



Utilizziamo il cloud AWS

PERCHÉ LE ORGANIZZAZIONI SCELGONO **FOXPASS + SSO**

Perché le organizzazioni usano Foxpass
oltre al proprio provider SSO/SAML:



Autenticazione
sulle reti Wi-Fi



VPN



Client
LDAP



Autenticazione
sui dispositivi

Automatizza il provisioning con la sincronizzazione automatica tra Foxpass e la tua directory principale

Oltre 100.000 dipendenti sono gestiti con Foxpass

hackerone



greenlots
A Member of the Shell Group



lyft

imgur



Rollbar



Segment

Controllo degli accessi per **reti wireless e cablate**

Cosa facciamo:

Offriamo, a scelta

- RADIUS ospitato nel cloud basato su nome utente/password
- RADIUS ospitato nel cloud basato su certificati
- PKI (SCEP): elimina la necessità di password, poiché solo i dispositivi con certificati installati possono accedere alla rete.

Perché proteggere la rete:

- Proteggere i dispositivi di rete dagli attacchi (computer, storage collegato, stampanti, ecc.)
- Difendersi dagli attacchi man-in-the-middle
- Fermare chi ruba larghezza di banda
- Impedire ai non dipendenti di usare l'indirizzo IP aziendale
- Requisiti di conformità PCI, SOX, SOC2 e HIPAA

Integrazione con OKTA:

- L'utente finale può usare la password Okta esistente per connettersi al Wi-Fi (con il metodo nome utente e password)
- Utenti e gruppi vengono sincronizzati automaticamente da Okta

Che cos'è RADIUS?

Mentre l'accesso wireless a casa o in un bar richiede che tutti conoscano la password condivisa, in un'azienda ogni utente dovrebbe avere credenziali proprie. RADIUS è il protocollo usato dall'access point per autenticare un utente rispetto a un'origine di credenziali.

E inoltre?

- Supporto completo degli attributi RADIUS
- Log RADIUS, con la possibilità di trasmetterli in streaming tramite AWS Kinesis per renderli accessibili in un SIEM come SPLUNK o SumoLogic
- Supporto di RadSec

Quanto costa?

Vedi <https://foxpass.com/pricing/>

(Sconti per acquisti annuali, organizzazioni non profit, MSP e grandi clienti)

