Multi-factor authentication plays a significant role in any access control approaches within organizations. The field continues to advance beyond the traditional ideas of using biometrics as a second factor. Read the following articles and provide answers to the subsequent questions.

[https://securityintelligence.com/multifactor-authentication-delivers-the-convenience-and-security-online-shoppers-demand/ (Links to an external site.)Links to an external site.](https://securityintelligence.com/multifactor-authentication-delivers-the-convenience-and-security-online-shoppers-demand/)

[https://searchsecurity.techtarget.com/feature/Explore-multifactor-authentication-products-in-depth (Links to an external site.)Links to an external site.](https://searchsecurity.techtarget.com/feature/Explore-multifactor-authentication-products-in-depth)

Questions:

1. From the first article, what terminology is used to describe authentication factors that are not visible? Describe how these authentication factors work?

* From the First Article, the major authentication factors the author describes is multi-factor authentication. The Authentication Factor where passwords are used previously is now being replaced with the many factors authentications like OTP and Password to fight back with the risks together.
* In the MFA is context-based authentication where authentication factors were made invisible to the user and are silently enrolled for the authentication without user’s knowledge. Some of the contest-based authentications are device fingerprinting, geolocation, IP reputation, device reputation, and mobile network operator (MNO) data these can contribute to identifying and verification. Some [threat intelligence platforms](https://exchange.xforce.ibmcloud.com/) can already provide most of this information to third-party applications and solutions.
* The Device is made to register into the security where if the user logins from another device or user must go through extra Login features or other authorization steps other than the personal device. The user is even asked to declare the device one who is logging in is a private or public device.
* Some of the steps to Context-based authentication which leads to invisible factors:
  + Register the device with/without user consent and ask the user to declare the device as personal or public.
  + Associate biometric credentials to registered devices, thus binding the legitimate device, user and online application
  + detect the known users retrieving data from unregistered devices and add required extra authentication steps.
  + Move to passwordless login, based on scanning a time-based QR code without typing a password
  + Verify the user presence, limiting the efficacy of reply attacks and other automated attacks
  + Use an authenticator app to access online services with 2FA that leverages the biometric device on the smartphone

1. Based on question 1, choose a non-visible based factor and do some research to describe how it is used and why it is beneficial compared to other MFA?
   * The non-visible based factor (context-based authentications) is which are being used widely more in intelligent adaptive authentication where the fraud detection and security logins are made more secure and easy. Geolocation, Biometric which can be used as the invisible login credentials.
   * Typically, The Device Registration to the application is the first step towards the login check after that context-based analysis is made using the Date, Time, Location and device info and signal strength of the device is taken into consideration. If anything, which is typically found unfamiliar then the step-up authentication is made to make sure to avoid the attack. If the Geolocation of the Login is entirely different and impossible to travel to the location in real, they can level up the authorization level which could be good enough to defend the attacker.
   * Based on the device capable of handling the security the authentication factor can choose one among that is biometric where the user is asked to provide the fingerprint if the Geolocation of the device is usually different and the login Pattern is different, or the device is different.
   * It is beneficial than other MFAs because it make system secure and it is easier for customers to get along.

3.) The second article describes different multi-factor products available on the market. Review some of these products and make a suggestion (including why) as to what would be best for smaller organizations compared to larger organizations. Have any of you interacted with these products in the past?

### The Article specifically suggest that MFA provided from the Secure Access MFA would be good for the small organization because it provides the well-secured MFA authentication required for the small organization like soft tokens, Real-time SMS passcodes, Native supported wearables etc which might fit into emerging techie mid-sized business also..

### Auth Point is cloud-based MFA tool from watch guard technologies which also aims to provide the service to the Small and mid-size companies. It collaborates with Google Authenticator or DropBox. They even analyze the cloned devices and also support SAML and also provide cloud-based security management.

### I have not interacted with any of the product which has been mentioned in the article, but I have used MFA authenticator which is Citrix Token which gives us authorization to work on the client side. Along with Token we must be in the listed employees where we have access to the sites from the It Department and from the client-side approvals were taken before we get our email and authentication were enabled.

### I have seen another company Using similar application which provides the MFA which can be referred as a soft token from which provide the soft tokens which are in the form of OTP(Random code of 6 digit) and this OTP is only valid for 10 secs upon which they should combine it with the pin within 10 secs. The Pin is set by the employee and is been authorized by the IT people.