Multi Factor Authentication for Enhanced Login Protections.

As login validity increases, so does the opportunity for stolen passwords and ultimately breaching your network perimeter.

Omega Systems' MFA package editions provide appropriately-sized solution options to ensure users and devices are trusted before granting them access to your network and applications.

84% of network breaches involve compromised credentials as a result of hacking and social engineering.

Verify user identity and device health before allowing connection to your network applications!

The adoption of varied Cloud environments, bring your own device (BYOD) initiatives as well as collaborative and remote work strategies has changed the effectiveness of firewall-based perimeter protections. Since attackers can unnoticeably masquerade as valid users inside your network, "zero-trust" Multi-Factor Authentication implementations are needed to defend your network from these impostors.

Gain ultimate protection regardless of where users are located, what devices they are using or where the application is located.

Select from Omega Systems' MFA package options based on your business' secure access needs:

MFA+ Basic

Find and access applications from a single sign on portal.

Omega Systems' MFA+ Basic Edition establishes identity validation and protects every user with a reliable, easy-to-use experience.

The login process is made easy with an SSO, allowing users to find and access cloud applications from a single portal.

The cloud-based deployment scales to meet the needs of even the most diverse user base and accurately delivers device insights summarizing the security posture of the devices in play.

MFA+ Enhanced

Gain unified device visibility and enforce BYOD securities.

Omega Systems' MFA+ Enhanced Edition amplifies the MFA+ Basic package with an admin-friendly "Unified Device Visibility" dashboard.

Each device is checked for up-to-date software, enabled security settings, location and network data. Policy enforcements and access restrictions can be universally applied based on specified criteria (individual users, groups, location, network data, device security posture, etc.) without the need for additional agents.

MFA+ Advanced

Simplify with application access dashboards.

Omega Systems' MFA+ Advanced Edition employs the max-level, zero-trust security framework while simplifying the user experience with a with custom dashboard of on-premises and cloud applications for application access simplicity.

MFA+ Advanced provides the ability to differentiate between corporate and employee-owned devices, and further allows you to develop controls for application access based on the trustworthiness of the device and the identity of the user requesting access.



Multi-Factor Authentication (MFA)	MFA+ Basic	MFA+ Enhanced	MFA+ Advanced
MFA+ Push for iOS and Android	✓	✓	✓
MFA+ with security keys, UF, OTP, phone callback, SMS & hardware tokens	✓	✓	✓
Telephony credits — 100 credits/user/year	✓	✓	✓
User self-enrollment & self-management	✓	✓	✓
Endpoint Visibility			
Dashboard of all devices accessing applications	✓	✓	✓
Monitor and identify risky devices		✓	✓
Visibility into security health of laptops and desktops		✓	✓
Visibility into security health of mobile devices		✓	✓
Detect anomalous / risky access		✓	✓
Identify corporate owned versus BYOD laptops and desktops			✓
Identify corporate owned versus BYOD mobile devices			✓
Identify if a third-party agent is enabled on the device (Ex: Anti-virus, Anti-malware)			✓
Adaptive Authentication & Policy Enforcement			
Assign & enforce security policies - globally or per application	✓	✓	✓
Enforce policies based on authorized networks	✓	✓	✓
Assign & enforce security policies per user group	✓	✓	✓
Enforce policies based on user's location		✓	✓
Block Tor and anonymous networks		✓	✓
Enforce device trust policies based on security health of laptops and desktops (out-of-date software, encryption, firewall, etc.)		✓	✓
Enforce device trust policies based on security health of mobile devices (encryption, tampered, screen lock, biometrics)		✓	✓
Notify users to remediate their devices		✓	✓
Remote Access & Single Sign-On (SSO)			
Unlimited application integrations	✓	✓	✓
Cloud-based SSO for all SAML2.0 applications	✓	✓	✓
Easy application access with central portal	✓	✓	✓
Limit device access to applications based on enrollment in endpoint management systems such as Landesk, JAMF, Microsoft Intune			✓
Limit mobile access to applications based on enrollment in MDMs (AirWatch, MobileIron, Microsoft Intune)			✓
Secure access to internal company web applications (Network Gateway)			✓
Secure access to specific internal servers via SSH (Network Gateway)			✓
Secure remote access to applications hosted in AWS, Azure, and GCP (Network Gateway)			✓