DTS IDENTITY CLIENT

The endpoint is worth its weight in gold for any hacker because we are surrounded by end devices. The number of networked devices is in the billions and rising, but some of them are outdated and dependent on user operation. 88% of all data breaches are caused by human error. If companies do not ensure that every device that is given access to internal resources also complies with security guidelines, there can be no better entry point. DTS Identity is THE platform for all identities. With the DTS Identity Client, we are now further hardening the solution and enabling REAL zero trust identity.

WHAT IS THE "CLIENT" FOR OUR DTS IDENTITY?

The DTS Identity Client is not a stand-alone solution, but is directly linked to the DTS Identity IAM. It makes it possible not only to identify and authenticate the user, but also to include the associated device and its status as an important factor. At the same time, we can extend the features of DTS Identity to clients. This gives our self-developed Identity & Access Management greater leverage for implementing a zero trust strategy.

To ensure that the latest version is always available, the solution is offered exclusively "as a service". This means that the DTS Identity Client can be used without any internal effort and without having to worry about hosting. Of course, the entire solution is only provided from our German, certified data centers.

FEATURES & THEIR ADVANTAGES

1. TRANSPARENCY

- Visibility of all devices in the network
- Status of devices can be viewed at the click of a button
- Overview of how many & when devices access company apps
- More transparency enables more sets of rules

2. RULE SETTING

- Setting up individual or universal endpoint & MFA guidelines
- Compliance guidelines are set centrally in DTS Identity using our Conditional Access feature
- Use case example: According to the compliance policy, access to company apps should only be possible with secure devices. The devices require an up-to-date version of the operating system and the necessary security, e.g. an active firewall and/or antivirus status. Access to (important) applications is only granted once this has been ensured.

3. ENFORCEMENT OF REGULATIONS AS WELL AS AUDIT & LOGS

- Tracking & allocation of compliance guidelines
- Transparency of logs allows you to see directly which clients are/ were active in which form & why
- Can be used for audits & compliance documentation

4. COMBINATION OF NETWORK, DEVICE & IDENTITY SECURITY

- Optimum linking of network security, the respective devices & identities:
  - DTS Identity: Login, MFA & Conditional Access (policy enforcement)
  - DTS Identity Client: Visibility of the device & the respective device status
  - ARP-GUARD NAC: Securing the network

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de

DTS-Identity Client ENG 15072024