JOHN LEWIS PARTNERSHIP | JOHN LEWIS | WAITROSE

Job title: Security Architect

Core information

Location: London head office	**Lines of business or shared capability area:** Architecture & Engineering, Shared Platforms
Reports to: Enterprise Architect	
People Management: No **Assignment Management:** No	
Partnership Level: Partnership level 6	**Manager's Partnership level:** Partnership level 5
Number of direct reports: **0**	**Partnership level(s) of direct reports:** None

About the John Lewis Partnership

The Partnership is the UK's largest employee-owned business and home to our two well-loved retail brands – John Lewis and Waitrose, as well as expanding into new areas beyond retail.

We aren't an ordinary business, though. The Partnership is different because everyone who works here isn't just an employee. We are Partners, with a shared responsibility for our success, and we share the rewards when we're successful.

Everything we do is powered by our unique Purpose: **Working in Partnership for a happier world.** Our Purpose inspires our principles, drives our decisions and acts as our guide, so that everything we do contributes to Happier People, Happier Business and a Happier World.

Critical purpose of the role

As a Security Architect you will work across our Architecture, Engineering, Infrastructure and InfoSec teams to design and guide the delivery of secure solutions. Solutions will include the build out of strategic security services as well as embedding our security architecture into functional platforms and products. In order to achieve this you will need to be a technical expert who is able to convey complex approaches with impactful simplicity, you will need to establish credibility and trust across technical Engineering teams as well as leadership. Whilst many of our solutions are cloud-native, we need to design in proportionate controls wherever and however a solution is deployed, in order to protect our solutions and data from modern threats and manage our risk position. You'll partner with other teams, acting as an integrated team member and able to meet them 'where they are'.

Primary Outcomes & Accountabilities	**Measures of success**
• Design security solutions for compelling services across our cloud platforms and traditional hosting environments; • Design end-to-end security solutions, blueprints and patterns that are effective, efficient, repeatable and sustainable making a tangible difference to the security of our business;	• Balance the need to deliver solutions to meet a functional need, whilst supporting incremental steps to deliver our long-term strategies; • Delivery of objectives and key results (OKR's), against the backdrop of our strategies, roadmaps and priorities. • Reduced delivery and operational risk position whilst optimising delivery and operational efficiency;

• Ensure security architecture best practice is brought to bear during solution design activities undertaken by delivery teams and 3rd parties to reduce delivery cost, operational risk and technical debt; • You'll advise and consult on the commercial and contractual implications of existing or new obligations. You'll consult on contractual terms of technologies and business services being procured or used within your domain and the impact of change both commercially and contractually; • Help ensure JLP delivers on its strategic aims and enables the Partnership to adapt and grow in a competitive and changing market; • Invest in your personal and professional development, utilising the opportunities available to you through your Profession to develop your skills and capabilities. • Leverage insight and internal and external networks, as appropriate, to keep abreast of key customer requirements, market conditions and trends, including technological advancements, and feed these into strategic thinking; • Design and maintain an accurate logical overview of the entire system throughout product lifecycle/delivery, including the end users needing consideration in the customer experience design.	• Accelerate our end-to-end delivery through through repeatable solutions; • Our solutions effectively and efficiently protect against modern threats and maintain regulatory compliance in order to maintain our overall risk position • We select the right solutions that efficiently integrate with our functional solutions whilst supporting contractual exposure for the Partnership;

Skills

Impactful security architect

Extensive experience and deep understanding of modern Security Architecture, with demonstrable evidence where you have been able to take roadmap intent, combine with good practice and business context through strong stakeholder engagement to define clear solutions. You will be an adaptable, technical and engineering-focused architect who is used to working across multiple service and domain teams through both waterfall and Agile delivery models.

Technology expert

We operate across a diverse technology estate, expert knowledge in security best-practice, associated frameworks and major technologies are essential for this role. You'll need expert knowledge with Google Cloud and SaaS applications, and you will be able to apply solutions that work across a hybrid-cloud environment.

Critical influence

Proven ability to empower and influence others to make decisions, resolve challenges and deliver outcomes that are in line with the strategy. Work across architecture, service and engineering teams to ensure that our security capabilities are bringing the intended value, actively optimising where opportunities arise through pattern definition and solution evangelism.

Qualifications & Experience (where applicable)

Essential

- Experience in holistic security design against a zero-trust architecture across cloud and traditional deployment models;

- Experience in facilitating threat modeling workshops;
- Experience in product evaluation / selection;
- Strong experience in securing AI deployments, including custom-build AI for commerce use-cases;
- An understanding of DevSecOps and SecOps frameworks with an understanding of tooling landscape; ;
- Security Frameworks: NIST Cybersecurity Framework, CSA Critical Controls Matrix;
- Cloud security: Google Cloud, Amazon Web Services, SaaS applications;
- An understanding of attacker tools, techniques and procedures, alongside pragmatic mitigations;
- Legal and compliance regulation: General Data Protection Regulation;
- Product and platform oriented delivery, working across waterfall and Agile contexts;
- Experience of influencing stakeholders at Leadership and Working Group levels on a major transformation or in an area with a high level of change;
- Have a security engineering background or expert understanding.

Desirable

- Experience designing SOC architectures (ie SIEM, SOAR and CTEM solutions);
- Experience in working within regulated environments, such as PCI-DSS.

Professional certifications

Whilst we prioritise demonstrable business impact, cross-team collaboration and being outcome focused, we also recognise the value of certification. The following certifications would be beneficial in this role:

- TOGAF and/or SABSA certified;
- (ISC)2 Certified Cloud Security Professional / Certified Information Systems Security Professional / Information Systems Security Architecture Professional;
- Certified Ethical Hacker;
- Google Cloud Generative AI Leader / Professional Cloud Architect / Security Engineer;
- Zscaler Zero Trust Cyber Associate / Digital Transformation Administrator;
- Cloud Security Alliance Trusted AI Safety Expert / Certificate of Competence in Zero Trust.

Version	**Created/updated by**	**Date**
1.1	*David Brown*	*10 Jul 2026*