# NTIVA MULTI FACTOR AUTHENTICATION (MFA)

Data Sheet

**Ntiva**
Managed IT & Cloud Services

Passwords alone no longer offer adequate protection against cyberattacks, data breaches and fraud.

Reduce password risk by making sure your users are really who they say they are, with Ntiva MFA!

## BOLSTERS SECURITY

Stolen user credentials are one of the top causes of security breaches. MFA ensures that only verified users can access your important business apps and services, by requiring more than just a password before access is granted.

## EASY TO USE

The user experience is slick and seamless. After the user enters their username and password, they'll be sent a push notification to their smartphone or tablet. One tap verifies that they have the registered device in their possession, and immediate access is granted.

## COST EFFECTIVE

MFA is a simple and cost-effective method of adding another layer of protection to your valuable business data. One monthly fee is based on number of users, and will protect as many applications as you want, both on premises and in the cloud.

# PASSWORD THEFT CONTINUES TO HAUNT US – PROTECT YOUR BUSINESS!

We all know someone who has been affected by some form of online fraud, or a business that has suffered a breach, and passwords are often at the root of the problem.

The most common issues are reusing the same password across different account, logging in from untrusted devices, weak passwords, passwords that are never changed or easily guessed – and as of late, phishing emails that trick employees into providing their credentials.

MFA helps protect against the shortcomings of passwords (and people.) Passwords, which are something users know, are only one "factor' in gaining access to applications and are easily stolen or guessed.

MFA adds another factor for identify verification – something unique your users must have in their possession. Smartphones are typically being used as that second factor, although there are other options.

By combining these two factors, hackers can't access your accounts even if they have managed to get hold of an employee's credentials.

# NTIVA MANAGED MFA – HOW IT WORKS

MFA can protect a wide range of business applications, ranging from your VPN, to Remote Desktop Services, Microsoft Office 365, Salesforce, and many more.
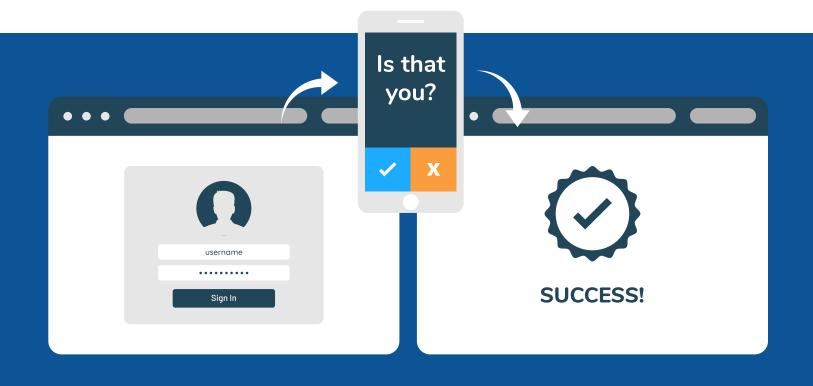
In short, almost any on-line app or service can be protected.

In preparation for the service, the only thing users will need to do is provide a mobile phone number from the device they plan to use, as well as download the MFA app.

When the user enters in their credentials to access the MFA protected application or service, they will immediately be sent a mobile push notification which will pop up on their registered device.

All the user has to do is tap a green button to accept and they will be immediately granted access.

That's it – we do the rest, including procurement, set up, implementation, user management, updates and all required maintenance for the service.

**Is that you?**

✔ X

username

••••••••••

Sign In

**SUCCESS!**