CloudHealth by vmware

VMware Secure State Interconnected Cloud Security

THE CHALLENGE

Public cloud has fundamentally changed the way organizations build applications.

Security in the cloud is composed of hundreds of configuration parameters. Ensuring proper configuration, monitoring malicious activity, and preventing unauthorized access is essential to protecting applications and data stored in public clouds.

However, correlating risk across misconfigurations and threats in a rapidly changing, dynamic cloud environment is a real challenge for teams. Solutions that periodically scan cloud accounts to validate the configuration of an object without the context of its surroundings can overlook serious vulnerabilities, generate false positives, and create usage conflicts due to excessive API calls to your cloud infrastructure.

"Through 2020, at least 95% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities"

Gartner, Clouds Are Secure: Are You Using Them Securely?, Jay Heiser, 31 January 2018

INTERCONNECTED CLOUD SECURITY

VMware Secure State is an intelligent cloud security solution that helps organizations minimize security risk and proactively mitigate threats across AWS and Azure. VMware Secure State helps customers build an interconnected cloud services model (ICSM), enabling users to explore and understand relationships between cloud objects.

With VMware Secure State's smart, real-time security approach, users can leverage machine learning algorithms to detect critical misconfigurations, violation chains across objects, and anomalies that elevate the risk of a security breach. The service then correlates these security findings with activity logs and delivers instant alerts on security violations to service owners with investigation context, visual graphs of interconnected objects, and recommended solutions.

Delivered as a service, VMware Secure State helps organizations automatically remediate cloud misconfigurations and build security guardrails that help developers innovate across multiple clouds without compromising on agility or security risk.

WANT TO LEARN MORE?

We would love to demo you our solution in action. In the demo, we'll walk you through our rich feature set and how you can improve your cloud security posture with simple steps. Visit us online at **go.cloudhealthtech.com/vmware-secure-state** to schedule a demo.

EXPLORE RELATIONSHIPS

You can't protect what you can't see. Secure State provides greater insight, so you understand not just what assets you have across different accounts, regions, and clouds, but also explore how these are interconnected. Visualize how a minor change in the configuration of an object can elevate the security risk of all adjacent objects, and how you can use custom queries to investigate and improve cloud visibility.

CORRELATE RISK

In security, ignorance isn't bliss. With Secure State, you do more than just basic API queries and use machine learning to gain a deeper insight into your most critical violations, such as violation chains across objects and anomalies. Correlate findings with user activity and environment context to protect your cloud accounts and workloads from external threats.

AUTOMATE ACTIONS

With Secure State, you proactively mitigate threats by detecting misconfigurations and malicious activity within seconds. Collaborate with development teams to isolate critical assets and security checks. Send instant alerts on security violations with resolutions on how to fix issues to proper service owners. Build security guardrails to automatically remediate violations and maintain your cloud's security posture.