

Duo für...

CISCO Duo Security is now part of Cisco.

# DSGVO

Duo unterstützt Unternehmen dabei, sich auf die Anforderungen der Datenschutz-Grundverordnung (DSGVO) schnell und einfach vorzubereiten.

## DIE HERAUSFORDERUNG:

# Schutz von personenbezogenen Daten für EU-Bürger

Datensicherheit ist eines der wichtigsten Sicherheitsbedenken für Unternehmen weltweit. Der Europäischen Union (EU) hat die stärksten Schritte unternommen, um die Datensicherheit für seine Bürger zu gewährleisten. Das Gesetz – Datenschutz-Grundverordnung (DSGVO) wurde in der EU verabschiedet, um den Einwohnern eine bessere und stärkere Kontrolle über das Speichern und die Nutzung ihrer persönlichen Daten zu ermöglichen.

Erhebliche Geldstrafen erwarten Unternehmen die sich nicht an DSGVO Bestimmungen halten.

Am 25. Mai 2018 hat die DSGVO alle ehemaligen Datenschutzgesetze der EU ersetzt und diese stärker an moderne Technologielandschaften angepasst. Dieses Gesetz betrifft alle Unternehmen und Organisationen, die personenbezogene Daten von EU-Bürgern erheben und verarbeiten, unabhängig davon wo auf der Welt die sich befinden.

Die DSGVO regelt wie Organisationen mit personenbezogenen Daten umgehen und diese schützen und wie sie Datenschutzverletzungen melden sollen. Das Gesetz hat schwerwiegende Konsequenzen für pflichtwidriges Verhalten. Die finanziellen Sanktionen können bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes einer Organisation betragen (je nachdem, welcher Wert höher ist).

“

**Duo was the flexible and agile solution we needed for a company that's rapidly growing.”**

Marian Danisek

IT Infrastructure and Operations Manager, Tajco

Duo lässt sich mit die beliebtesten Apps integrieren, unter anderem:



## UNSERE LÖSUNG:

# Secure Access mit Duo

Die drei Vorteile von Duo Secure Access:

## 01

### Zeit Sparen

Überprüfen Sie die Identität Ihrer Benutzer bevor Sie den Zugriff auf Anwendungen gewähren, welche möglicherweise persönliche Informationen speichert, mit einer starken 2-Faktor Authentifizierung.

Und verstärken Sie Benutzerzugriffsrichtlinien, um Anmeldungen basierend auf IP, Länder, anonymen Netzwerken usw. zu blockieren, um die Kontrolle zu stärken.

## 02

### Überprüfen Sie den Zustand aller Benutzergeräte

Verschaffen Sie sich einen Überblick und die Fähigkeit, Unternehmens- und persönliche Geräte die auf Ihre Unternehmensanwendungen zugreifen zu identifizieren, und ermitteln Sie, welche den zugänglichen Geräten ohne einen Agenten verwaltet oder veraltet sind.

Zusätzlich können Sie die Sicherheitshygiene der Benutzergeräte überprüfen bevor Sie den Zugriff gewähren und blockieren, benachrichtigen oder beschränken, je nach Risikozustand des Gerätes.

## 03

### Sicherer Zugriff auf alle Anwendungen

Verwalten Sie auf welche internen Apps Remotebenutzer zugreifen können, um die Gefährdung von persönlichen Informationen zu begrenzen und setzen Sie diese durch Zugriffsrichtlinien auf Anwendungsebene.

Sichern Sie VPNs und RAS-Gateways wie Cisco, Juniper usw., um Anwendungen mit vertraulichen Informationen eine weitere Sicherheitsebene hinzuzufügen.



**Duo's just been really simple, straightforward, and it hasn't got in the way of what we've been trying to do."**

Richard Fuller

Linux and Information Security Team Leader

