# **[Cloud Solution Architecture (CSA) - Security](https://www.seek.com.au/job/77530718?ref=search-standalone&type=standout&origin=jobTitle" \l "sol=228f6a0e0cfba465cd2d10f5ac7a7b41aa99bf5d" \t "_blank)**

**Overview**

With over 17,000 employees worldwide, the mission of the Customer Experience & Success (CE&S) organization is to empower customers to accelerate business value through differentiated customer experiences that leverage Microsoft’s products and services, ignited by our people and culture. Come join CE&S and help us build a future where customers achieve their business outcomes faster with technology that does more.

We are looking for a Cloud Solution Architect (CSA), specializing in Security who is passionate about driving our customers’ security & AI transformation on the Microsoft Platform. This is a customer-facing role, owning the technical relationship between the customer and Microsoft, helping customers to leverage their Microsoft investments through architecture, implementation, and operational health engagements. This role is flexible in that you can work up to 50% from home.

Microsoft’s mission is to empower every person and every organization on the planet to achieve more. As employees we come together with a growth mindset, innovate to empower others, and collaborate to realize our shared goals. Each day we build on our values of respect, integrity, and accountability to create a culture of inclusion where everyone can thrive at work and beyond.

**Qualifications**

**Required/Minimum Qualifications**

* Bachelor's Degree in Computer Science, Information Technology, Engineering, Business or related field AND 4+ years experience in cloud/infrastructure technologies, information technology (IT) consulting/support, systems administration, network operations, software development/support, technology solutions, practice development, architecture, and/or Business Applications consulting
  + OR equivalent experience.
* Breadth of technical experience and knowledge in foundational AI, architecture design, with depth / Subject Matter Expertise in security, in **two or more** of the following security solution areas:
* Threat protection; SIEM and Incident Response; Extended Detection and Response (XDR); Security Orchestration, Automation, and Response (SOAR); Security Operation Center (SOC) Management; Identity and Access Management; Cloud Infrastructure; Cloud Security; Data Security & Information Protection.

**Additional or Preferred Qualifications**

* Technical aptitude and experience to: learn new cloud security technologies; understand relevant cloud security market trends; knowledge of security landscape and of cloud security platforms and competitors;
* Certification in one or more of the following technologies preferred: Microsoft Cybersecurity Architect (SC-100), Microsoft Security Operations (SC-200), Microsoft 365 Security Administrator (MS-500), Azure Security Engineer (AZ-500), Cloud Security (CCSP), CISSP, CEH, OSCP, GSEC.

**Responsibilities**

* Customer Centricity​
  + Customer Satisfaction - Drive positive Customer Satisfaction & become a trusted advisor.
  + Customer/Partner Insights - Provide feedback & insights from customers/partners.
  + Be the Voice of Customer to share insights and best practices, connect with Global Security teams at Microsoft, Engineering and Product teams to remove blockers and influence the solution roadmap.
  + Land an end-to-end value prop for Security (i.e., Zero Trust) which spans the breadth of Microsoft Security offerings, and with focus on Threat Protection, ID + Access Management and Cloud Security.
* Business Impact​
  + Position and deliver solutions that drive Security product usage and develop opportunities to drive Customer Success business results & help Customers get value from their Microsoft investments.​
  + Identify resolutions to Customer blockers by leveraging SA subject matter expertise. Deliver according to MS best practices & using repeatable IP. ​
  + Accelerate Business Value of overall Security adoption by improving security posture and ensuring that the solution exhibits “Secure by Design” framework, such as high-performance levels, security, scalability, maintainability, appropriate reusability, and reliability upon deployment.
* Technical Leadership​
  + Learn It All – Align individual skilling to team/area demands & Customer Success goals​.​
* Accelerate customer outcomes - Share expertise, contribute to IP creation & re-use to accelerate customer outcomes.
* Run Architectural Design Session to build a plan for implementing the solution – governing design in line with customer business goals and their technical environment. Outcome is consensus on solution design and next steps toward production.
* Collaborate and orchestrate with other Cloud Solution Architects and MS stakeholders including FastTrack, partner, and Microsoft Consulting in developing complex end-to-end Enterprise solutions with the Microsoft Security platform.

Benefits/perks listed below may vary depending on the nature of your employment with Microsoft and the country where you work.

* Industry leading healthcare
* Educational resources
* Discounts on products and services
* Savings and investments
* Maternity and paternity leave
* Generous time away
* Giving programs
* Opportunities to network and connect

# Interview Script

**Interview Question 1: Technical Expertise in Security**

**Interviewer:** "Can you tell us about a time when you had to address a security challenge in a cloud environment? What steps did you take to resolve it?"

**Less Effective Response**

**Interviewee:** "Uh, yeah, I had a problem with a security thing once. I think it was a vulnerability or something, but we fixed it. I, um, did some stuff with the firewall and then it was fine."

**More Effective Response**

**Interviewee:** "Certainly! In my previous role, we encountered a significant vulnerability in our cloud infrastructure that could have exposed sensitive data. I took a systematic approach to resolve the issue. First, I conducted a thorough assessment to understand the scope of the vulnerability. Then, I implemented enhanced firewall rules and configured intrusion detection systems to mitigate the immediate threat. I also collaborated with the development team to patch the affected systems and conducted a post-incident analysis to improve our security posture. This experience reinforced the importance of a proactive and comprehensive security strategy."

**Interview Question 2: Experience with Microsoft Products and Services**

**Interviewer:** "How have you utilized Microsoft's security tools in your previous work?"

**Less Effective Response**

**Interviewee:** "I used some of the Microsoft stuff like Azure. It was good, I guess. We did some security things, but I can't really remember the details."

**More Effective Response**

**Interviewee:** "In my last position, I leveraged Microsoft's suite of security tools extensively. For instance, we used Microsoft Sentinel for our Security Information and Event Management (SIEM) needs. This allowed us to gain real-time insights into potential threats and streamline our incident response process. Additionally, I utilized Azure Security Center to maintain a secure posture across our cloud resources, implementing best practices for security and compliance. This integration not only enhanced our security capabilities but also aligned with our overall IT strategy, ensuring a robust defense against cyber threats."

**Interview Question 3: Customer-Centric Approach**

**Interviewer:** "Can you describe a situation where you had to align a security solution with a customer's business goals?"

**Less Effective Response**

**Interviewee:** "We had this client, and they wanted something with security. I just set up some standard security measures, and they were happy, I think."

**More Effective Response**

**Interviewee:** "Absolutely. In one of my projects, a client in the healthcare sector needed to comply with stringent regulatory requirements while migrating to the cloud. I worked closely with them to understand their specific business goals, including ensuring patient data confidentiality and improving operational efficiency. By implementing a Zero Trust security model, we enhanced data protection across all touchpoints. I also provided training to their staff on best practices, aligning the solution not only with compliance standards but also with their broader business objectives of patient trust and care quality."

**Interview Question 4: Collaboration and Teamwork**

**Interviewer:** "Can you share an experience where you collaborated with cross-functional teams to implement a security solution?"

**Less Effective Response**

**Interviewee:** "I worked with other teams sometimes. We did a project together and, um, it was okay. We just made sure the security was good."

**More Effective Response**

**Interviewee:** "Certainly! In a previous role, we undertook a major project to enhance our organization's cloud security framework. This required collaboration between the IT security team, developers, and the compliance department. I took the lead in organizing regular cross-functional meetings to ensure alignment on security objectives and regulatory requirements. We implemented a multi-layered security strategy, combining network security controls with application-level protections. By fostering open communication and sharing insights across teams, we not only met our security goals but also strengthened our overall organizational resilience."

**Interview Question 5: Continuous Learning and Growth**

**Interviewer:** "How do you stay updated with the latest trends in cloud security?"

**Less Effective Response**

**Interviewee:** "I, uh, read some articles online sometimes. And maybe take a course if I have time."

**More Effective Response**

**Interviewee:** "Staying updated in the rapidly evolving field of cloud security is crucial. I regularly engage in professional development by following industry leaders on platforms like LinkedIn and attending webinars and conferences. I also invest in certifications; for instance, I've completed the Azure Security Engineer (AZ-500) and Microsoft Cybersecurity Architect (SC-100) certifications. Additionally, I'm an active member of several professional organizations, which allows me to exchange knowledge and best practices with peers. This commitment to continuous learning ensures that I can provide the most current and effective security solutions to my clients."

**Interview Question 6: Problem-Solving Skills**

**Interviewer:** "Describe a time when you encountered an unexpected issue during a project. How did you handle it?"

**Less Effective Response**

**Interviewee:** "There was this one time when something went wrong with the project. I think it was a server issue. We tried to fix it, and eventually, it got sorted out."

**More Effective Response**

**Interviewee:** "During a critical migration project, we unexpectedly encountered a server compatibility issue that threatened to delay the timeline. I immediately gathered a task force, including developers and network specialists, to diagnose the problem. We quickly identified that the issue stemmed from a configuration mismatch between the old and new server environments. To resolve this, I proposed a temporary rollback and then worked with the team to adjust the configurations and test thoroughly before proceeding. This proactive and collaborative approach minimized downtime and ensured a smooth transition, keeping the project on track."

**Interview Question 7: Understanding of Security Frameworks**

**Interviewer:** "How do you ensure that your security solutions are compliant with industry standards and regulations?"

**Less Effective Response**

**Interviewee:** "I usually just follow the basic guidelines that are available. I think it’s important to make sure everything is up to standard."

**More Effective Response**

**Interviewee:** "Ensuring compliance with industry standards and regulations is a key priority in my work. I stay updated on the latest standards, such as ISO 27001 and NIST, and apply these frameworks to design security solutions that meet regulatory requirements. For instance, in a project for a financial client, I led the implementation of a comprehensive compliance program that included data encryption, regular audits, and access controls. This not only met the compliance standards but also enhanced the client's trust in our security measures."

**Interview Question 8: Adaptability and Flexibility**

**Interviewer:** "Can you provide an example of a time when you had to quickly adapt to a change in project scope or priorities?"

**Less Effective Response**

**Interviewee:** "Yeah, there was a time when the project scope changed, and we had to adjust. It was challenging, but we managed somehow."

**More Effective Response**

**Interviewee:** "In a recent project, we experienced a sudden change in scope when the client decided to expand the security features beyond the initial plan. This required us to integrate additional threat detection capabilities on short notice. I quickly organized a re-assessment of the project timeline and resources, and led a brainstorming session with the team to identify the best approach to integrate these new requirements. By remaining flexible and communicating transparently with the client, we were able to successfully deliver the enhanced solution within the revised timeline."

**Interview Question 9: Communication Skills**

**Interviewer:** "How do you explain complex technical concepts to non-technical stakeholders?"

**Less Effective Response**

**Interviewee:** "I try to simplify things as much as I can. I just tell them what they need to know without going into too much detail."

**More Effective Response**

**Interviewee:** "Communicating complex technical concepts to non-technical stakeholders is crucial for ensuring understanding and alignment. I use analogies and real-world examples to make the concepts more relatable. For instance, when explaining data encryption, I liken it to sending a letter in a locked box, where only the recipient has the key. I also provide visual aids and ensure that I am available for any follow-up questions. This approach not only clarifies the technical aspects but also builds confidence in our solutions."

**Interview Question 10: Initiative and Proactivity**

**Interviewer:** "Can you share an example of when you took the initiative to improve a process or system?"

**Less Effective Response**

**Interviewee:** "I once suggested we update our software. It was outdated, and I thought it could be better."

**More Effective Response**

**Interviewee:** "In my previous role, I noticed that our incident response process was slow, primarily due to manual logging and reporting. I took the initiative to propose and implement an automated incident response system using a SOAR platform. This system integrated with our existing SIEM and other tools, automating the initial triage and reporting process. This not only reduced response times significantly but also freed up our analysts to focus on more critical tasks. The improvement was well-received and became a new standard practice within the team."