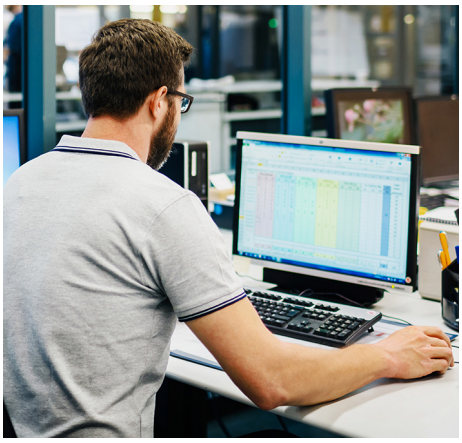
opentext™



Rationalisez l'accès au mainframe grâce à Automated Sign-On

Albert Einstein a dit : « La folie, c'est de faire toujours la même chose et de s'attendre à un résultat différent. » De la même manière, il est absurde d'espérer sécuriser davantage l'accès au mainframe en appliquant les mêmes mesures de sécurité année après année.

Si les mesures de sécurité en matière d'accès aux applications d'entreprise ont évolué pour faire face aux nouvelles menaces de sécurité, celles qui ont trait aux applications des mainframes, elles, n'ont pas changé depuis des décennies. Trois causes principales expliquent cette stagnation :

- Premièrement, les applications héritées installées sur les mainframes jouent toujours un rôle crucial dans la plupart des entreprises. Les modifier est donc à la fois risqué, difficile et coûteux. De plus, il est quasiment impossible de trouver les ressources humaines nécessaires pour mettre à jour les contrôles d'accès de sécurité pour ces applications.
- Deuxièmement, les grandes entreprises sont souvent peu enthousiastes à l'idée d'ouvrir la boîte de Pandore qu'est le mainframe. Le service informatique se dit : « Et si nous cassions quelque chose ? Et si c'était beaucoup plus compliqué que prévu ? Et si cela nuisait à notre entreprise ? Nous ne pouvons pas sécuriser le mainframe et résoudre tous les problèmes tout en poursuivant nos activités... De plus, le coût (en temps et en argent) de la duplication de cet environnement serait trop élevé. »
- Troisièmement, les entreprises ont l'impression que le mainframe est en sécurité derrière le pare-feu et que seuls les utilisateurs autorisés peuvent y accéder. Mais il est tout à fait possible qu'une personne malveillante vole ou pirate les informations d'identification d'un autre utilisateur afin d'y accéder. Ces anciennes applications utilisent des mots de passe faibles, à huit caractères et non sensibles à la casse. Aucun administrateur réseau au monde n'estime que ces mots de passe permettent de protéger quoi que ce soit, et encore moins les informations protégées par la propriété intellectuelle et relatives aux clients.

La question est de savoir comment mettre fin à ce comportement complètement insensé alors qu'il repose sur des peurs bien réelles et justifiées.

La discordance entre les systèmes de sécurité de l'entreprise

La plupart des entreprises comptent deux systèmes de sécurité. Le premier est le système Identity and Access Management (IAM), utilisé pour donner accès aux ressources et applications de l'entreprise. Les systèmes IAM nécessitent l'utilisation d'un mot de passe complexe (comprenant généralement au moins 12 caractères, des minuscules et des majuscules, des chiffres et des caractères spéciaux). Les mots de passe complexes sont beaucoup plus difficiles à pirater ou à voler.

Les systèmes de mainframe ont également leur propre type de gestion des identités et des accès, généralement appelé RACF ou Top-Secret. Ces solutions permettent d'authentifier et d'autoriser l'accès aux ressources du mainframe. Le problème est que les applications qui utilisent ces systèmes ne requièrent que des mots de passe faibles à huit caractères.

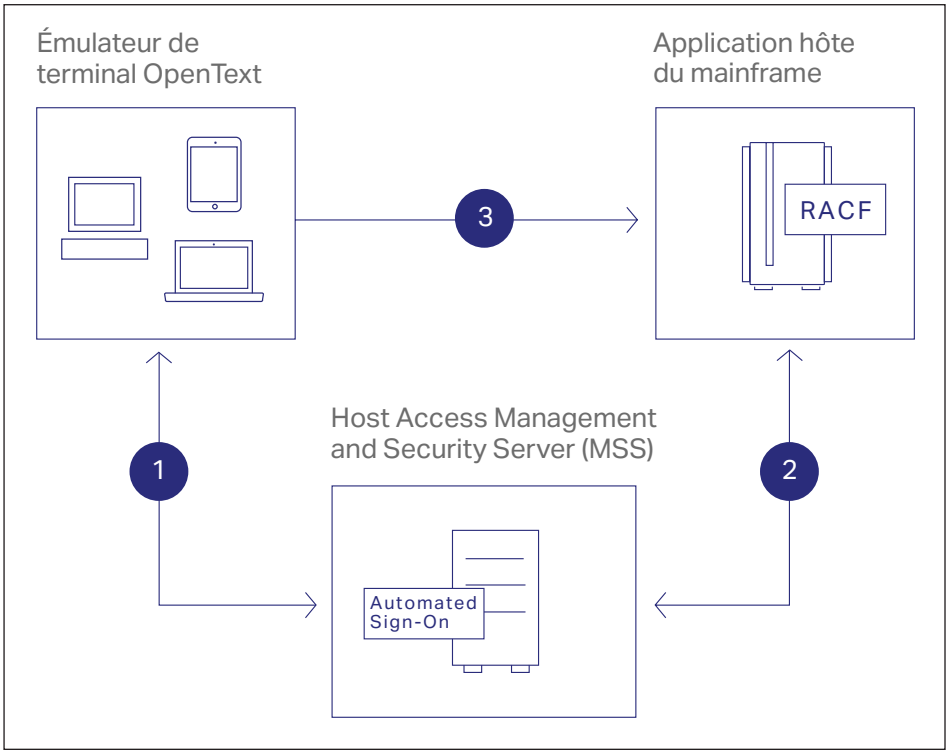
Il existe donc deux systèmes distincts permettant d'accéder aux ressources d'entreprise. Mais pourquoi exiger une authentification complexe pour permettre l'accès aux applications d'entreprise et se contenter d'une authentification faible pour permettre l'accès aux applications stratégiques de mainframes, sur lesquelles repose l'entreprise ? Cela n'a aucun sens.

En finir avec cette folie

Et si nous vous disions que vous pouvez utiliser votre système IAM pour contrôler et gérer l'accès à votre système hôte ? La solution : OpenText™ Host Access Management and Security Server (MSS).

MSS permet d'intégrer votre mainframe à votre système de gestion des identités et des accès (IAM) existant. MSS ajoute un point de contrôle de sécurité entre vos systèmes hôtes et les utilisateurs qui ont besoin d'accéder au mainframe. Il utilise votre structure IAM existante (et plus particulièrement son authentification complexe) pour autoriser l'accès au mainframe.

MSS comprend également le produit complémentaire Automated Sign-On for Mainframe pour vous permettre de rationaliser encore plus vos systèmes. Automated Sign-On for Mainframe permet aux utilisateurs de se connecter automatiquement aux applications du mainframe, leur évitant ainsi de devoir saisir des identifiants et des mots de passe. Imaginez un peu : plus aucun mot de passe pour accéder au mainframe.



1. L'émulateur démarre une session et demande à Automated Sign-On de lui fournir les informations d'identification de l'utilisateur pour accéder à l'application hôte.
2. Automated Sign-On demande des informations d'identification PassTicket à usage unique au système RACF et les renvoie à l'émulateur.
3. L'émulateur utilise les informations d'identification PassTicket à usage unique pour connecter automatiquement l'utilisateur à l'application hôte.

MSS propose également d'autres produits complémentaires qui renforcent considérablement la sécurité de l'accès aux hôtes :

- **Extension Security Proxy :** fournissez un chiffrement de bout en bout et contrôlez l'accès au périmètre au moyen d'une technologie de sécurité brevetée.
- **Extension Advanced Authentication :** activez l'authentification multi-critères pour autoriser l'accès à vos précieux systèmes hôtes.
- **Extension PKI Automated Sign-On :** connectez-vous automatiquement à vos systèmes d'entreprise stratégiques à l'aide d'une infrastructure de clés publiques.
- **Extension Terminal ID Management** : allouez dynamiquement des ID de terminal en fonction du nom d'utilisateur, du nom DNS, de l'adresse IP ou de la réserve d'adresses.

MSS et ces produits complémentaires tirent parti de vos ressources et infrastructures existantes pour que vous puissiez utiliser ce que vous avez déjà mis en place afin de sécuriser et gérer l'accès aux hôtes. Ils apportent une valeur métier durable et réduisent le coût d'investissement. De cette manière, ils participent également à la rationalisation de la sécurité de l'entreprise.

Pour en savoir plus, rendez-vous sur : **www.opentext.com**

Communiquez avec nous

261-FR0182-002 | O | 02/24 | © 2024 Open Text

opentext™