Cyber threats are growing, and regulatory audits are getting tougher. Business leaders can no longer afford to treat security as an afterthought.

Business and Governance must be built-in, not bolted on - starting from day one of your SAP implementation.

Let's build a secure ERP together.

Scan the QR code or visit **delaware.pro** to learn more.

Get in touch with us at **info.sg@delaware.pro** to learn more.

delaware

SAP Platinum Partner

Secure ERP. Trusted Compliance. Peace of Mind.

Fast-track your SAP journey with security, compliance, and confidence. Tailored for Singapore businesses.

we commit. we deliver.

Pre-Audit Readiness

- Password policy & access review
- SSO/MFA configuration
- RFC & port whitelisting
- Patch updates
- SOP & documentation hygiene

Post-Audit Findings

- SoD violations
- Excess privilege access
- Unsecured ports
- Lack of internal controls

Companies often face challenges around audits. Pre-audit issues include weak password policies, outdated configurations, missing access reviews, and incomplete security documentation. Post-audit gaps typically involve SoD violations, excessive access rights, and lack of privilege controls. Our experience helps address these through structured pre-audit preparation and targeted remediation. With deep expertise, we proactively close gaps through structured pre-audit preparation and remediation. This approach ensures our clients are audit-ready and establishes a strong governance posture.

Our Area of Focus

1. Infrastructure (cloud/hybrid)
2. Application security parameters
3. User roles & access rights
4. SoD & privilege governance
5. Ongoing monitoring & updates

We don't just talk about SAP security – we implement it.

Our recommended tools include:

- SAP-certified SecurityBridge for real-time threat detection and patch management.
- SAP IAG (Identity Access Governance) for access control, SoD enforcement, and compliance.
- delaware brings these platforms into your landscape seamlessly as part of our implementation.
- We help you identify gaps, configure tools, and manage access risk from day one.