



SecureFactor

Multi-Factor Solution That's Powerfully Easy

Using stolen credentials to breach network resources is the #1 tactic that hackers use.* By requiring additional proof of identity beyond a simple password, multi-factor authentication (MFA) is the single most important safeguard to protect your business.

T. Daniels Consulting's unique multi-factor authentication solution (MFA), **SecureFactor**, not only reduces network disruptions and data breaches arising from weak or stolen credentials, but we deliver this important capability entirely from the Cloud for easy set-up and management.

Moreover, **SecureFactor** goes beyond traditional 2-factor authentication (2FA) by incorporating innovative ways to identify users. For example, using your Mobile Device DNA. With our large ecosystem of 3rd party integrations, this means that strong protection can be consistently deployed across the network, VPNs, Cloud applications – wherever it's needed. Even non-technical users find the friendly **SecureFactor** mobile app easy and convenient to use. Ultimately, T. Daniels Consulting **SecureFactor** is the right solution at the right time to make multi-factor authentication (MFA) a reality for businesses who understand the necessity to keep their business safe from attacks.

Effective Multi-Factor Protection with Mobile Device DNA

Multi-factor authentication (MFA) requires users to supply information they know (username and password), and information provided on something they have, as well as other factors that can be associated to the specific individual. **SecureFactor** provides a highly secure MFA product using a push message, QR code, or one-time password (OTP); and our mobile device DNA matches the authorized user's phone when granting access to systems and applications. Therefore, **any attacker who clones a user's device** to access a protected system **would be blocked**, since the device DNA would differ.

Easy-to-Use Secure Factor Mobile App

T. Daniels Consulting's **SecureFactor** app allows users to authenticate right from their own phone! No need to carry key fobs or thumb drives; instead install and activate the Secure Factor app in seconds, and then use it to authenticate from a smartphone. It enables speedy push-based authentication as well as offline authentication using QR codes with the phone's camera. The app is available in 11 languages and downloads free of charge from the AppStore and Google Play.

Broad Coverage with Web SSO

T. Daniels Consulting's ecosystem includes dozens of 3rd party integrations with **SecureFactor** – allowing companies to require users to authenticate before accessing sensitive Cloud applications, VPNs and networks.

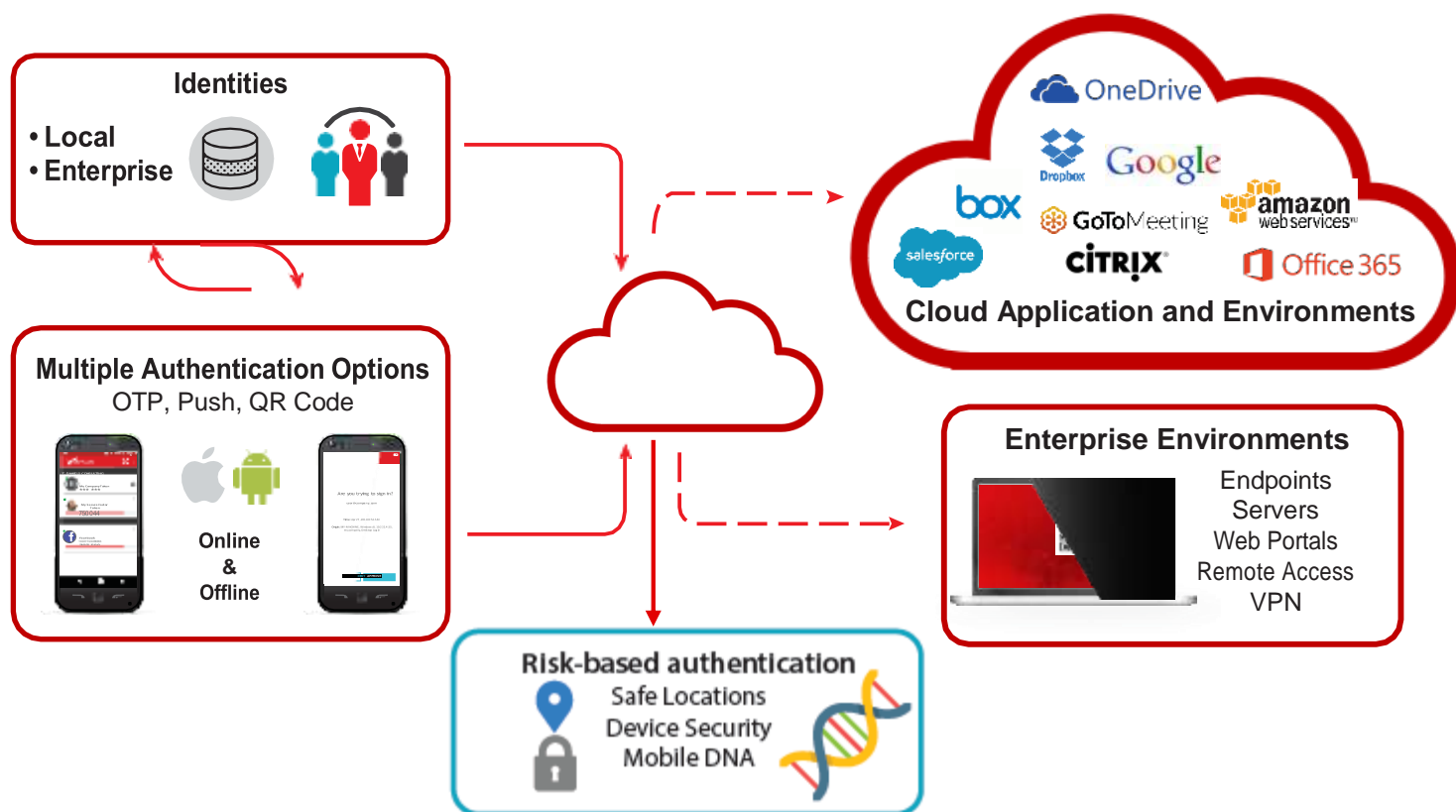
SecureFactor supports the SAML standard, permitting users to log in once to access a full range of applications and services. In addition, the secure login feature provides online and offline authentication to Windows and Mac machines using the **SecureFactor** app.

A Low TCO Cloud-Based Service

Companies with limited IT staff and security expertise benefit from MFA protection that's easy to deploy and manage from the Cloud. **SecureFactor** is available from wherever you are. There is no need to install software, schedule upgrades or manage patches. Moreover, the platform easily accommodates a single global account view or many independent accounts, so that distributed enterprises and managed service providers can display only the data relevant to a person's role.

*Verizon Data Breach Investigations Report 2018

Keep Imposters Off Networks, VPNs, Cloud Resources and More!



Cloud Platform

- 100% Cloud-based management
- Authenticator allocation and activation
- Authentication policies based on groups and resources
- Logs and reports
- Role-based access
- Intuitive, attractive user interface

SecureFactor Mobile App

- Three authentication methods in one:
 1. Push messages
 2. One-time passwords
 3. QR codes when offline
- Mobile authenticator – no additional hardware to carry
- 11 languages
- Multi-token support
- iOS and Android – free to download
- PIN/biometrics protection (on certain devices)
- Mobile device DNA – added authentication factor
- Self-service mobile token migration to new devices

SecureFactor Gateway

- Corporate network gateway
- AD and LDAP user authentication and sync
- RADIUS proxy

SecureFactor Agents

- Integration with 3rd party applications without native multi-factor authentication (MFA) support
- Computer login protection for Windows and macOS

SecureFactor Ecosystem

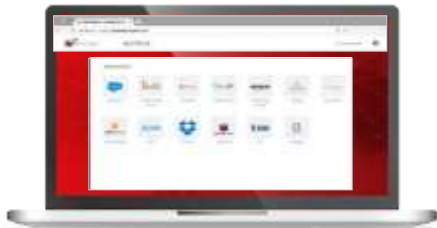
- Add MFA to Cloud resources, applications, databases and web resources
- Support for SAML and RADIUS standards
- Comprehensive integration guides for many popular 3rd party solutions

Recommended Use Cases

VPNs / Remote Access

Same user experience as username + password BUT more secure, and with a single-click confirmation.

1. Request connection with username & password
2. Confirm VPN connection – request through **SecureFactor** app



Cloud Applications – Web SSO

1. Access the Identity Portal (IdP)
2. Authenticate using OTP, push or QR code
3. Access all the apps to which you are entitled – no need to authenticate again!

PC Login – Online Authentication

1. Click on “Send push”
2. Confirm PC login request through **SecureFactor** app
3. Login is done



PC Login – Offline Authentication

1. Select “QR code” to authenticate
2. Scan the QR code using the **SecureFactor** app
3. In this example, you would type the response 717960

SecureFactor delivers on the promise of MFA by limiting the business risk associated with poor passwords without compromising on ease of use for employees and IT staff alike.

Everything in a Cloud service – with no hardware to install and software to maintain...MFA is now considered core protection, and it comes from T. Daniels hassle-free.

What Is Multi-Factor Authentication (MFA)?

Use of 2 or more authentication factors from:

- **Something you know** (password, PIN)
- **Something you have** (token, mobile phone)
- **Something you are** (fingerprint, face)



SecureFactor factors:

1. Your password
2. Approval on your mobile authenticator
3. Correct mobile phone DNA
4. A fingerprint to access (with certain phone models)





Making the Case for Multi-Factor Authentication (MFA)

When considering the direct and indirect expenses associated with a data breach, the costs can add up. After a breach, a company often hires specialists to investigate the cause of the breach, and then adds security measures to address any failures, as well as pays regulatory fines, legal fees, and more. Even so, the indirect costs from reduced employee productivity, and lost current and future customers can be more substantial. To put a number on it, a Ponemon Institute study¹ puts the **average cost of a data breach at \$141 per data record** with sensitive data...or \$1.32M when you consider the average data breach of 9,350 records.

How likely is it that you will experience a breach from a weak or shared password? Data shows that 3 out of 100 people² use the weak password "123456"³ and **6 out of 100 use the same password for all online accounts**. So, you must ask yourself, how likely is it that one or more of your employees are mishandling their passwords. This may be why more regulatory bodies are requiring two-factor authentication (2FA) or multi-factor authentication (MFA) for at least some portion of compliant companies' users – such as with the additions to the Payment Card Industry Data Security Standard (PCI-DSS) v 3.2.

The good news is that you can mitigate these risks with **SecureFactor** authentication for a reasonable cost! With no expenses for additional infrastructure, hardware tokens, and software support and maintenance to reduce the likelihood of the aforementioned \$1.32M in breach expenses.

¹ 2017 Ponemon Institute Cost of Data Breach Study and 2017 Ponemon State of SMB Cybersecurity Report 2

² <http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/>

³ <https://www.statista.com/statistics/763091/us-use-of-same-online-passwords>

THE T. DANIELS CONSULTING SECURITY PORTFOLIO



Network Security

In addition to delivering enterprise-grade security, our platform is designed from the ground-up to focus on ease of deployment, use, and ongoing managing, making T. Daniels Consulting the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.



Secure Wi-Fi

T. Daniels Consulting's SecureWi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.



Multi-Factor Authentication

T. Daniels Consulting's **SecureFactor** is the right solution to close the password-driven security gap that leaves companies vulnerable to a breach. It provides multi-factor authentication on an easy-to-use Cloud platform. Our unique approach adds "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Find out more

For additional details about **SecureFactor**, visit: <http://www.tdaniels.com/secure-factor/>

About T. Daniels Consulting

T. Daniels Consulting is your experienced, cloud certified leader in network security, secure Wi-Fi, and network intelligence products and services. The company's mission is to make enterprise-grade security accessible to SMB's (small & medium business) throughout the Midwest and beyond through simplicity, making T. Daniels Consulting an ideal solution for distributed enterprises and SMB's. T. Daniels Consulting is headquartered in Fenton, MI. To learn more, visit www.tdaniels.com