

## Kein direkter Zugriff

Um den direkten Zugriff auf eine Anlage oder ein System zu verhindern kommt Privileged Access Management (PAM) zur Anwendung. Dabei werden die Endpunktbenutzer aus einer Anlage oder einem System entfernt und ein Zugriff erfolgt via dedizierter Appliance auf einen Jump-Host, von welchem aus auf die notwendige Anlage zugegriffen wird.

Der Jump-Host fungiert als gehärtetes und überwachtes System und die Appliance als Zwischenstelle für die Verbindung. Damit wird verhindert, dass Benutzer direkt auf Ressourcen zugreifen, die sich in einem anderen Sicherheitsbereich befinden.

### Least-Privilege-Prinzip

Benutzern werden nur die minimal notwendigen Zugriffsrechte gewährt, die für die Ausführung ihrer Aufgaben erforderlich sind. Damit wird die Sicherheit von Daten und System erhöht.

### Kontinuierliche Überwachung

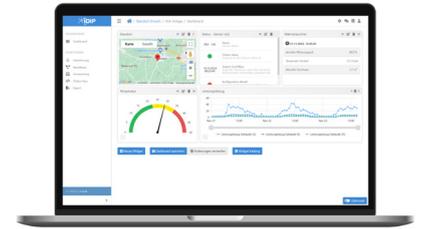
Benutzeraktivitäten werden in Echtzeit überwacht und durch Videoaufzeichnung historisiert. Damit auf verdächtige oder ungewöhnliche Aktivitäten reagiert werden kann.

### Rollenbasierte Zugriffskontrolle

Benutzern wird aufgrund ihrer Rollen und Verantwortlichkeiten der Zugriff auf bestimmte Ressourcen gewährt um so die Sicherheit und den Schutz sensibler Daten zu gewährleisten.

### Zeitlich begrenzte Zugriffe

Benutzer können nur für einen begrenzten Zeitraum auf Ressourcen zugreifen. Damit wird das Risiko von unbefugtem Zugriff und Missbrauch zu minimiert.



### iDIP IoT Service Portal

- Live Dashboards mit KPI
- Alarmierung und Überwachung
- Fernwartung
- Remote Visualisierung von Anlagen
- Fernzugriff als PAM
- Berichterstellung für Reporting
- Datenaustausch über REST API
- Multimandantenverwaltung
- Eigenes Kundenportal mit White-Label-Branding
- Datenkonnectoren (OPC-UA, Modbus TCP, MQTT, REST API)
- Sensorintegration via LoRa, LTE-M
- Schweizer Rechenzentrum (ISO 27001 / ISO 50001)

## Volle Zugriffskontrolle bei Anlagen und Systemen

