Horangi Warden.

Stop Breaches On The One-Click Cloud Security Platform. Warden gives you your own secure cloud control plane, set up in minutes.

www.horangi.com
hello@horangi.com

Google Cloud Platform · aws · Azure · Alibaba Cloud · HUAWEI CLOUD

HORANGI
CYBER SECURITY

Enterprise-Grade Compliance Automation Recognized By Gartner

Listed In *Gartner 2020 Market Guide For Compliance Automation Tools In Devops*

vodacom · SAFEGRAPH · veraset · Singlife · mekari · Zave · WALLEX

Who Is Warden For?

- Security Teams
- Compliance Teams
- DevSecOps Teams

Warden By The Numbers

270+
RULES

9.3M
MISCONFIGURATIONS IDENTIFIED

11
COMPLIANCE STANDARDS

99% Of Cloud Infrastructure That Warden Has Scanned Have Exposed Security Vulnerabilities That Could Have Led To Data Breaches.

Reduce 80% of IaaS Security Risks with Warden CSPM

10 MINS

FULL ASSET DISCOVERY AND MANAGEMENT

Get instant multi-cloud visibility to see how cloud resources are configured.

10X

FASTER COMPLIANCE AUDIT AND EVIDENCE

Supercharge time to compliance with 100% of Warden security controls mapped to compliance requirements.

70%

REDUCTION IN OVERHEADS AND BILLABLE

Warden's automated remediation reduces 95% of time spent on threat handling, at 8% the cost of an InfoSec headcount.

> “No longer do we have to log in and check 15 different access advisors or build our own tooling around analyzing cloud audit logs. Warden has been a godsend as a centralized tool to do this detailed level of monitoring. Best of all, it is so easy to use, no matter your level of expertise.
>
> **— VINOO GANESH, CTO, VERASET**

Get Unparalleled Cloud Visibility And Control

Security

Continuous security monitoring to protect you from data breaches and compliance violations.

Real-time security monitoring and threat detection for multi-cloud environments to help you respond to issues faster. Take advantage of Warden’s best-in-class alert prioritization, dynamic scanning, and one-click remediation.

Compliance

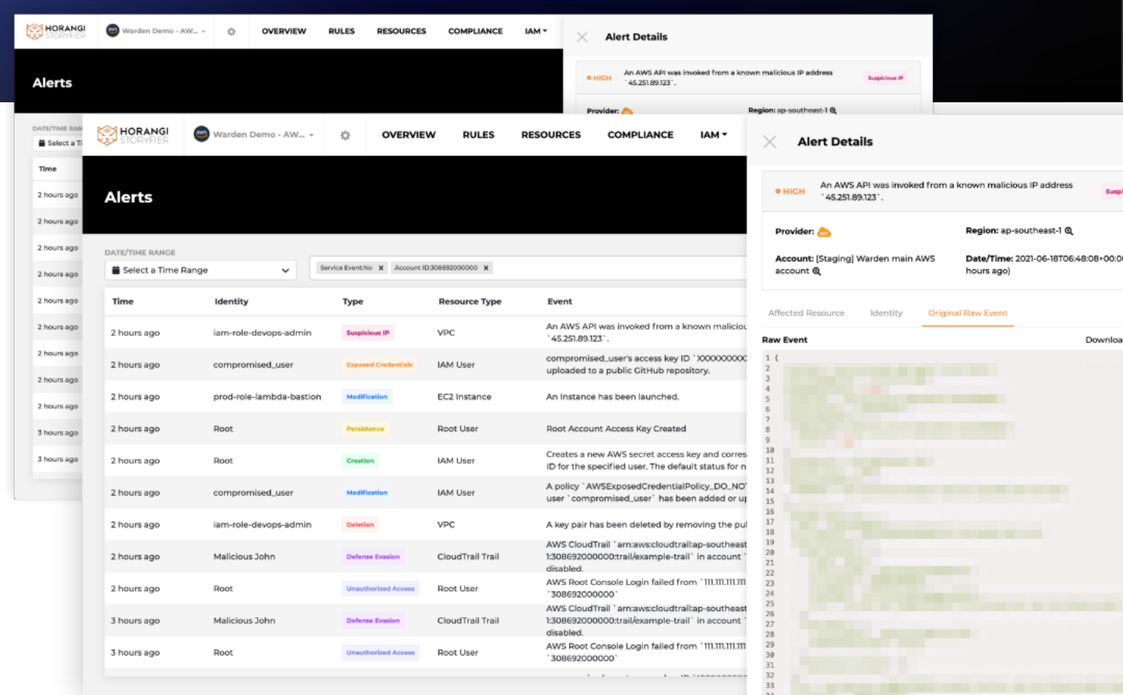
Ensure continuous cloud compliance with automated mapping of technical controls to compliance requirements.

Multi-cloud compliance has never been easier with Warden’s out-of-the-box compliance mapping and report generation for standards including ISO 27001, PCI DSS, GDPR, APRA, and MAS TRM.

Ease Of Use

Enterprise-grade cloud security within a 10-minute no-code setup.

See your multi-cloud security and compliance posture and trending issues on the Warden dashboard. No cloud expertise is required to fix security issues and setup integrations with Slack, GitHub, or your preferred SIEM.



Threat Detection

Threat Intelligence on Warden helps you gain unified visibility of all user activity, whether expected or suspicious. Based on the MITRE ATT&CK framework, this rapid threat detection helps you respond quickly to incidents across your multi-cloud environment.

Why Is Threat Detection Needed?

Prevention Is Not Enough

With a whopping $3.86M being the global average total cost of a breach just last year, we can safely say that prevention is never enough, you need real-time threat monitoring to predict and remediate potential vulnerability issues before they occur.

Native Tools Have Limitations

Threat actors in the cloud typically leverage the cloud management plane and not just the network layer. Traditional tools are not equipped to detect threats in the management plane, hence compromising your team's decision-making on what hackers and how to mitigate those risks.

Slow Response Leads To Massive Damage

Time to respond is even more critical nowadays in the cloud as it can take just seconds for a hacker to infiltrate your infrastructure to steal large amounts of data, hijack cloud accounts, or set up compute-intensive operations like cryptomining without your knowledge.

The Need For Speed

Manual monitoring is very time consuming with many false positives and constant management needed to keep up with the speed of the cloud (new services, new threats).

Detect Privilege Escalation/Credential Compromise

Within minutes of configuration, Warden has complete visibility of all your account activity. If someone obtains unauthorized privileges to launch an EC2 instance or to steal API keys, our Threat Intelligence platform immediately detects such unauthorized IAM changes to help you respond faster.

Remediate With Real-Time Threat Detection Insights

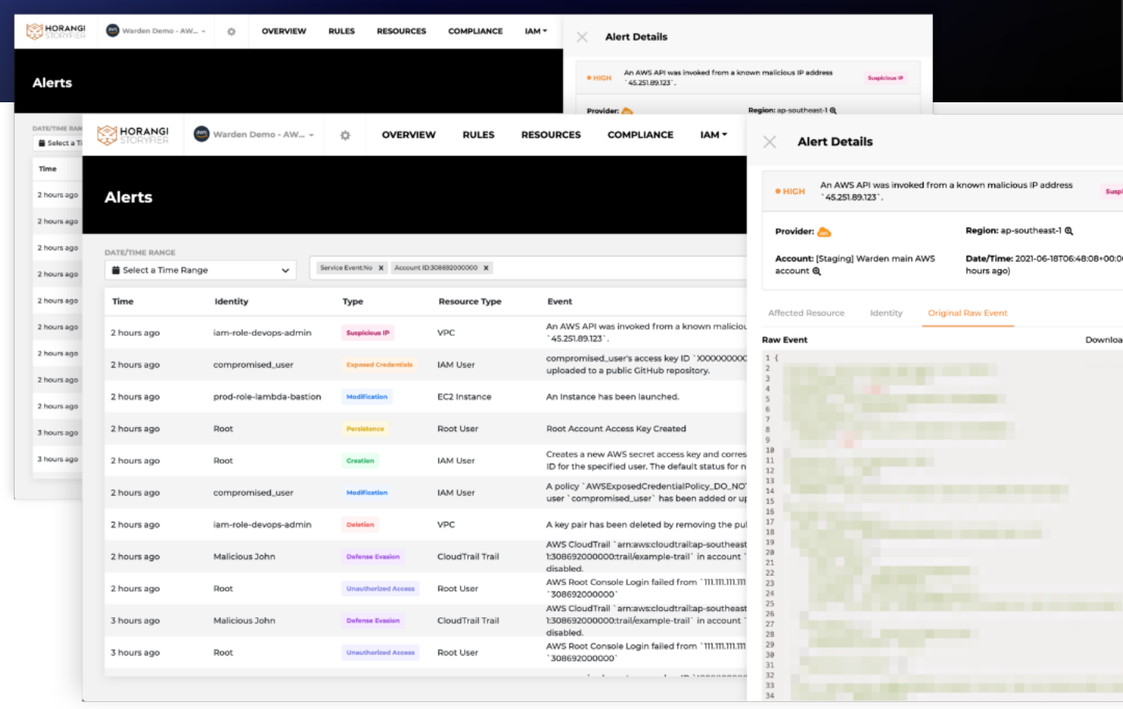
On Warden's unified dashboard you can see a history of all changes to your multi-cloud environment. These are not just alerts, but actionable insights that help you stay audit-ready and in the know of potential threats to your infrastructure.

Reduce Investigation Meantime With Rapid Threat Detection

On average, it takes about 280 days for incident responders to detect and contain a breach. With Warden's Threat Intelligence, you can instantly identify and zoom in on a suspected asset and understand the full context from both a configuration and activity perspective with associated event severity, thereby reducing your meantime (and money) to detecting, investigating, and remediating threats.

Detect Suspicious User Activity

Warden helps you detect possible threat behaviour based on the MITRE ATT&CK framework. You can detect activity from malicious IP addresses, the use of anonymization services like TOR and Proxy/VPN services, or brute-force login/ authentication attempts.

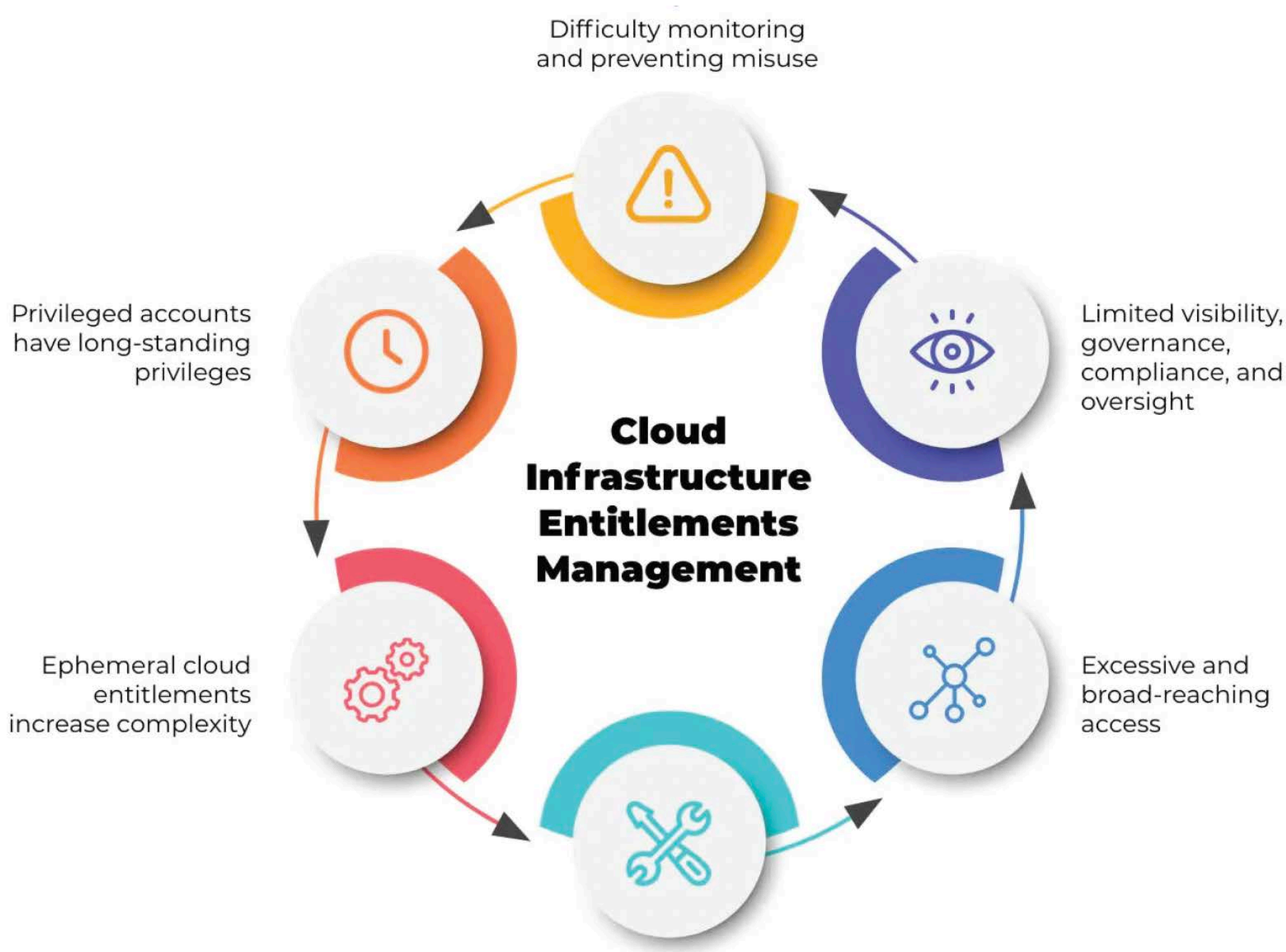


Identity & Access Management (IAM)

Limit the impact of a potential breach by 80% and tackle increasing complexity in managing infrastructure entitlements with Warden's Identity and Access Management. Warden IAM governs identities and access entitlements, and enables enterprises to automatically enforce least privilege and mitigate risks at scale.

Why is IAM Needed?

You simply cannot wait until a crisis to invest in IAM. Shift from loss prevention to protecting fragile experiences with Warden IAM.



> "There is a lot of talk about the Principle of Least Privilege, but Warden's IAM access graph is providing something that I could never do before on the native cloud console. In the past, I could never confidently tell who in my organization had access to specific buckets. The microscopic clarity into relationships between permissions is really useful for us to understand the complexity of IAM and how we can immediately update over privileged and outdated policies found.
>
> **— FELIX CHEUNG, VP ENGINEERING, SAFEGRAPH**

Warden IAM Capabilities

You simply cannot wait until a crisis to invest in IAM. Shift from loss prevention to protecting fragile experiences with Warden IAM.

Unified View of Accounts and Entitlements Across the Cloud

Get full visibility of your multi-cloud IAM without opening multiple windows, cloud provider consoles, or any dependency on team members. You can also analyze all access policies, human and machine identities with a flattened view of entitlements, from a single dashboard.

Real Time Updates With Dynamic Scans

IAM data is updated on the dashboard within minutes of changes with frequent Dynamic Scans or once-a-day daily scans, to suit your preferences and infrastructure needs, tackling ever-growing com

Microscopic Resource-Level Access Review

Warden IAM is a single platform to get both security exposure insights and visibility into your identities and access management setup, reducing cloud-related security incidents due to misconfiguration by up to 80%.

Enforce Least Privilege Policy

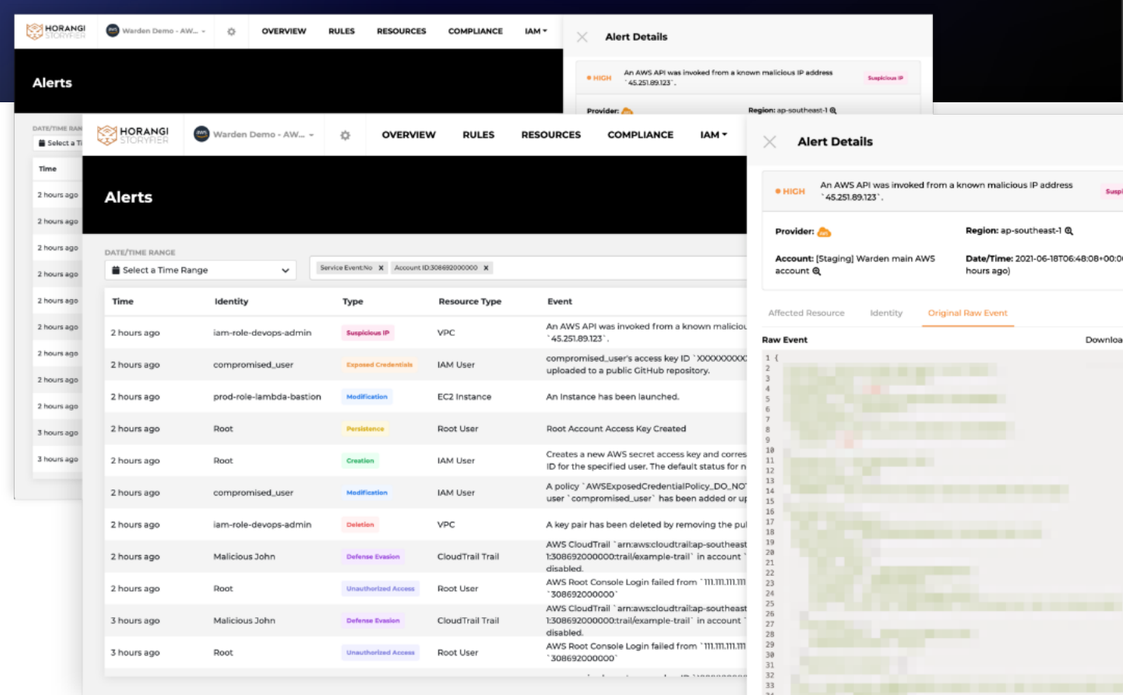
Warden IAM is a cloud-agnostic platform that helps you govern all identities and entitlements to eliminate excessive access and privileges based on actual access patterns and data sensitivity.

Reveal Sensitive Identities

Warden IAM helps you detect backdoor access to your crown jewels by flagging suspicious access behavior such as sensitive data access, privilege escalation, and resource deletion.

Investigate Access Path With Graph Visualization

Besides the basic question “Who has which access rights on what resource?” Warden IAM has powerful access intelligence capabilities to answer “How did a user get his access rights?”. In our Access Intelligence system, you can see complete access rights structure into a single path as a base for visualization.



Vulnerability Remediation

Warden gives you multiple ways to remediate the most critical vulnerabilities. The visibility into the vulnerabilities in your multi-cloud environment provides microscopic clarity into how those vulnerabilities translate into business risk and which are most likely to be targeted by attackers.

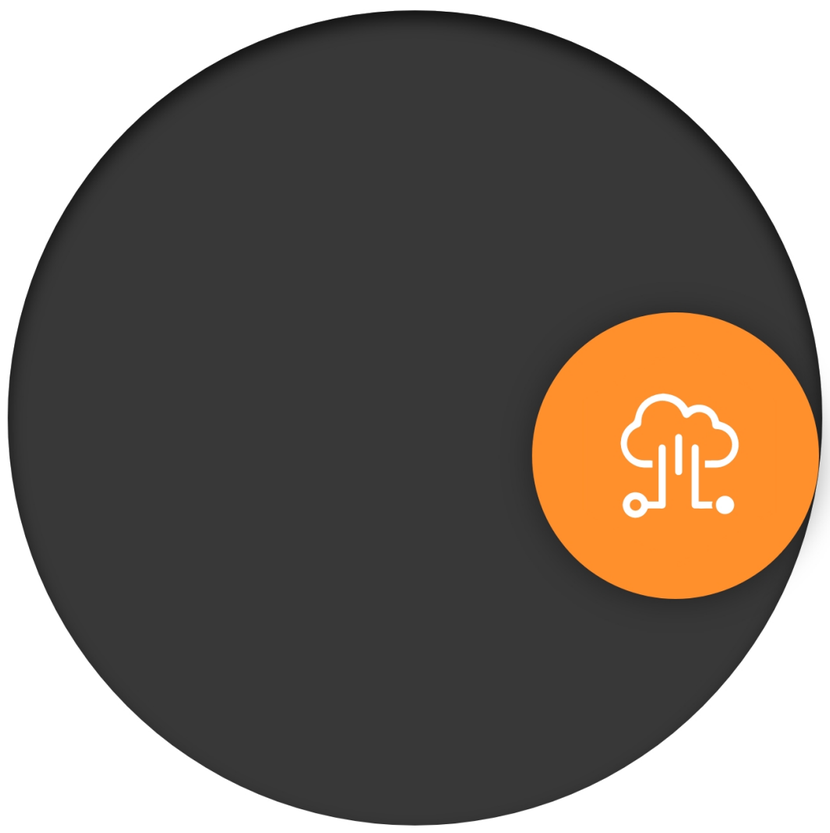
Why Intelligent Vulnerability Remediation Matters

Warden's data-driven platform automatically prioritizes for you the vulnerabilities to fix first, with detailed description of risk and a dashboard to quantify your organization's cloud risk posture.

PRIORITIZE

Single biggest improvement.

- Vulnerabilities you have
- Ones being exploited in the wild



Focus your attention on what **matters the most** with Warden

Remediate With Impact and Confidence

Playbook Remediation

Run a code playbook to remediate an issue rather than having to go through a manual process to do so. This helps you cut down the time spent on fixing issues.

One-Click Remediation

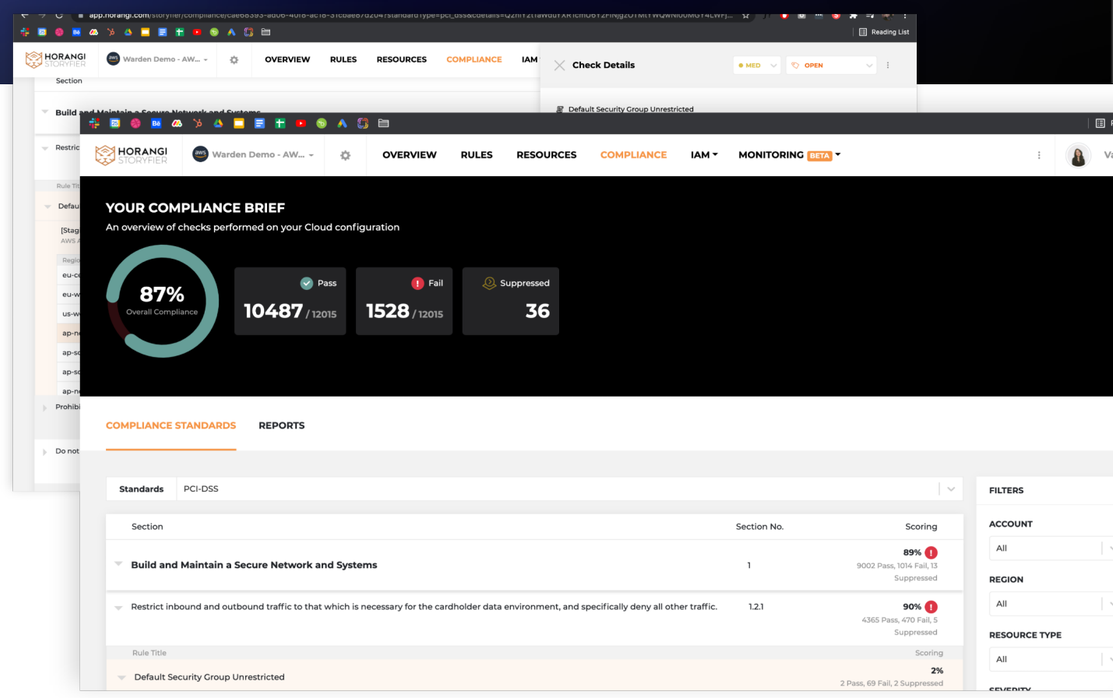
Need more speed? You can remediate findings in bulk with just a single click. All vulnerability findings are supported with descriptions to help you prioritize efficiently.

Terraform Remediation

Built for Terraform users, Warden supports remediation Terraform code snippets for all related rules. Based on the sample code snippet, you can easily make changes on your Terraform templates, fixing vulnerabilities at build time.

Manual Remediation

Be in complete control of what to fix and how to go about it with descriptive findings and hands-on-the wheel approach.



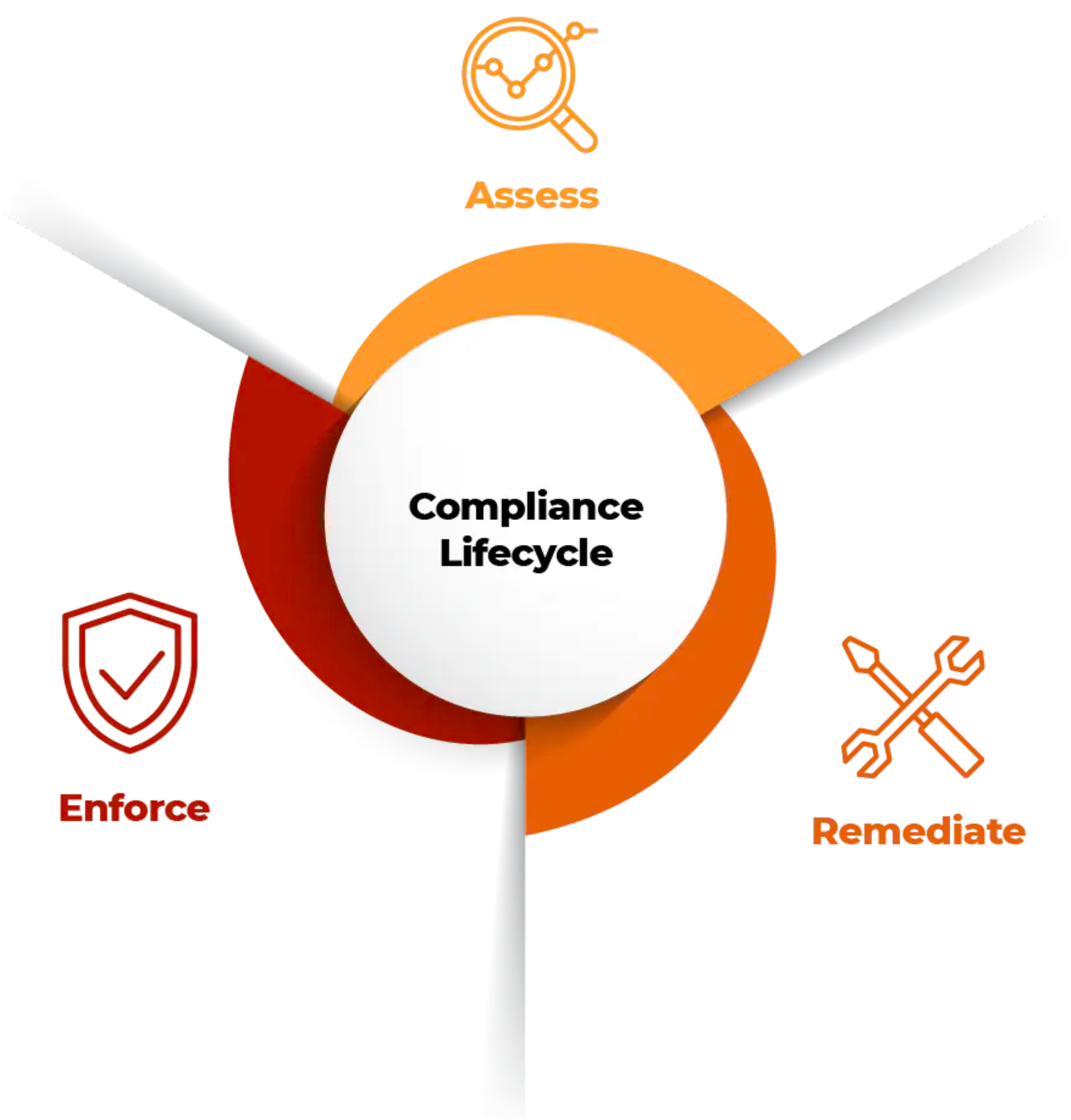
Compliance Automation

Warden offers the fastest path to cloud security and compliance automation for your multi-cloud infrastructure, enabling enterprises to dramatically accelerate cloud deployments and time-to-market. It wraps around your existing or new cloud resources to make you compliant with MAS-TRM, PCI DSS, APRA, GDPR, ISO 27001, SOC 2 and more within minutes of a no-code setup.

Why Compliance Automation Matters

Compliance is never “one and done”. Given the highly dynamic, distributed nature of cloud environments and the fact that the rate of cloud deployments is only accelerating, cloud compliance can be exceedingly complex. Here’s how you can improve your cloud security and automate compliance reporting with Warden.

Warden is a fast, turnkey solution to demonstrate cloud compliance to auditors within minutes of setup. It enables continuous compliance tracking and enforcement to meet the agile needs of cloud native deployments and ensures compliance and governance of workloads.



Warden Compliance Automation Capabilities

Continuous & automated Compliance monitoring

Warden supports a huge breadth of compliance standards, including PCI DSS, APRA, GDPR, SOC 2, ISO 27001, MAS-TRM, with 300+ cloud security rules in place, with custom reporting from your dashboard.

Instant Correction Of Compliance Violations

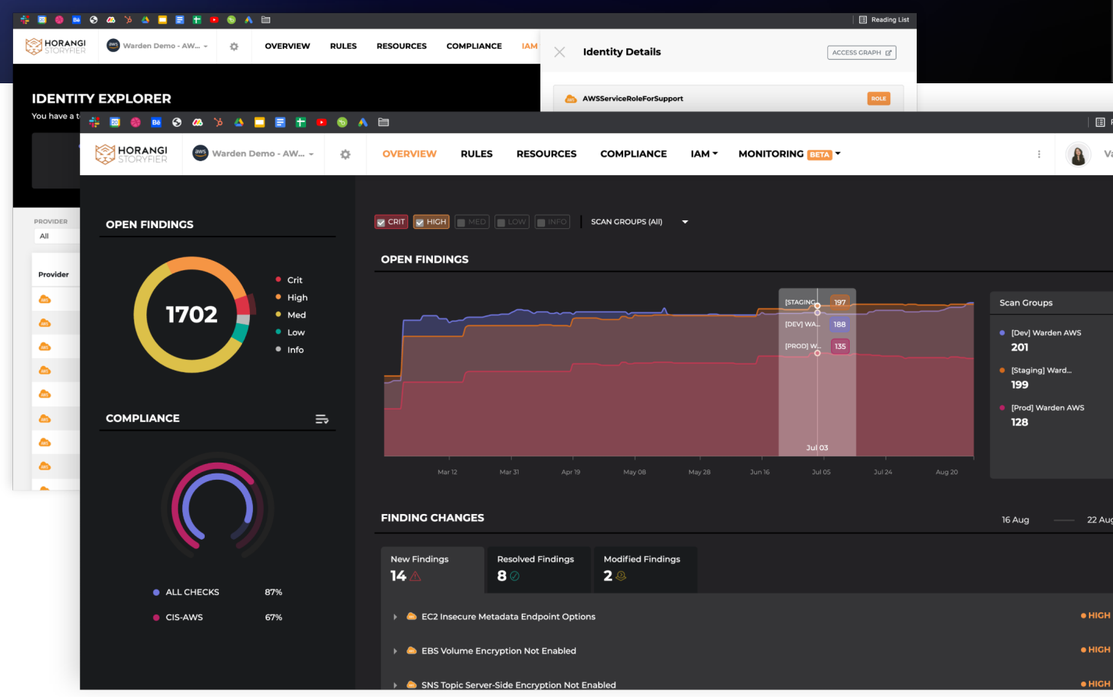
Warden's automated playbook and one-click remediation shortens your time to compliance by tackling multiple compliance violations simultaneously.

Rich And Interactive Dashboard

Take advantage of out-of-the-box support for global and regional compliance standards on a rich interactive dashboard, enabling even the most resource-constrained security teams to easily manage and enforce compliance across multi-cloud environments.

Prioritize With One-Click Audit Reporting

Generate audit-ready custom reports against any compliance standard in a single click. Understand the root cause with granular details and identify the specific violating resources and provide the necessary guidance to correct specific compliance issues.



Cloud Posture Management

Reduce the complexity of securing and managing compliance for multi-cloud environments with comprehensive visibility and continuous monitoring of new and existing assets and threats.

Warden is Asia's first one-click, all-in-one solution to bring automation, speed, and scale to cloud security, enabling enterprises to innovate in the cloud at the speed of DevOps.

Why Is Cloud Posture Management Needed?

Cloud Data Breaches On The Rise

Through 2025, 99% of cloud security failures will be the customer's fault. A single misconfiguration can expose hundreds or thousands of systems or highly sensitive data to the internet.

Achieving Cloud Security At The Speed Of Cloud Innovation

Without security automation and robust reporting capabilities, users in multi-cloud environments can find it time-consuming to manage the separate native tools available to maintain a year-round compliant posture, regardless of the team size.

Lack of Visibility Can Create Blind Spots

Gaining deep visibility into all your cloud resources as well as entitlements and user permissions adds the level of depth required for high-fidelity alerts and a clear understanding of risk. While native tools do offer some protection, it might not be enough, depending on the complexity of your infrastructure setup.

Warden Compliance Automation Capabilities

Unparalleled Visibility, Compliance, & Governance

Gain continuous visibility across all cloud resources from a single console. Within minutes of setup, you can enforce configuration guardrails with 300+ policies to automatically fix misconfigurations before they lead to security incidents. Get continuous compliance posture monitoring and one-click remediation (MAS-TRM, GDPR, ISO-27001, PCI-DSS, SOC 2, etc.) to easily investigate and remediate compliance violations.

Control Entitlements & Permissions On A Unified Dashboard

Get full visibility of your multi-cloud IAM without opening multiple windows, cloud provider consoles, or any dependency on team members. You can also analyze all access policies, human and machine identities with a flattened view of entitlements, from a single dashboard. With real-time Dynamic Scans and Graph Visualization, enforcing least privilege will become easier than before.

Prioritize And Remediate Vulnerabilities In Your Cloud Stack

Warden helps you prioritize the most critical vulnerabilities based on a risk score, enabling teams to address those that are most crucial. It also delivers quick and easy remediation, integrating seamlessly into your existing Security and DevOps workflow.

Real-time Threat Detection Based on MITRE ATT&CK Framework

On average, it takes about 280 days for incident responders to detect and contain a breach. With Warden's comprehensive cloud security coverage you can instantly identify and zoom in on a suspected asset and understand the full context from both a configuration and activity perspective with associated event severity, thereby reducing your meantime (and money) to detecting, investigating, and remediating threats.