ZEISER VIRTUAL PILOT

ZEISER VIRTUAL PILOT

Der ZEISER-Support ist für Sie und Ihr ZEISER System garantiert, auch wenn der Zugang unserer Experten vor Ort nicht möglich ist!

Der ZEISER VIRTUAL PILOT ist eine Software für den Fernzugriff, bei der die erweiterte und virtuelle Realität genutzt wird. Diese Technologie eröffnet ein großes Portfolio von Funktionen für Support Dienstleistungen, einschließlich Installationen, Fehlerbehebungen, Schulungen und routinemäßiger Wartungen.

Die Hauptmerkmale

SICHER
- Die sicherste Lösung auf dem Markt
- Weltweit für datenkritische Infrastruktur zugelassen

ZUVERLÄSSIG
- Funktioniert in jedem Netzwerk von 4G bis Satellit
- Garantierte Bildqualität bei geringer Bandbreite

EINFACH
- Einfache Verwendung auf Telefonen, Tablets, PCs und Smart-Brillen

Die Vorteile

Intelligenter und innovativer Service kombiniert mit optimierten Workflow-Prozessen garantieren eine enge Zusammenarbeit mit dem Kunden.

Beispiel – Screenshots einer Support Sitzung:

App & Datensicherheit

- Die Kontoauthentifizierung neuer Geräte erfolgt mit einer authentifizierten SMS mit einem 5-stelligen Code (kryptografisch starker Zufallszahlengenerator mit einer 10 ^ 5-Kombination).

- Lokaler Speicherschutz auf zwei Arten (Anmeldeinformationsdatei wird durch AES-256-Verschlüsselung verschlüsselt und zweitens das Kennwort, das automatisch aus ca. 10 ^ 53 Kombinationen gemäß FIPS 140-2 generiert wird.

- Die Sicherheit des Kommunikationskanals wird von einem TLS (Transport Layer Security) über Port 443 organisiert. Das TLS-Sicherheitszertifikat verwendet RSA-Schlüssel mit einem 2048-Bit-Modul und SHA-256-Hash.

- Virtual Private Cloud (VPC), die externe eingehende Verbindung ist ausschließlich TLS / 443, die über einen einzigen Zugriffspunkt (Elastic Load Balancer) geleitet wird. "Inter-Region VPC-Peering" verschlüsselt den Inter-Region-Verkehr, der immer im globalen AWS-Backbone verbleibt und niemals das öffentliche Internet berührt, wodurch Bedrohungsvektoren wie häufige Exploits und DDoS-Angriffe reduziert werden."

- ISO 27001-Standard, Authentifizierungsinformationen (Passwort) werden auf dem Server gespeichert (SHA2-512)

- Einzelner Standardport 443

- Apache Tomcat-Webserver mit kryptografischem Subsystem, das über OpenSSL implementiert wurde

- Layer 1 DDoS-Schutz, Elastic Load Balancer