| **Title / Role** | **Top 3 Challenges in 2025** | **3 Symptoms of the Challenge** | **Impact on KPIs & Business** | **Benefit of Using SEEBURGER** |
| --- | --- | --- | --- | --- |
| **CIO** | - Legacy systems increase costs- Slow partner onboarding- Lack of central platform | - Long onboarding timelines- High maintenance effort- Frequent integration failures | - Slower innovation- Higher TCO- Missed deadlines | - Simplified IT stack- Faster time to market- Reduced costs |
| **Head of IT Infrastructure** | - Fragmented tools- Difficult file/data management- Poor monitoring/control | - Operational silos- Repeated manual tasks- Lack of real-time visibility | - Wasted resources- Risk of downtime- Support bottlenecks | - Unified control- Better automation- Lower ops workload |
| **VP of Compliance** | - Data exchange not audit-ready- Poor encryption standards- Hard to prove compliance | - Audit failures- Regulatory concerns- Constant firefighting | - Legal risk- Penalties or fines- Lost customer trust | - GDPR-ready platform- Full audit trail- Reduced compliance anxiety |
| **IT Manager / Director** | - Too many disconnected systems- Pressure to modernize- Hard to support outdated tools | - Complex integrations- Overloaded team- High downtime during changes | - Lower IT morale- Slow delivery cycles- Frequent escalations | - Centralized integration- Fewer tools to manage- Agile updates |
| **Digital Transformation Mgr/Dir** | - Legacy slowing down innovation- Disparate data pipelines- Hard to launch new digital services | - Projects delayed- Business units waiting- Partners complaining | - Missed transformation goals- Slower adoption of new services | - Fast partner onboarding- Automated data flows- Clear upgrade path |
| **Integration Manager** | - Manual file transfers- Custom scripts breaking- Too many integration endpoints | - Inconsistent workflows- Constant fixes- Lost files or delays | - Lost productivity- Angry stakeholders- Missed SLAs | - Standardized connections- Fewer errors- Scalable integrations |
| **Application Manager** | - Legacy apps not integrating- No central hub for app communication- High support demand | - Constant app issues- Manual data handoffs- Complaints from end users | - Low application uptime- Frustrated internal teams- Higher support costs | - Smooth app integration- Centralized management- Fewer tickets |
| **CISO** | - Data not secure in transit- No control over shadow IT transfers- High-risk exposure in file exchange | - Policy violations- Breach alerts- Lack of encryption or audit controls | - Compliance gaps- Risk of breaches- Executive scrutiny | - Encrypted transfers- End-to-end control- Alignment with security frameworks |

| **Title / Role** | **Top 3 Challenges (2025-specific)** | **Symptoms of Those Challenges** | **Impact on KPIs & Business Outcomes** | **Benefit of Using SEEBURGER** |
| --- | --- | --- | --- | --- |
| **CIO** | - Inability to modernize legacy systems fast enough- Growing tech debt from fragmented integration stack- Poor agility in partner/customer data onboarding | - 6–12 month lead times for new integrations- Budget overruns due to patchwork IT- Business leaders bypassing IT to move faster | - Slow innovation cycles- Higher operating expenses- Misalignment with business needs | - A unified, agile platform to reduce legacy load- Retire redundant apps- Enable fast, secure data flows for business scalability |
| **Head of IT Infrastructure** | - Operational inefficiencies due to manual support- Poor observability across critical file exchanges- Tools not built for modern hybrid environments | - Frequent outages or failures in file transfers- Support team overwhelmed with low-value tickets- No end-to-end view of integration performance | - Higher MTTR (Mean Time to Recovery)- Increased OPEX from labor and fixes- Business disruption during downtime | - Intuitive UIs for users and admins- Full visibility and alerting across all flows- Reduced load on infrastructure and support teams |
| **VP of Compliance** | - Rising risk of non-compliance (GDPR, PCI-DSS, MiFID II)- Siloed systems make audits painful- No encryption/anonymization standards across all data flows | - Stressful audits with manual data pull- Exposure to fines or internal risk escalations- Can't prove data lineage or control access points | - Legal and reputational risk- Inability to meet board-level governance goals- Low trust in systems | - Automated compliance controls- Centralized audit logs and user access tracking- Encryption and policy enforcement out of the box |
| **IT Manager / Director** | - Too many point-to-point integrations- Fragile homegrown scripts- Lack of skilled resources to maintain them | - High failure rate in transfers- Constant firefighting instead of strategic projects- Difficult to onboard or train new hires | - Missed IT delivery deadlines- Low engineering morale- Higher attrition from burnout | - Replace fragile code with scalable templates- Visual tools for integration setup- Free up team for strategic work |
| **Digital Transformation Mgr/Dir** | - Legacy systems block innovation initiatives- Data flows not adaptable to cloud/SaaS models- Stakeholders frustrated with integration delays | - Project backlogs from integration delays- Transformation KPIs not met- Department seen as bottleneck instead of enabler | - Slow launch of digital products- Low NPS/internal satisfaction- Missed strategic milestones | - Flexible deployment (cloud/hybrid/on-prem)- Accelerated project rollout- Support for modern APIs, formats, and protocols |
| **Integration Manager** | - High complexity of mapping, routing, and monitoring- Constant vendor-side disruptions- No way to govern integration standards across the org | - Constantly fixing partner-side integration breaks- Lack of standardized documentation- Duplication of effort across teams | - Inconsistent partner experience- Missed SLAs with business units- High cost of rework | - Robust integration governance- Prebuilt templates and reusability- Proactive monitoring and exception handling |
| **Application Manager** | - Legacy business apps don’t communicate with each other- Data handoffs done manually or via fragile middleware- Business users experience downtime or data delays | - App updates frequently break connections- Duplicate or missing data- Endless user complaints | - Low uptime- Poor user satisfaction- High cost of ownership | - Secure, scalable connectors- Event-driven data sync- Visibility into app-to-app flows |
| **CISO** | - Sensitive file transfers lack control or visibility- Shadow IT solutions for file exchange- Increased threats from phishing and file-based attacks | - No alerting when sensitive data moves externally- Employees bypass IT due to friction- No automated deletion or encryption policies | - Data breach risk- Failed audits- Brand/reputation damage | - Enterprise-grade MFT + BIS platform- Real-time monitoring and controls- Encryption (in-flight & at-rest) + anonymization |

| **Title / Role** | **Top 3 Challenges (2025-specific)** | **Symptoms** | **Impact on KPIs / Business** | **Benefit of Using SEEBURGER** |
| --- | --- | --- | --- | --- |
| **CIO** | - Legacy systems slowing down digital initiatives- Complexity in managing fragmented file/data exchange- Escalating compliance risk in regulated markets | - Long integration timelines- Business teams building workarounds- Heavy IT dependency for compliance reporting | - Innovation delays- High TCO from system sprawl- Low business confidence in IT | - Single integration layer replacing legacy stack- Secure, compliant, scalable platform- Aligns IT with business speed |
| **Head of IT Infrastructure** | - No centralized visibility across data flows- High support costs from fragmented tools- Difficulty managing growing data exchange volume | - Reactive firefighting- Support tickets for file failures- No monitoring across B2B flows | - Rising OPEX- Low efficiency- Limited control and observability | - Unified control panel- Automated exception handling- Self-service tools for internal teams |
| **VP of Compliance** | - Inability to track or audit data exchanges- Misalignment with GDPR, PCI-DSS, or MiFID II- Growing board pressure on risk posture | - Failed or stressful audits- High manual effort for compliance evidence- Shadow IT use for data exchange | - Legal risk exposure- Non-compliance fines- Erosion of trust | - Full encryption + anonymization- Centralized audit trail- Automated policy enforcement at scale |
| **IT Manager / Director** | - Resource drain from maintaining outdated scripts/tools- Projects delayed by integration bottlenecks- Pressure to modernize under tight budgets | - Integration failures- High dev/support burden- No roadmap for legacy systems | - Low morale- Team burnout- Missed tech goals | - Visual mapping + low-code workflows- Replace brittle code with managed platform- Consolidate tools and reduce tech debt |
| **Digital Transformation Mgr/Dir** | - Legacy tech slowing innovation- New digital services delayed by integration- No flexible platform to connect new apps/partners | - Missed delivery dates- Frustration from business teams- Constant rework for new data channels | - Low stakeholder confidence- Missed strategic goals- Slower time to market | - Rapid partner/customer onboarding- Modern API and hybrid cloud support- Agile data flow automation |
| **Integration Manager** | - Disconnected workflows across partners/apps- Manual mappings and partner setups- Inability to govern data exchange standards | - Repetitive troubleshooting- Delays in onboarding new connections- Errors in file routing or translation | - Missed SLAs- High rework cost- Partner friction | - Prebuilt templates + flexible mapping- Centralized integration governance- Smart onboarding flows |
| **Application Manager** | - Apps don’t talk to each other natively- Manual handoffs cause delays/errors- End users complain about data gaps or delays | - App update breaks data flows- Missed SLAs for internal teams- Constant complaints from stakeholders | - Low uptime- Poor end-user experience- High support load | - Native integration connectors- Real-time data sync- One platform for app-to-app + B2B |
| **CISO** | - Uncontrolled data movement- Shadow file transfers outside IT policies- No protection for sensitive data in-flight or at-rest | - Data breaches or exposure events- No logs for investigation- Conflicts with IT around control vs. agility | - Risk of fines- Brand damage- Low stakeholder trust | - Secure MFT platform- Role-based access + encryption- Full monitoring + retention control |