



# COMPARING DUO SECURITY TO IDaaS Vendors

Multi-factor authentication (MFA) is one of several products offered by Identity-as-a-Service (IDaaS) vendors alongside cloud-based directory, provisioning and deprovisioning, single sign-on, etc. IDaaS vendors offer MFA bundled with their IDaaS solution to secure access to cloud-based applications.

A bundled MFA solution may look attractive on paper from cost and vendor consolidation standpoint, but there are other requirements that should be considered when evaluating an MFA solution:

- Time to deploy or coverage
- End user productivity
- Security efficacy
- Product architecture

- Compliance requirements

Duo Security does not publish or endorse negative views of competitive vendors. Instead, here are some points to consider when comparing Duo's Trusted Access platform to IDaaS vendors.

## The Duo Advantage

### END-USER PRODUCTIVITY

#### Ease of Use

End users have the flexibility to choose between several authentication options such as Duo Push, OTP, U2F, SMS and phone callback

#### User Experience

Consistent workflow for users to access all of their applications (on-premises and cloud)

#### New User Enrollment

Users can enroll within minutes using options such as in-line, self-service portal, in person, etc.

#### Help Desk Resources

Several enrollment and self-service options reduce help desk volume up to 75%

### TIME TO SECURITY

#### Application Integrations

*Includes on-premises apps such as VPN, RDP and cloud apps such as Office 365, Google, etc.*

Unlimited application integrations with several out-of-the-box integrations for VPNs, RDP, SSH, email, and cloud apps

#### Custom Applications

Admins can integrate customer applications using APIs and SDKs without any professional services

#### Documentation & Support

##### Publicly available

Integrations are well-documented and available to all administrators

## SECURITY EFFICACY

---

### Device Identification

Distinguish a personal device from a corporate-owned device

### Insight into Devices

*(OS, browsers, Flash, Java)*

Deep insights into security posture of devices without using any agents

### Remediation

Users are notified when running out-of-date software and can self-update

### Policies & Controls

Admins can set policies for each application: on-premises or in the cloud, based on users and devices

## SECURITY ARCHITECTURE

---

### Separation of Primary and Secondary Credentials

Organizations integrate Duo with their primary identity source. Ex: Active Directory. Duo only provides secondary authentication

## COMPLIANCE

---

### EPCS Requirements

*Electronic Prescription of Controlled Substances*

Duo has been audited by a DEA-accredited third-party vendor to meet two-factor authentication (multi-factor) requirements for EPCS

### HIPAA Patient Data Security

*Health Insurance Portability and Accountability Act*

Provides visibility into users and devices accessing patient data



# The Most Loved Company in Security

Duo Security makes security painless, so you can focus on what's important. Duo's scalable, cloud-based Trusted Access platform addresses security threats before they become a problem. Thousands of organizations worldwide use Duo, including Facebook, Panasonic and MIT. Duo is backed by Google Ventures, True Ventures, Radar Partners, Redpoint Ventures and Benchmark. Duo is located from coast to coast and across the sea.

North America

**866.760.4247**

Europe, Middle East & Africa

**+44 8003 585 309**

Email

**sales@duo.com**