SOLUTION BRIEF

Mitigating Cloud Security & Compliance Risks with VMware Secure State

CloudHealth by vmware

Reducing misconfigurations, monitoring malicious activity, and preventing unauthorized access are foundational activities necessary to ensure security and compliance of applications and data in the cloud. As criminals become more sophisticated in their abilities to exploit cloud misconfiguration vulnerabilities, security teams need a smarter approach to prevent security breaches.

VMware Secure State is an intelligent cloud security and compliance monitoring platform that helps organizations reduce risk and protect millions of cloud resources by remediating security violations and scaling best practices at cloud speed.

MULTICLOUD SECURITY

Build a unified approach for managing risks across clouds

DEEPER INSIGHTS

Graphically visualize resources, relationships, and risks

AUTOMATED RESPONSE

Automate reports, alerts, and remediation of violations

REAL-TIME DETECTION

Detect security events and violations within minutes

RISK PRIORITIZATION

Focus on resources with maximum security exposure

TEAM COLLABORATION

Enable security, operations, and developer teams

According to Gartner, through 2025, 99% of cloud security failures will be the customer's fault and 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.[1]

[1] Smarter With Gartner, Is The Cloud Secure?, October 10, 2019, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

How VMware Secure State Works

Foundational to VMware Secure State is an Interconnected Cloud Security Model, an intermediate data layer that leverages cloud APIs, change events, and native threat data that help security teams visualize resource misconfigurations, connections, and their associated risks. As objects, data, and relationships change, the service intelligently updates the model in near real-time to correlate direct and indirect risks of each change.

Delivered as a Service, VMware Secure State is easy to onboard and provides support for both pre-defined and custom security and compliance policies. Once configured, VMware Secure State helps security prioritize violations, visualize context, report issues, and plan actions necessary to remediate risks.

Who can benefit from VMware Secure State?

Cloud Security Architects

Security Operations

Governance, Risk, and Compliance

Vulnerability Management

Cloud Operations Engineer

DevOps Engineers

In cloud, security is a shared responsibility between a cloud provider and a customer's security and application teams. VMware Secure State helps organizations operationalize security by supporting multiple cloud providers and enabling security administrators to distribute insights across application owners at real-time speed. With easy access to security findings and actions via API, application owners can proactively verify configurations at the time of deployment and minimize the cost associated with implementing security policies.

Key Use Cases

Posture Management

Improve cloud security posture with real-time visibility into resource relationships, misconfigurations, risk scores, and change activity

Continuous Compliance

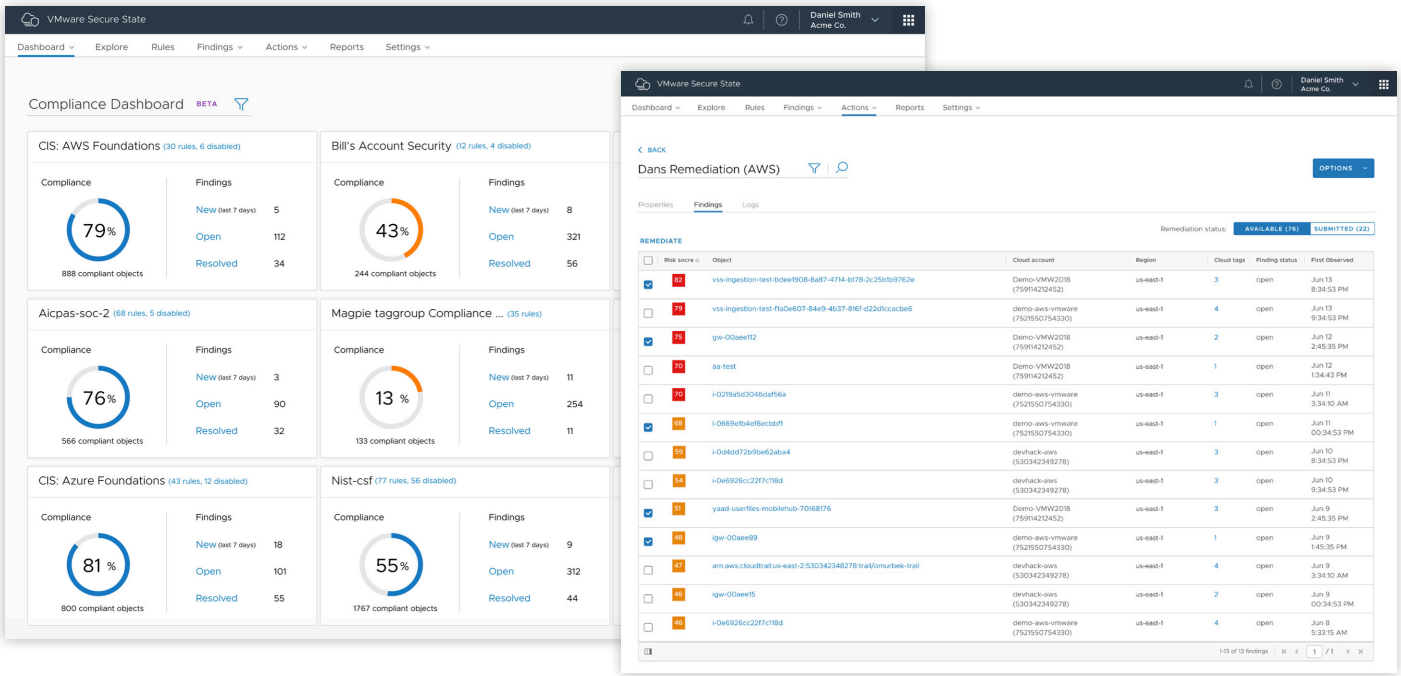
Continuously assess and improve compliance with support for a range of compliance frameworks including CIS, NIST, GDPR, SOC 2, PCI, and HIPAA

Threat Correlation

Correlate events from cloud native threat feeds with resource misconfigurations to monitor suspicious activities, run investigations, and respond quickly

DevSecOps / Shift Left

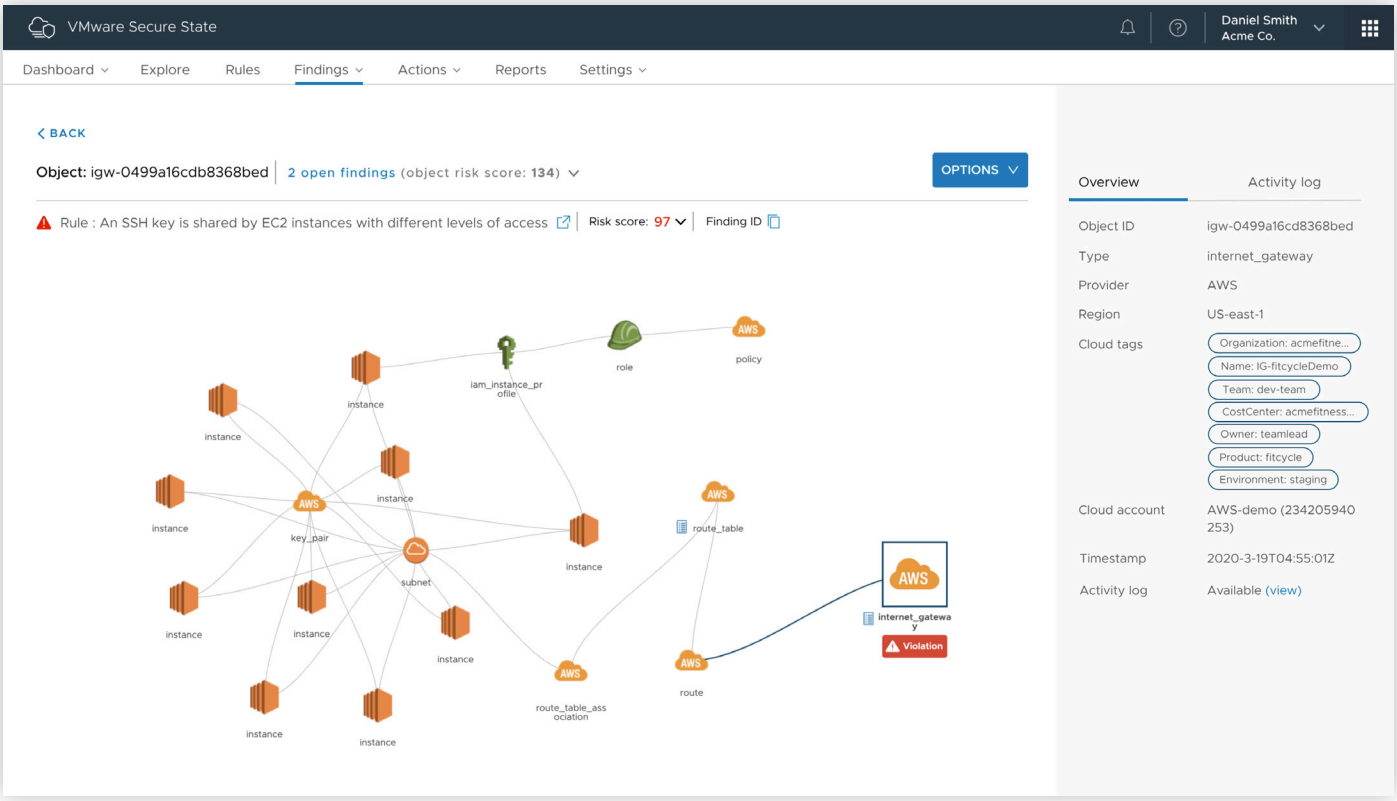
Proactively verify configurations as a part of CI/CD pipeline, notify developers on violations, and build guardrails to scale security



> ***"VMware Secure State enables us to visualize risk with a graph view, so that we can easily convey the impact of changes to key stakeholders – for example, we can show that something is not just affecting a server but also certain databases that are connected to it."***

KOLBY ALLEN
Platform Operations Architect | zipwhip

Key Features



Features	Benefits
Graph Context	Visualize misconfigurations and threats in context with resource relationships, metadata, and change activity
Risk Scores	Prioritize violations by understanding blast radius and severity based on quantified risk
Resolved Violations	Audit changes and track progress developers are making by resolving violations across cloud accounts
Suppressions	Allow exceptions to security policies and white list cloud environments to eliminate false positives
Explore	Search inventory and visually navigate cloud topology to investigate risks
In-Account Remediation	Remediate misconfigurations without elevating write privileges to VMware Secure State SaaS application

Key Integrations and APIs

Integrations	Benefits
Splunk	Enable security operations teams to detect and report on cloud misconfigurations and threats in Splunk App
AWS GuardDuty	Detect and correlate GuardDuty alerts with misconfigurations and object relationship context
Slack	Detect and correlate GuardDuty alerts with misconfigurations and object relationship context
Amazon SQS	Automatically notify developers on security violations and remediation actions
Findings API	Query, filter and aggregate findings data such as violations, events, and anomalies across your cloud accounts
Entity Data API	Search, filter, and aggregate cloud inventory data to gather deeper insights about your cloud environment
Rules API	Explore details about security controls and compliance frameworks in place for internal reporting

Want to learn more?

With VMware Secure State's real-time detection and remediation capabilities, you can proactively mitigate risks across cloud environments. To talk to an expert on cloud security and compliance best practices, or request a free VMware Secure State trial, visit https://go.cloudhealthtech.com/vmware-secure-state