Ingram Micro

InstantFramework for AWS

Kick-starting AWS accounts with AWS best practices and
CIS hardening in 5 Minutes

Ingram Micro
AWSdeutschland@ingrammicro.com
+49 (89) 4208 3484

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

Real-world pain points shared by our AWS partners

Confidence & security know-how

- “How do I secure an AWS account for my customer?”
- Security in-depth exceeds our AWS expertise level
- “We use AWS Organizations for our customers – aren‘t we safe?“

Security guidance

- What AWS best practices do you advise?
- “Which are the minimum required recommended security basics you would recommend?”?

Ownership & diversification

- Security falls entirely to the SMB customer if no managed service was ordered.”
- Multi-Account Landing Zone slow us down — we just want simple but secure AWS accounts to start quickly.

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

Problem areas

Organizational and technical level

Compliance & Governance

- Compliance requirements
- Governance & policies
- Documentation & testing

Resources & Speed

- Limited staff & time
- Manual setup → drifts
- Cloud-skill gap

Handover & Ownership

- Split responsibilities
- Conceptual & interface gaps
- Reseller-to-customer hand-off

AWS Partner expertise ≠ customer cloud maturity!

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

What if?

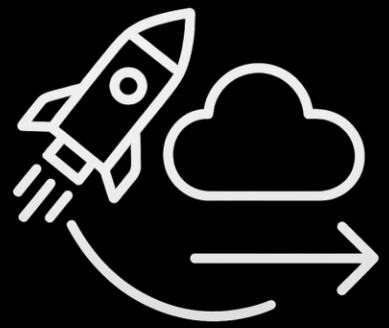
Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

Ingram Micro InstantFramework for AWS

Ingram Micro InstantFramework for AWS (IMIF) kickstarts new AWS accounts with secure, efficient setup based on proven best practices.

Secure

Automated



Instant

Standardized

Highly secured AWS account – < $50 monthly cost (MRR).

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

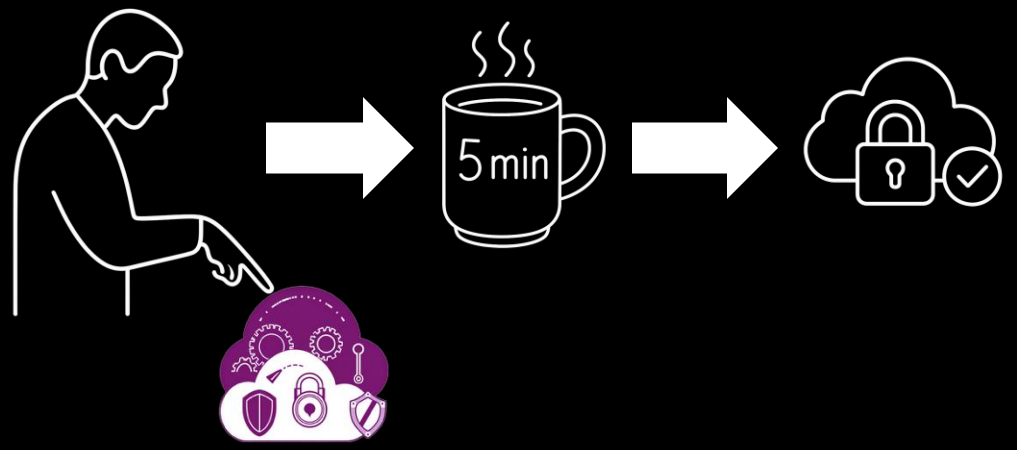
Start secure from day 1.

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

Everyone gets a secure AWS account!

This is how IMIF works

~~Requirements~~
~~Compliance~~
~~Governance~~
~~Concept~~
~~Expertise gaps~~
~~Time / resources~~
~~Split responsibilities~~
~~Manual setup~~
~~Documentation~~
~~Tests~~



IMIF

Best-practice-hardened AWS account

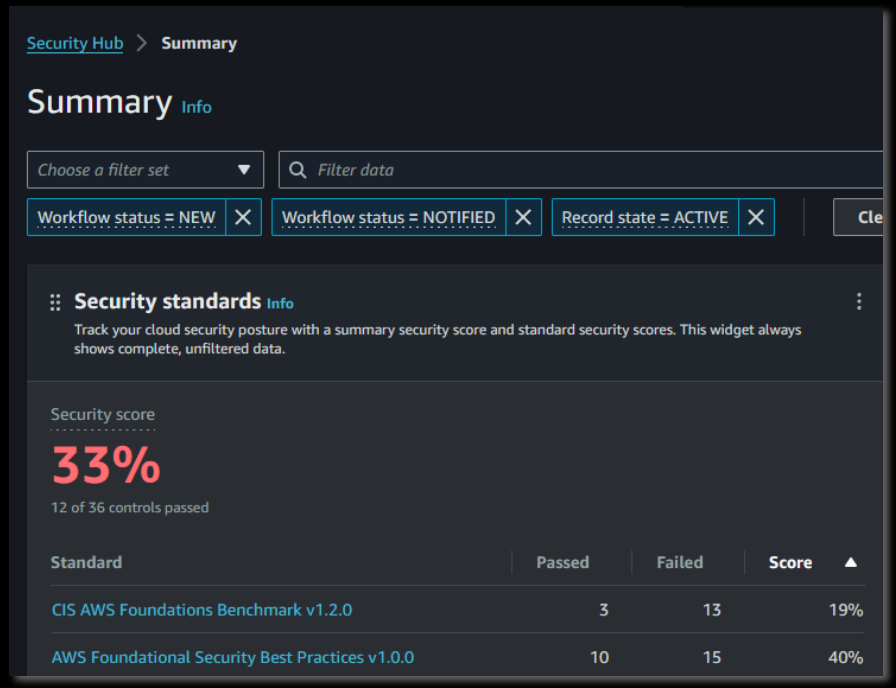
- AWS best-practices
- CIS hardened
- Highly secure
- Production-ready for customer workloads

AWS reseller value-add

AWS (SMB) customer

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

New AWS account… → …with IMIF



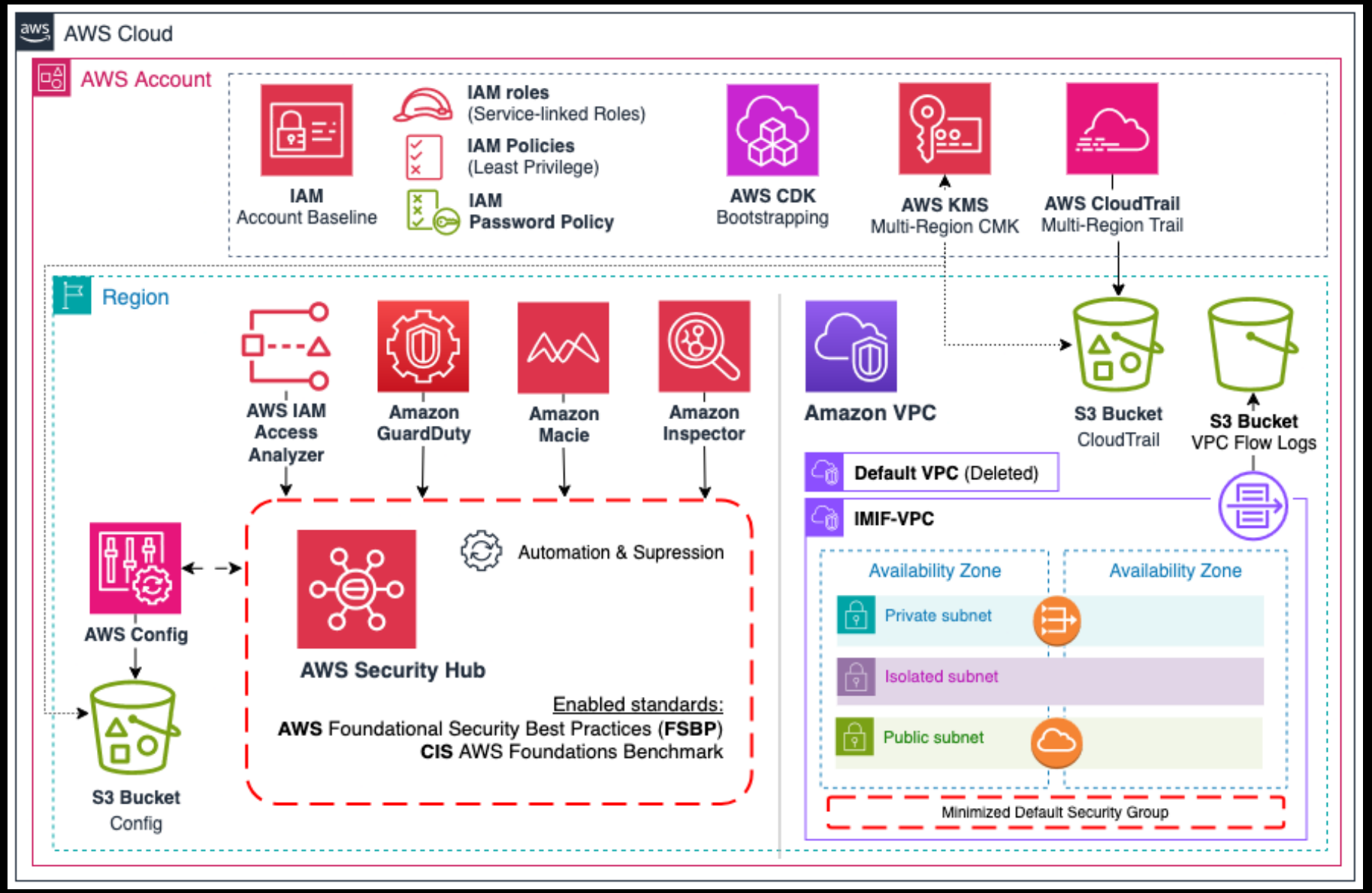
Manually enabled
AWS Security Hub & AWS Config (1-click setup)

New AWS account kickstarted with
Ingram Micro InstantFramework for AWS

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

IMIF Architecture

All AWS-native



Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

AWS Security Maturity Model v2

… where IMIF is build around

Security monitoring & detection

Enabling and optimal config of Amazon GuardDuty, AWS Security Hub & AWS CloudTrail

Data protection

Using of KMS encryption, and enabling and optimal config of Amazon Macie

Compliance & governance

Enabling of AWS Config, setup of optimal least-privilege IAM policies

Vulnerability management

Enabling and optimal configuration of Amazon Inspector

Info: Aligned with AWS Well-Architected Framework and AWS Cloud Adoption Framework.

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

AWS Security Hub Standards
… which are enabled by IMIF

AWS Foundational Security Best Practices v1.0.0 (FSBP)

- A set of AWS Security Hub controls to detect deviations from AWS security best practices.
- Continuously evaluates accounts and resources, providing actionable guidance.
- Covers multiple AWS services, with controls categorized by security function.

CIS AWS Foundations Benchmark v3.0.0

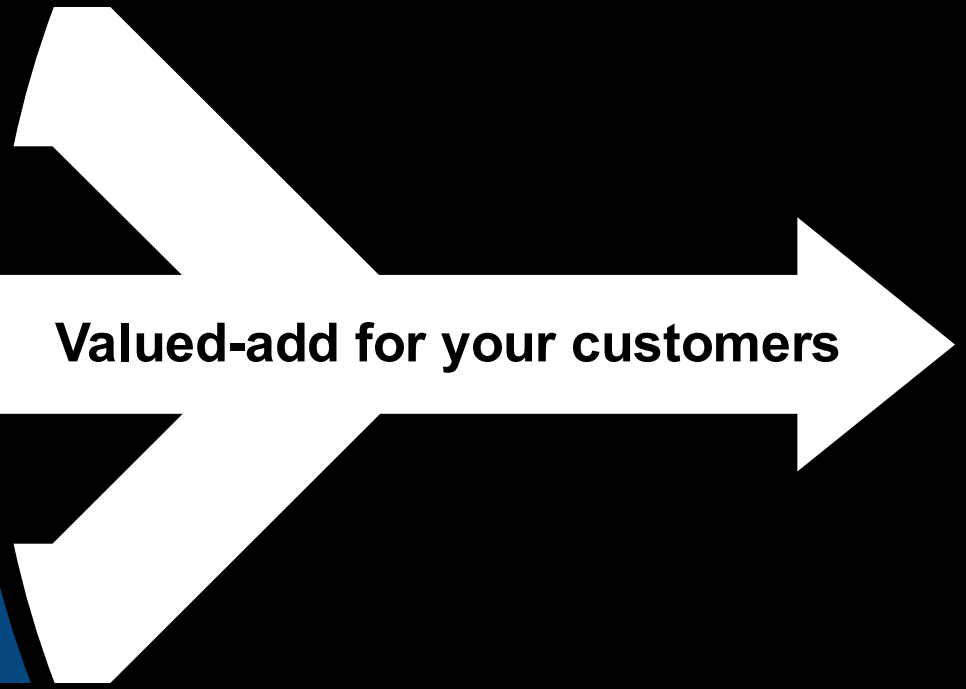
- Developed by the Center for Internet Security (CIS) to guide secure AWS configurations.
- Provides best practices to protect cloud services, operating systems, and networks.
- Helps protect systems across cloud services, OS, and networks.

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

Increased Security

Reduced effort/time

Low costs



Key takeaways

Why IMIF matters

Quickly deliver secure AWS accounts – giving customers the freedom to build on a hardened, production-ready single account landing zone.

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.

Reach out to discover how IMIF can supercharge your AWS business:
AWSdeutschland@ingrammicro.com | +49 (89) 4208 3484

Thanks

Ingram Micro

Proprietary information of Ingram Micro — Do not distribute or duplicate without Ingram Micro's express written permission.