Les menaces liées aux accès privilégiés en France en 2019

73%

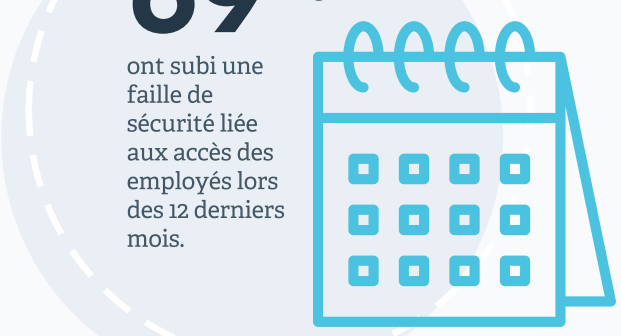
des sondés français pensent que leur entreprise sera victime d'une faille de sécurité et d'une fuite d'informations liées à l'accès des fournisseurs tiers, des employés ou des périphériques iOT d'ici 2 ans si leurs processus et leurs solutions PAM restent inchangés.

72%

confirment que les compromissions par les insiders sont la plus grosse menace à laquelle ils sont confrontés pour la sécurité de leurs réseaux.

69%

ont subi une faille de sécurité liée aux accès des employés lors des 12 derniers mois.

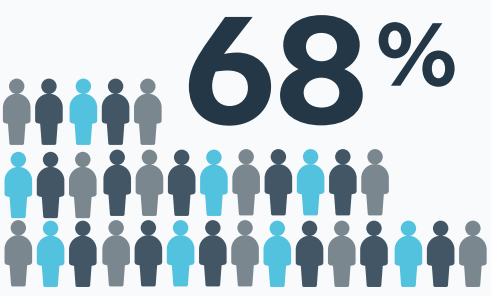


92%

pensent qu'il est important que leurs solutions PAM soient intégrées mais seulement...

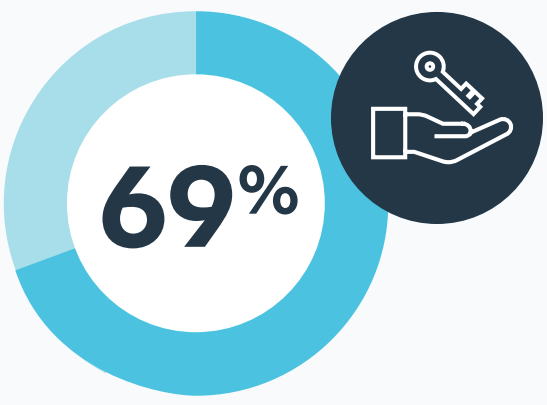
...43%

pensent que c'est réellement le cas.



68%

partagent des identifiants privilégiés ou admin entre plusieurs employés.



69%

ont vu le nombre de leurs tiers accédant à leurs réseaux augmenter de plus de **20%** au cours des 2 dernières années.

Seuls 17%

font entièrement confiance à leurs tiers.

71%

savent avec exactitude combien d'appareils IoT accèdent à leurs systèmes et réseaux. [**chiffre le plus bas de l'étude par rapport aux autres pays interrogés**]

Seuls 14%

pensent avoir éliminé les menaces liées aux appareils IoT et 17% pour les appareils BYOD.

D'après les résultats de l'étude BeyondTrust Privileged Access Threat Report 2019 (chiffres France)