A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — Cyber Security Solution Architecture

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

The Gartner Cyber Security Solution Architecture service supports the development and deployment of a client's cyber security capabilities, which include significant architecture, design, or integration elements. The scope includes facilitation for rapid progression from definition of requirements and operating context through to detailed capability architecture specification and solution option evaluation.

Service Description

The Cyber Security Solution Architecture service addresses key challenges in the architecture, design and integration of cyber security controls and capabilities. This includes integration across an enterprise's technical security controls, secure data exchange and management, and interfaces with enabling services such as asset and configuration management systems.

The scope of this service definition includes all technical cyber security domains. Examples of relatively high-complexity and extended-integration capability areas include:

- **Risk-Based Vulnerability Management (RBVM).** A capability architecture specification would be expected to cover:
  - Integration of application, infrastructure and network layer vulnerability management technology
  - Vulnerability intelligence feeds
  - Integration with change management, asset and configuration management systems
  - Coupling with other cyber security controls, notably incident response and protective monitoring services
- **Zero Trust (ZT) Domain Design.** This would include:
  - The design of Zone Enforcement Technologies (ZETs): The ZETs will provide the micro-segmentation capability to group the ZT services into their distinct network enclaves. Distinct network enclaves are fundamental to reducing the attack surface of infrastructure and application assets
  - Access services. Typically, it includes an access proxy and context-based access control service to protect access to the ZT domain. Adaptive identity concepts are key

The analysis uses best practice methodologies, frameworks and reference architectures. These include:

- **Methodologies.** The service can adapt to security architecture methodologies specified by clients. Our default methodologies are TOGAF and SAFe, supplemented by SABSA and the Open Enterprise Security Architecture (O-ESA)
- Key reference standards and frameworks: NCSC Assessment Framework, NIST SP Series, ISO/IEC 27000, OWASP ASVS, NIS-R, PCI-DSS
- **Reference architectures and patterns.** A library of architecture patterns accelerates the development of tailored capability architectures and high-level designs

Service Benefits

- Improved security control integration within ICT and OT services
- Rationalisation of security technologies, reducing cost of ownership
- Support for transition to cloud and zero trust adoption
- Reduced build and run costs for security controls
- Optimised investments in cyber security solutions
- Reduced cyber-portfolio risk through effective implementation of complex capabilities
- Reduced implementation risk/cost uncertainty for technical security controls
- Future-proofed adaptive, extensible and scalable security architecture
- Accelerates delivery of actionable insights through proven analytical capabilities
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Service Features

- Analysis of operational context and ICT/OT service environment factors
- Comprehensive solution option identification
- Adapts to client-specific methodologies, frameworks, standards and regulations
- Adheres to global best practice architecture methods and approaches
- High-integrity documentation supports solution continuous development and maintenance
- Access to Gartner’s world-class technical research and analyst support

Full List of Service Features

The Gartner Cyber Security Solution Architecture service guides the architecture and design of components and services that protect the availability and integrity of information and data while assuring the availability of systems and services and providing accountability for digital transactions, including access to the managed information and data.

A holistic approach ensures that the following aspects are accounted for in the solution architecture and design process:

- Operational context (the environment and way in which the business operates), compliance and regulatory requirements, budget/cost, schedule, resource and sourcing constraints
- Business requirements, both functional and non-functional
- User requirements — focused attention is given to the operations staff who operate the solution, which may be integrated into a wider service
- IT and OT infrastructure, including cloud hosting and platform service-related requirements
- Maintainability, extensibility and scalability of the solution

This approach maintains focus on the interoperability, integration, maintainability and ability of security solutions to scale, extend and adapt as the protected digital services and the threat to those services evolves. It combines global architecture best practices with domain-specific cyber security expertise and leverages Gartner’s research to optimise the architecture and design of ICT and OT security solutions and services.

Project Approach

This approach is to be tailored to the specific characteristics of the targeted solution.

Stage 0: Project initiation (Week 0)

- Conduct a kick-off meeting to ensure an understanding of the project objectives, scope, schedule, milestones, roles, responsibilities and required resources
- Discuss and identify any anticipated risks and mitigation plans based on lessons learned from experience
- Identify key people and stakeholders required for information discovery and analysis through to the target state definition.

Stage 1: Define the operational context and baseline state (Week 1)

- Discover and document the operational context of the ICT and/or OT services to be protected
- As appropriate, identify the system-of-system integration points with infrastructure, operational support and other security controls. This may include manual process integration
- Discover and document the baseline (current) state of any existing control(s) in the solution capability area

Stage 2: Capture the requirements and architecturally significant factors (Week 2-3)

- Develop the requirements baseline for the target solution through a combination of stakeholder interviews, analysis of the required product, output and risk-mitigating effect for the required solution. Functional and non-functional requirements (NFRs) are covered.
- Develop and document the architecturally significant factors that may impact on the solution. Key factors include:
  - Risk to be mitigated by the solution. It may include associated factors such as threat and vulnerability information
  - Build and run risks for the solution
  - Costs, schedule, people and sourcing
  - Technical interfaces
  - Solution data requirements
  - NFRs, including resilience, compliance, availability, scalability, application performance and latency/response requirements

Stage 3: Define the target capability architecture and gap analysis (Week 4-5)

- This is typically a TOGAF Capability-level architecture that meets the analysed requirements
- It accounts for the identified architecturally significant factors
- It is defined in sufficient detail to support the subsequent gap analysis and solution specification

- A gap analysis compares the current and target states for the required solution or service

Stage 4: Solution specification, options evaluation and implementation and deployment planning (Week 5-6+)

- The capability architecture and gap analysis drive a solution specification that includes sufficient detail to identify and support the evaluation of solution options
- Solution options, covering delivery model as well as technical aspects, are identified
- As appropriate, a weighted evaluation of feasible solutions is run
- Outline implementation and deployment plans cover the build and transition to operations phases for the required security solution(s)

Project Schedule

The approach above is adapted across a wide range of security solution domains and according to the characteristics of the protected environment(s) and the target integration complexity.
This service description is based on an 8-week engagement; however typically, engagements will usually range between 6 weeks and 4 months.