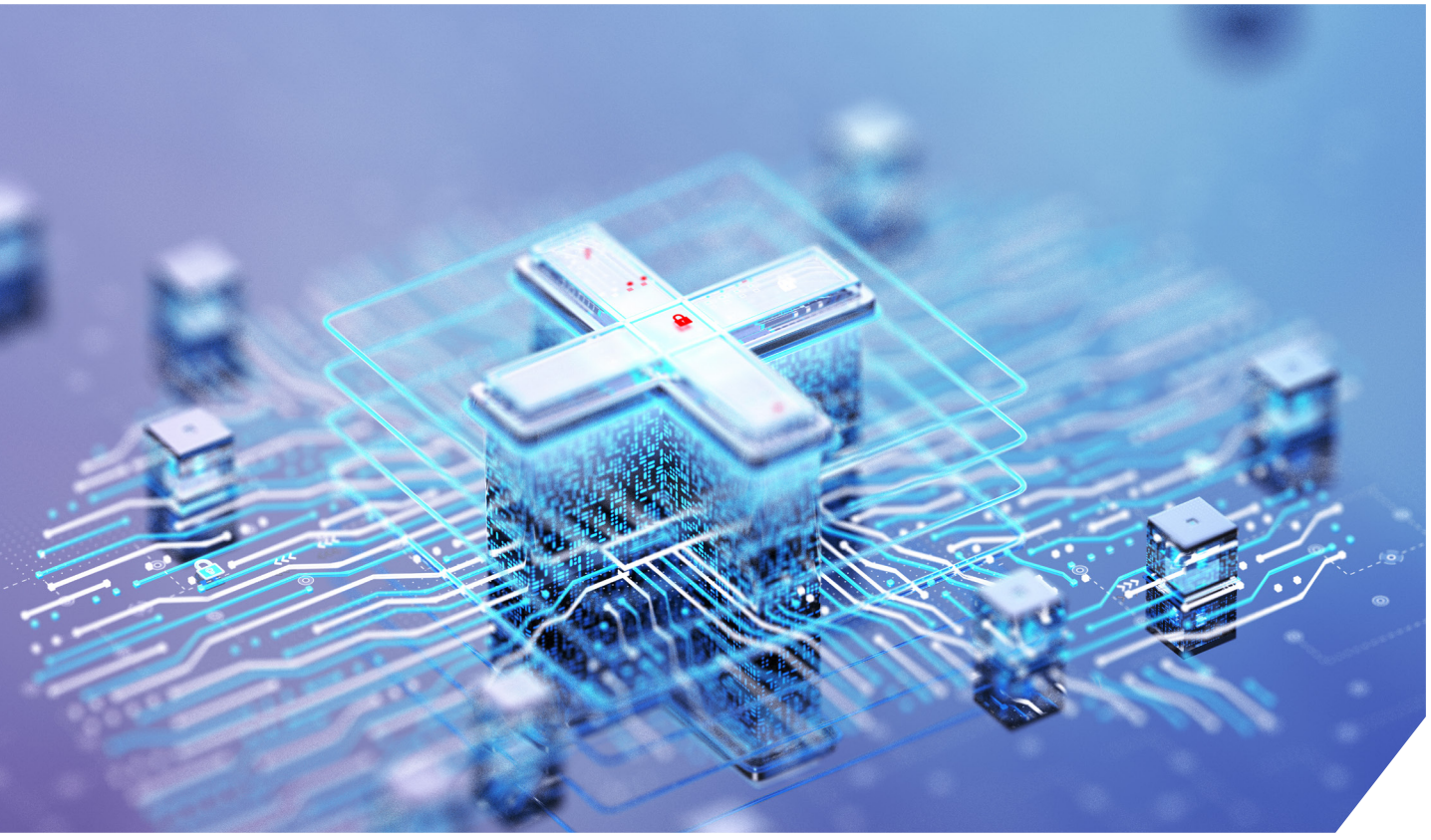
La sécurisation des infrastructures de sauvegarde repose sur une authentification indépendante, un cloisonnement réseau, la mise en œuvre de la règle 3-2-1-1-0, et une supervision continue. L'objectif est de protéger les données contre toute altération ou compromission.

Veeam intègre des mécanismes de sauvegardes immuables, une architecture Zero Trust, une détection des menaces cyber et des fonctions de supervision avancées pour garantir la fiabilité des copies et la conformité réglementaire.

4. Tests et validation (D2.O4)

Les tests réguliers de sauvegarde et de restauration sont essentiels pour garantir la capacité réelle de reprise. Ils permettent d'identifier les points de fragilité et de renforcer les plans PCA/PRA sur les systèmes critiques.

Veeam facilite ces tests grâce à leur automatisation dans des environnements isolés et à des rapports automatisés validant la conformité, l'efficacité et la fiabilité des restaurations pour pouvoir déclencher votre plan de reprise d'activité avec confiance.



Solution Brief

Comment Veeam soutient la conformité et la résilience du Domaine 2

Les solutions Veeam sont conçues pour répondre aux exigences du Domaine 2 en matière de sauvegarde, de restauration et de résilience numérique :

- Sauvegardes inaltérables protégeant contre les ransomwares ;
- Restauration rapide et orchestrée des systèmes critiques ;
- Supervision et reporting centralisés pour la conformité de l'Agence du Numérique en Santé ;
- Cloisonnement et Architecture Zero Trust ;
- Compatibilité avec les environnements cloud, on-premises et SaaS ;
- Tests et documentation automatisés de restauration et validation des plans PCA/PRA.
- Veeam Cyber Secure

Veeam Cyber Secure pose les fondations de la protection des données exigée dans le domaine 2 du programme CaRE via la gouvernance, l'architecture sécurisée et la montée en compétence. Il répond aux exigences de préparation aux incidents grâce à l'évaluation continue des risques, aux outils de réponse et à la veille sur les menaces.

Les piliers du nouveau programme Veeam Cyber Secure

Protéger

- Responsable de programme dédié
- Examen annuel de l'architecture et évaluation du degré de maturité de la résilience des données
- Formation d'ingénieur en cybersécurité
- Technical Account Manager (TAM)*

Construisez une base solide et sécurisée dès le premier jour.

Préparer

- Évaluations de sécurité trimestrielles
- Rapport de synthèse pour la direction
- Kit de réponse aux incidents
- Briefings trimestriels sur les cybermenaces

Restez en avance grâce à des conseils d'experts continus et des renseignements sur les menaces à jour.

Prévaloir

- Assistance rapide en cas d'incident
- Service Coveware pour la préparation et la réponse aux extorsions cyber*
- Garantie couvrant les frais de ransomware jusqu'à 5millions de dollars*

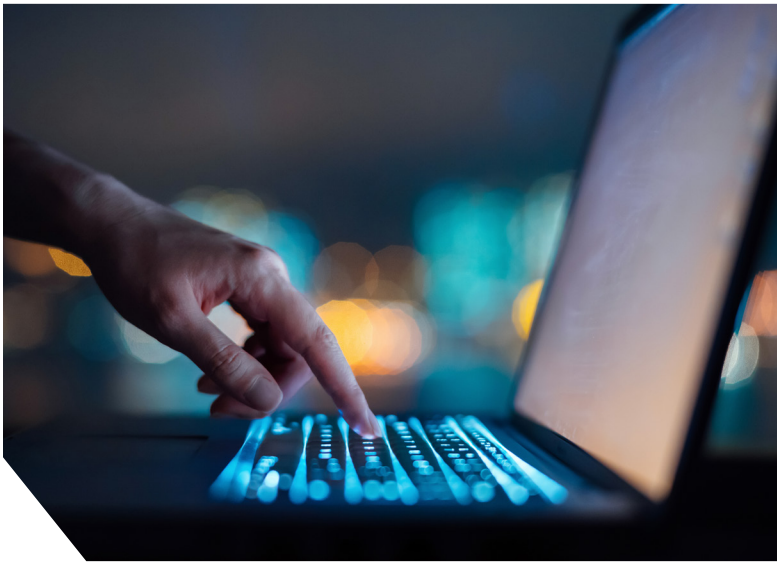
Soyez prêt à réagir et à vous remettre rapidement d'une attaque sereinement, en toute confiance, avec une protection financière.

* VCS Premium edition

Solution Brief

De la conformité à la confiance — La résilience comme avantage stratégique

La conformité au Domaine 2 ne constitue pas une simple obligation réglementaire : c'est une opportunité stratégique. En adoptant les principes de résilience et de protection des données soutenus par Veeam, les établissements de santé renforcent leur capacité à maintenir les soins, à protéger leurs données et à instaurer la confiance. La résilience devient un levier de performance et de crédibilité pour l'ensemble de l'organisation.



Passer à l'action avec le Domaine 2 du programme CaRE

Le Domaine 2 du programme CaRE est une étape clé pour renforcer la cybersécurité et la résilience des établissements de santé. Veeam s'impose comme un partenaire stratégique, offrant les technologies et l'expertise nécessaires pour atteindre les objectifs fixés par l'ANS. Sécuriser, sauvegarder et restaurer : trois actions essentielles pour garantir la continuité des soins et la confiance numérique.

À propos de Veeam Software

Pour Veeam®, leader mondial de la résilience des données, chaque entreprise doit avoir la totale maîtrise de l'ensemble de ses données, à tout moment et en tous lieux. Veeam assure la résilience des données grâce à des fonctions de sauvegarde, de restauration, de portabilité, de sécurité et d'intelligence des données. Basée à Seattle, Veeam protège plus de 550 000 clients dans le monde qui lui font confiance pour assurer le bon fonctionnement de leur entreprise. Allez sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.

→ En savoir plus : veeam.com