Misuse of personal information

Strong authentication can (not-rightfully) act as an enabler for companies to increase the level and amount of private and sensitive information stored and managed online in the cyberspace. Indeed, strong authentication services, like biometric authentication or one-time passwords, can increase users' level of trust and the certainty of who they say they are. Moreover, with strong authentication in place, and robust access controls and audit logging running, many services achieve a good level of security. Governments store and manage private details of their citizens online, as long as there are robust authentication services and access controls in place. Yet, endpoint security makes most of the devices vulnerable and even **strongest authentication services can become void if the endpoint has been compromised**.

Endpoint security is more than screen mirroring in effect, or keyloggers. Companies going global with their systems and services need to be able and willing to take and manage the risk doing so. Global cyberspace is not just profits and capabilities; it is increased risks and uncertainties (referring e.g. to a recent Australian governmental paper expressing the need to balance risks and benefits of going global with services and businesses). Globalization of markets, labor, and services also include the globalization of data misuse. With strong authentication services, one may feel secure that the users are who they say they are on a practical certainty, yet additional measures need to be taken to ensure that globalized data and, more importantly, personal data, are not misused and endanger additional measures taken to strengthen the authentication mechanisms.

Multipolarity of the world

Addressing data misuse on a global level is more challenging than within territorially divided sociopolitical context. The diversity of the world produces a multitude of forms of corruption and a wide variety of attack vectors. Single sign-on services, same authentication used across services globally and even across companies or entities, can create a vulnerable weak single spot that cannot resist a diversity of attack vectors.

Data misuse, therefore, can be a challenge for global cybersecurity. We at AltiPeak aim to provide strong authentication solutions that can fulfill and act in accordance with local and particular traditions. We acknowledge that effective governance for one might be ineffective for another. Since there is barely a single global scale, there must be multitude and custom solutions as well that provide secure and reliable IAM services for any particular use or context.