Trellix

DATA SHEET

Trellix Cloudvisory

A command center for cloud security management

Highlights

- Gives security teams unified control over cloud sprawl and infrastructure misconfiguration with cloud-native microsegmentation
- Integrates detection and response for cloud environments (AWS, Azure, Google Cloud, Kubernetes, OpenStack, traditional virtualized, bare metal)
- Automates the collection, processing, and primary analysis of security events from workloads and cloud services across multiple cloud accounts and providers
- Certified by CIS, GDPR, HIPAA, NIST, PCI, and OpenStack Security Checklist
- Leverages 1,800-plus built-in security compliance checks to maintain a robust security posture 24/7

Overview

While cloud usage and adoption are on the upswing, most enterprises still need to manage complex multicloud environments. Monitoring and managing these distributed, dynamic ecosystems become easier if a single consistent interface can help control all assets across all cloud environments.

Trellix Cloudvisory is your command center for managing any cloud environment. It's a cloud security management cloud solution that delivers visibility, compliance, and governance for your infrastructure. It runs cloud-native microservices for asset discovery and compliance scanning to enable end-to-end automation of detection and response for complex multicloud environments. With Cloudvisory, you can take complete control of your cloud security.

Global cloud revenue is projected to reach $474 billion in 2022, which makes sense because cloud allows organizations to collaborate more, access data better, and access more applications.[1] But for many organizations, this is also a cause of concern. As more data and applications move to the cloud, what happens to data security, governance, and compliance? It's understandable to worry about business information or intellectual property being exposed because of accidental or planned leaks or due to sophisticated cyberthreats. And the situation gets further compounded when we consider multicloud environments, which are evolving ecosystems.

1. Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences, Gartner, 2021

Key benefits

- **Terraform APIs:** Help identify and address vulnerabilities and misconfigurations early in the process before they impact infrastructure
- **No misconfigurations:** Runs continual assessments to ensure that processes are secure and don't drift from the original configurations
- **Asset inventory inspector:** Helps drill down to a granular level on a per-asset basis to shape them further
- **IAM Policy inspector:** Helps with forensic investigation by mapping user and resource access for IAM policies
- **Compliance check inspector:** Delivers GDPR, HIPPA, NIST, PCI, S3 bucket fixes
- **Cloud surface landscape visibility:** Delivers a comprehensive view and recommendations on probable threat vectors
- **Playbooks:** Offers cloud-native remediations with customizable workflows and playbooks for business processes

This is where Cloudvisory can make a difference for you. It's a centralized command center for managing multicloud environments and workloads. Its API integrations with multiple cloud providers can be leveraged to automatically discover cloud assets and their associated risks. An agentless approach helps simplify different types of workload deployments in data center, public cloud, and private cloud environments—including workload-centric security protections for bare metal servers, orchestrated containers, serverless functions, and virtual machines.

Cloudvisory is designed to leverage a cloud provider's existing cloud-native security controls to enforce workload microsegmentation, define security controls, and deliver services. By using cloud-native APIs, you can eliminate misconfigurations and minimize the overhead associated with managing least-privilege polices at scale.

Cloudvisory brings together the Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) features in a single cloud security framework for public- and private-cloud environments. By merging and correlating CSPM and CWPP data, it provides a consolidated management interface for clouds and workloads—delivering considerable benefits to security operations teams.

Centralized visibility

Cloudvisory provides a single pane-of-glass view for monitoring, managing, and controlling complex multicloud environments. It delivers centralized visibility into assets, workloads, and associated security controls across your organization's cloud infrastructure so you can fully understand your cloud landscape.

With ad-hoc security audits, you can get insights into actual operational, administrative, security, and performance controls. You'll know if offerings from cloud vendors are delivered with the appropriate attention to specific controls and if they're adhering to best practices and appropriate standards. Continuous cloud security analytics help you drive proactive security incident detection and response to detect threats in real time and get insights into incidents, their impacts, and timelines. Network flow visualizations help with network monitoring and analysis, visually charting the data path through network devices and metrics.

Continuous compliance

Cloudvisory ensures that compliance requirements are adhered to while deploying components. It extends your compliance framework to remediate any compliance failures without the need for extra deployment components such as agents, appliances, and functions. With compliance guardrails, you can ensure limits on cloud self-service and detect policy violations.

With risk analysis and remediation, you can identify the most important cloud assets across your environment, with an overview of threats, associated risks, and mitigation measures to be taken should an attack occur. Cloud vulnerability management also supports compliance by charting a map of all cloud assets, then naming, evaluating, and treating them and reporting on security vulnerabilities. When combined with other security measures, it will help you prioritize probable threats and minimize their attack surface.

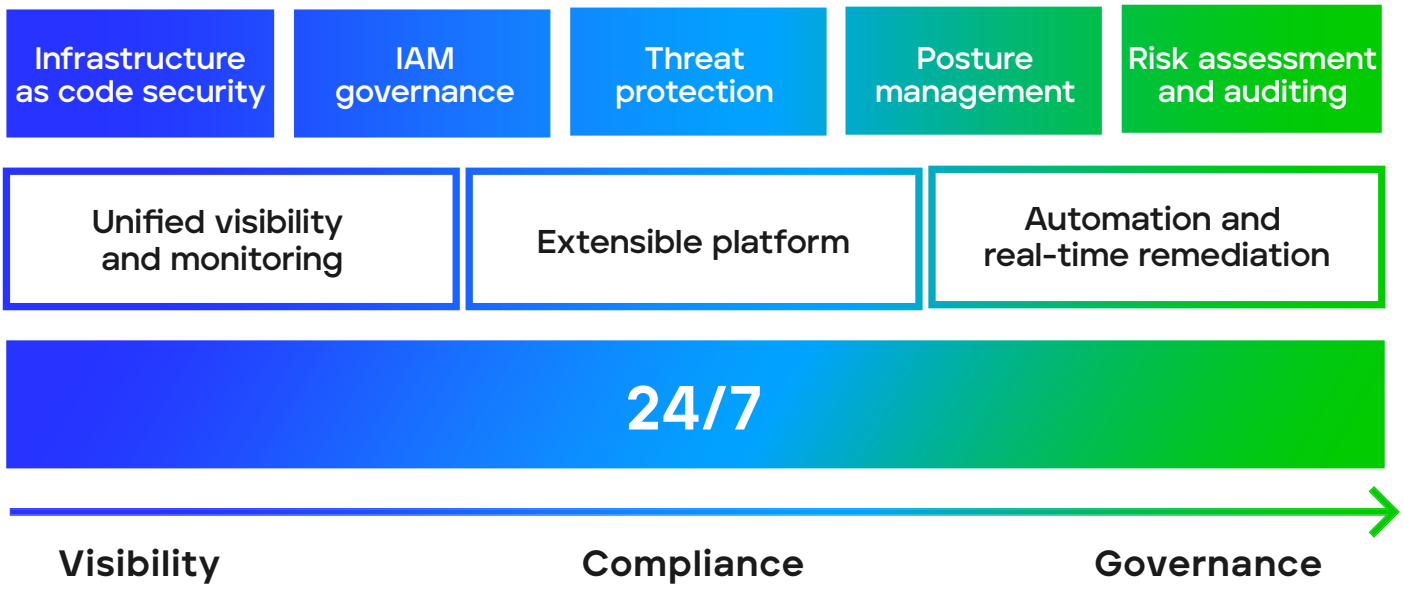

Figure 1. Cloudvisory delivers always-on visibility, compliance, and governance over your cloud environments

In-line governance

Cloudvisory's baseline is to keep your cloud security posture intact. To do this, it enforces end-to-end threat detection and response using machine learning to intelligently detect anomalies within any cloud environment.

It also blocks and quarantines attacks using intelligent microsegmentation by creating granular blocks within the cloud infrastructure so you can limit the size and impact of an attack surface. If any block gets compromised, all remaining blocks are sealed and protected. By managing policies centrally, Cloudvisory ensures that all cloud assets are in line with your organization's security parameters. And by automating policies, it ensures your routine tasks are taken care of without any compromise in your security posture.

Learn more about Trellix Cloudvisory at trellix.com.

Awards and recognition

2021 Cybersecurity Excellence Awards Cloud Security

Cloudvisory recognized by CIO Applications in top 25 Amazon Solution Providers

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com