Adaptive User Authentication

Easy on Users. Tough on Hackers.
CensorNet Multi-Factor Authentication (MFA) balances strong security for your business with high convenience for your users. The solution provides a superior user experience by taking full advantage of contextual information to adapt the level of authentication as needed.

We love it! We think it's a great product! Our staff feels more secure, and IT can sleep soundly at night knowing that every employee can log in from anywhere in the world, and the access is protected by CensorNet MFA.

Gregory R. Zilliox,
Director of IT Services
P&A Group

The world has changed. The way we access, share and use data has changed and so the way we authenticate must change as well. Basic username and password authentication is no longer enough to verify the identity of your users. The traditional hard- and soft-token solutions no longer provide sufficient protection against modern threats; they are cumbersome, expensive to manage and tend to work against the users rather than for them.

CensorNet is pioneering a new generation of more intelligent and user-centric authentication that allows you to increase remote access security without sacrificing convenience. With a track record of thousands of client installations around the world, we know what it takes to protect your systems and cloud applications, whether your users are logging in from London, New York, Berlin or Bangalore.

Here is how it works: CensorNet MFA authenticates users by sending a real-time, uniquely secure session-specific OTP (One-Time-Passcode) to the user’s mobile phone. Once the OTP has been validated, the user is granted access. It’s that simple!

CensorNet MFA delivers industry-leading value in four key areas: Security, Convenience, Ease of Administration and Returns.
Prevent Security Breaches with Contextual Intelligence

CensorNet MFA uses real-time generated, session-specific passcodes and takes advantage of contextual information when validating the user, thereby protecting against identity theft and modern threats.

Cyber threats have escalated dramatically and hackers have tools at their disposal that are more advanced than ever before. Underestimating these threats can have a devastating impact on your organization.

Weak or stolen user credentials is the preferred weapon used by hackers, and exploited in more than 60 percent of all network breaches. The threat is real and it is growing. With Multi-Factor Authentication from CensorNet however, you can effectively disarm the hackers of their preferred weapon.

CensorNet MFA uses real-time generated, session-specific passcodes and takes advantage of contextual information when validating the user, thereby protecting against identity theft and modern threats.

More than 60% of all network breaches involve weak or stolen credentials

More Factors Working to Your Advantage
CensorNet MFA looks at multiple factors surrounding each particular login. These factors include: Session-ID, geo-location, network IP, system being accessed, time of login, etc. The factors establish a context that helps determine the level of trust around each login, and whether or not the user is allowed access.

Real-Time and Session-Specific
For maximum security, all passcodes are generated in real-time and are locked to the session-ID of each particular login attempt, which eliminates the consequences of Phishing attacks. No pre-issued passcodes. No seed files to be hacked. And no passcodes are stored on the user's mobile phone.

Advanced Attack Protection
Innovative use of contextual information, such as the geo-location, enables CensorNet MFA to detect and alert a user if an advanced attack - like real-time phishing or man-in-the-middle attack - is taking place. The system can be configured to notify the user in the OTP message itself.

High Passcode Security
Passcodes are cryptographically strong random generated OTPs using FIPS-140 validated crypto modules and all communication between components is AES 256-bit encrypted. In addition CensorNet MFA offers advanced "brute force" and "denial-of-service" attack detection and protection.

Unmatched Reliability
CensorNet MFA’s OTP delivery platform and automatic fail-over mechanism ensures that passcodes always reach the users regardless of when and from where they are logging in.

Location Aware Message Dispatching
CensorNet MFA can be configured to automatically select the most appropriate OTP delivery method based on the login context of the user, e.g. the geographical location. So for example, if a user is on a business trip to India, the solution can be set up to deliver the OTP via a local service provider, to keep the reliability of delivery higher. And in the event that a user is in an area with poor cellular coverage the solution will deliver the OTP via the CensorNet App or any of the available secondary delivery methods.

Status Feedback
CensorNet MFA provides unrivaled status feedback that enables the user to follow the login progress. Status feedback inspires user confidence and reduces the number of helpdesk calls.

Flash SMS
By default, passcodes are sent as Flash SMS, which automatically pop up on the user’s mobile phone without any user action. An extra advantage is that the Flash SMS is not stored on the phone. Regular SMS is supported as an option.

MemoPasscodes™
CensorNet MFA makes innovative use of letter combinations to provide users with easy-to-remember passcodes, helping to support the intuitive login process.

Make Security Hassle-Free and Painless for Your Users
CensorNet MFA improves security without sacrificing the user experience. The solution is so intuitive that end users will happily maintain compliance.

By leveraging the one thing users always carry with them - their mobile phone - the solution provides a superior user experience that incorporates contextual information, without the need for installing anything on the end-users device. Based on this information, the platform can be configured to assess the threat level and dynamically adjust the level of user authentication needed.

For example, if a user logs in from a trusted location, such as the comfort of his home (where he has logged in from before), he will not be prompted for an OTP in order to authenticate. Whereas if he is attempting to log in while travelling e.g. from an airport lounge or hotel with public Wi-Fi, then an OTP is mandatory to gain access. In addition to the adaptive login process, other components also contribute to the great user experience that CensorNet MFA is known for:

More than 60% of all network breaches involve weak or stolen credentials

Welcome!
Easy for IT to Implement, Manage and Scale

CensorNet MFA is easy to install, deploy and manage. The platform offers flexible policy-driven administration and protects multiple systems on a global scale. The solution seamlessly integrates to both remote access systems and cloud applications.

The CensorNet MFA platform allows you to get up and running in less than an hour. Run plug-and-play installation of the Multi-Factor Authentication software, setup the preferred dispatch mechanism(s), and the system is ready for use. Rollout involves no software deployment on user devices and practical training of the user group is not needed. CensorNet MFA comes with one-click integration to Active Directory and LDAP Directories. No schema changes or extensions are required.

User Management

Users are synchronized from Active Directory and/or general LDAP Directories like OpenLDAP or AD LDS. Users can be imported by selecting a specific user group, or by use of an LDAP filter. It is even possible to import users from multiple domains, or let users self-enroll, which is particularly helpful in large enterprises and hosting environments.

User Group Policies

Every user is assigned to a User Group Policy and automatically inherits the specified permissions. A permission change affects every user in the group. Multiple User Group Policies can be defined. This means that you can define different permission sets for individual groups of employees, external consultants, etc. The day to day maintenance of permissions can conveniently be handled in Active Directory.

Reliable OTP Delivery

CensorNet MFA ensures maximum reliability through a number of real-time OTP delivery methods combined with a sophisticated automatic fail-over mechanism. With the introduction of Dispatch Plugin Modules customers now have even greater flexibility in defining how one-time-passcodes should be delivered. Customers can choose from a comprehensive list of messaging providers and plugin modules, and even have the flexibility to create their own plugin modules.

Detailed Reporting Capabilities

CensorNet MFA provides reporting and analytic functionality that allows you to monitor usage, identify trends in login attempts, threats, high-risk locations, or even potential attacks. And it gives you the means to monitor failover services and the overall performance of the setup.

Reduce Costs and Improve Return on Investment

With a lower TCO than traditional solutions, CensorNet MFA offers an affordable multi-factor authentication platform that is highly secure, easy to deploy, manage and use. This keeps costs to a minimum, enhances ROI while boosting productivity.

Many companies are still reluctant to open up for remote access to business critical systems - and for good reason! In the Ponemon Institute’s 2015 Global Cost of Data Breach Study an average consolidated total cost of a data breach is estimated at $3.8 million, representing a 23 percent increase since 2013. These are staggering numbers. But opening up for remote access in a secure and controlled manner reveals multiple productivity benefits. And as companies adopt cloud services on a grand scale, every user essentially becomes a remote user.

With a lower TCO than traditional solutions, CensorNet MFA offers an affordable multi-factor authentication platform that is highly secure, easy to deploy, manage and use. This keeps costs to a minimum, enhances ROI while boosting productivity.

Effective Breach Prevention

The implementation and maintenance costs of CensorNet MFA, relative to the increased security level that it provides, is marginal compared with the tidal wave of costs associated with your systems being compromised.

Empowered Workforce

After implementing CensorNet MFA, customers typically experience an increase in the use of remote access. This means that more employees access more data and more applications on a regular basis, which is a good indicator for productivity gains. Offering employees the opportunity to work from home, or allowing external consultants access to relevant systems yields a significant increase in productivity.

Administrative Cost Reduction

For customers moving from a legacy hardware based authentication solution to CensorNet MFA, savings will typically be around 50 percent. Customers looking to introduce an additional layer of authentication will benefit from the easy administration and reduced helpdesk costs.

Low-Friction Implementation

Despite the many benefits of CensorNet MFA, the impact of an installation on your existing infrastructure is minimal. The system is self-contained, which is a great advantage in terms of ROI because the lifecycle of the installation is almost independent of the supporting systems and processes. An installation can run side-by-side with a token-solution during migration and just a single license covers all your systems.

Costs are typically 50% lower than hardware based solutions.
CensorNet App

Version 9 gives customers even greater freedom and flexibility to choose how users authenticate. Users can now have their one-time-passcodes (OTPs) delivered to the CensorNet App on their mobile phone as push notifications.

The CensorNet App is a powerful extension to the CensorNet MFA platform, and it’s future use cases extend well beyond “just” OTP delivery. In the future the CensorNet App could help provide contextual information around logins and increase the security even further.

The CensorNet App integrates fully into the renowned CensorNet MFA dispatch infrastructure, meaning you can configure it according to your specific needs using Dispatch Policies. For example, you might configure one group of users to receive messages primarily using the CensorNet App, and secondary by SMS (failover) – while other users will receive messages by SMS only. You can also take advantage of the contextual message dispatching feature and have the solution automatically select the most appropriate delivery method based on the context of the user.

Increased security: Push notifications are sent encrypted, end-to-end from the CensorNet MFA installation to the CensorNet App. Every single app installation will use its own, auto-generated encryption key, meaning only the intended receiver of a message will be able to decrypt it.

Possibly lowered costs: In some scenarios, receiving push notifications might be less expensive than receiving SMS messages. Push notifications will only require a small amount of data traffic. Please evaluate your specific scenarios, what the costs of data traffic are compared to the costs of SMS messages.

Solution Highlights

Seamless Integration: the Multi-Factor Authentication platform integrates seamlessly to login systems and cloud solutions, for an intuitive and user-friendly remote access experience.

Adaptive Authentication: balance high security and strong user compliance with a solution that automatically adapts the level of authentication needed based on the threat level.

Automatic Failover: set up highly sophisticated failover mechanisms to ensure that the OTPs always arrive. The solution can even adapt between transmissions based on the login context of the user, e.g. the location.

Broad Directory Support: users can be synchronized from Active Directory and general LDAP Directories like OpenLDAP or AD LDS. Users can be imported by selecting a specific user group, or by use of an LDAP filter.

Real-Time: all passcodes are generated in real-time at the point of login. No pre-issued passcodes. No seed files to be hacked.

Session-Specific: all passcodes are locked to the session-ID of each particular login attempt for maximum security. Advanced attacks are detected and the user is notified in the OTP message they receive.

PowerShell: CensorNet MFA includes PowerShell support for admins to manage and automate tasks through PowerShell scripting. Admins can use PowerShell to set up role based access, integrate to other systems, or automate daily tasks such as checking license availability or country specific logs.

Status Feedback: CensorNet MFA provides unrivaled status feedback enabling the user to follow the login progress. Status feedback inspires user confidence and reduces the number of helpdesk calls.

Flash SMS: by default, passcodes are sent as Flash SMS, which automatically pop up on the user’s mobile phone without any user action, and the Flash SMS is not stored on the mobile phone. Regular SMS is supported as an option.

Location and Behavior Aware: CensorNet MFA takes full advantage of contextual information such as login behavior patterns and geo-location information to effectively grant or deny user access.

Secure Device Provisioning: Secure Device Provisioning allows users to quickly and easily enroll new ActiveSync devices by themselves without compromising security.

MemoPasscodes™: CensorNet MFA makes innovative use of letter combinations to provide users with easy-to-read and easy-to-remember passcodes that support the intuitive login process. Passcodes and notifications alike can be customized to your specific needs.

OTP Delivery Methods: with Dispatch Plugin Modules and standard delivery methods like app, SMS, voice call, secure e-mail, cloud keys, and hard / soft tokens, CensorNet MFA can support your business requirements now, and in the future.

Advanced database auditing: CensorNet MFA includes advanced auditing capabilities to help customers comply with strict industry regulations and audit control requirements.
Protect All Your Systems and Applications

Regardless of whether you want to protect cloud applications or a remote access system, CensorNet MFA gives you all the integration and scalability you need.

The solution supports a broad set of login systems for remote access and cloud services. The platform is designed to integrate seamlessly to the most popular third party systems to ensure a secure and intuitive login process for end-users.

The deployment of CensorNet MFA was very fast, and we had exceptional support throughout the process. The users have found the solution intuitive to use and convenient because they always have their mobile phone with them. We have achieved our security goals and are now able to provide remote access with more confidence.

JD Brown, Systems Administrator
Carolina Bank

For a full list of supported systems, please see the back page.
## Supported Systems

CensorNet MFA supports a broad set of login systems used for remote access. The platform is designed to integrate seamlessly into any of the third party systems listed below, to ensure a secure login process that is intuitive to the end-user.

### The following systems are supported:

#### RADIUS VPN/SSL VPN Clients
- Check Point
- Cisco ASA
- Netscaler Gateway & Citrix Access Gateway (GAG)
- Juniper
- Microsoft Forefront (UAG)/Direct Access
- Barracuda SSL VPN and NG firewalls
- VMware Horizon View
- Microsoft SharePoint Portal Server
- Any other RADIUS client supporting challenge/response
- Palo Alto
- F5 BIG-IP
- NCP VPN

#### Microsoft AD FS Protection
- AD FS 2.0 plug-in for multi-factor authentication
- AD FS 3.0 multi-factor authentication adapter

**Transparent support for MFA when:**
- Accessing Cloud Applications such as Saleforce.com, Microsoft Office 365, Google Apps etc. (AD FS 2.0/3.0)
- Accessing websites published through the Microsoft Web Application Proxy (AD FS 3.0), such as SharePoint and Outlook Web Access
- Approving devices during workplace joins (AD FS 3.0)

#### Internet Information Services (IIS) Websites
**Support for the following types of websites:**
- Remote Desktop Web Access
  (Windows Server 2008 R2 / 2012 R2)
- Microsoft SharePoint Portal Server
- IIS websites using Basic or Integrated Windows Authentication
- Any website not requiring Authentication Delegation

#### Microsoft TMG Server & Websites
**Support for Microsoft TMG published websites:**
- Remote Desktop Web Access
  (Windows Server 2008 R2 / 2012 R2)
- Microsoft SharePoint Portal Server
- IIS websites using Basic or Integrated Windows Authentication
- Any website not requiring Authentication Delegation

#### Windows Logon, Remote Desktop Services
**Support for the following Services and Services:**
- Remote Desktop Services (RDP Connections)
- Windows Servers 2008 R2 / 2012 / 2012 R2
- Windows 7, Windows 8, Windows 8.1 and Windows 10
- VMware Virtual Desktop Portal & Client Access

### Citrix Web Interface

(1) Protection of SharePoint Portal Server using RADIUS is only supported, if the SharePoint Portal server is published through an Application Gateway, which will ensure that the user is only required to authenticate once during the initial logon. E.g. using the Microsoft IAG/UAG, Citrix Access Gateway configured to make use of persistent cookies.