# SaaS-mageddon : pourquoi vos fournisseurs deviennent votre maillon faible

11 mai 2026 • Mis à jour le 17 mai 2026 • 8 min de lecture • 1199 mots • 49 vues • ♥

Trois compromissions d'Instructure en huit mois, ShinyHunters omniprésent : le SaaS est devenu le maillon faible structurel des SI. Analyse et angles d'attaque.

En huit mois, le même groupe a percé Instructure trois fois. Pendant ce temps, des centaines d'écoles signent des contrats SaaS sans même savoir qui héberge leurs données. On a déporté la valeur business dans le cloud sans déporter la responsabilité cyber. Le résultat est désormais sous nos yeux : la fuite n'est plus un événement, c'est un service récurrent.

## Le problème n'est plus le périmètre, c'est l'agrégation

Pendant vingt ans, les RSSI ont durci des périmètres. Pare-feu, EDR, SIEM, ZTNA — tout ce qu'il faut pour contrôler ce qui entre et sort. Très bien. Sauf qu'aujourd'hui, 70 % de la valeur business d'une organisation moyenne ne réside plus derrière ce périmètre. Elle est chez Salesforce, chez Workday, chez Notion, chez Instructure, chez n'importe quel fournisseur SaaS dont le contrat tient sur une page et dont le SOC 2 Type II n'a jamais été lu en interne.

Le problème n'est même plus que ces fournisseurs soient mal sécurisés individuellement. Le problème, c'est qu'ils agrègent. Quand ShinyHunters compromet Instructure, ils ne touchent pas une école — ils touchent 9 000 écoles d'un coup. Quand un opérateur Salesforce se fait piéger via OAuth, ce ne sont pas dix entreprises qui sont exposées, c'est l'ensemble du portefeuille du fournisseur qui passe en ligne de fuite potentielle. L'économie SaaS a créé des points de concentration de risque dont l'ampleur n'avait pas d'équivalent dans le monde on-premise.

## Le SOC 2 ne vous sauvera pas

Je vois passer des dizaines de questionnaires de tiers chaque mois en mission. La grande majorité demande la même chose : "Êtes-vous conforme à SOC 2 ? Avez-vous ISO 27001 ? Faites-vous des pentests