ProcessLink

Security Whitepaper

Umfassende Sicherheitsarchitektur
für Prozessdokumentation

Version 1.0 | Oktober 2024

Vertraulichkeit: Öffentlich

Inhaltsverzeichnis

Executive Summary

ProcessLink ist eine SaaS-Plattform zur videobasierten Prozessdokumentation mit KI-gestützter Analyse. Dieses Whitepaper beschreibt die Sicherheitsarchitektur und erklärt, wie ProcessLink sensible Unternehmensdaten schützt.

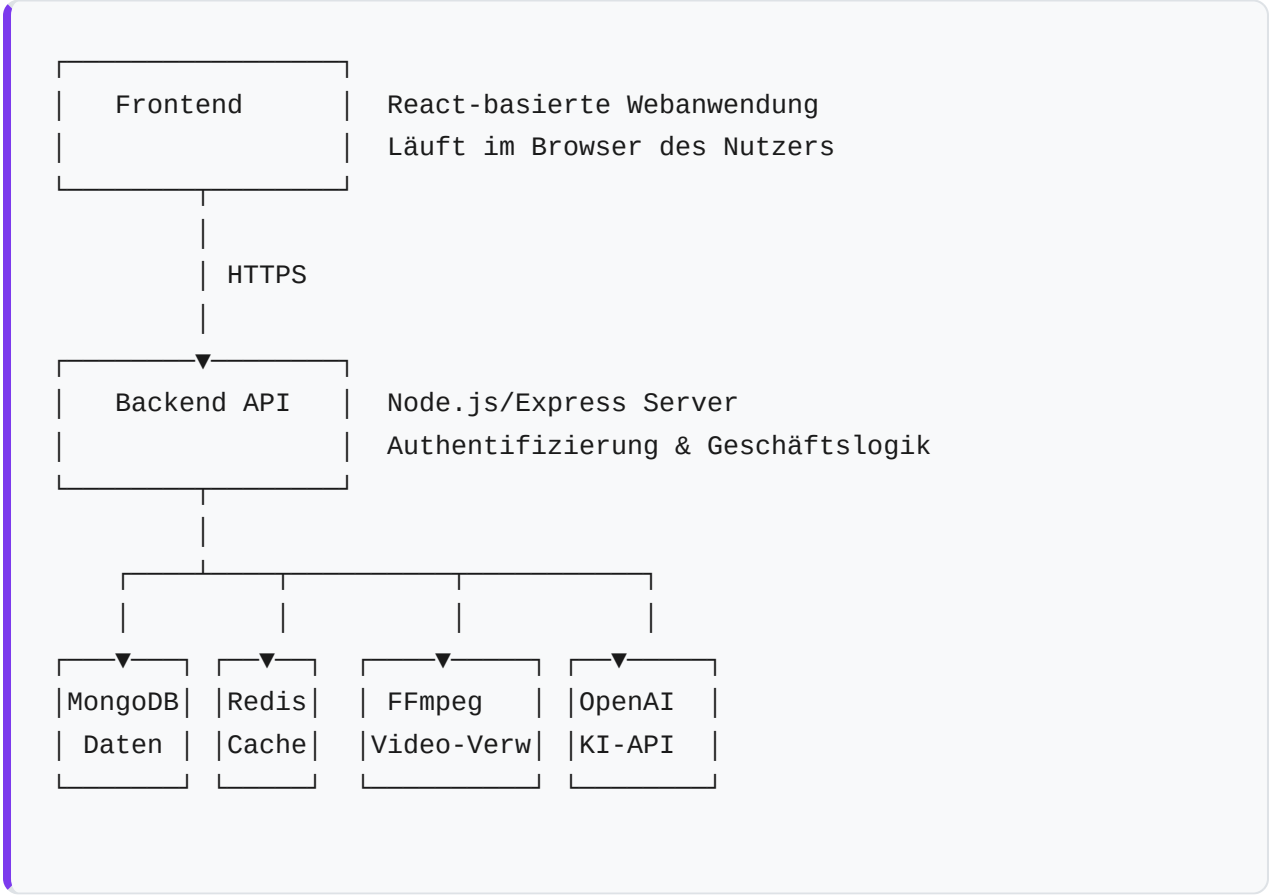
Kernmerkmale der Sicherheitsarchitektur:

- **IP-basierte Zugriffskontrolle (IP-Guard)** für Firmennetzwerk-Beschränkung
- **Multi-Tenant Isolation** mit vollständiger Datentrennung
- **Rollenbasierte Zugriffskontrolle (RBAC)** mit drei Berechtigungsstufen
- **Eingeschränkter Prozesszugriff** mit expliziter Freigabe
- **Deaktivierbares Link-Sharing** für maximale Kontrolle
- **Vollständige Audit-Logs** mit 90-Tage-Aufbewahrung
- **DSGVO-konforme Datenhaltung** auf EU-Servern

1. Architektur-Übersicht

1.1 Systemkomponenten

ProcessLink basiert auf einer modernen, mehrschichtigen Architektur:



1.2 Datenfluss

1. **Upload:** Nutzer lädt Video über HTTPS hoch
2. **Authentifizierung:** JWT-Token validiert Nutzer und Tenant
3. **Verarbeitung:** Video wird komprimiert, transkribiert und analysiert
4. **Speicherung:** Verschlüsselte Speicherung in MongoDB und Hetzner Storage
5. **Zugriff:** Mehrschichtige Autorisierungsprüfung bei jedem Zugriff

2. IP-Guard: Firmennetzwerk-basierte Zugriffskontrolle

2.1 Funktionsweise

IP-Guard schützt geteilte Prozesse durch Einschränkung auf bestimmte IP-Adressen oder IP-Bereiche. Dies geht weit über einfaches Geo-Blocking hinaus.

Unterschied zu Geo-Blocking:

Feature	Geo-Blocking	IP-Guard
Basis	Geografische Region	Spezifische Firmen-IP
VPN-Umgehung	✗ Leicht möglich	✓ Verhindert
Präzision	Ungenau (Stadt-Ebene)	Exakt (IP-Adresse)
Firmennetzwerk	✗ Nicht möglich	✓ Exakt möglich

2.2 Technische Implementierung

```
// Wenn ein geteilter Link aufgerufen wird:
1. System extrahiert Client-IP-Adresse
2. Bereinigung der IP (IPv6 → IPv4 Konvertierung)
3. Lookup: Welchem Tenant gehört dieser Share-Link?
4. Prüfung: Ist IP-Guard für diesen Tenant aktiviert?
5. Validierung: Ist Client-IP in der Whitelist?
   - Unterstützt einzelne IPs: 203.0.113.50
   - Unterstützt IP-Bereiche: 203.0.113.0/24
   - Unterstützt CIDR-Notation
6. Zugriff gewähren oder ablehnen
```

2.3 Anwendungsfälle

Szenario 1: QR-Code für Produktionshalle

- QR-Code wird in der Produktionshalle aufgehängt
- Mitarbeiter scannen mit Mobilgerät
- IP-Guard prüft: Ist das Gerät im Firmen-WLAN?
- Zugriff wird nur bei positiver Prüfung gewährt

Szenario 2: Mehrere Standorte

- Unternehmen mit Büros in München, Berlin, Hamburg
- IP-Bereiche aller drei Standorte werden hinterlegt
- Prozess ist von allen Standorten abrufbar, aber nicht von außen

Szenario 3: Remote-Zugriff

- Unternehmen nutzt VPN für Homeoffice
- VPN-Gateway IP wird in Whitelist aufgenommen
- Mitarbeiter können von zuhause über VPN zugreifen

3. Rollenbasierte Zugriffskontrolle (RBAC)

3.1 Rollen-Hierarchie

Rolle	Berechtigungen	Anwendungsfall
Owner	Vollzugriff inkl. Abrechnung, Team-Verwaltung, Sicherheitseinstellungen	Account-Eigentümer
Admin	Prozesse verwalten, Team-Mitglieder einladen, IP-Guard konfigurieren, Activity Log einsehen	Abteilungsleiter
User	Eigene Prozesse erstellen, freigegebene Prozesse ansehen	Standard-Mitarbeiter

3.2 Berechtigungs-Matrix

Aktion	Owner	Admin	User
Eigene Prozesse erstellen	✓	✓	✓
Eigene Prozesse löschen	✓	✓	✓
Fremde Prozesse ansehen*	✓	✓	✓
Fremde Prozesse bearbeiten	✓	✓	✗
Fremde Prozesse löschen	✓	✓	✗
Team-Mitglieder einladen	✓	✓	✗
IP-Guard konfigurieren	✓	✓	✗
Activity Log einsehen	✓	✓	✗
Abrechnung verwalten	✓	✗	✗

* Nur wenn explizit freigegeben oder nicht eingeschränkt

4. Eingeschränkte Prozesse

4.1 Konzept

Eingeschränkte Prozesse bieten eine zusätzliche Sicherheitsebene:

- **Sichtbarkeit:** Prozess taucht in Suchergebnissen auf
- **Metadaten:** Titel und Tags sind sichtbar
- **Inhalte:** Video, Transkript und Details bleiben verborgen
- **Zugriff:** Nur mit expliziter Freigabe möglich

4.2 Automatische Sicherheitsmaßnahmen

Wenn ein Prozess als "eingeschränkt" markiert wird:

1. **Link-Sharing wird automatisch deaktiviert**
   - Bestehende Share-Links werden ungültig
   - Neue Share-Links können nicht erstellt werden
2. **Viewer-Liste wird aktiviert**
   - Nur explizit freigegebene Nutzer können zugreifen
3. **Audit-Log wird aktualisiert**
   - Änderung wird protokolliert
   - Wer hat die Einschränkung aktiviert?
   - Wann wurde sie aktiviert?

4.3 Anwendungsfälle

Szenario 1: Buchhaltungssoftware

- **Prozess:** "Jahresabschluss in DATEV erstellen"
- **Einschränkung:** Aktiv
- **Freigabe nur für:** Buchhaltungs-Team (3 Personen)
- **Andere Mitarbeiter sehen:** "Jahresabschluss in DATEV erstellen" in Suche
- **Beim Klick:** "Zugriff verweigert - Kontaktieren Sie Ihren Administrator"

10. DSGVO-Compliance

10.1 Rechtliche Grundlagen

ProcessLink erfüllt alle DSGVO-Anforderungen:

Rechtsgrundlage der Verarbeitung:

- Art. 6 Abs. 1 lit. b DSGVO: Vertragserfüllung
- Art. 6 Abs. 1 lit. f DSGVO: Berechtigtes Interesse (Sicherheit)

Betroffenenrechte (Art. 12-22 DSGVO):

- ✓ Auskunftsrecht (Art. 15): Export aller Nutzerdaten
- ✓ Recht auf Berichtigung (Art. 16): Profil-Einstellungen
- ✓ Recht auf Löschung (Art. 17): Account-Löschung
- ✓ Recht auf Datenübertragbarkeit (Art. 20): JSON/CSV-Export
- ✓ Widerspruchsrecht (Art. 21): Deaktivierung

10.2 Auftragsverarbeiter (Art. 28 DSGVO)

Dienst	Zweck	Standort	AVV
Hetzner Cloud Server (MongoDB)	Datenbank	Deutschland (Falkenstein)	✓
Hetzner Storage	File Storage	Deutschland (Falkenstein)	✓
Hetzner Cloud	Server-Hosting	Deutschland (Falkenstein)	✓
OpenAI	KI-Transkription	EU	✓
Stripe	Zahlungsabwicklung	EU	✓

Alle Auftragsverarbeiter:

- Haben AVV (Auftragsverarbeitungsvertrag) abgeschlossen
- Sind DSGVO-konform
- Verarbeiten Daten nur in EU
- Nutzen Daten nicht für eigene Zwecke

14. Sicherheits-Roadmap

14.1 Bereits implementiert

Implementiert

- IP-Guard mit IP-Range-Support
- Rollenbasierte Zugriffskontrolle (Owner/Admin/User)
- Eingeschränkte Prozesse mit Viewer-Kontrolle
- Activity Logging mit 90-Tage-Aufbewahrung
- Link-Sharing Deaktivierung
- Multi-Tenant-Isolation
- HTTPS/TLS-Verschlüsselung
- JWT-basierte Authentifizierung
- Brute-Force-Schutz
- DSGVO-konforme Datenhaltung

14.2 In Entwicklung

In Entwicklung

- **Zwei-Faktor-Authentifizierung (2FA/MFA)**
  - TOTP-basiert (Google Authenticator, Authy)
  - SMS-Backup (optional)
  - Hardware-Token-Support (YubiKey)
- **Single Sign-On (SSO)**
  - SAML 2.0 Support
  - OAuth 2.0 / OpenID Connect
  - Integration mit Azure AD, Google Workspace, Okta
- **Erweiterte Audit-Logs**
  - Export in SIEM-Systeme (Splunk, ELK)
  - Real-time Alerting
  - Anomalie-Erkennung

14.3 Geplante Features

Geplant

- **Ende-zu-Ende-Verschlüsselung (E2EE)**
- **Erweiterte DLP (Data Loss Prevention)**
- **Compliance-Zertifizierungen** (ISO 27001, SOC 2 Type II, TISAX)
- **On-Premise Deployment**
- **Advanced Threat Protection**

16. Anhang

16.1 Glossar

Begriff	Erklärung
Access Token	JWT-basierter Token für Authentifizierung (7 Tage gültig)
Activity Log	Audit-Trail aller sicherheitsrelevanten Aktionen
AVV	Auftragsverarbeitungsvertrag (gemäß Art. 28 DSGVO)
CIDR	Classless Inter-Domain Routing (IP-Adressbereich, z.B. 192.168.1.0/24)
DSGVO	Datenschutz-Grundverordnung (EU-Recht)
E2EE	Ende-zu-Ende-Verschlüsselung
IP-Guard	ProcessLink-eigene IP-basierte Zugriffskontrolle
JWT	JSON Web Token (Standard für Authentifizierung)
Multi-Tenant	Architektur für mehrere Kunden auf einer Plattform
RBAC	Role-Based Access Control (Rollenbasierte Zugriffskontrolle)
TLS	Transport Layer Security (Verschlüsselungsprotokoll)
ZDR	Zero Data Retention (OpenAI-Feature: keine Datenspeicherung)

16.2 Compliance-Checkliste

DSGVO-Compliance:

- ✓ Datenschutzerklärung vorhanden
- ✓ AVV mit allen Auftragsverarbeitern
- ✓ Löschkonzept implementiert
- ✓ Betroffenenrechte umsetzbar
- ✓ Datenverarbeitung in EU
- ✓ Technische und organisatorische Maßnahmen (TOMs)

IT-Sicherheit:

- ✓ Verschlüsselte Datenübertragung (HTTPS/TLS)
- ✓ Verschlüsselte Datenspeicherung
- ✓ Authentifizierung und Autorisierung
- ✓ Audit-Logging
- ✓ Backup-Strategie

Fazit

ProcessLink bietet eine umfassende Sicherheitsarchitektur, die speziell für den Schutz sensibler Prozessdokumentationen entwickelt wurde. Mit IP-Guard, mehrstufiger Zugriffskontrolle, eingeschränkten Prozessen und vollständigem Audit-Trail haben Unternehmen die volle Kontrolle über ihr Wissen.

Die DSGVO-konforme Umsetzung mit EU-Hosting, Zero-Data-Retention bei OpenAI und transparenter Datenverarbeitung gewährleistet höchste Datenschutz-Standards.

Für Fragen oder detaillierte Informationen zu spezifischen Sicherheitsaspekten kontaktieren Sie bitte unser Security-Team unter security@processlink.de.

OperativeX GmbH
Warendorf, Deutschland
https://processlink.de

Dieses Dokument wird regelmäßig aktualisiert. Letzte Aktualisierung: Oktober 2025