The Server Labs G-Cloud 15 Service Description

The TSL Service Model, AWS Trusted Foundation Services

Zero Trust & Security Hardening

Ref: TSL/GCLOUD15/SERVICE_DESC
Issue : 1.0
Date: Jan 2026 For: **G-Cloud-15**

Zero Trust Security Maturity & Risk Assessment for AWS

Overview

With over twenty years of AWS platform engineering experience, The Server Labs helps organisations establish a clear, factual view of their current security posture and readiness for zero trust architecture.

Many AWS environments have grown organically, resulting in fragmented identity models, inconsistent access controls, and unclear trust boundaries. This assessment provides an engineering-led evaluation of how security controls operate in practice, identifying material risks and architectural gaps that must be addressed before zero trust can be enforced reliably.

Benefits

- Establishes a clear baseline of security maturity
- Identifies material risks in identity and access models
- Reveals gaps in segmentation and trust boundaries
- Focuses on technical controls, not policy intent
- Suitable for regulated and high-assurance environments

What This Service Provides

Zero trust is only effective when it is grounded in a realistic understanding of the existing platform.

This service examines how identity, access, and security controls are currently implemented across the AWS estate. The focus is on how trust is established, enforced, and monitored in practice, rather than how it is described in policy or documentation. Particular attention is given to identity models, privilege boundaries, network exposure, logging coverage, and the consistency of control application across environments.

The assessment also considers how security controls interact with delivery pipelines and operational processes, highlighting areas where manual intervention, inconsistent configuration, or implicit trust introduces avoidable risk. The outcome is

a clear, evidence-based view of security maturity and the practical constraints that must be addressed to move toward an identity-led, zero trust security model.

Who This Is For

This service is suited to organisations operating AWS environments that support sensitive, regulated, or mission-critical workloads and require a clear understanding of their current security posture.

It is particularly relevant where zero trust is an explicit strategic goal, but the current state of identity, access, and segmentation is not well understood or consistently enforced.

What's Included

- Review of identity and access models across AWS accounts
- Assessment of privilege boundaries and access patterns
- Network exposure and segmentation review
- Logging, monitoring, and visibility coverage assessment
- Evaluation of security control consistency across environments
- Identification of implicit trust and high-risk assumptions
- Zero trust maturity baseline and risk profile
- Prioritised improvement backlog and recommendations

Delivery Approach

The assessment is delivered through a structured, engineering-led review of the AWS environment, focusing on how security controls operate under real conditions.

Work begins with analysis of identity and access configurations, network architecture, and security services to establish a factual baseline. This is followed by targeted examination of how controls are applied across environments and how effectively they limit trust, privilege, and lateral movement.

Findings are consolidated into a clear risk and maturity assessment, with recommendations focused on architectural and platform changes rather than procedural controls or manual oversight.

Key Deliverables

- Zero Trust Security Maturity & Risk Assessment Report
- Identity and access risk analysis summary
- Network segmentation and exposure findings
- Security control coverage and consistency review
- Prioritised zero trust improvement backlog
- Executive-level summary for technical and leadership audiences

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security and Operational Excellence pillars.

Assessment activities typically reference the following AWS services and frameworks:

- AWS Well-Architected Framework and Tool
- AWS Identity and Access Management (IAM)
- AWS Organizations and account boundaries
- Amazon VPC and network security services
- AWS CloudTrail and AWS Config
- AWS Security Hub

The specific services reviewed will vary depending on the client's AWS architecture, operating model, and regulatory context.

Pricing & Commercial Model

This service is delivered as Professional Services, with pricing provided on request based on scope, environment complexity, and the applicable rate card.

Listing Title

Zero Trust Blueprint + IaC Guardrails Pack for AWS

Overview

With over twenty years of AWS platform engineering experience, The Server Labs defines and delivers deployable zero trust security architectures with enforceable guardrails built directly into infrastructure and platform design.

Many organisations understand the principles of zero trust but struggle to translate them into concrete, enforceable controls. This service provides a reference security blueprint and a set of deployable infrastructure-as-code guardrails that make identity-led security real, consistent, and repeatable across AWS environments.

Benefits

- Establishes a clear zero trust security architecture
- Enforces identity-led access through deployable guardrails
- Reduces reliance on manual security controls
- Improves consistency across environments and teams
- Suitable for regulated and high-assurance environments

What This Service Provides

Zero trust only works when security controls are embedded into the platform rather than applied through process.

This service defines the target zero trust security architecture for AWS, focusing on identity-driven access, explicit trust boundaries, and least-privilege enforcement. The blueprint sets out how users, services, and workloads authenticate, how access is authorised, and how trust is continuously verified across the platform.

Alongside the architecture, this service provides a deployable IaC guardrails pack that encodes security controls directly into the platform. These guardrails enforce consistent patterns for identity, access, network segmentation, logging, and encryption, preventing insecure configurations from being deployed in the first place. Controls are expressed as reusable, versioned artefacts that can be applied across accounts and environments.

The outcome is a security foundation that is enforceable by design, rather than dependent on manual review or post-deployment remediation.

Who This Is For

This service is suited to organisations that have assessed their security posture and require a practical, enforceable zero trust foundation before undertaking platform hardening or broader security initiatives.

It is particularly relevant for organisations operating regulated, sensitive, or mission-critical workloads where security controls must be applied consistently and demonstrably across environments.

What's Included

- Zero trust reference architecture for AWS
- Identity-led access and trust boundary design
- Network segmentation and service isolation patterns
- Deployable infrastructure-as-code guardrails
- Policy-as-code security control definitions
- Standardised logging and monitoring guardrails
- Architecture and guardrail documentation for adoption

Delivery Approach

The engagement is delivered through structured security architecture design followed by development of deployable guardrails aligned to the agreed blueprint.

Work begins with definition of the zero trust reference architecture, establishing how identity, access, and trust boundaries should operate across the AWS estate. This architecture is then translated into infrastructure-as-code guardrails that enforce the desired patterns automatically during platform provisioning and change.

Guardrails are designed to be reusable, maintainable, and compatible with existing delivery pipelines, allowing organisations to apply zero trust controls consistently without introducing manual gates or operational friction.

Key Deliverables

- Zero Trust Security Blueprint for AWS
- Deployable IaC Guardrails Pack
- Identity, access, and segmentation control patterns
- Policy-as-code artefacts enforcing security standards
- Adoption guidance for platform and delivery teams

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security pillar and identity-led design principles.

Architectural designs and guardrails typically reference:

- AWS Well-Architected Framework and Tool
- AWS Identity and Access Management (IAM)
- AWS Organizations and account boundaries
- Amazon VPC and network security services
- AWS CloudTrail and AWS Config
- AWS Security Hub
- Infrastructure-as-code tooling

The specific services and guardrails implemented will vary depending on the client's AWS architecture, operating model, and regulatory context.

Pricing & Commercial Model

This service is delivered as Professional Services, with pricing provided on request based on scope, environment complexity, and the applicable rate card.

Platform Hardening & Control Implementation for AWS

Short Description

With over twenty years of AWS platform engineering experience, The Server Labs implements security hardening and control configurations that make zero trust enforceable in day-to-day platform operation.

Many AWS environments rely on partially applied benchmarks, manual configuration, or inconsistent controls that leave gaps over time. This service delivers practical hardening across infrastructure, platforms, and services, embedding security controls as engineered defaults rather than optional overlays.

Benefits

- Enforces consistent security hardening across environments
- Reduces risk from misconfiguration and configuration drift
- Embeds controls directly into platform operation
- Produces evidence through configuration and automation
- Suitable for regulated and high-assurance environments

What This Service Provides

Zero trust architectures require a hardened platform to be effective.

This service focuses on implementing security controls across the AWS environment in line with the agreed zero trust blueprint and guardrails. Hardening is applied across identity configurations, network boundaries, encryption settings, logging coverage, and platform services to reduce implicit trust and limit blast radius.

Controls are implemented using AWS-native capabilities and infrastructure-as-code where appropriate, ensuring consistency across accounts and environments. Emphasis is placed on preventative controls and secure defaults that reduce reliance on detection and remediation after issues occur.

The result is a hardened platform where security controls are continuously applied and verifiable through configuration state rather than manual review.

Who This Is For

This service is suited to organisations that have defined their zero trust security architecture and require practical implementation of hardening and controls across their AWS environment.

It is particularly relevant for environments supporting sensitive, regulated, or mission-critical workloads where security posture must be demonstrable and repeatable.

What's Included

- Identity and access configuration hardening
- Network segmentation and boundary enforcement
- Encryption and key management configuration
- Logging, monitoring, and audit trail enablement
- Platform service hardening and baseline controls
- Integration with existing guardrails and delivery pipelines
- Validation of control application and coverage

Delivery Approach

The engagement is delivered through hands-on engineering focused on applying and validating security controls across the AWS platform.

Work begins with confirmation of the target hardening baseline and control requirements, followed by implementation across accounts, environments, and services. Controls are applied using automated, repeatable mechanisms wherever possible to reduce manual intervention and ensure consistency.

Validation activities confirm that controls are correctly applied and operating as intended, producing technical evidence through configuration state and platform telemetry.

Key Deliverables

- Hardened AWS platform aligned to zero trust principles
- Implemented security control configurations
- Validation summary of control coverage and effectiveness
- Evidence artefacts derived from configuration and automation
- Operational guidance for maintaining hardened posture

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security and Reliability pillars.

Hardening and control implementation typically reference capabilities provided by **Amazon Web Services**, including:

- AWS Identity and Access Management (IAM)
- AWS Organizations and account boundaries
- Amazon VPC and network security services
- AWS Key Management Service (KMS)

- AWS CloudTrail and AWS Config
- AWS Security Hub
- Native logging and monitoring services

The specific controls implemented will vary depending on the client's architecture, operating model, and regulatory context.

Pricing & Commercial Model

This service is delivered as Professional Services, with pricing provided on request based on scope, environment complexity, and the applicable rate card.

Continuous Security Assurance Enablement for AWS

Overview

With over twenty years of AWS platform engineering experience, The Server Labs enables continuous security assurance by making visibility, evidence, and control effectiveness observable through platform operation.

Many organisations rely on periodic reviews or manual reporting to understand security posture, which quickly becomes outdated in fast-moving environments. This service establishes continuous assurance by surfacing security signals, control status, and operational evidence directly from the AWS platform.

Key Benefits

- Provides continuous visibility of security posture
- Produces assurance evidence through platform telemetry
- Reduces reliance on manual reporting and reviews
- Supports proactive identification of security drift
- Suitable for regulated and high-assurance environments

What This Service Provides

Continuous assurance depends on reliable signals from the platform itself.

This service focuses on enabling visibility into how security controls are operating in real time across the AWS environment. It establishes dashboards, alerts, and reporting mechanisms that reflect the actual state of identity controls, network boundaries, logging coverage, and hardened configurations.

Rather than introducing new manual processes, assurance is derived from configuration state, runtime telemetry, and control outcomes. This allows security posture to be monitored continuously and deviations to be identified early, before they escalate into material risk.

The result is an assurance capability that scales with platform change and supports informed decision-making without slowing delivery.

Who This Is For

This service is suited to organisations that have implemented zero trust controls and require ongoing visibility into their effectiveness.

It is particularly relevant for regulated, mission-critical, or high-assurance environments where confidence in security posture must be maintained continuously rather than assessed periodically.

What's Included

- Security posture dashboards and visualisation
- Alerting for control failures and drift
- Configuration and control state reporting
- Integration with existing security tooling
- Operational security visibility guidance
- Evidence outputs aligned to assurance needs

Delivery Approach

The engagement is delivered through focused configuration and integration work to surface meaningful security signals from the AWS platform.

Work begins by identifying the controls and signals that provide the strongest assurance of zero trust effectiveness. Dashboards and alerts are then configured to reflect those signals accurately and consistently. Reporting outputs are validated to ensure they are suitable for operational and assurance use.

The approach prioritises clarity and reliability, ensuring that assurance data remains actionable and trusted over time.

Key Deliverables

- Security posture dashboards reflecting platform state
- Alerting configuration for control degradation and drift
- Assurance reporting outputs derived from automation
- Operational guidance for interpreting security signals
- Summary of assurance coverage and limitations

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security and Operational Excellence pillars.

Assurance enablement typically references capabilities provided by **Amazon Web Services**, including:

- AWS Security Hub
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon EventBridge

- Native logging and monitoring services

The specific services and dashboards implemented will vary depending on the client's architecture, operating model, and regulatory context.

Pricing & Commercial Model

This service is delivered as Professional Services, with pricing provided on request based on scope, environment complexity, and the applicable rate card.

Continuous Security Assurance Enablement for AWS

Overview

With over twenty years of AWS platform engineering experience, The Server Labs enables continuous security assurance by making visibility, evidence, and control effectiveness observable through platform operation.

Many organisations rely on periodic reviews or manual reporting to understand security posture, which quickly becomes outdated in fast-moving environments. This service establishes continuous assurance by surfacing security signals, control status, and operational evidence directly from the AWS platform.

Key Benefits

- Provides continuous visibility of security posture
- Produces assurance evidence through platform telemetry
- Reduces reliance on manual reporting and reviews
- Supports proactive identification of security drift
- Suitable for regulated and high-assurance environments

What This Service Provides

Continuous assurance depends on reliable signals from the platform itself.

This service focuses on enabling visibility into how security controls are operating in real time across the AWS environment. It establishes dashboards, alerts, and reporting mechanisms that reflect the actual state of identity controls, network boundaries, logging coverage, and hardened configurations.

Rather than introducing new manual processes, assurance is derived from configuration state, runtime telemetry, and control outcomes. This allows security posture to be monitored continuously and deviations to be identified early, before they escalate into material risk.

The result is an assurance capability that scales with platform change and supports informed decision-making without slowing delivery.

Who This Is For

This service is suited to organisations that have implemented zero trust controls and require ongoing visibility into their effectiveness.

It is particularly relevant for regulated, mission-critical, or high-assurance environments where confidence in security posture must be maintained continuously rather than assessed periodically.

What's Included

- Security posture dashboards and visualisation
- Alerting for control failures and drift
- Configuration and control state reporting
- Integration with existing security tooling
- Operational security visibility guidance
- Evidence outputs aligned to assurance needs

Delivery Approach

The engagement is delivered through focused configuration and integration work to surface meaningful security signals from the AWS platform.

Work begins by identifying the controls and signals that provide the strongest assurance of zero trust effectiveness. Dashboards and alerts are then configured to reflect those signals accurately and consistently. Reporting outputs are validated to ensure they are suitable for operational and assurance use.

The approach prioritises clarity and reliability, ensuring that assurance data remains actionable and trusted over time.

Key Deliverables

- Security posture dashboards reflecting platform state
- Alerting configuration for control degradation and drift
- Assurance reporting outputs derived from automation
- Operational guidance for interpreting security signals
- Summary of assurance coverage and limitations

AWS Services & Framework Alignment

This service is aligned with the AWS Well-Architected Framework, with particular emphasis on the Security and Operational Excellence pillars.

Assurance enablement typically references capabilities provided by **Amazon Web Services**, including:

- AWS Security Hub
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon EventBridge

- Native logging and monitoring services

The specific services and dashboards implemented will vary depending on the client's architecture, operating model, and regulatory context.

Pricing & Commercial Model

This service is delivered as Professional Services, with pricing provided on request based on scope, environment complexity, and the applicable rate card.

Why The Server Labs

The Server Labs is the first UK AWS Partner and brings over twenty years of experience enabling security assurance through platform engineering.

Our teams specialise in making security posture observable and trustworthy through automation, rather than dependent on manual reporting or retrospective review.

Next Steps

Engage with The Server Labs through G-Cloud-15 to establish continuous visibility into your zero trust security posture and maintain confidence as your AWS environment evolves.