MFA for Laptops and Mobile Phones

Regarding MFA for laptops/mobile devices/personal devices this is often implemented in ways that are less visible to the users of the devices.

Here is an example:

* An organization could require the presence of a physical device to login to a computer. Smart cards ([Smart card - Wikipedia](https://protect-us.mimecast.com/s/88klCM8WAnHZ7KnwiwJI14?domain=eur02.safelinks.protection.outlook.com)) have been traditionally used for this purpose. On older, thicker devices, there used to be a port for inserting these cards. As laptops have gotten smaller, these cards are more often utilized using NFC ([Near-field communication - Wikipedia](https://protect-us.mimecast.com/s/YeIHCNkWBoTBzKgOt46p8B?domain=eur02.safelinks.protection.outlook.com)). This is most likely to be found in the public sector (federal), or by defense contractors. Lately, YubiKeys have started fulfilling this purpose in other areas of the private sector. Google is the biggest public proponent.

The following is applicable to both MFA for remote access and MFA for laptops/mobile devices/personal devices:

* An organization could use some form of MDM (Mobile Device Management) solution to register a device and associate that device with a specific user. By leveraging fingerprint and / or facial recognition scanners on devices, an organization could have a higher degree of confidence that the person being authenticated is the intended user. This would be an ideal implantation because it requires both physical access to the device, and the required biometric information to unlock it. One MDM platform is Microsoft Intune (which is cloud based). If there is a questionable sign in with a corporate account, it is possible to lock an account out of a device (if it is owned by the company and the device has an internet connection). To regain access to the device, the associated user would have to provide a second means of authentication. For situations where a more permanent change is needed, the company could remove this option as well.
* An organization could use an MDM solution where corporate data is sandboxed within a specific app. This is often utilized for BYOD purposes. The primary use is for corporate email. Through the use of Office 365 (AKA M365), this has expanded to a number of other documents outside of email. The reason why this approach falls under both options for this question is because these apps can save data locally to the device. As such, the registered user of the device could access corporate data locally on a personal device without an internet connection. However, the device(s) must be registered to a specific user. And the MDM platform could leverage the biometric scanners on the device to authenticate the specific user that is registered to the device. This would deter an unauthorized individual from using a stolen device in combination with the stolen credentials of any corporate user.

The following is an example of MFA for remote access:

* An organization could install a certificate onto the device when its software is being installed. That certificate would indicate that the device is trusted by the organization. The user of the device would still need to present a username and password. However, that measure would not verify that the person that is logging into the device is trusted. Thus, this would not be ideal.
* An organization could utilize a VPN solution (such as Cisco AnyConnect) to allow remote devices to connect to another network and operate as if the device was on the local network. By pairing the VPN solution with an MFA solution such as Duo, an organization could register an individual with an authenticating device (through an app on an external mobile device). The integration with the VPN and MFA solutions could make the authentication process relatively seamless. And it most likely the reason why Cisco purchased Duo not too long ago.
  + Alternatively, an organization could allow authorized users to remotely access a virtual desktop environment (such as Citrix). They could require the use of MFA with this solution. This would be preferable to a VPN solution because the mouse and keyboard commands are sent to the VDI environment, and the visual consequences of those actions are relayed back to the remote user. This is often used to grant third parties (such as auditors) access to limited resources.