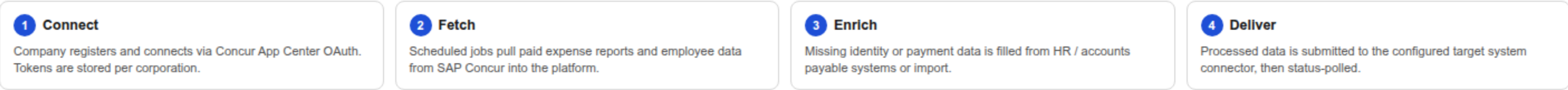
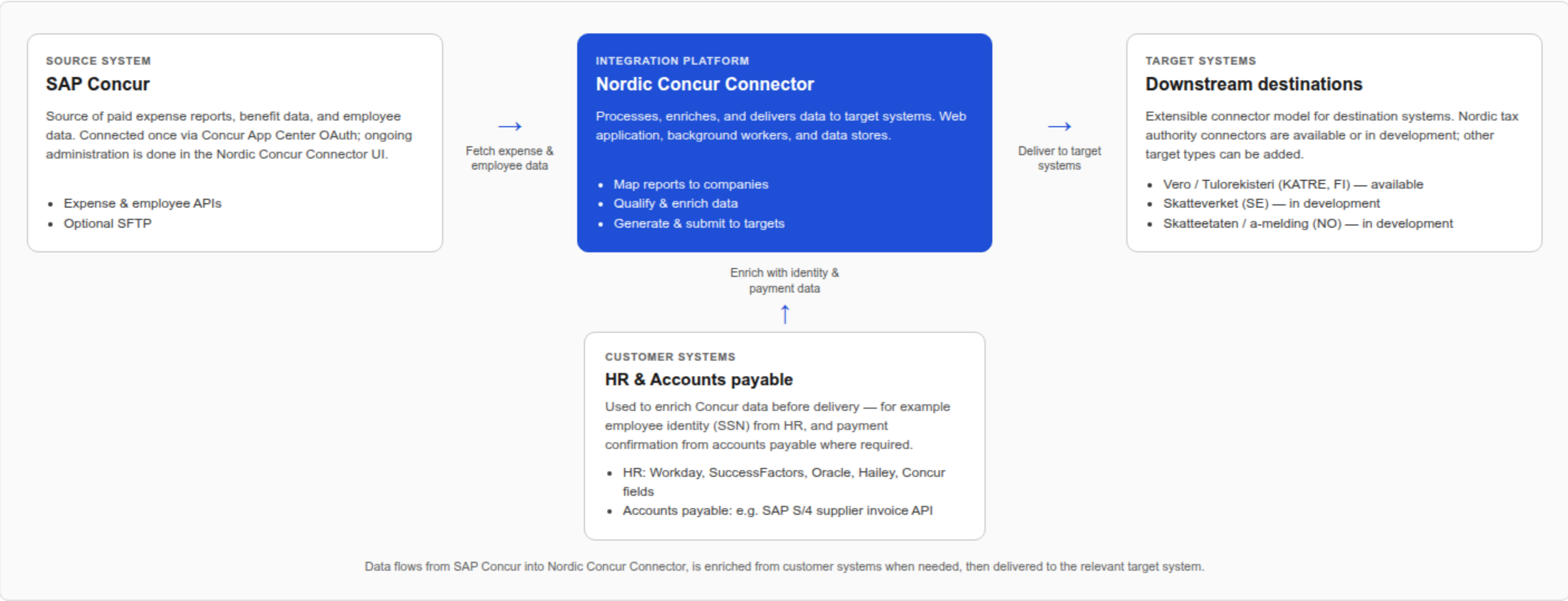


Nordic Concur Connector — Architecture

Multi-tenant SaaS that connects SAP Concur expense and employee data to target systems (Nordic tax authorities available or in development), with optional enrichment from the customer’s HR and accounts payable systems.



Security & data protection

As data processor under GDPR (customer is the controller), Nordic Concur Connector protects employee and expense data with the following measures. A Data Processing Agreement is included in the Terms of Service.

Encryption

Personal data encrypted at rest and in transit. In transit, TLS 1.3 is preferred; TLS 1.2 is also available. Sensitive fields (including SSNs) are encrypted in the database.

SSN masking

Social security numbers are masked on the server before they reach the browser, so the full SSN is never sent to the UI for client-side masking.

Access control & SSO

Role-based access with corporation/company isolation. Single Sign-On (SAML / OIDC) supported for customer identity providers. Strong passwords, account lockout, and session timeout where password login applies.

EU data residency

Production servers are located in secure datacenters in the EU. Production customer data does not leave production servers.

No subprocessors

All processing happens inside the Nordic Concur Connector application. Customer data is not sent to third parties for processing.

Backups & monitoring

Daily backups to a secure remote location (retained 30 days). Servers are hardened and kept up to date. Breach notification commitments apply under GDPR.

Vulnerability scanning

Periodic vulnerability scans are performed to identify and remediate security issues in the application and infrastructure.

IN PROGRESS

Web application firewall

A WAF is being added in front of the web application to filter malicious traffic and strengthen edge protection.

Secure tax submission

KATRE filings are submitted over HTTPS with our client certificate (mTLS) and digitally signed XML, using Nordic Concur Connector’s Vero PKI certificate.

Secrets hygiene

Integration credentials and secrets are protected in application configuration. Sensitive parameters (passwords, tokens, SSNs, certificates) are filtered from application logs.

Key management

Secrets and encryption keys are managed in a dedicated secrets management solution, centralizing and hardening handling of integration credentials and application secrets.

Tenant isolation

Multi-tenant design isolates each corporation’s configuration, employees, expenses, and filings so customers only access their own data.