Gestion d’accès à privilèges : BeyondTrust et ServiceNow toujours plus intégrés

BeyondTrust confirme la disponibilité de Defendpoint 5.3, sa solution de gestion d’accès à privilèges (PAM) de postes de travail sous Windows et macOS.

Une solution orientée vers les administrateurs IT.

Defendpoint inclut désormais un moteur de règles métier (Power Rules) permettant d’autoriser ou non une application à s’exécuter, ou à s’exécuter avec des droits adminsitrateur. Et ce en automatisant l’intégration de sources tierces. ServiceNow, partenaire technologique de BeyondTrust, est la première intégration promue.

En s’appuyant sur PowerShell (le langage de script orienté objet développé par Microsoft), les entreprises utilisatrices peuvent écrire un script et l’intégrer dans la règle elle-même « facilement », selon les promoteurs de l’offre.

Ainsi, il est possible de faire remonter automatiquement un incident dans la plateforme de gestion des services informatiques (ITSM) de ServiceNow, ou d’annuler la requête.

Le ticket ServiceNow inclut, entre autres, le nom du programme et de son éditeur, le chemin d’accès ainsi que la justification « métier » fournie par l’utilisateur final.

ServiceNow Workflow

Un administrateur peut « agir sur l’incident dans ServiceNow et adresser un code de réponse à l’utilisateur », a précisé BeyondTrust par voie de communiqué.

Ce code de réponse peut être utilisé pour « déverrouiller » l’application et autoriser son exécution. « Toute application conforme à la règle déclenchant alors le workflow ServiceNow ».

Les Power Rules intégrées à Defendpoint permettent d’autres intégrations. Pour établir, par exemple, une interface avec un système de supervision des vulnérabilités CVE (Common vulnerabilities and exposures).

(crédit photo de une © shutterstock)