



---

# Improve the security posture of your business

Build a pragmatic security strategy with the SoftwareOne Security Posture Assessment for AWS to help you pinpoint, reduce and manage risk



# Ongoing security threats are a constant strain for organisations

Enterprise security is a moving target with new vulnerabilities identified daily. To maintain a good security posture your organisation's people, processes and technology must work seamlessly together. A weakness in any one of these domains can lead to a security breach resulting in reputational damage, loss of revenue, and potential financial penalties.



**According to IBM's Cost of Data Breach study, the average global cost of a breach was \$4.35M, and in the US \$9.44M in 2022**

## Reduce risk and plan to improve security posture

SoftwareOne Security Posture Assessment for AWS helps you assess your AWS cloud environments' security posture against best practice based on our extensive real-world experience of securing enterprise grade systems.

Our assessment gathers the information you need quickly to build an understanding of your risk profile, plus a short- and medium-term prioritised remediation plan to focus effort on where it will reduce risk the most.

"SoftwareOne has been a competent, flexible, and trusted partner to Viber, and we recommend their services to other organisations that are looking to raise the security bar for their Cloud systems."

Amir Ish-Shalom – Viber Chief Architect

## Key considerations for cloud security

### Visibility of business security risks

What industry best practices have you implemented to maintain visibility of your current security risks?

### Aligned governance & compliance

What security strategy and policies have you adopted regarding infrastructure, data, access, and incident detection?

### Enhanced operational excellence

What processes and procedures have you put in place to ensure you deliver business value whilst ensuring you remain secure?

### Reduced risk

How do you define your security posture and risk profile, and determine your vulnerabilities?

### Increased security awareness

How do you educate and train your staff and privileged users in their roles in maintaining the security of your business systems?

# Security Posture Assessment for AWS

## Kick-off

- Introduce resources and stakeholders
- Run through the process and prerequisites
- Finalise questionnaire
- Agree workshop outline, schedule and attendees

## Data gathering & analysis

### Questionnaire-based discovery themes with key stakeholders

- Organisational security
- Core security
- Extended security

### Tooling-based discovery across all in-scope accounts

- Validation of workshop infrastructure topics
- Infrastructure & environment vulnerabilities
- Infrastructure regulatory compliance validation

## Consolidation & presentation

### Executive summary & detailed issue report

- Summary of gaps with posture mapping
- Detailed list of issues and vulnerabilities

### Remediation plan

- Short-term high priority remediation plan listing all severe vulnerabilities and issues
- Medium-term remediation plan focusing on changes required to processes and staff awareness

## Make informed decisions to protect your business

**The strategic framework** for assessing and managing security across your business gives you comprehensive insight into the strengths and weaknesses of your people, processes, and technology.

**Organisational security** recommendations ensure that your security strategy and policies are aligned with your business and regulatory requirements, and that these are implemented appropriately in the cloud. It encourages embedded security-first thinking.

**Process and procedure** recommendations will help you adhere to best practice identity management, specifically onboarding, and offboarding, outline an effective incident response process, place security at the core of your development process, and focus your remediation effort where it is most needed.

**The infrastructure remediation plan** outlines how vulnerabilities should be addressed, monitored, and managed on an ongoing basis, at an appropriate level for your business, and for your most critical systems.

**The training plan** aims to educate your general staff and privileged users in their roles in maintaining the security of your business systems.



# Get secure, keep secure then take the next step together with SoftwareOne

If you're already operating in AWS and struggling to maintain your security posture due to the ever-evolving threat landscape or experienced an outcome from an AWS Well Architected Review that has raised concerns about your security risk, then please talk to us. We also offer follow-on remediation and adoption & change management services should you need support post-Security Posture Assessment.

## CONTACT US TODAY

Find out more at

[www.softwareone.com/AWS](http://www.softwareone.com/AWS)

SoftwareOne AG | Headquarters

T. +41 44 832 4169

E. [info@softwareone.com](mailto:info@softwareone.com)

Copyright © 2023 by SoftwareOne AG, Riedenmatt 4, CH-6370 Stans. All rights reserved. SoftwareOne is a registered trademark of SoftwareOne AG. All other trademarks are the property of their respective owners. SoftwareOne shall not be liable for any error in this document. Liability for damages directly and indirectly associated with the supply or use of this document is excluded as far as legally permissible. © Imagery by: Adobe Stock and Getty Images.

