BigCheese

aws PARTNER Premier Tier Services

Start Now Security Check Pack SOW

Optimization

Version 1.0

May 9, 2024

By: Uriel Agustín Grosso – Pre-Sales Solutions Architect

Index

Introduction

Protect your environment before it's too late.

At **BigCheese**, an AWS Premier Partner, we understand that in the cloud, security is not an "add-on" , it's a baseline requirement. Organizations operating on AWS face increasingly complex risks: unnecessary access permissions, exposed configurations, and silent vulnerabilities that can compromise their entire operation.

That's why we apply our **Think Big, Start Small** approach to security as well:

- **Think Big** means building a continuous governance strategy where security is integrated by design, automated, auditable, and scalable.
- **Start Small** means taking a concrete, low-risk first step: a fast, technical, results-oriented **Security Check**.

With the **Start Now Security Check Pack**, we activate native AWS services like **Security Hub** and **GuardDuty**, perform a full assessment of the **Security Pillar** of the **AWS Well-Architected Framework** through a **Well-Architected Review (WAR)**, and implement immediate quick wins on critical configurations.

At the end of the process, you'll receive a full report including:

- **Detected findings**
- **Remediation actions taken**
- **A roadmap with suggested next steps**

This approach brings three key benefits:

- Real visibility into the current security state of your account
- Immediate improvements without disrupting operations
- Clear recommendations to move toward a continuous security strategy

In just 1 month, you can identify vulnerabilities before they escalate, strengthen your security posture, and take the first step toward robust and effective cloud governance.

Why secure your environment with BigCheese?

At **BigCheese**, we are an **AWS Premier Partner** with multiple official AWS certifications. We are also certified under the **ISO/IEC 27001 international standard**, the world's most recognized framework for information security management.

Over the past few years, we've conducted more than **60 Well-Architected Reviews (WARs)** with a focus on security. In **over 80% of those cases**, we discovered **critical vulnerabilities** in accounts that *appeared* to be properly configured.

From unnecessary permissions to lack of encryption, inactive monitoring, or publicly exposed resources, our experience has taught us one key lesson:

The biggest risk is not the attack, it's not knowing you're exposed.

Securing your environment with BigCheese means having a certified team that:

- Detects real risks, not just theoretical ones

- Applies quick wins that strengthen your security posture from the very first month
- Provides visibility, documentation, and clear next steps

And most importantly, helps turn security into a continuous practice, embedded across your organization and aligned with your business

Business Case: Risk isn't a possibility, it's a certainty

In the cloud, security incidents rarely come with a warning. A misconfiguration, an incorrectly assigned permission, or an exposed service can, in seconds, turn into a data leak, service outage, or reputational disaster.

The **Start Now Security Check Pack** is designed for organizations that:

- **Process payments, transactions, or sensitive customer data**

eCommerce businesses, fintechs, payment gateways, subscription platforms, or any company managing credit cards, bank accounts, digital identities, or purchase histories.

A data breach or attack can result in lost trust, legal sanctions, or irreversible brand damage.

- **Operate with many internal users and differentiated access**

Companies with multiple technical, commercial, or administrative teams, where different user profiles access internal systems, making it hard to maintain full control over permissions.

A poorly applied policy or inherited access can leave doors open to users who should no longer have privileges.

- **Handle confidential or legally protected information**

Law firms, notaries, healthcare services, or public/private organizations storing personal data, medical records, contracts, or legally sensitive documents.

Poor encryption or exposed storage can compromise privacy and create direct legal liability.

- **Cannot afford even a minute of downtime**

Logistics, retail, manufacturing, or critical service companies relying on 24/7 infrastructure. An attack, misconfiguration, or automatic service suspension can halt operations, and cost thousands of dollars per hour.

Security is not just about protecting data, it's about **ensuring business continuity.**

- **Believe "it won't happen to us" because it hasn't yet**

Organizations that have a working environment and believe everything is fine, simply because nothing has gone wrong... yet.

The most common issue we find isn't a breach, it's a **false sense of security**.

With this pack, you'll detect **real vulnerabilities** before they become headlines.

Because the most dangerous thing about a misconfigured environment... is not knowing it's misconfigured.

Objective

The objective of the Start Now Security Check Pack is to help the client identify, remediate, and document critical vulnerabilities in their AWS environment within just 30 days. This is achieved by:

- Activating key security controls
- Performing a structured analysis of the Security Pillar through a Well-Architected Review (WAR)
- Laying the groundwork for a continuous governance strategy and a security posture aligned with the organization's real-world operations and risks

This service empowers organizations to:

- Make decisions based on evidence
- Strengthen security without friction
- Prepare their team to elevate cloud security practices — with visible results in the first month

What do we need from the client for a successful Security Check?

To ensure an accurate assessment and effective improvements, the following are essential:

- **Access to the AWS account(s) to be evaluated**
  This can be granted through read-only permissions or temporary role setup, depending on the client's internal policies.

- **Technical points of contact for validation and consultation**
  Individuals with knowledge of the current environment who can answer questions, validate findings, and authorize quick wins.

- **Context about the environment and critical use cases**
  Understanding which services are production, which environments are actively used, and which ones can be safely modified.

- **A commitment to an open and honest review**
  This is not an audit for punishment, it's a collaborative process to identify improvement opportunities and raise the security standard.

- **Availability for a result presentation session**
  Where we will share the report including findings, applied improvements, and recommended next steps.

With this foundation in place, the Start Now Security Check Pack can be executed smoothly, without friction or blockers, delivering results from day one.
Detect. Improve. Protect. That's how a serious security strategy begins.

Service Scope

The **Start Now Security Check Pack** is executed over a **30-day period** with the goal of detecting vulnerabilities, applying immediate improvements (quick wins), and delivering a **clear and actionable diagnosis** of the AWS environment's current security posture.

The scope includes:

- **Definition of success criteria and technical priorities**

Together with the client, we assess which **threats, environments, or services** are most critical to the business, aligning efforts with the organization's real operational risks.

- **Activation and configuration of native AWS security services**

We implement tools such as **AWS Security Hub**, **GuardDuty**, and other key services to **centralize alerts**, **detect threats**, and **visualize the overall security state** of the environment.

- **Structured analysis of the Security Pillar via a Well-Architected Review (WAR)**

We conduct a comprehensive assessment of the **Security Pillar** based on the **AWS Well-Architected Framework**, evaluating technical controls, governance, visibility, incident response, and data protection.

- **Execution of quick wins**

We apply **immediate improvements** to sensitive configurations, such as:

  - Closing exposed ports
  - Removing obsolete access credentials
  - Enabling encryption in transit and at rest

    - Hardening IAM roles and key security policies

- **Findings report and recommendations**

We deliver a **report** including:

    - Detected issues ranked by **risk level**
    - **Corrective actions taken**
    - Results from the **Well-Architected Review**
    - A **roadmap** with next steps and suggested improvements

- **Knowledge transfer**

We present the results to the client's technical team, explaining:

- What was done
- What was found
- How to continue **improving security maturity** in a sustainable way

This service is **not meant to cover the entire cloud security universe**, but to provide a **clear, measurable first step** aligned with **AWS standards** — helping strengthen governance and prepare the environment for more complex security challenges.

Success criteria

To consider the **Start Now Security Check Pack** successful, the following **measurable and verifiable criteria** must be met:

- **Effective activation of AWS native security services**
  AWS Security Hub, GuardDuty, and associated services must be correctly implemented and fully operational, generating relevant alerts and findings for the client's environment.

- **Execution of the Well-Architected Review (Security Pillar)**
  The WAR must be completed with all Security Pillar questions answered, identifying critical risks, opportunities for improvement, and generating actionable recommendations aligned with the AWS Well-Architected Framework.

- **Validated quick wins applied**
  A set of immediate improvements must be implemented on previously identified insecure configurations (IAM, networking, encryption, visibility), with functional validation of each action and no negative impact on active workloads.

- **Technical and executive reports delivered and understood**
  The technical and executive reports must reflect the current state, actions taken, persistent risks, and next-step recommendations, and must be reviewed in a session with the client's technical and/or executive stakeholders.

- **Clear and applicable knowledge transfer**
  The client's technical team must receive a detailed explanation of the process carried out, understand how to use the activated services, and have a practical roadmap to continue strengthening the environment's security posture.

- **Positive perception of value by the client's team**
  The client's technical and security stakeholders must confirm that the assessment was useful, the actions improved their environment, and the process provided clarity, control, and direction toward a more robust security strategy.

Deliverables

During the 30-day execution of the **Start Now Security Check Pack**, the client will receive a comprehensive set of technical and strategic deliverables aimed at strengthening their security posture on AWS, generating operational visibility, and aligning their environment with the standards of the AWS Well-Architected Framework.

As part of the process, **a Well-Architected Review (WAR) focused on the Security Pillar** will be delivered, following the official guidelines of the AWS Well-Architected Framework. This assessment will **identify gaps, risks, and opportunities** for improvement related to access governance, data protection, operational visibility, incident response, and secure service configurations. The findings from the WAR will be documented and prioritized, forming the basis of a roadmap to strengthen security in a structured and scalable way.

In addition, native AWS services such as Security Hub, GuardDuty, and other key tools will be activated and configured to centralize alerts, detect threats, and visualize the overall security state of the environment. A series of quick wins will be applied, including restriction of unnecessary access, removal of exposed resources, activation of encryption, version control, and hardening of IAM policies.

A complete technical report will be provided, including all detected issues (both from the WAR and enabled tools), the risk level of each finding, the corrective actions applied, and any remaining risks. This will be complemented by an executive report, tailored to decision-makers, summarizing the initial state, the improvements implemented, and a suggested roadmap for continuing the process.

A continuity checklist will also be delivered, offering practical recommendations to automate alerts, establish continuous governance processes, and increase cloud security maturity. Finally, a closing and knowledge transfer session will be held, where the client's technical team will receive a detailed explanation of the actions taken, the tools enabled, and the recommended next steps.

This package is not just about remediating isolated vulnerabilities, it's designed to leave the client with a stronger, better-informed, and internationally aligned security posture.

Visibility. Action. Governance. It all starts here.

Involved Team

The **Start Now Security Check Pack** is executed by a certified AWS technical team with proven experience in **cloud security**, **governance**, and **operational best practices**. Depending on the scope and complexity of the environment, the core team may include:

- **Project Manager / Technical Lead**
  Responsible for overall coordination of the service, task planning, progress tracking, and communication with the client's team.

- **Security Specialist**
  Cloud security expert in charge of identifying vulnerabilities, classifying risks, applying quick wins, and defining corrective actions. Applies best practices from the AWS Security Pillar and CIS Benchmarks.

- **Cloud Engineer**
  Technician responsible for executing the necessary configurations, interventions, and automations in the client's AWS account, in compliance with the defined policies.

- **Solutions Architect (if applicable)**
  In more complex environments, it contributes to the overall architecture analysis to detect structural risks and propose design-level improvements.

The team works in an agile manner and in direct coordination with the client's technical stakeholders, ensuring a streamlined process, proper documentation, and high-value deliverables.

Because security isn't about luck, it's about the right team.

Action Plan

Phase	Activity	Comments
Start	Kick-off and definition of success criteria	Meeting with the client, mapping priorities, environments, and critical services
	Initial technical assessment	Account access, preliminary configuration review and inventory
Service Activation	Configuration of Security Hub, GuardDuty, and key security services	Activation, account integration, and event validation
	Configuration review per account/region	Review of initial findings and general environment status
Quick Wins	Immediate improvements (access, ports, IAM, encryption)	Fixes in critical configurations, basic automations
Posture Analysis	Evaluation against best practices (Well-Architected, CIS Benchmarks)	IAM, segmentation, logging, traceability, access controls
Reports	Technical report of findings and quick wins applied	Technical document with issues, corrective actions, and remaining risks
	Executive security posture report	Initial state, improvements applied, and a summarized roadmap

Knowledge Transfer	Presentation of results, closing session	Final meeting with technical and strategic walkthrough, delivery of final checklist

Estimated Timeline

	Month 1			
Phase	**S1**	**S2**	**S3**	**S4**
Start				
Service Activation				
Quick Wins				
Posture Analysis				
Reports				
Knowledge Transfer				

Presupuesto

Total team hours: **40 horas.**

USD 3,200 + VAT

AWS Marketplace discount (50%):

USD 1,600 + VAT

What comes after the Start now security check?

The Start Now Security Check Pack is just the beginning, the first step toward professionalizing your AWS security posture.

Once vulnerabilities have been identified, quick wins applied, and a clear diagnostic delivered, the next phase is moving from reactive fixes to continuous governance.

Depending on your organization's maturity and priorities, the next step may take different forms:

- **Implement a Continuous Security Strategy**

Activate regular reviews, automate alerts, centralize logs, and assign clear ownership by account, service, and environment.

- **Strengthen the architecture with a security-first approach**

Review the overall design focusing on segmentation, blast radius limits, secure scalability, and structural best practices.

- **Monthly support with a dedicated security squad**

Include a Security Specialist as part of a Certified Squad or a continuous service to keep improving and address deeper risks.

- **Train the internal team**

Transfer knowledge so that your own team can sustain and scale the best practices identified during the Security Check.

What we did was open the door: now you know where you stand.

What comes next is building a robust, automated, and sustainable security posture.

With BigCheese, you're not just safer. You're more prepared.