Centrify
THE BREACH STOPS HERE

yubico

Context-based Adaptive Authentication with Yubico and Centrify

CENTRIFY ALLIANCE

The rise of cloud and mobile means that business employees are using more varied devices than ever to access an ever-growing number of cloud and on-premises apps — each with their own username and password. With so many credentials to remember, employees resort to re-using simple passwords across apps and devices which makes it easy for hackers to guess or steal credentials. Centrify and Yubico provide a frictionless security solution that eliminates passwords, bolsters security, and provides secure access to apps, devices, and IT resources.

Centrify Single Sign-on & Provisioning

Eliminate Passwords Wherever Possible and Insist on Multi-factor Authentication for Critical Apps

Corporate data is officially well outside the boundaries of the traditional network. Mobile devices and cloud applications have paved the way for a new type of mobile workforce that demands to be productive anywhere, at any time. Without the protection of the corporate firewall and security perimeter, all that stands between attackers and business data are simple usernames and passwords.

Given the massive amount of credentials that have been compromised in the recent past, it's safe to assume that every password has been stolen, and made available to attackers.

Multi-factor authentication (MFA) reduces the risk of compromised credentials, but is often too cumbersome for end users, or — in the case of smart cards — requires dedicated readers on all end-user devices. Companies are looking to bolster security, and prevent attacks based on compromised credentials: but must balance the security of any solution with employee satisfaction.

Centrify and Yubico Protect You from Hackers Compromising Your Credentials

Centrify Identity-as-a-Service + Yubico YubiKeys = Productive and Safe Users

With password theft rampant, and headline-level breaches a near-daily event, Multi-factor authentication has become critical for every business. Yubico and Centrify provide simple, context-based, adaptive authentication across enterprise users and resources. Whether it's for PIV-based authentication, OATH one-time passwords, or as a physical NFC token for mobile devices — Centrify and Yubico provide IT the flexibility to enforce security without user frustration.

Centrify's Identity Platform provides the policy layer that lets IT create adaptive rulesets to integrate MFA into cloud apps, on-premises apps, servers, smartphones, Macs, and more. And thanks to the simplicity, portability, and flexibility of YubiKeys, users always have a secure second factor that works across devices.

This integration means IT has the flexibility to provide simple Multi-factor Authentication no matter what their authentication requirements. The Centrify Identity Platform leverages multiple capabilities in the Yubikey — PIV, OATH OTP, or physical NFC token — for secure adaptive authentication without hassles. Centrify can leverage the Yubikey for use cases such as:

- Smartcard AD-based login to Mac or Linux
- Re-authentication for privilege escalation on Windows
- Smartcard login to Centrify's cloud service for SSO, secure remote access, or administration
- Yubikey OATH H/TOTP for as a second factor for secure SSO to individual cloud applications, or to a portal of cloud apps
- Yubikey as OATH H/TOTP for MFA to servers for privileged session control
- Yubikey as physical NFC token for MFA to secure access to apps on mobile devices

How Does It Work?

A login can be as simple as plugging the YubiKey into your device and typing a PIN (smartcard login), in order to gain access to a secure cloud application. In other cases, users may make use of NFC merely touch the YubiKey against their mobile device for quick and easy authentication to apps, servers, and more. Enrolment is streamlined, and policy is created simply and enforced across all business users.

5000+ Customers, including over half of the Fortune 100, rely on Centrify

Centrify
THE BREACH STOPS HERE

yubico

Centrify and Yubico support FIDO U2F

The partnership between Yubico and Centrify, both members of the Fast IDentity Online Alliance (FIDO), further acceleratesthe adoption of multi-factor authentication. Using the specially designed FIDO U2F Security Key by Yubico with Centrify's support for the FIDO Alliance's Universal 2nd Factor (U2F) specification, the Centrify Identity Platform provides the broadest IAM support for various use cases across platforms, devices, and apps. This includes:

- FIDO U2F within the Centrify platform
- NFC for login to smartphone apps
- OATH-HOTP for secure SSO to cloud apps and servers
- Smart card PIV re-authentication for Windows privilege escalation
- Active Directory-based login to Mac OS X and other platforms to meet NIST regulations

By extending its current authentication methods, Centrify gives enterprises the option of using devices that comply with the FIDO U2F requirement as well as meet NIST 800-63b strongest Authentication Assurance Level 3 requirements when combined with the user's password.

Advantages of FIDO U2F include:

- **Heightened security** - public key cryptography protects against phishing, session hijacking and malware attacks
- **Increased ease of use** - no codes to re-type and no drivers to install
- **Higher privacy** - no personal information is associated with a key
- **Scalable usage** - unlimited number of accounts can be protected by one single device

More about the FIDO U2F Security Key

Each Security Key has an individualized secure chip which performs cryptographic functions triggered by a simple touch of the key. You never see the details, but behind the scenes a FIDO U2F Security Key provides a unique public and private key pair for each application it protects. Only those keys can correctly complete the cryptographic challenge required for login.

The secure chip is of the same class as those used in SIM Cards, electronic passports, military electronic IDs and chip-and-pin credit cards. Like those devices, the chip is specially "hardened" so it's extremely difficult to steal the secrets hidden inside. The secrets contained in the Security Key belong to the end-user exclusively and are never transferred, copied or stored by a service provider or any other application provider.

Benefits for IT

- Use Multi-factor Authentication Everywhere
- Protect Sensitive Commands with MFA
- Protect Sensitive Servers with MFA
- Protect High Value Apps with MFA
- Easy to implement using existing AD

Benefits for End Users

- Secure single sign-on — across devices
- No passwords to remember or create
- Fast, easy authentication
- Support for all popular mobile devices and laptops
- Logins are no longer a barrier to productivity

Benefits

- **Simplify security:** One platform secures all your users, and one Yubikey enables MFA across devices, apps, and servers
- **Speed adoption:** Users get secure access to the apps they need, from the devices they choose — without training or confusion
- **Save cost:** Eliminate helpdesk calls for password reset thanks to secure SSO across devices
- **Meet regulations:** Enable BYOD while still complying with NIST regulations requiring smartcard authentication

Centrify
THE BREACH STOPS HERE

As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit **www.centrify.com**. The Breach Stops Here.

SANTA CLARA, CALIFORNIA	+1 (669) 444 5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11 3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	sales@centrify.com
WEB	www.centrify.com

BRF003415EN-12152017