8 west
CONSULTING

APRIL / 2025

WELL ARCHITECTED SECURITY

CONFIDENTIAL

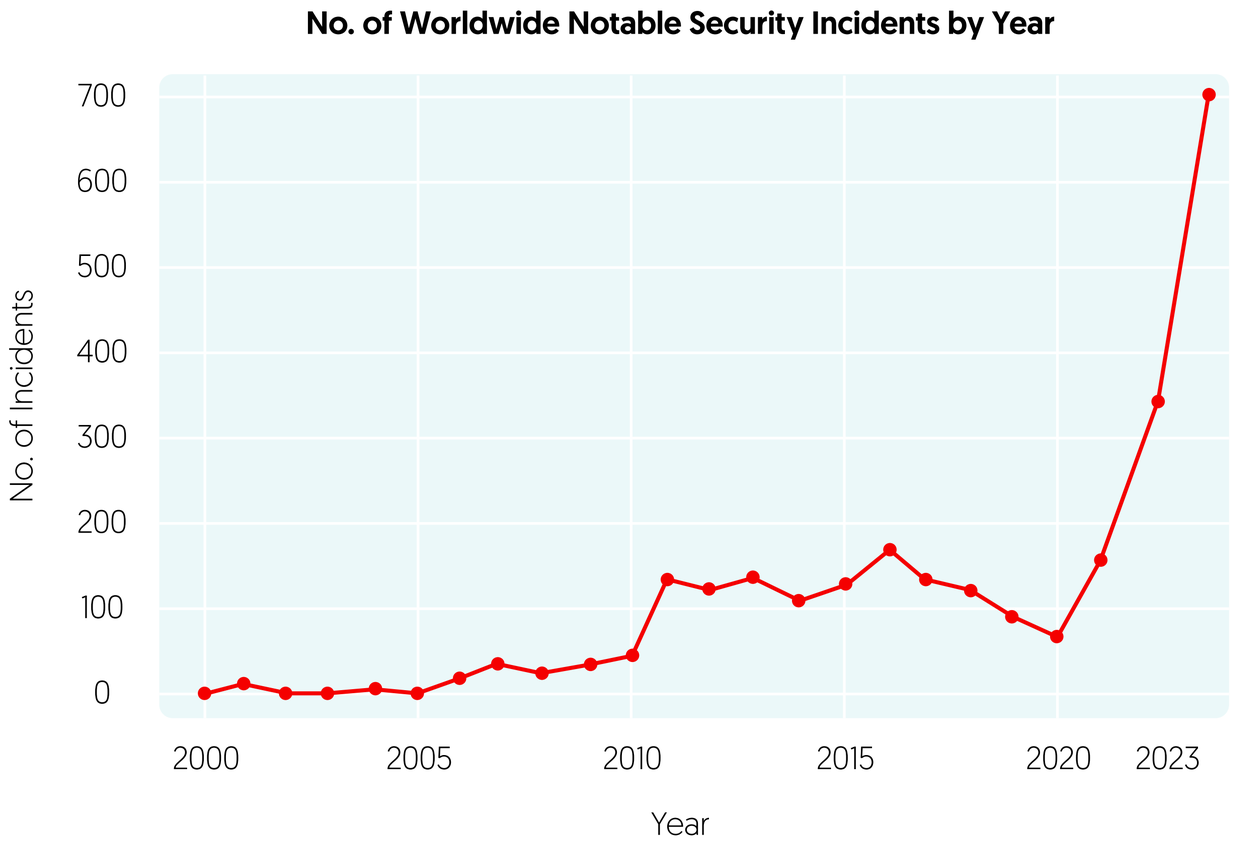
All Rights Reserved. This material contains the valuable properties and trade secrets of 8 West Consulting. No part of this material may be reproduced or transmitted in any form or by any means, electronic, mechanical or otherwise, including photocopying and recording, or in connection with any information storage or retrieval system without the permission of a Director of 8 West Consulting.

INFORMATION SECURITY
ISO/IEC 27001:2022
NSAI Certified

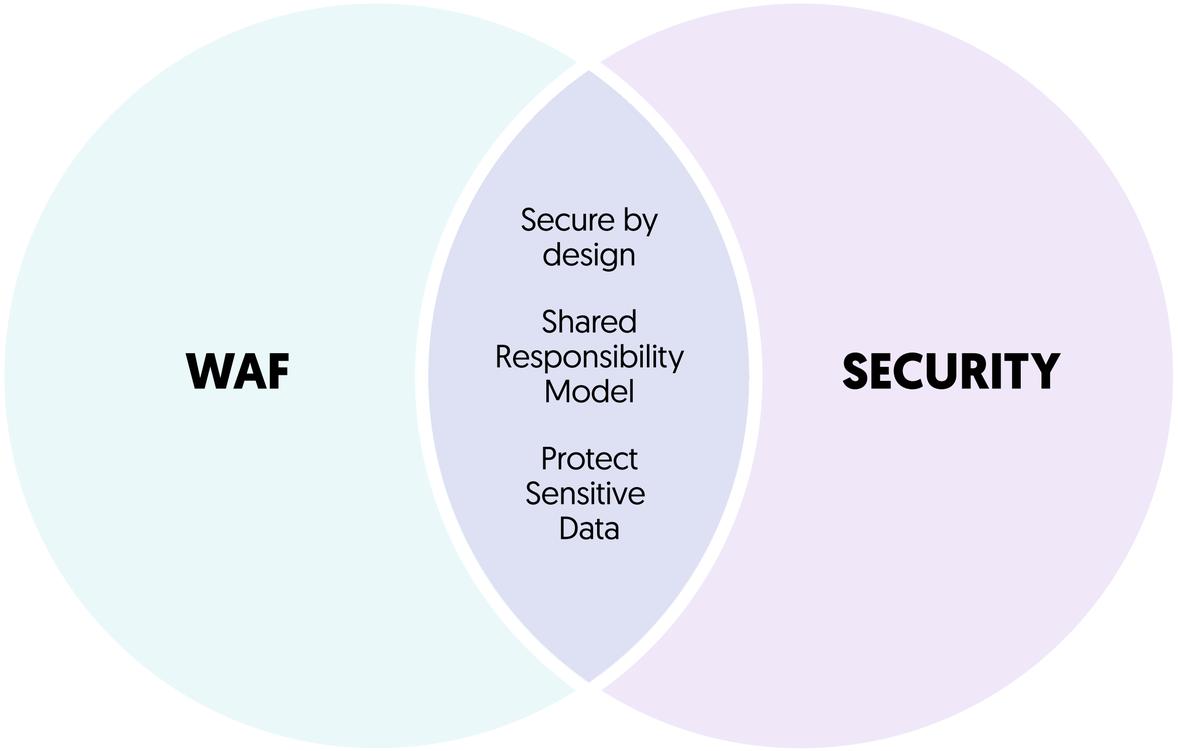
Why Security?

Security is one of the Six pillars of the well architected framework, but why is it so important, especially in cloud environments?

- Each year, the number of cybersecurity attacks increases drastically, with threat actors using more advanced Techniques, Tactics and Procedures by the day.
- 80% of companies have encountered an increase in the frequency of cloud attacks. [1]



Security in the Well Architected Framework



The WAF's security pillar is designed to help organizations create secure and reliable cloud architecture.

It ensures that sensitive data is protected, access is managed efficiently, and potential threats get identified before becoming issues.

By integrating security in every stage of the development process, business can safeguard their operations, build trust, and meet compliance standards.

Security Goals

What are the goals?

Confidentiality	Protect sensitive and confidential data from unauthorised individuals.
Integrity	Prevent unauthorised changes in your environment.
Availability	Ensure your system and services offer uninterrupted access, minimizing downtime.
Accountability	Establish ownership and traceability of systems and data.
Resilience	Ensure that you company can quickly recover from security incidents.

Why pursue them?

- **Protect Business Reputation**
  Data breaches and other security incidents can negatively impact customer's trust and can pose a serious financial cost.
- **Ensure Regulatory Compliance**
  Meet legal requirements to avoid fines and penalties.
- **Mitigate Financial Risks**
  Reduce costs associated with breaches, legal fees and downtime.
- **Enhance Customer Confidence**
  Gain trust by showing commitment to security.

Typical Security Challenges



Defending against a constantly evolving threat landscape

In 2023, Google observed 97 zero-day vulnerabilities being exploited in the wild, highlighting the need of an adaptive and proactive defence strategy.



Maintaining business momentum

Implementing security measures can be time consuming, which is why streamlined processes and automation are critical to ensure security without slowing down the business.



Balancing security and usability

Security shouldn't come at the cost of usability. Finding the right balance means protecting your systems while ensuring the smoothest experience possible for the users.

Security Pillar Core Concepts

Compliance and Governance

Aligns security with industry standards and regulatory requirements.

Identity and Access Management

Ensure the right individuals have secure, controlled access to resources.

Shared Responsibility Model

Defines the distinct security roles of the organization and its cloud providers.



Infrastructure Protection

Safeguards networks, systems and hardware from external and internal threats.

Incident Detection and Response

Monitors for threats and enable swift action to mitigate breaches.

Data Protection

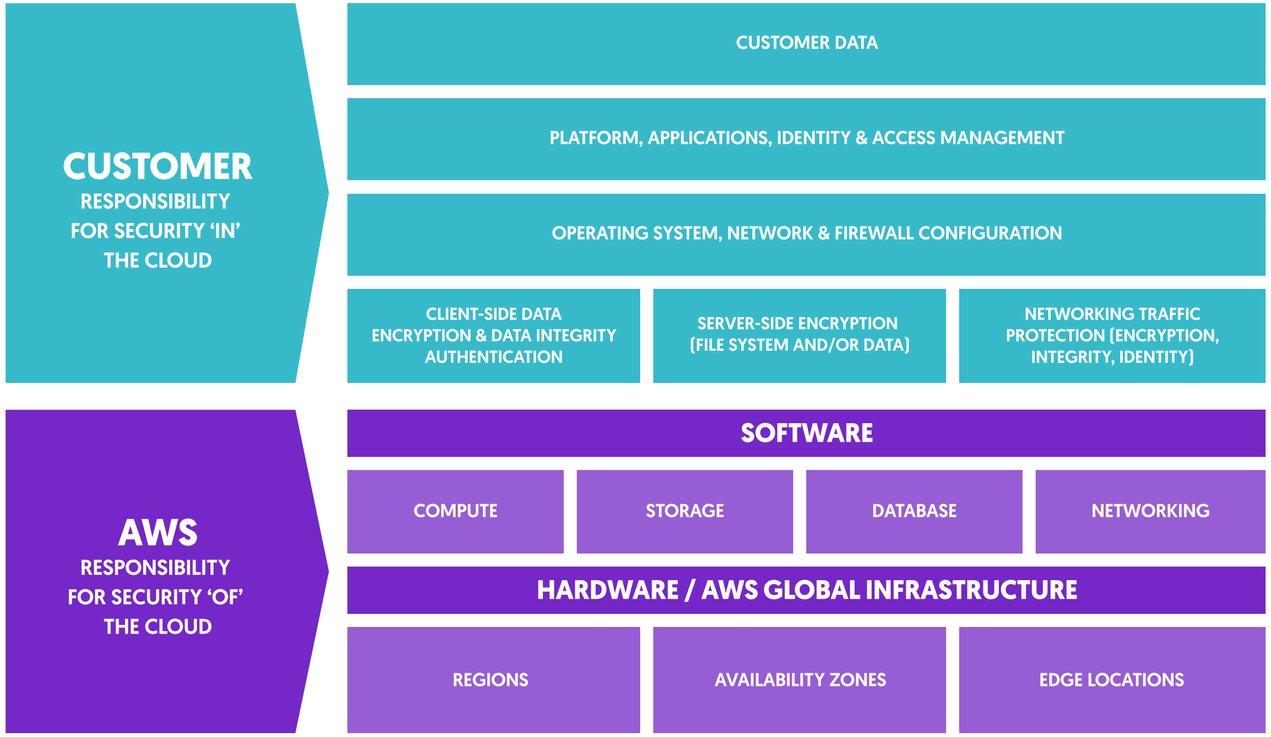
Protects sensitive information through encryption, backup and secure storage.

Shared Responsibility Model

The shared responsibility model defines how security responsibilities are divided between your organization and the cloud provider.

In this model, the cloud provider is responsible of the security “in” the cloud, such as physical infrastructure and networking, while the customer is responsible for security “of” the cloud, as managing data, access, application security and configurations.

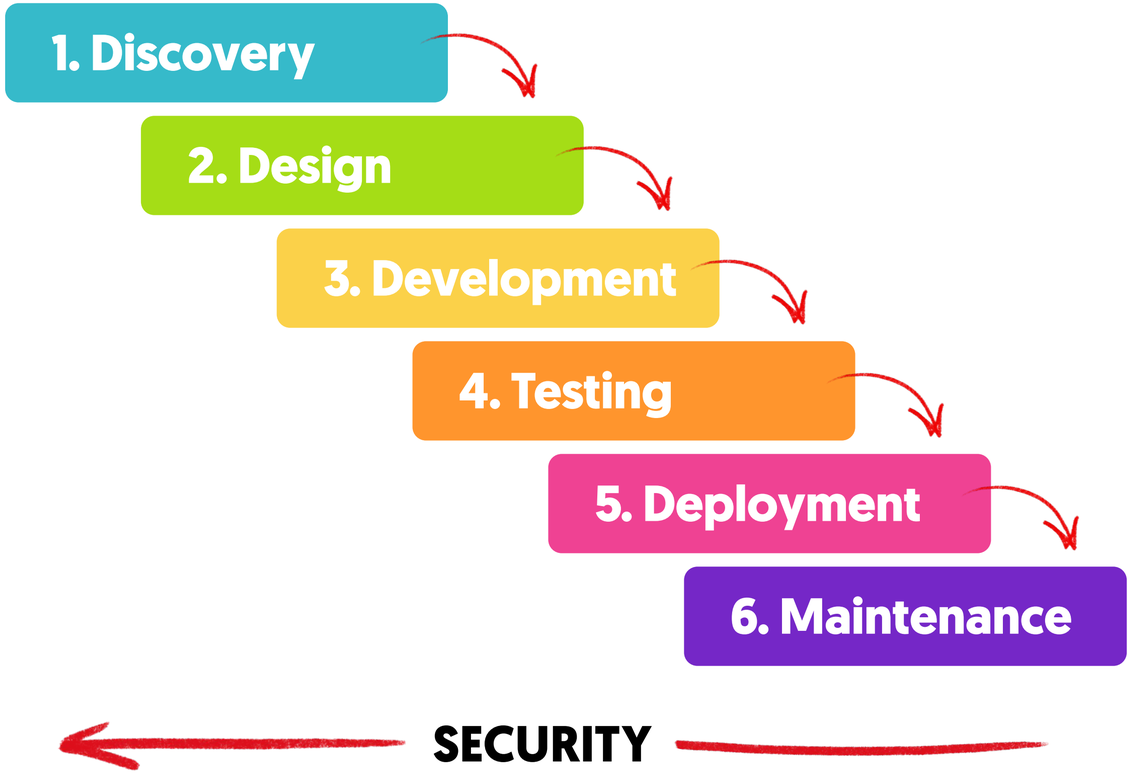
Understanding this model is critical to ensure secure and compliant workloads.



Implementing Security

Shift Left

Catching security issues quickly is critical to save time and cost, which is why having multiple security checks early in SDLC is the optimal way of catching bugs before it becomes too hard and expensive to solve them.

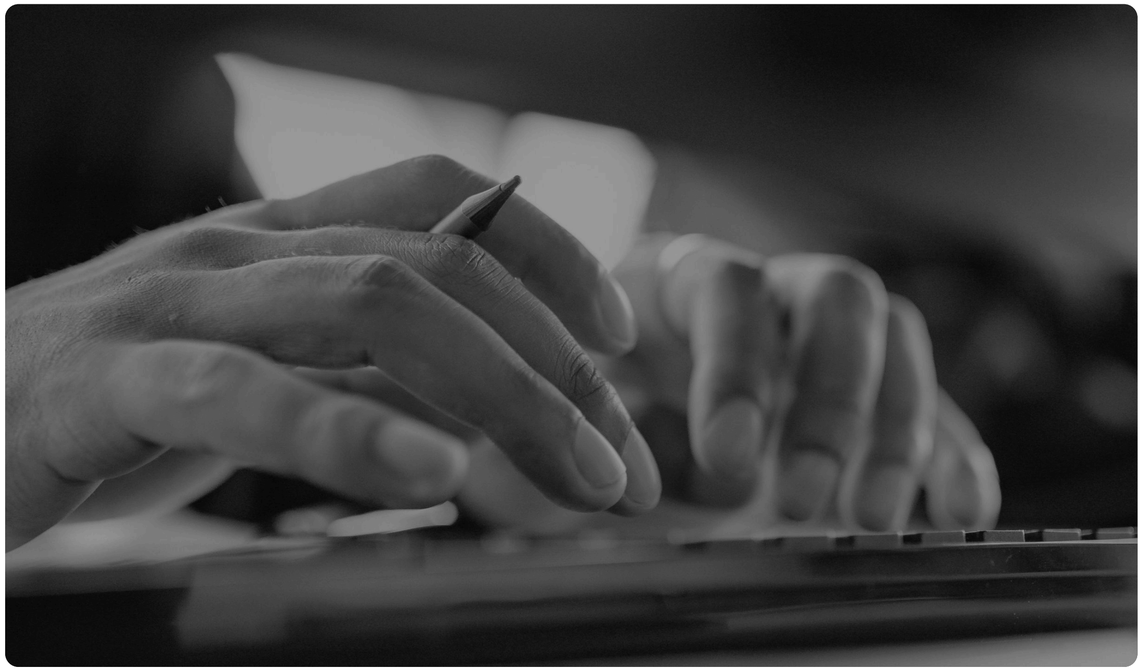


Measuring Security

An effective security implementation begins with understanding the organization's maturity.

To achieve this, we use the Crawl/Walk/Run model for an easy-to-understand, high-level view, and the DevSecOps Maturity Model for a more focused and detailed view of security governance, development and operation.

This dual approach helps us pinpoint gaps and guide a structured approach to fix them.



Measuring Security: Crawl/Walk/Run

To understand the organization's maturity, we use the Crawl/ Walk/Run model for a high-level view.

CRAWL



Foundations

- Basic manual security practices are in place
- Processes are driven by compliance.
- Approach to threats and vulnerabilities is reactive.

WALK



Improving Capabilities

- Security processes are partially automated.
- Partial integration of security in the SDLC.
- Approach to threats and vulnerabilities is proactive.

RUN

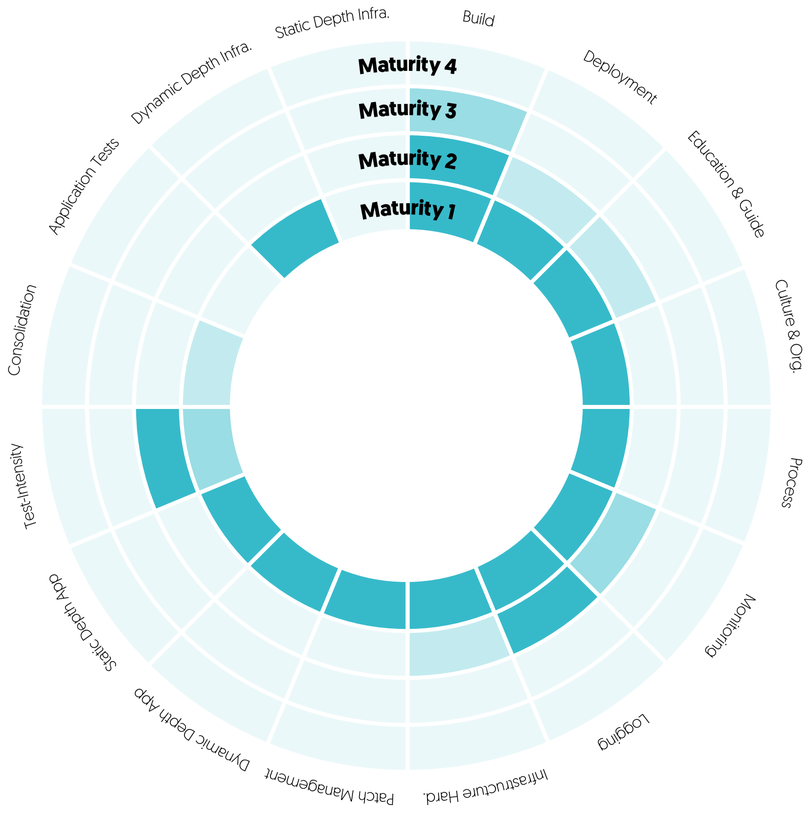


Full Integration

- Threat intelligence is used to prioritize risks.
- Security is fully integrated in the SDLC.
- Advanced and proactive security mechanisms.

Measuring Security: DSOMM

Identification of the degree of implementation



The DevSecOps Maturity Model helps organizations integrate security into every stage of the development lifecycle by giving a maturity score to each area separate area, highlighting the gaps that need improvement.

Security in the Organization

- Establish clear lines of ownership and governance.
- Automate and monitor for non-technical KPIs.
- Integrate security considerations into business operations (e.g. budgeting).



Regulatory Compliance Rate

Ensure the organisation complies with legal and industry standards.



Operational Efficiency Posture

Ensure security controls enhance and don't hinder operational performance.



Business Continuity Readiness

Ensure the resilience of the business in case of disruptive security incidents.

RACI

The **RACI** (Responsible, Accountable, Consulted, Informed) matrix is a tool that can help identifying the responsibilities inside the organisation making the workload more manageable.

ACTIVITY / PROCESS	DEVELOPMENT	SOC MANAGER	CISO	DEVOPS	EXECUTIVE	LEGAL
Define security policies and standards	I	C	R	I	A	C
Code security (e.g., secure coding practices)	R	I	C	R	A	I
Static Application Security Testing (SAST)	I	R	C	C	A	I
Dynamic Application Security Testing (DAST)	I	R	C	R	A	I
Vulnerability management	I	R	C	R	A	I
Incident response	R	R	C	R	A	I
Cloud infrastructure security	I	I	C	R	A	I
Access management and authentication	I	C	R	R	A	I
Monitoring and threat detection	I	R	C	R	A	I
Compliance and regulatory audits	I	C	R	I	A	R
Training on secure coding practices	R	I	C	R	A	I
Risk assessments	I	R	R	I	A	C
Security tools configuration/maintenance	I	C	C	R	A	I
Executive reporting on security posture	I	I	R	I	A	I
Legal and regulatory compliance	I	C	C	I	A	R

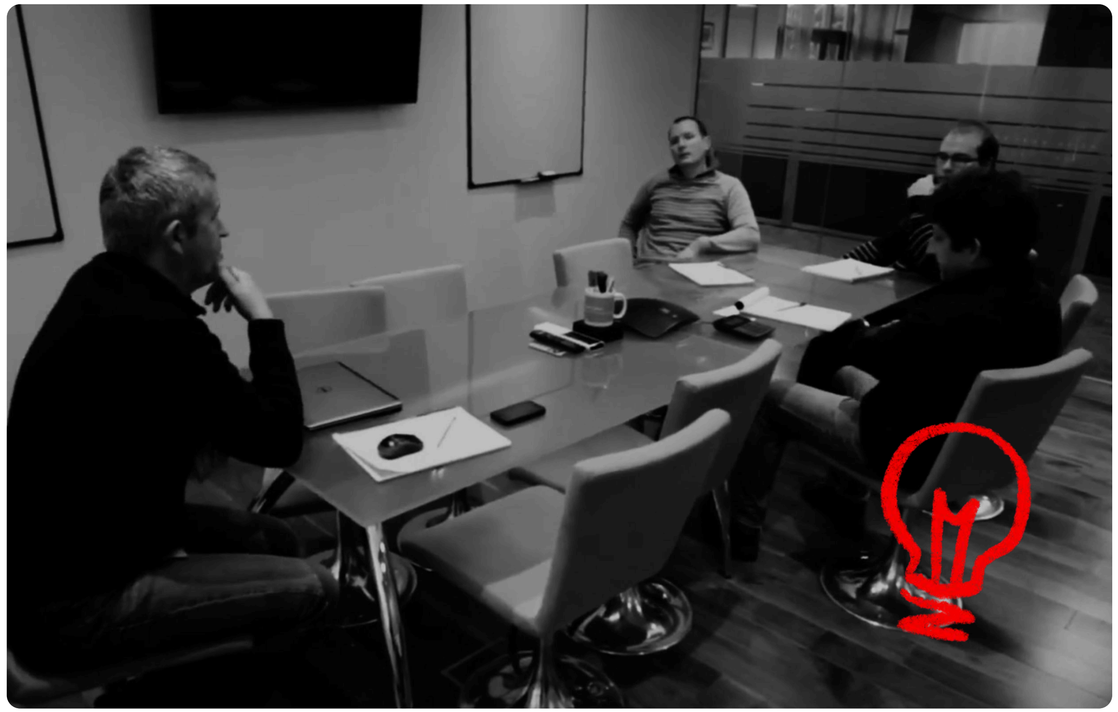
How 8 West Can Help

Strategy

Hardening your organisation's security can be daunting.

With years of experience and a clearly-defined, structured approach to security maturity assessment, 8 West can help to simplify the approach, reduce the complexity and define a clear set of actionable items.

By finding the areas that need improvement and creating an organized timeline of security workload packages to improve your security posture, 8 West will accelerate the path to security excellence within your IT organisation and applications.



Engagement & Onboarding

8 West's cloud engineering team is comprised of certified cloud architects, security professionals and other specialists that cover all the pillars of the well architected framework.

We can provide the centralized hub that communicates across your company divisions to drive best practices and successful governance.

- Dedicated specialists to engage with teams, drive collaboration and provide regular monitoring and reports
- Carefully curated tool suites where we have partnered with the best providers to deliver visibility and transparency
- Management of automated processes and AI tooling that will save time and money
- The implementation of a roadmap for long-term success
- Establishment of Security best practices to gradually harden your security posture and protect yourself from costly security incidents

Step 1 - Data Gathering

Our process begins by collecting data about your organization through a structured conversation with our experts, with the aid of the AWS Well-Architected Framework Tool and frameworks, and by observing your cloud security posture through the use of our partners premium insight tools.



TIMELINE: 2 WEEKS APPROX.

Step 2 - Analysis



Using the data gathered in the first step, our specialists will apply the frameworks and pinpoint gaps and areas of improvement.

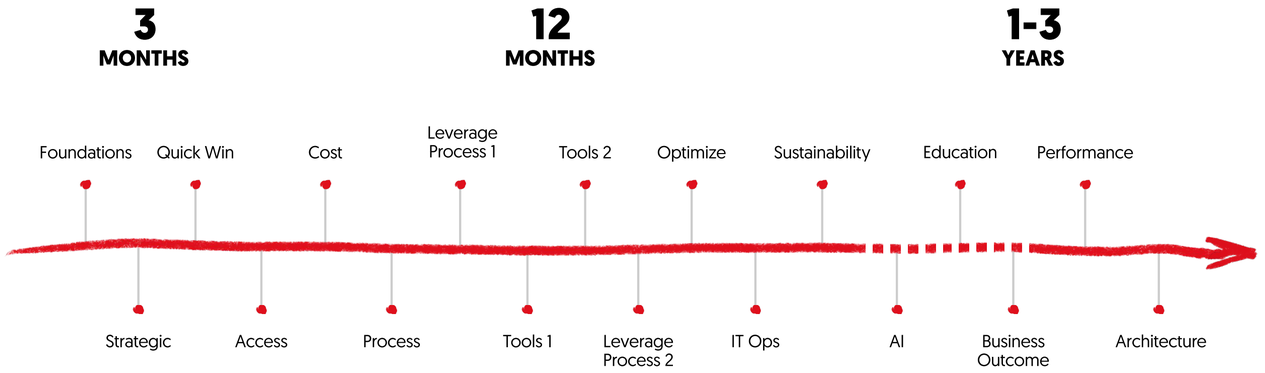
These findings will be used to create a detailed report which will include a pillar-by-pillar analysis, a maturity assessment, a roadmap for remedial actions and recommended tools and resources based on your needs. Accompanying this will also be a report for each pillar.

TIMELINE: 2 WEEKS APPROX.

Step 3 – Tactical & Strategic Planning

With a clear picture of the maturity of the organization and its needs, we create a series of workload packages based on priority of the changes.

These packages will be laid into a clear roadmap divided in short-term, mid-term and long-term actions ensuring steady progress towards high maturity across all pillars.



Step 4 – Implementations

The reports we deliver are designed to provide a clear series of actions that your organization needs. However, the way you choose to implement them is up to you.

Use the roadmap to implement the changes internally with your own team or engage with certified 8 West cloud architects to implement some or all the recommendations, leveraging our expertise and premium partner tools, or collaborate with 8 West to oversee and guide your team as they implement the changes, ensuring optimal results.



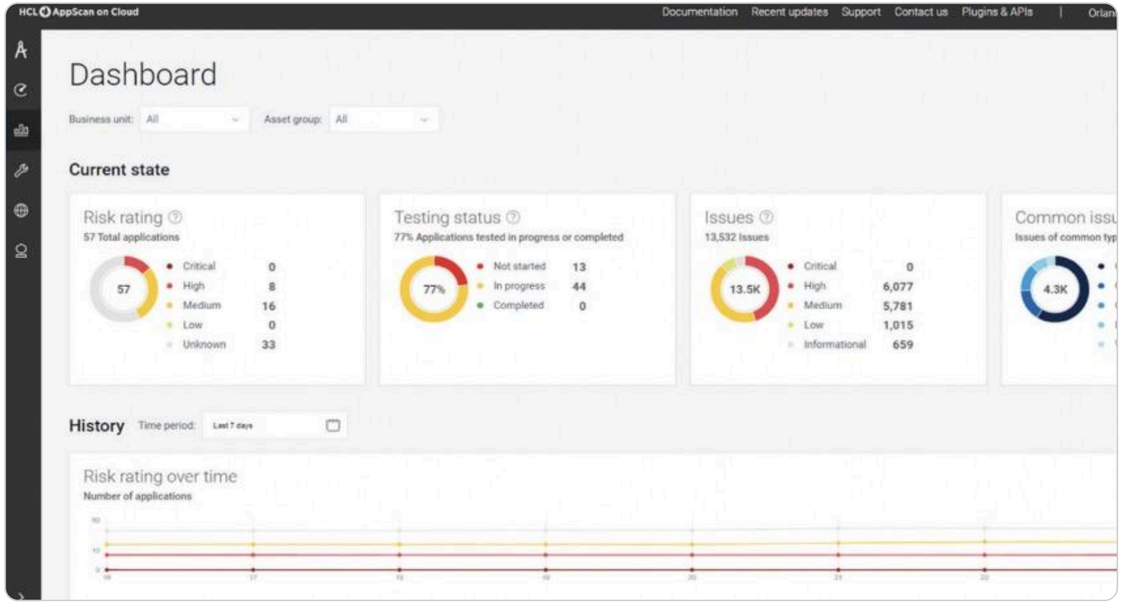
Tools & Resources - DAST & SAST

Dynamic and Static Security Testing Tools

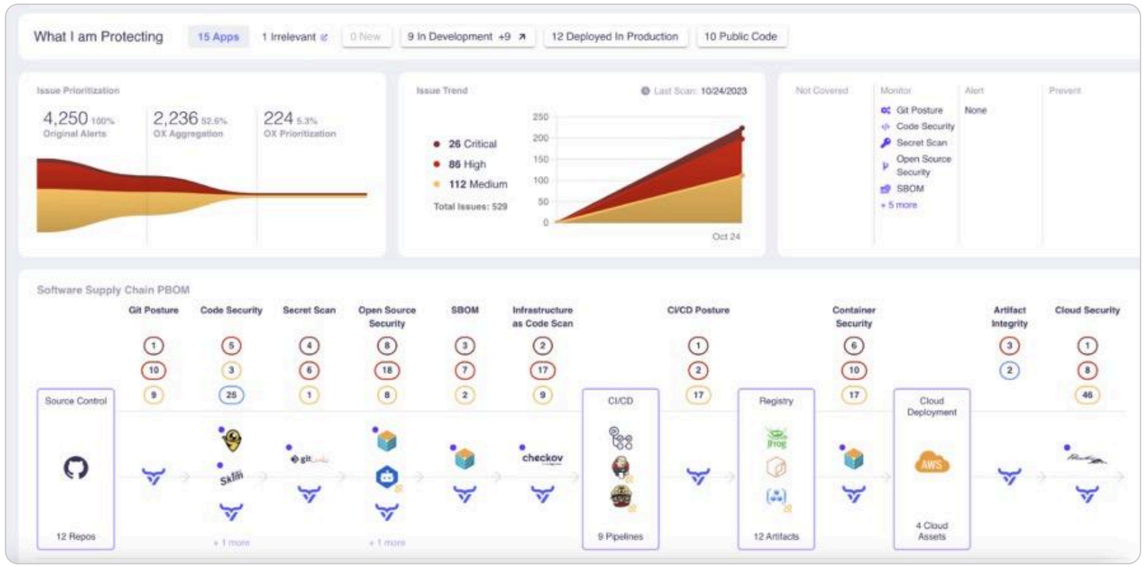
Hardening your organisation's security can be daunting.

With years of experience and a clearly-defined, structured approach to security maturity assessment, 8 West can help to simplify the approach, reduce the complexity and define a clear set of actionable items.

By finding the areas that need improvement and creating an organized timeline of security workload packages to improve your security posture, 8 West will accelerate the path to security excellence within your IT organisation and applications.



Tools & Resources



Application Security Posture Management

ASPM focuses on end-to-end visibility, control, & remediation across the entire software supply chain by integrating with CI/CD pipelines, detecting vulnerabilities, misconfigurations, & potential risks in code, dependencies, & workflows.

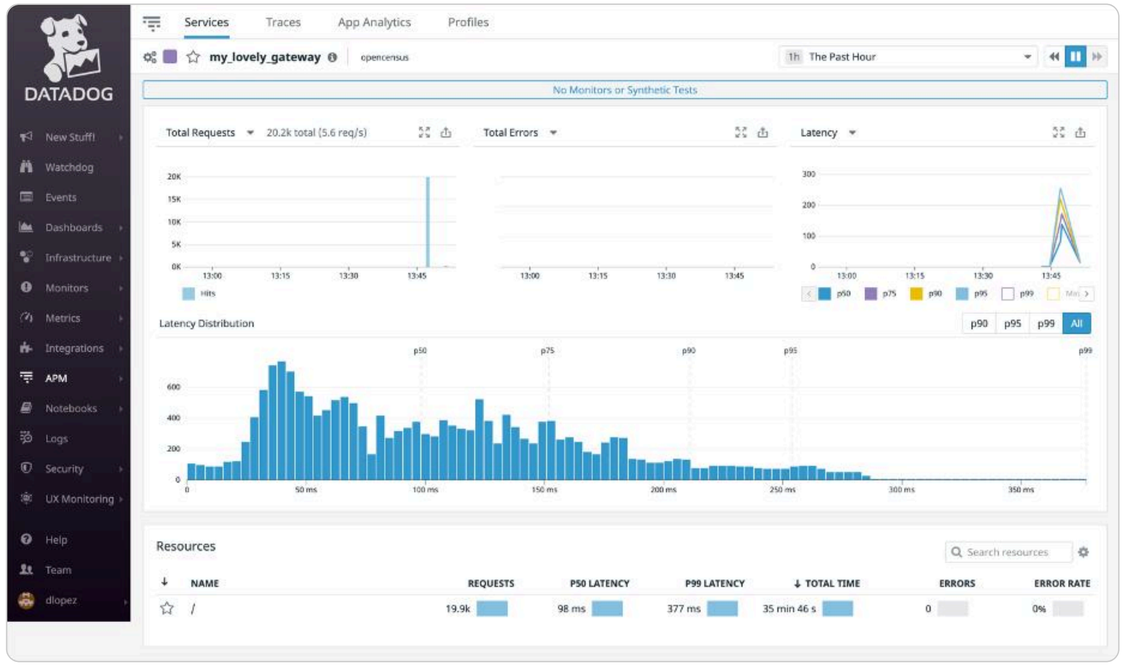
oxsecurity

Tools & Resources

Observability

Having a comprehensive view of your cloud usage and security is critical, especially if using more than one cloud provider.

- Dynatrace
- Datadog
- New Relic



Ready to Take the Next Step?

Simply arrange a date and time for your no obligation introductory meeting with our cloud engineering team, either as part of a wider well architected framework review or as a standalone Security discussion.

Already have specific needs in other areas? We can arrange for you to meet with one of the specialists in our other core areas of competency:

- Architectural services
- Security services
- FinOps services

OR Request a summary of our services and tech talent rate card

References

- [1] 50+ Cloud Security Statistics in 2024
- [2] EuRepoC: European Repository of Cyber Incidents
- [3] A review of zero-day in-the-wild exploits in 2023

8 west
CONSULTING

LET US KNOW HOW WE CAN HELP

or request our rate card and service listing

info@8west.ie