

Sécurité : CyberArk renforce son portefeuille SaaS

CyberArk, qui vient de rejoindre la [Microsoft Intelligent Security Association](#), a enrichi son offre SaaS (Software as a Service) de [sécurité des comptes et accès à privilèges](#).

Des nouveaux services et améliorations sont proposés :

CyberArk [Endpoint Privilege Manager](#), gestionnaire d'accès à privilèges pour terminaux sous Windows et macOS, inclut désormais une fonctionnalité d'accès « juste à temps ».

Les équipes IT et les fournisseurs de services managés de sécurité peuvent ainsi fournir un accès administrateur à la demande aux terminaux concernés pendant une période donnée. Ils disposent d'un journal d'audit et peuvent supprimer l'accès, si besoin.

Par ailleurs, le service CyberArk [Privilege Cloud](#) inclut de nouvelles fonctionnalités conçues pour les entreprises de taille intermédiaire. Les organisations disposent de capacités renforcées de gestion en continu des identifiants à privilèges.

L'éditeur met l'accent sur « la prise en charge de plus de 150 intégrations prêtes à l'emploi pour la gestion des identifiants et des sessions à privilèges » via sa [Marketplace](#). Un ensemble conçu pour faciliter l'intégration dans l'infrastructure existante du client.

L'entreprise a également annoncé la disponibilité, dans les prochaines semaines, d'Alero.

CyberArk Alero

La nouvelle offre SaaS [CyberArk Alero](#) fournit un accès « Zero Trust » aux fournisseurs tiers qui se connectent à distance à la solution CyberArk Privileged Access Security.

L'objectif est de réduire les risques de piratage.

Pour ce faire, l'approche « Zero Trust » (ou la confiance zéro en matière de sécurité réseau, qui implique de toujours vérifier avant d'autoriser), l'authentification biométrique et la mise à disposition au moment voulu (just-in-time provisioning) sont combinées.

Gil Rapaport (CyberArk) l'a expliqué dans un [billet de blog](#) :

« Les fournisseurs qui se connectent à distance n'ont plus à s'inquiéter de VPN, d'agents ou de mots de passe lorsqu'ils obtiennent un accès privilégié à des systèmes internes critiques. Ils ont simplement besoin d'un smartphone ordinaire et de CyberArk Alero. »