



HOW TO PROTECT YOUR CUSTOMERS TODAY



Identity attacks like spear phishing, man-in-the-middle, credential shuffling, brute force, and rainbow tables are becoming increasingly sophisticated and dangerous. The best way to combat these attacks is a comprehensive defense strategy. This should include implementing controls and policies like a secure password policy, multi-factor authentication (MFA), single-sign on (SSO), self-service password reset (SSPR), and conditional access. As a Microsoft Gold Partner with competencies in Identity, Security, and Cloud Productivity, ConvergeOne can help take your identity posture to the next level by implementing the above features as part of your defense strategy. The good news is that if you have any of the following licenses, then you already have these features—you just need them to be enabled and configured: Microsoft 365 Business Standard, Microsoft 365 Business Premium, Microsoft 365 F3, Microsoft 365 E3, Microsoft 365 E5, Microsoft 365 A3, Microsoft 365 A5, or Azure AD Premium Plan 1.



Multi-Factor Authentication (MFA)

MFA adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone.



Single Sign-On (SSO)

SSO is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.



Self-Service Password Reset (SSPR)

SSPR allows users who have either forgotten their password or triggered an intruder lockout to authenticate with an alternate factor, and repair their own problem, without calling the help desk.



Conditional Access

Conditional Access is the protection of content by requiring certain criteria to be met before granting access to the content



DON'T BECOME ANOTHER NEWS STORY

ConvergeOne Microsoft Security Experts can identify gaps in your strategy so you can stay better protected. Get started today:
convergeone.com/partners/microsoft/security