

## Le CERN déploie des clés YubiKey pour protéger les comptes d'administration et l'accès aux serveurs



Étude de cas



supplier

Industrie  
Recherche scientifique

Protocoles  
OTP, U2F

Produits  
YubiKey 4

Déploiement  
Employés

### À propos du CERN

Fondé en 1954, le CERN est le Centre européen pour la recherche nucléaire et l'un des centres de recherche scientifique les plus respectés au monde. Situé près de Genève, l'établissement abrite certains des instruments scientifiques les plus grands et les plus complexes au monde utilisés pour étudier la matière et fournir des aperçus sur les lois fondamentales de la nature.

### Protection des comptes d'administrateur et des accès

En tant que grand organisme de recherche de renommée mondiale, le CERN devait trouver un moyen de sécuriser l'accès à ses actifs les plus critiques. Comme l'organisation dispose de nombreux services informatiques critiques ainsi que des opérations sur les accélérateurs, la protection des comptes pour les administrateurs et les opérateurs était devenue une préoccupation majeure.

« Nous évaluons en permanence notre empreinte de sécurité et, tout en continuant à améliorer notre sécurité informatique, nous avons identifié un certain nombre de comptes qui pourraient être considérés comme un point unique de défaillance. C'est pourquoi nous avons choisi de déployer l'authentification multifactorielle. »

— Stefan Lueders, CISO, Département informatique du CERN

### Évaluer la bonne solution 2FA

Dans le cadre des futurs plans de déploiement, il était important que le CERN choisisse une solution d'authentification simple à utiliser et pouvant être facilement intégrée dans divers systèmes. L'organisation adhère à une politique BYOD (bring your own device, « apportez vos appareils personnels »), de sorte que la flexibilité de travailler avec plusieurs systèmes d'exploitation, y compris Linux, Mac OS et Windows, a été une considération clé pour l'organisation. L'objectif était de pouvoir déployer une solution pour tous les utilisateurs avec des exigences minimales en matière de backend.

Étant donné l'impossibilité d'avoir une solution miracle dans l'environnement universitaire du CERN, le CERN a examiné plusieurs options d'authentification pour les utilisateurs. Ils voulaient également envisager un périphérique d'authentification matériel pour plus de commodité. Les cartes à puce ont été envisagées au départ, mais elles étaient trop difficiles à intégrer en raison du besoin de pilotes et de lecteurs coûteux.

Dans sa recherche d'une solution simple et robuste, l'équipe du CERN a choisi la clé YubiKey, qui répondait à tous les critères préétablis de convivialité et d'intégration.

Vincent Brillault, Sécurité informatique et réponse aux incidents, Département informatique du CERN

« Nous avons choisi la clé YubiKey parce que nous avons trouvé qu'elle s'intègre assez facilement avec n'importe quel système d'exploitation et avec n'importe quel client. Nous pouvions donc la déployer pour tous nos utilisateurs, sans avoir à changer quoi que ce soit du côté des utilisateurs. »

---

Étude de cas



supplier

Industrie

Recherche scientifique

Protocoles

OTP, U2F

Produits

YubiKey 4

Déploiement

Employés

---

## Protéger les employés et les clients grâce à une forte 2FA

La clé YubiKey peut facilement s'intégrer à tout système ou client existant, et fournir une protection transparente à l'utilisateur par une simple pression sur la clé. Cela a rendu la clé YubiKey facile à déployer du point de vue de l'utilisateur. Non seulement cela a éliminé la nécessité de changer quoi que ce soit aux périphériques ou aux systèmes utilisés par les employés, mais cela a également permis au CERN de maintenir ses propres déploiements du côté serveur.

### Mise en œuvre de la clé YubiKey

En 2012, la mise en œuvre initiale de la clé YubiKey s'est déroulée sur quelques mois, avec un déploiement concentré au sein de l'équipe de sécurité informatique du CERN. Depuis lors, le déploiement de YubiKey s'est étendu à un public plus large au sein de l'informatique et au-delà, à commencer par les administrateurs Windows. Actuellement, la clé YubiKey est utilisée comme l'un des nombreux tokens d'authentification multi-facteurs lors de la connexion unique pour les applications Web et pour la connexion SSH aux serveurs.

Stefan Lueders, CISO, Département informatique du CERN

« En ce qui concerne le déploiement et l'utilisation de la clé YubiKey, si notre personnel ne dit rien, c'est un signe qu'ils sont généralement heureux. Vu le silence, la clé YubiKey a été un véritable succès. »

### L'avenir de l'authentification forte au CERN

À l'avenir, le CERN prévoit de déployer des clés YubiKey dans l'ensemble de l'organisation, y compris tous les administrateurs du département informatique et certains utilisateurs ayant un accès administratif aux systèmes du centre de données en dehors du département informatique.

---

« C'est ici que l'équipe de sécurité a sa tâche principale. Trouver le bon équilibre entre un niveau de sécurité accru grâce à l'authentification multi-facteurs, dont la clé YubiKey, et un déploiement de solutions aussi simples pour notre communauté élargie d'utilisateurs que pour les administrateurs, afin que nos utilisateurs ne commencent pas à chercher d'autres moyens de contourner la solution. »

— Stefan Lueders, CISO, Département informatique du CERN

---

---

**À propos de Yubico** Yubico établit de nouvelles normes mondiales pour un accès facile et sécurisé aux ordinateurs, serveurs et comptes Internet. Fondée en 2007, Yubico est une entreprise privée qui possède des bureaux en Australie, en Allemagne, à Singapour, en Suède, au Royaume-Uni et aux États-Unis. Découvrez pourquoi neuf des 10 plus grandes marques Internet et des millions d'utilisateurs dans plus de 160 pays utilisent notre technologie sur [www.yubico.com](http://www.yubico.com).

**Yubico AB**  
Kungsgatan 44  
2<sup>nd</sup> floor  
SE-111 35 Stockholm  
Sweden

**Yubico Inc.**  
530 Lytton Avenue, Suite 301  
Palo Alto, CA 94301 États-Unis  
844-205-6787 (numéro vert)  
650-285-0088