NRZ-System Integrations-szenarien

Strategische Optionen für IT, Rechenzentrum, CISO und Endkunden

JANUAR 2026

Management Summary

Strategische Erkenntnisse für die Geschäftsleitung

STRATEGISCHE FLEXIBILITÄT

Kein "One-Size-Fits-All". Fünf Szenarien ermöglichen die Anbindung jeder Kundenumgebung – von hochsicheren Rechenzentren bis zu restriktiven Behördennetzen.

100%
MARKTABDECKUNG

SKALIERBARE SICHERHEIT

Das Sicherheitsniveau wächst mit den Anforderungen. Zentral gehostete Lösungen (Szenario 3 & 4) bieten ISO-zertifizierten Schutz ohne lokalen Aufwand für den Kunden.

Zero Trust
ARCHITEKTUR-ANSATZ

OPERATIVE EXZELLENZ

Integration ist der Schlüssel zur Effizienz. Automatisierte Datenflüsse reduzieren manuelle Fehler, beschleunigen Abrechnungsprozesse und entlasten Fachkräfte.

< 12 Mon.
ROI ERWARTUNG

EMPFEHLUNG

Priorisieren Sie **Szenario 4 (Managed API)** als Standard für maximale Skalierbarkeit und Sicherheit. Nutzen Sie Szenario 5 als taktische Brückenlösung für schnelle Marktdurchdringung.

Executive Summary

Fünf Wege zur modernen NRZ-Integration

Das NRZ-System bietet fünf strategische Integrationsszenarien, die unterschiedliche Anforderungen an Sicherheit, Kontrolle und Funktionalität adressieren.

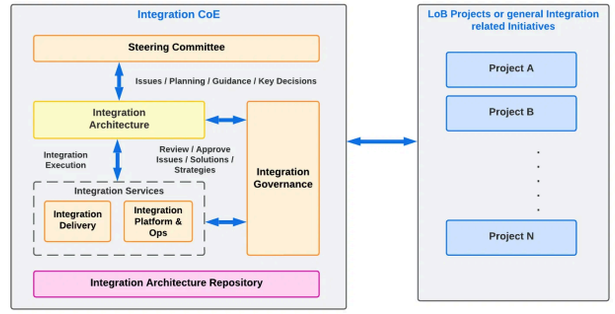
01 **Kundenseitige API (Nur-Lesen):** Maximale Kontrolle für Reporting und Dashboards.

02 **Kundenseitige API (RW):** Vollständige Integrationskontrolle für eigene Apps.

03 **Rechenzentrum-API (Nur-Lesen):** Höchste Sicherheit durch Netzwerkisolation.

04 **Rechenzentrum-API (RW):** Managed Service mit maximaler Sicherheit.

05 **XCare XChange Tool:** Pragmatische Rückfalllösung ohne Infrastruktur.

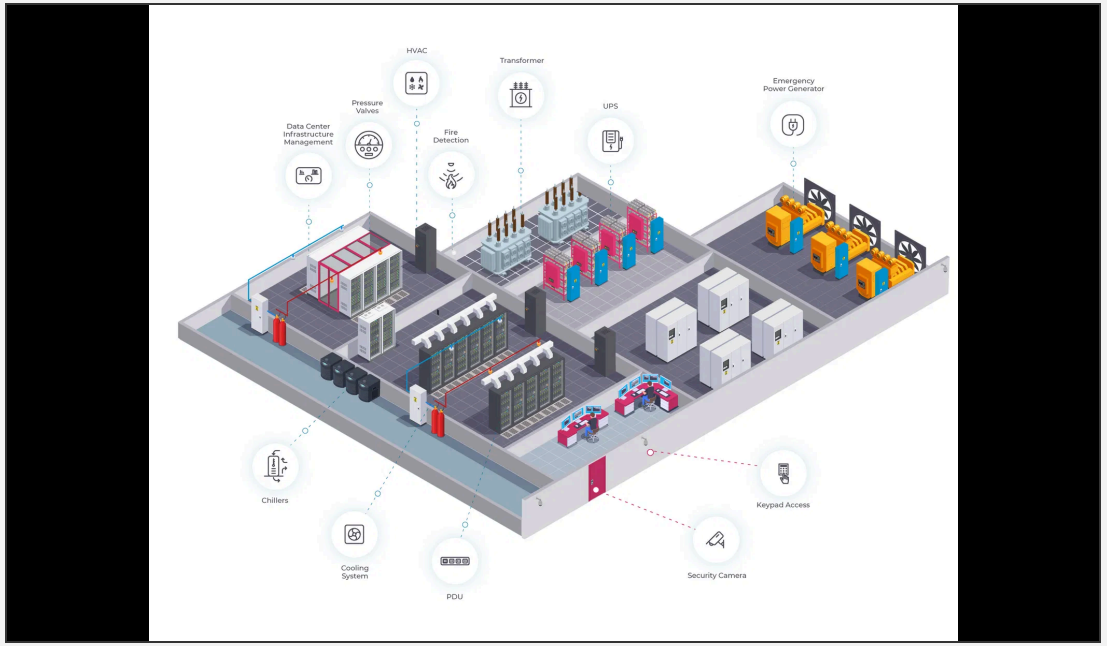


ZENTRALE ERKENNTNISSE

- Maßgeschneiderte Strategien für jede Sicherheitsstufe.
- Wahl abhängig von IT-Kapazitäten und Compliance.
- Hybride Ansätze ermöglichen schrittweise Migration.

NRZ-Systemarchitektur

Fundament der Integration



Hochsichere Rechenzentrumsumgebung mit redundanten Komponenten

KERNKOMPONENTEN

NRZ Server 1	Zentrale Anwendungslogik & Prozesse
NRZ Server 2	Backend Database (Single Source of Truth)
ProAlert	Frontend / Terminal-Server UI
FS Server	Dedizierter File Storage & Versionierung
GK Server	Systemfunktionen, Monitoring & Logging

SICHERHEITSARCHITEKTUR

VPN-basierter Zugang mit **Multi-Faktor-Authentifizierung**, Firewall-geschützte Datenbankzugriffe, georedundante Spiegelung über mehrere Rechenzentren und strikte **Netzwerksegmentierung** zur Isolation kritischer Komponenten.

XCare-Integrationswerkzeuge

Technologische Enabler für flexible Implementierungen

XCare-API (RESTful Backend)

Moderne RESTful-Architektur mit JSON-Datenformaten und **OAuth 2.0 Authentifizierung**. Bietet vollständige CRUD-Operationen und eine umfassende Swagger-Dokumentation für Entwickler.

XCare-Web-Oberfläche

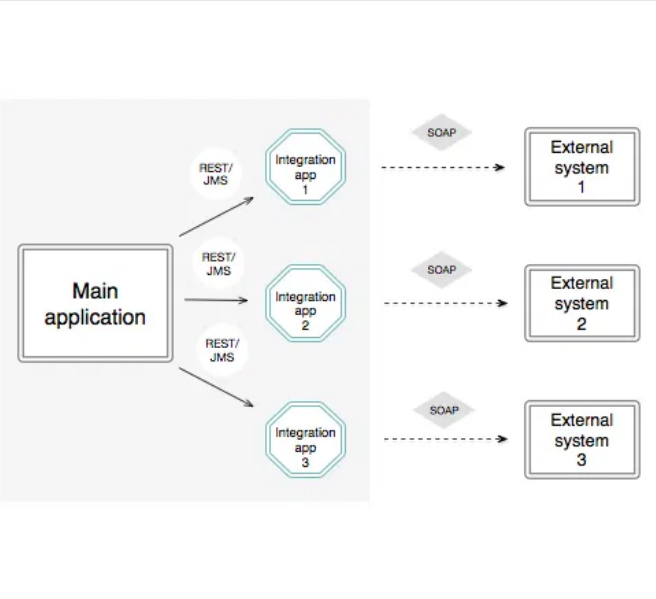
Responsive Web-UI mit Single Sign-On (SSO) Integration. Ermöglicht direkten Zugriff auf Systemfunktionen über die API-Schicht ohne VPN-Zwang für Endanwender.

XCare XChange Tool

Dateibasierte Import-/Export-Lösung für restriktive Umgebungen. Unterstützt CSV, XML und JSON mit integrierter Validierung vor dem Datenimport.

Multi-Import & Pro-Import Tools

Spezialisierte Werkzeuge für Massendatenimporte und komplexe Mapping-Anforderungen. Ideal für Migrationen und regelmäßige Batch-Verarbeitungen.



Die XCare-Toolchain deckt das gesamte Spektrum von manuellen Datei-Uploads bis zu vollautomatisierten API-Workflows ab.

Szenario 1: Kundenseitige API

Maximale Kontrolle für Reporting & Analytics

NUR-LESEN

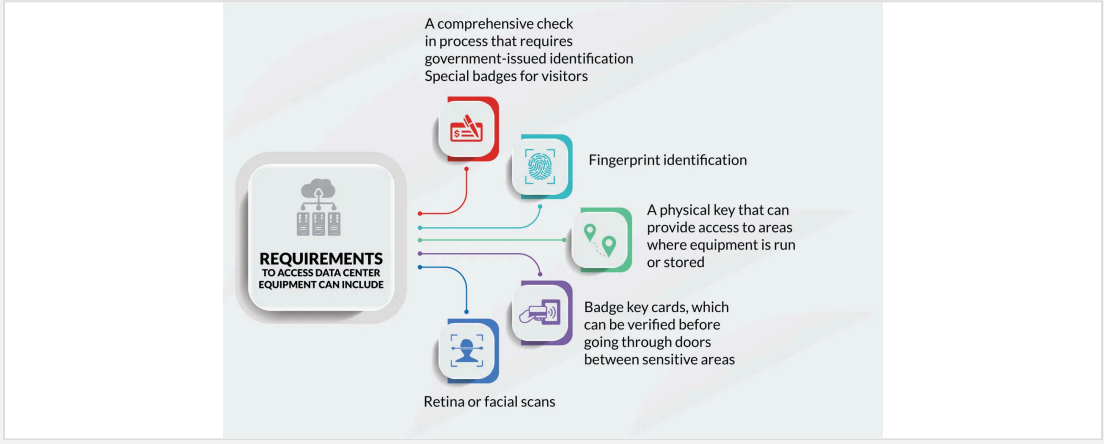
TECHNISCHE IMPLEMENTIERUNG

In diesem Szenario hostet der Kunde die XCare-API auf der eigenen Infrastruktur. Ein sicherer VPN-Tunnel verbindet die Kundenumgebung mit dem Rechenzentrum.

- →**Hosting:** On-Premise / Private Cloud des Kunden
- →**Verbindung:** Site-to-Site VPN Tunnel
- →**Firewall:** Port 3050 (Datenbank) geöffnet
- →**Berechtigung:** Striktes Read-Only auf Datenbankebene

PRIMÄRE ANWENDUNGSFÄLLE

- →Business-Intelligence-Dashboards (PowerBI, Tableau)
- →Zentrale Datenanalyse-Plattformen
- →Mobile Anwendungen für Außendienst (Informationsabruf)
- →Integration von Drittanbieter-Reporting-Tools



VORTEILE

- + Volle Kontrolle über API-Infrastruktur
- + Integration in eigenes Monitoring
- + Unabhängigkeit von RZ-Prozessen
- + Skalierbarkeit nach eigenem Bedarf

ÜBERLEGUNGEN

- - Volle Betriebsverantwortung
- - Technisches Fachwissen nötig
- - Keine Schreibzugriffe möglich
- - Firewall-Konfiguration erforderlich

Szenario 2: Kundenseitige API (Lesen-Schreiben)

Vollständige Integrationskontrolle für bidirektionale Prozesse

TECHNISCHE IMPLEMENTIERUNG

Erweiterung von Szenario 1 um Schreibzugriff. Die XCare-API läuft in der Kundeninfrastruktur mit VPN-Tunnel zum Rechenzentrum. Ermöglicht vollständige **CRUD-Operationen** (Create, Read, Update, Delete) auf der Datenbank. Erfordert striktes IP-Whitelisting, RBAC (Role-Based Access Control) und detaillierte Audit-Logs.

PRIMÄRE ANWENDUNGSFÄLLE

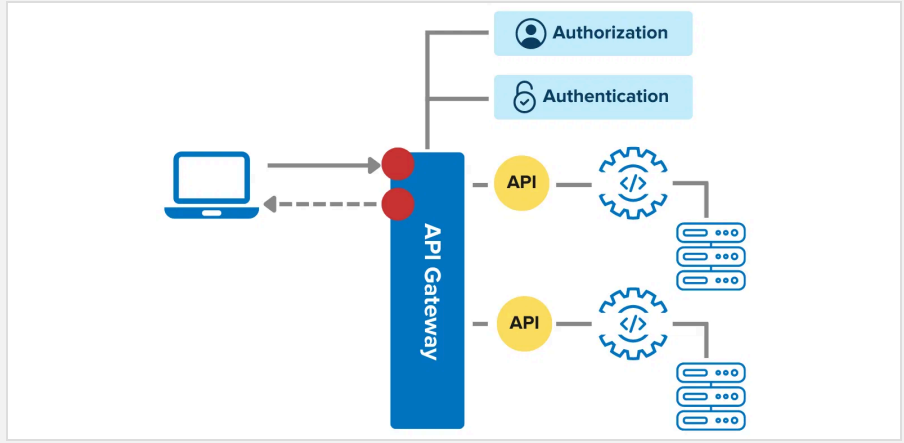
- Workflow-Automatisierung & Prozesssteuerung
- Self-Service-Portale für Endanwender
- Tiefe Integration in CRM/ERP-Systeme

Vorteile

+ Einheitlicher API-Ansatz
+ Echtzeit-Synchronisation

Überlegungen

! Erhöhte Sicherheitsanforderungen
! Verantwortung für Datenintegrität

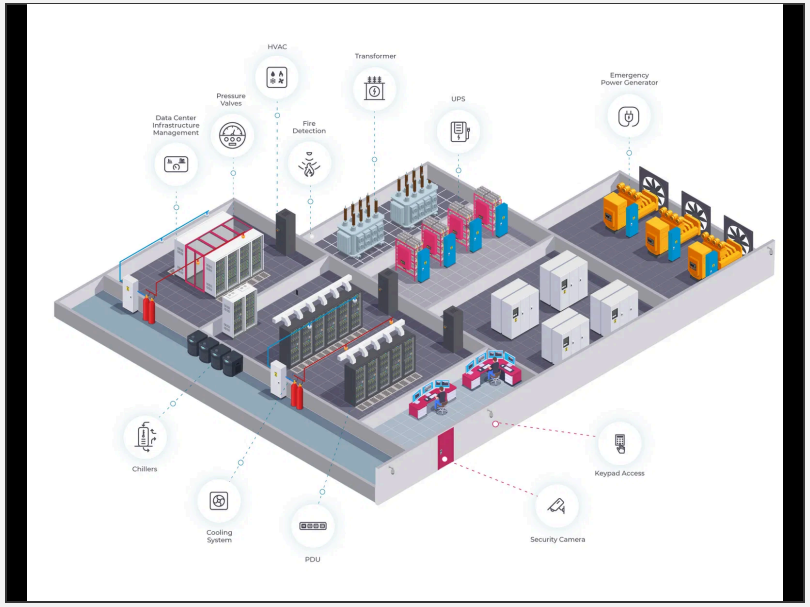


SICHERHEITS-FOKUS

Bei Schreibzugriffen ist die **Datenintegrität** kritisch. Implementieren Sie robuste Validierungslogik auf Client-Seite und nutzen Sie Transaktionen, um inkonsistente Datenzustände bei Verbindungsabbrüchen zu vermeiden.

Szenario 3: Rechenzentrum-API (Nur-Lesen)

Maximale Sicherheit durch Netzwerkisolation



SICHERHEITS-FOKUS

Keine externen Datenbankports. Vollständige Isolation im Rechenzentrum. Zugriff ausschließlich über gesicherte VPN-Tunnel.

Technische Implementierung

Die XCare-API läuft auf einem dedizierten Server direkt im Rechenzentrum. Alle Datenbankzugriffe erfolgen über das interne Netzwerk. Kunden greifen via VPN (HTTPS) auf die API zu.

Primäre Anwendungsfälle

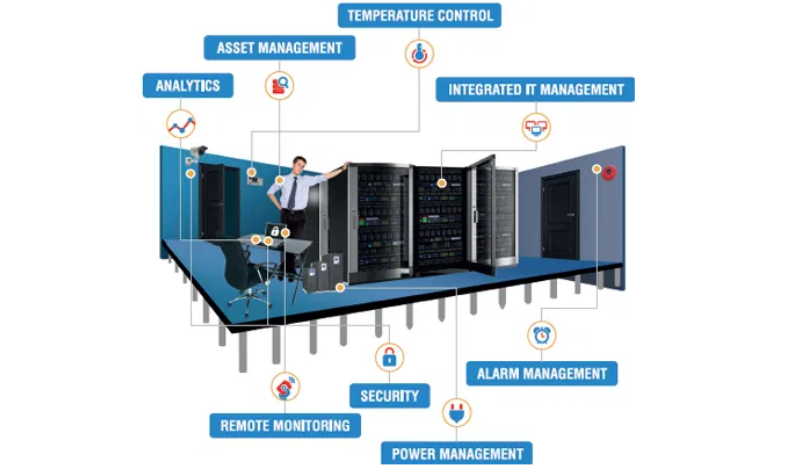
- Organisationen mit strengen Sicherheitsrichtlinien (keine externen DB-Ports).
- Finanzinstitute und Gesundheitswesen.
- Regierungsbehörden mit Compliance-Anforderungen.

Vorteile

- Höchstes Sicherheitsniveau durch Netzwerkisolation.
- Keine Änderungen an externen Firewalls nötig.
- Vereinfachte Compliance-Audits & Managed Service.

Szenario 4: Rechenzentrum-API (RW)

Optimale Balance von Sicherheit und Funktionalität



TECHNISCHE IMPLEMENTIERUNG

Identisch zu Szenario 3, jedoch mit **vollständigen Lese-Schreib-Berechtigungen** (CRUD) über das interne Netzwerk. Erweiterte Sicherheitsmaßnahmen wie OAuth 2.0, JWT und RBAC sind zwingend.

Kombiniert die höchste Sicherheit der Netzwerkisolation mit der vollständigen Funktionalität einer bidirektionalen Integration. Ideal für regulierte Umgebungen.

Primäre Anwendungsfälle

- Workflow-Automatisierung mit höchsten Sicherheitsanforderungen
- Self-Service-Portale in regulierten Branchen
- Tiefe Systemintegration unter Compliance-Vorgaben

Überlegungen

- Höchste Implementierungskomplexität
- Robuste Sicherheitsmaßnahmen im RZ erforderlich
- Klare SLAs und Premium-Service-Kosten

STRATEGISCHE VORTEILE

Maximale Sicherheit
Netzwerkisolation ohne Funktionseinbußen.

Managed Service
Professioneller Betrieb und SOC-Überwachung.

Compliance Ready
Zentrale Audit-Protokollierung und Kontrolle.

Full Feature
Keine Einschränkungen in der Funktionalität.

Szenario 5: XCare XChange Tool

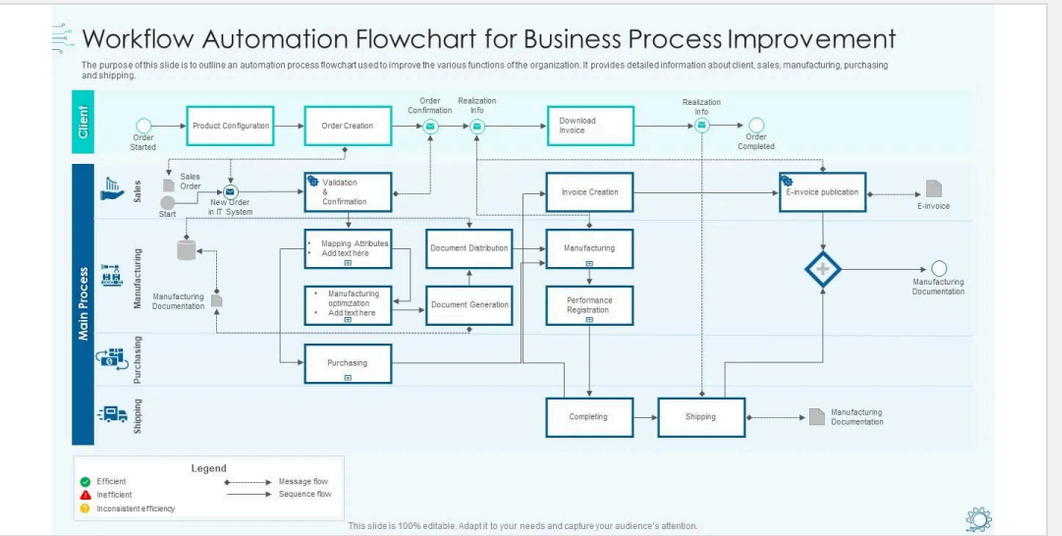
Pragmatische Rückfalllösung für restriktive Umgebungen

TECHNISCHE IMPLEMENTIERUNG

Dateibasierte Import-/Export-Lösung, die auf Client-Systemen installiert wird. Daten werden in standardisierten Formaten (CSV, XML, JSON) exportiert. Benutzer laden Dateien manuell über Remote-Desktop auf den Terminal Server.

PRIMÄRE ANWENDUNGSFÄLLE

- Organisationen mit restriktiven IT-Richtlinien (keine API erlaubt)
- Regierungsbehörden mit starren Change-Control-Prozessen
- Ad-hoc-Datenextraktionen und Proof-of-Concept-Projekte
- Pilotprogramme vor vollständiger Integration



VORTEILE

+ Minimale Infrastruktur
+ Schnelle Bereitstellung (Minuten)
+ Keine Genehmigungsprozesse
+ Benutzerfreundliche Oberfläche

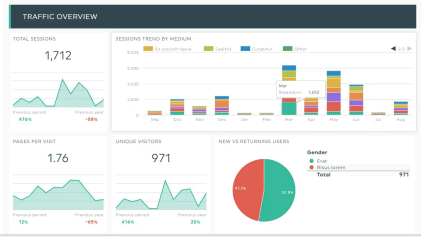
NACHTEILE

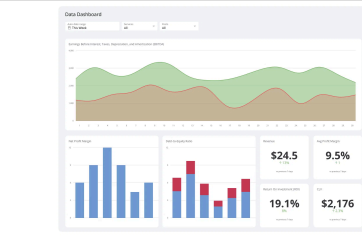
- Eingeschränkte Automatisierung
- Keine Echtzeit-Integration
- Manuelle Initiierung nötig
- Abhängigkeit von Terminal Server

Szenario-Vergleich

Entscheidungsmatrix für die optimale Wahl

KRITERIUM	SZENARIO 1 & 2 KUNDENSEITIG	SZENARIO 3 & 4 RECHENZENTRUM	SZENARIO 5 XCHANGE TOOL
Sicherheitsniveau	Mittel	**Sehr Hoch**	Hoch
Netzwerkexposition	**Port 3050 extern**	**Keine externen Ports**	Nur Terminal Server
Lesezugriff	Vollständig	Vollständig	Batch (Datei)
Schreibzugriff	S2: Vollständig	S4: Vollständig	Batch (Datei)
Automatisierung	**Hoch (Echtzeit)**	**Hoch (Echtzeit)**	Niedrig (Manuell)
Betriebsverantwortung	Kunde	Rechenzentrum	Geteilt
Setup-Aufwand	Mittel-Hoch	**Niedrig (für Kunde)**	**Sehr Niedrig**
Time-to-Market	2-8 Wochen	1-4 Wochen	**1-3 Tage**





EMPFEHLUNG

Wählen Sie **Szenario 3/4** für maximale Sicherheit bei kritischen Daten. Nutzen Sie **Szenario 5** für schnelle PoCs oder wenn keine Infrastruktur verfügbar ist.

Entscheidungshilfe

Wann welches Szenario optimal ist

SZENARIO 1 & 2

Kundengehostet

- ✓ Starke interne IT-Fähigkeiten.
- ✓ Direkte Kontrolle über Infrastruktur.
- ✓ API-Plattformen bereits verwaltet.
- ✓ Globale Anwendungslokation.
- ✓ Unabhängig von RZ-Prozessen.

SZENARIO 3 & 4

Rechenzentrum

- ✓ Externe DB-Ports verboten.
- ✓ Regulierte Branche, Compliance.
- ✓ RZ-Managed-Fachwissen nutzen.
- ✓ Keine starken internen Ops.
- ✓ Maximale Sicherheitsstufe.

SZENARIO 5

Rückfalloption

- ✓ API-Bereitstellung eingeschränkt.
- ✓ Strenge Budgetlimits.
- ✓ Temporäre PoC-/Pilotbedarfe.
- ✓ Schnelle Bereitstellung notwendig.
- ✓ Periodische Datenübertragung ok.

HYBRIDE ANSÄTZE

Kombinieren Sie Szenarien: Start mit schnelleren Optionen, dann schrittweise zu sichereren und skalierbaren Lösungen migrieren.

Sicherheitskonzepte im Vergleich

Differenzierte Schutzmaßnahmen für API, Rechenzentrum und Büro

API-LÖSUNG

HAUPTFOKUS

Zugriffskontrolle & Daten

KRITISCHE ASSETS

Geschäftsdaten, API-Keys

PRIMÄRE BEDROHUNGEN

- API-Missbrauch
- Datenlecks
- DDoS-Angriffe

MASSNAHMEN

- OAuth 2.0 / JWT
- API Gateway
- Rate Limiting

RECHENZENTRUM

HAUPTFOKUS

Infrastruktur & Netzwerk

KRITISCHE ASSETS

Server, Datenbanken

PRIMÄRE BEDROHUNGEN

- Netzwerkeinbrüche
- APTs
- Physischer Zugang

MASSNAHMEN

- Netzwerksegmentierung
- Firewalls / IDS / IPS
- Physische Sicherheit

BÜROUMGEBUNG

HAUPTFOKUS

Endpoint & Benutzer

KRITISCHE ASSETS

Workstations, User-IDs

PRIMÄRE BEDROHUNGEN

- Phishing
- Malware / Ransomware
- Social Engineering

MASSNAHMEN

- MFA / SSO
- Endpoint Protection
- Security Awareness

Jede Domäne erfordert spezifische Sicherheits-Frameworks und Compliance-Standards (ISO 27001, SOC 2, DSGVO), um einen ganzheitlichen Schutz zu gewährleisten.

Netzwerksicherheit und Verschlüsselung

Fundamentale Schutzschichten im Detailvergleich

NETZWERKSICHERHEIT

API-LÖSUNGEN

- **API Gateway** als zentrale Schutzmauer
- Rate Limiting & Throttling gegen Überlastung
- Striktes IP-Whitelisting für Clients

RECHENZENTRUM

- Umfassende **Netzwerksegmentierung**
- Mikrosegmentierung für Workloads
- Next-Gen Firewalls & IDS/IPS

BÜROUMGEBUNG

- Unternehmens-Firewalls am Perimeter
- Network Access Control (NAC)
- WLAN-Segmentierung (Gast/Intern)

VERSCHLÜSSELUNG

API-LÖSUNGEN

- **TLS 1.3** für Data in Transit
- Opaque Tokens für externe Clients
- Minimierung sensibler Daten in Payloads

RECHENZENTRUM

- Verschlüsselung auf allen Ebenen (Rest/Transit)
- Hardware Security Modules (**HSM**)
- Key Management Service (KMS)

BÜROUMGEBUNG

- Full Disk Encryption (BitLocker/FileVault)
- E-Mail-Verschlüsselung (S/MIME)
- VPN-Tunnel-Verschlüsselung

Monitoring, Compliance & Kosten

Operative und finanzielle Aspekte im Vergleich

MONITORING

API-LÖSUNG

- Protokollierung aller API-Zugriffe
- Echtzeit-Monitoring & Analytics
- Automatisierte Alerts bei Anomalien

RECHENZENTRUM

- Umfassende SIEM-Systeme
- 24/7 Security Operations Center (SOC)
- Automatisierte Incident Response

BÜROUMGEBUNG

- Endpoint Detection & Response (EDR)
- User Entity Behavior Analytics (UEBA)
- IT-Helpdesk Support

COMPLIANCE

API-LÖSUNG

- DSGVO & CCPA Konformität
- Detaillierte API-Dokumentation
- Regelmäßige Security Assessments

RECHENZENTRUM

- ISO 27001, SOC 2, PCI-DSS
- BSI IT-Grundschutz Zertifizierung
- Jährliche externe Audits

BÜROUMGEBUNG

- Security Awareness Trainings
- Clean Desk Policy
- Regelmäßige Access Reviews

KOSTENSTRUKTUR

API-LÖSUNG

Initial:
10k - 50k €
Betrieb:
500 - 5.000 € / Monat

RECHENZENTRUM

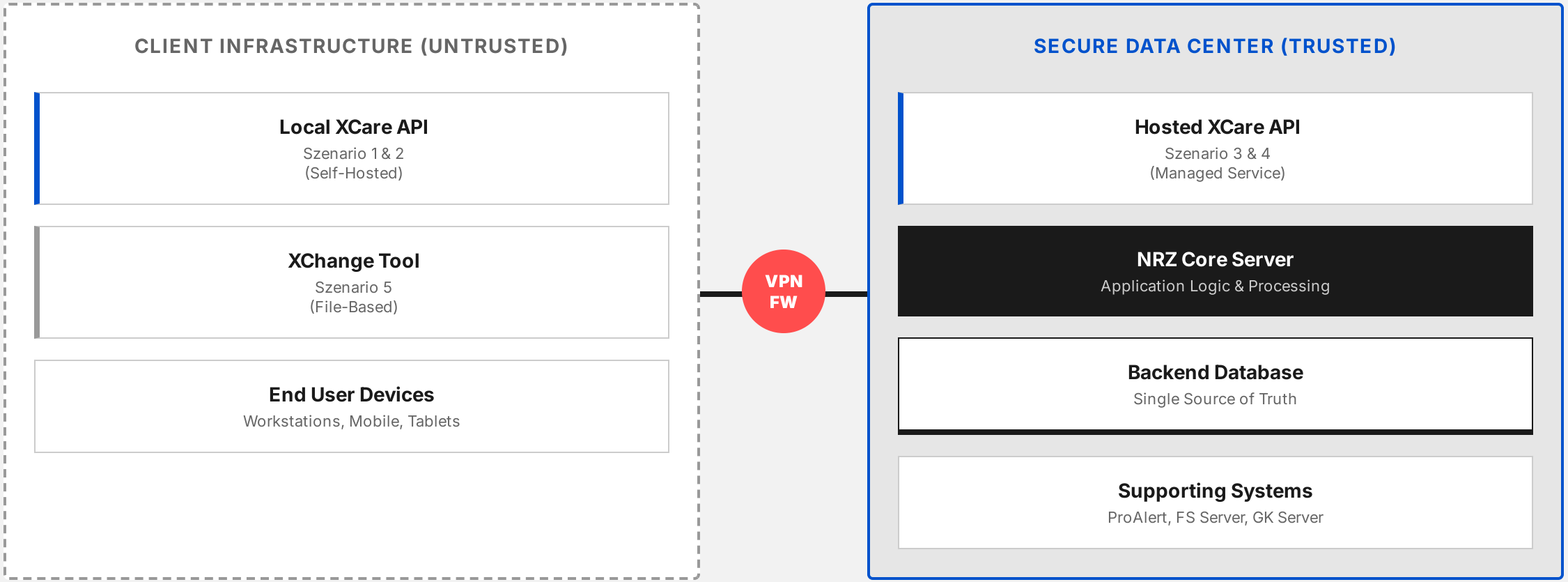
Initial:
100k - 1M €
Betrieb:
10k - 100k € / Monat

BÜROUMGEBUNG

Software:
30-100 € / User / Jahr
Betrieb:
50-200 € / User / Monat

NRZ-Systemarchitektur Visualisierung

Schematische Darstellung der Komponenten und Sicherheitszonen



API Integration Core System Security Layer Client Zone

Empfehlungen für IT-Teams

Technische Best Practices für Implementierung und Betrieb

KUNDENGEHOSTETE API

SZENARIO 1 & 2

- **Infrastruktur:** Containerisierung mit Docker/Kubernetes für Skalierbarkeit und Infrastructure as Code (IaC).
- **Sicherheit:** Implementierung von **OAuth 2.0 mit PKCE** und JWT-Validierung.

RECHENZENTRUM-API

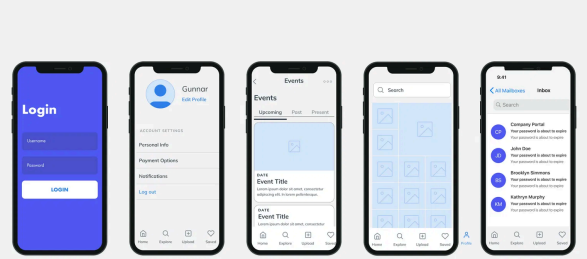
SZENARIO 3 & 4

- **Zusammenarbeit:** Definition klarer SLAs (99.9% Verfügbarkeit) und Change-Management-Prozesse.
- **Entwicklung: API-First-Design**, Bereitstellung von SDKs und umfassende Swagger-Dokumentation.

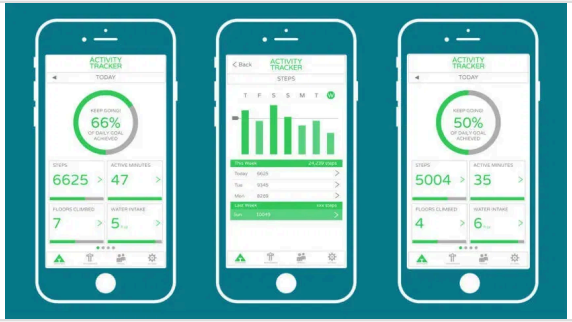
XCARE XCHANGE TOOL

SZENARIO 5

- **Prozessoptimierung:** Standardisierung der CSV/XML-Formate und automatisierte Transformations-Skripte.
- **Fehlerbehandlung:** Robuste Validierung vor dem Upload und definiertes Exception-Handling.



Strukturierte Entwicklungsprozesse sichern Qualität.



Endnutzer profitieren von performanten Interfaces.

Empfehlungen für Rechenzentren

Betrieb und Service Excellence

INFRASTRUKTUR & HOSTING

- Hochverfügbare Terminal-Server-Infrastruktur mit Load Balancing.
- Dedizierte API-Server und Gateway-Infrastruktur für Szenarien 3 & 4.
- Separate Umgebungen (Dev/Test/Prod) und Blue-Green-Deployment.
- Proaktives Monitoring und Kapazitätsplanung.

SICHERHEIT & COMPLIANCE

- Netzwerksegmentierung und Firewall-Regeln nach Least Privilege.
- Einsatz von PAM (Privileged Access Management) und Just-in-Time Access.
- Umfassende Audit-Protokollierung und regelmäßige Access Reviews.
- VPN-Infrastruktur mit Multi-Faktor-Authentifizierung.

SERVICE-MANAGEMENT

- **SLAs:** 99.9% Verfügbarkeit, API-Response < 200ms.
- **Support:** Reaktionszeit < 1 Stunde bei kritischen Incidents.
- **Change-Management:** Strukturierte Prozesse mit Testphasen.

Empfehlungen für CISOs

Strategien für Risikomanagement, Compliance und Governance

RISIKOMANAGEMENT

- → Implementieren Sie einen **Zero Trust Ansatz**: Vertrauen Sie keiner Verbindung implizit, auch nicht im RZ-LAN.
- → Bevorzugen Sie API-Integrationen (Szenario 3/4) gegenüber dateibasierten Transfers für bessere Sichtbarkeit und Kontrolle.
- → Führen Sie regelmäßige Penetrationstests für alle extern erreichbaren Endpunkte durch (besonders Szenario 1 & 2).

"Sichtbarkeit ist die Voraussetzung für Sicherheit."

COMPLIANCE & GOVERNANCE

- → Erzwingen Sie **Datenminimierung**: Übertragen Sie nur operativ notwendige Datenfelder.
- → Etablieren Sie lückenlose Audit-Trails für alle Datenzugriffe und -transfers zur Erfüllung der DSGVO-Nachweispflicht.
- → Definieren Sie klare Verantwortlichkeiten (RACI) für Daten in Transit und Daten at Rest.

"Compliance durch Design, nicht als Nachgedanke."

STRATEGISCHE AUSRICHTUNG

- → Wandeln Sie Security vom Blocker zum Enabler, indem Sie **sichere Standardmuster** (Blueprints) bereitstellen.
- → Integrieren Sie Sicherheitsprüfungen automatisiert in die CI/CD-Pipeline (DevSecOps).
- → Fordern und prüfen Sie regelmäßig die Sicherheitszertifikate (ISO 27001) Ihrer Rechenzentrumspartner.

"Sicherheit als Qualitätsmerkmal des Services."

Empfehlungen für Endkunden

Geschäftswert realisieren und Integration meistern

GESCHÄFTSWERT

EFFIZIENZSTEIGERUNG

Automatisierung eliminiert repetitive Aufgaben und schafft Kapazität für Wertschöpfung.

DATENQUALITÄT

Direkte Systemkopplung verhindert Übertragungsfehler – eine einheitliche Datenbasis.

KOSTENSENKUNG

Schnellere Durchlaufzeiten und weniger Korrekturen reduzieren operative Kosten.

ANWENDUNGSFÄLLE

PATIENTENMANAGEMENT

Echtzeit-Synchronisation von Stammdaten zwischen KIS und Subsystemen.

ABRECHNUNG & FAKTURA

Automatischer Datentransfer zu Abrechnungssystemen zur Beschleunigung des Cash-Flows.

MANAGEMENT REPORTING

Zentrales Dashboarding und Controlling auf Basis aggregierter Live-Daten.

ROADMAP

1

Analyse & Auswahl

Prüfung der Infrastruktur und Auswahl des passenden Szenarios.

2

Pilotierung

Proof-of-Concept mit unkritischen Daten für schnelle Erkenntnisse.

3

Integration

Technische Anbindung (APIs) und Sicherheitsmaßnahmen implementieren.

4

Go-Live & Skalierung

Produktivsetzung, Schulung und Rollout auf weitere Standorte.

Business Value Matrix

Vor- und Nachteile aus Endkunden-Sicht

	VORTEILE (BUSINESS VALUE)	NACHTEILE (RISIKEN/KOSTEN)	IMPACT
1 & 2 Self-Hosted	+ Volle Datenhoheit im eigenen Haus + Unabhängigkeit von Drittanbietern + Maßgeschneiderte Anpassung möglich	- Hohe interne IT-Personalbindung - Verantwortung für 24/7 Betrieb - Investitionskosten (Hardware)	MITTEL
3 & 4 Managed (RZ)	+ "Rundum-Sorglos": Kein IT-Aufwand + Höchste Verfügbarkeit (SLA) + Skalierbarkeit ohne Investition	- Laufende monatliche Service-Kosten - Abhängigkeit vom RZ-Provider - Standardisierte Prozesse (weniger Flexibilität)	HOCH
5 XChange Tool	+ Sofort einsatzbereit (Quick Win) + Keine komplexe Infrastruktur nötig + Günstigste Einstiegsoption	- Keine Echtzeit-Daten (Zeitversatz) - Manuelle Arbeitsschritte notwendig - Fehleranfällig durch Medienbruch	NIEDRIG

Zusammenfassung & Nächste Schritte

Der Weg zur erfolgreichen NRZ-Integration

KERNBOTSCHAFTEN

- **Maximale Flexibilität**

  Fünf Integrationsszenarien decken das gesamte Spektrum ab – von vollständiger On-Premise-Kontrolle bis hin zu Managed Services im Rechenzentrum.

- **Maßgeschneiderte Sicherheit**

  Sicherheitskonzepte skalieren mit den Anforderungen: Vom Basisschutz im Büro bis zur Hochsicherheitszone im Rechenzentrum.

- **Strategischer Mehrwert**

  Die Integration ist kein reines IT-Projekt, sondern ein Business-Enabler für effizientere Prozesse und bessere Datenqualität.

AKTIONSPLAN

1. **Status Quo Analyse**

   Prüfung der vorhandenen IT-Infrastruktur, Compliance-Vorgaben und internen Ressourcen.

2. **Szenario-Auswahl**

   Entscheidung für das optimale Szenario (1-5) basierend auf der Entscheidungsmatrix.

3. **Stakeholder Alignment**

   Abstimmung zwischen IT-Leitung, CISO, Rechenzentrum und Fachabteilung.

4. **Pilotphase Starten**

   Beginn der Implementierung mit einem definierten Scope (z.B. Szenario 5 als Quick Win).

Starten Sie heute die Transformation. **Wählen Sie das Szenario, das zu Ihrer Strategie passt.**