KDFM eXplorer

PLATFORM SECURITY

- Servers located in the EU
- Independent Software Vendor (ISV) not tied to any manufacturer of hardware
- Recurring-cycle of DCA Application Security Assessments by independent cybersecurity consulting firms
- Platform certified with ISO27001 and complies with the European Data Protection Regulation (GDPR).
- GDPR compliance: a Data Processing Agreement (DPA) via automated e-signing process
- DCA agent version 3 supports SNMPv1 / v2 in Read mode only. DCA version 4 under testing phase with support for SNMPv3 and hostnames filtering.
- All web services are protected by RSA SHA -2 256 Bit TLS encryption. 1.2
- SOC 2 Type 1 Security Audit Compliance: the practices and controls comply with the Security, Availability, Confidentiality requirements established by AICPA (American Institute).
- Advanced User Authentication: Two-factor authentication, Single Sign-On (SSO) for Active Directory users (portal access via Windows authentication), granular user permissions, user deactivation after 5 unsuccessful attempts or if there is no connection within 90/180 days, DCA executable file disabled after 5 times.
- Certifications: SOC 2 Type 1, Okta, BLI Security validation test, ISO 27001 TUV

Additional info:

1. The Cloud can’t “call” the DCA installed on the PC so NO port or service is exposed to the internet by the customer networks.
2. It is always the DCA that starts the communication through HTTP protocol and to an HTTPS endpoint (port 443) and the communication is encrypted using the SSL certificate.
3. The calls are common for HTTP calls:
   HTTP GET when we ask the cloud to get information
   HTTP POST when we send information or files back to the cloud.
4. The DCA uses the SNMP protocol on port 161 to read printers MIB in the customer network and only for the range of IP Address configured.
5. The DCA can send ICMP packets (there is no port specification) as well (this is used during troubleshooting)
6. There aren’t any other port or protocol.

TÜV SÜD ISO 27001

Oct. 2021