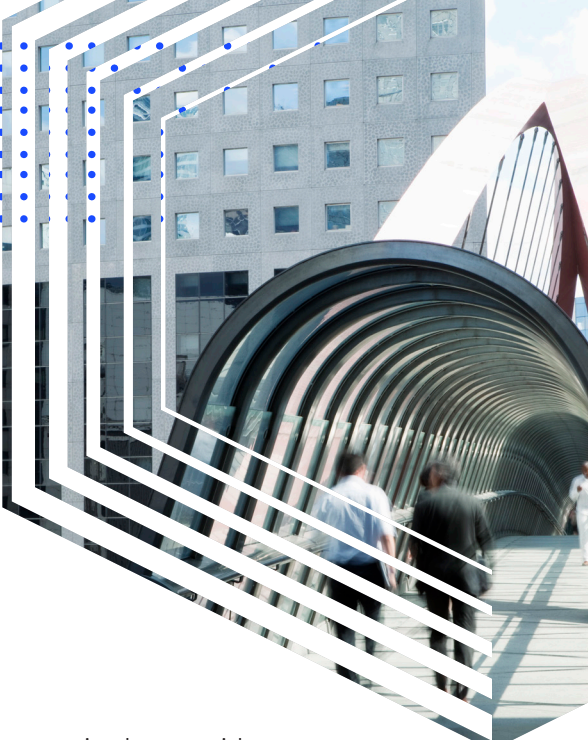
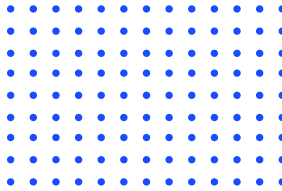


A Logicalis Guide

Multi-Factor Authentication and Beyond






Enterprise Corporate security attacks and breaches are on the rise from a variety of criminals armed with advanced (and frequently automated) tools and techniques that make them a serious threat to your organization.

One of the main vectors of attack has been to obtain authorized end-user credentials to gain access to valuable assets. This is done not only through technical means but also by persuading users to freely provide their credentials. According to the 10th edition of the [Verizon Data Breach Investigations Report](#), more than 80% of security breaches involve either stolen or weak passwords.

Planning for these attacks is different from using endpoint protection and firewall technology. Firewalls and endpoint security generally do little to prevent credential theft. Instead, these types of credential-focused attacks require a different type of security solution that does not pose a burden to your end-users. The security solution most frequently deployed is multi-factor authentication.

More than Password Strength




Strengthening passwords to prevent attacks on secured data is bread and butter for any Chief Information Security Officer. As IT security teams fill their schedules maintaining anti-virus software, firewalls, and encryption technology, they also acknowledge that without multi-factor authentication (MFA) solidly in place, all the other measures can be easily bypassed with stolen credentials, regardless of password strength. For a truly secure solution, MFA is not nice-to-have, it's must-have for all users.

MFA & Beyond

With MFA, users are required to provide two or more factors of authentication — something they know (a knowledge factor, such as a password), something they have (a possession factor, such as a security token) and/or something they are (an inherent factor, for example, a fingerprint) — before they may access enterprise resources.

MFA typically uses the primary factor of a username/password tightly coupled with a second source of validation, such as a mobile phone or hardware token, to verify user identity before granting access to an enterprise resource. Some companies hesitate to implement MFA, believing the user experience can be less-than-elegant, or even “clunky.” Such systems are largely a thing of the past. Today, MFA provides a foundation that includes rapid onboarding, self-enrollment and self-management. MFA is used by all types of organizations and can be purchased for a small monthly per-user rate. Most importantly, MFA provides a simple, streamlined and frictionless login experience for every user and any application whether on-premise or in the cloud, all while integrating easily with existing technology.

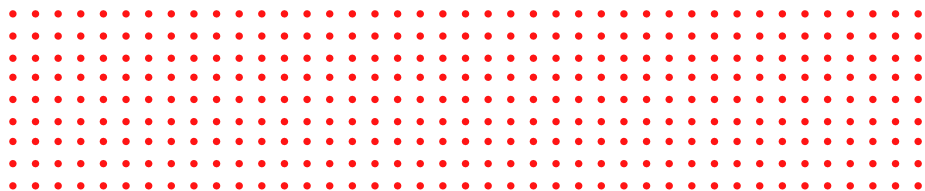


This Logicalis Guide will discuss Multi-factor Authentication and make recommendations for steps you should follow as part of your MFA journey.

MFA Considerations

Here are some considerations for your organization's MFA implementation plan.

- 1. Employ Adaptive MFA** — Adaptive MFA is an elegant and effective solution that goes beyond validating credentials to also incorporate context. For instance, access to a cloud application such as Salesforce could be denied – even if a user provides proper credentials – if the user does not access the application from a trusted corporate network.
 - 2. Establish Device Trust** — Using outdated browsers or not establishing screen timeouts and locks poses security risks. Rather than just blocking users, you should inform them why they have been locked out of a resource and provide them with directions for correcting the issue themselves. Corporate-issued devices (desktops, laptops and mobile devices) are typically far more secure than user-owned devices (so-called BYODs). It's important that your MFA solution can distinguish between corporate-owned and non-issued devices that may be less secure before providing access to enterprise resources.
 - 3. Think Twice before using Texts with MFA** — Short Message Service (SMS) is considered a risk for MFA, according to the National Institute of Standards and Technology (NIST). For example, a mobile phone could be cloned, or the service provider could be socially engineered into making the mobile phone number available to a criminal. Instead, consider using a more secure solution like push technology with a native smart phone application. This also provides a better end user experience, by simply requiring your users to click an approve button, rather than manually copying a code from text message to a separate authentication window.
 - 4. Ensure MFA is Integrated & Monitored** — Your MFA solution should be a component of your larger security architecture that is monitored for trends. MFA authentication logs provide a wealth of information that other Security Information and Event Management (SIEM) tools and your managed security service provider can leverage to take proactive action.
 - 5. Invest in IT Security Expertise** — Cybercriminals adapt quickly to thwart security practices. Your in-house IT security team or outside security provider must be continuously vigilant. Gartner notes that dedicated experts are better suited to fulfill today's cybersecurity needs because they can more efficiently tackle specific attacks to minimize risks. Security preparedness is a continuous process that should include regularly scheduled training, live workshops, and online as well as traditional classroom instruction.
- MFA is effective when it's easy to use and applied across every user and application in your organization. The harder it is for criminals to access your organization's data, the lower the risk of a breach. At the same time, MFA solutions must be flexible and easy to use for users within your organization. That way, MFA is both secure and convenient — hallmarks of a solution that will be used consistently to protect your company's valuable assets.



Logicalis + Cisco: Taking Business Transformation Seriously

An award-winning, Cisco-certified partner, Logicalis is trusted to deliver the expertise you can count on to transform your organization and enable business outcomes. We bring unrivaled knowledge, skills, and experience to deliver IoT, cloud and security solutions that maximize existing investments, meet your needs and drive confidence.

To learn more, visit
us.logicalis.com/cisco-and-logicalis/.

Source: [Verizon Data Breach Investigations Report](#)

