Guide

Cloud Workload Protection Platforms (CWPP): Everything You Need to Know in 10 Pages

uptycs

Table of Contents

© 2024 All Rights Reserved

01 What is CWPP?

Organizations are accelerating their migrations to the cloud while continuing to use on-premises systems. This cloud/on-prem mix offers significant flexibility and scalability, but it also complicates protecting an organization's shifting attack surface.

Traditional tools developed for securing on-premises workloads, such as heavyweight agents, are often ineffective in the cloud. Cloud-native workflows demand earlier detection of vulnerabilities, malware, and misconfigurations—preferably during development—to prevent risks from escalating into production environments.

These challenges have driven a rethinking of workload visibility and security. A cloud workload protection platform (CWPP) has emerged as a solution for securing systems across hybrid and multi-cloud environments. According to Gartner, a CWPP is a workload-centric security tool that addresses the "unique protection requirements of server workloads in modern hybrid, multi-cloud data center architectures."

CWPP solutions provide visibility and protection for physical and virtual machines (VMs), containers, and serverless workloads across any environment. They typically employ a combination of network segmentation, system integrity protection, application control, behavioral monitoring, host-based intrusion prevention, and anti-malware scanning.

CWPP takes on the role of a guardian for workloads, "regardless of location" (Gartner). With the ability to combine machine learning, behavioral analysis, and automated defenses, CWPP continuously monitors workloads to detect and mitigate emerging threats before they cause real damage.

© 2024 All Rights Reserved | Uptycs | www.uptycs.com

02 What Does a CWPP Do?

CWPPs deliver unified protection for workloads across on premises, cloud, and hybrid environments. They:

- **Scan workloads** to identify vulnerabilities, misconfigurations, and malware.
- **Detect threats** using machine learning and behavioral analysis to spot anomalies in real-time.
- **Automate responses** by activating playbooks to neutralize threats instantly.
- **Enforce security policies** across development, staging, and production environments.

CWPP provides cybersecurity professionals with a single, centralized vantage point for managing their technology estate, eliminating the need to switch context between tools.

© 2024 All Rights Reserved

03 Layers of CWPP Controls

CWPP solutions integrate multiple layers of controls to deliver comprehensive workload protection. According to Gartner, these layers include:

Hardening, Configuration, and Vulnerability Management

- The foundational layer for cloud workload protection platforms. CWPP scans workloads for vulnerabilities and prioritizes them based on severity, exploitability, and asset importance, helping organizations address the greatest risks first.

Network Firewalling, Visibility, and Microsegmentation

- CWPP tools secure workloads through segmentation of network communications, east-west traffic monitoring, and encryption of network traffic. This layer helps prevent lateral movement of threats within virtual private clouds (VPCs).

System Integrity Assurance

- CWPP continuously monitors workload integrity during pre-boot and post-boot phases, ensuring that critical files, configurations, and registries remain secure.

Application Control and Allowlisting

- By adopting a default-deny posture, CWPP blocks unauthorized executables, preventing malware execution and ensuring compliance with security policies.

Exploitation Prevention and Memory Protection

- CWPP integrates with operating system features or additional functionality to prevent exploits of known vulnerabilities, especially in allowlisted applications.

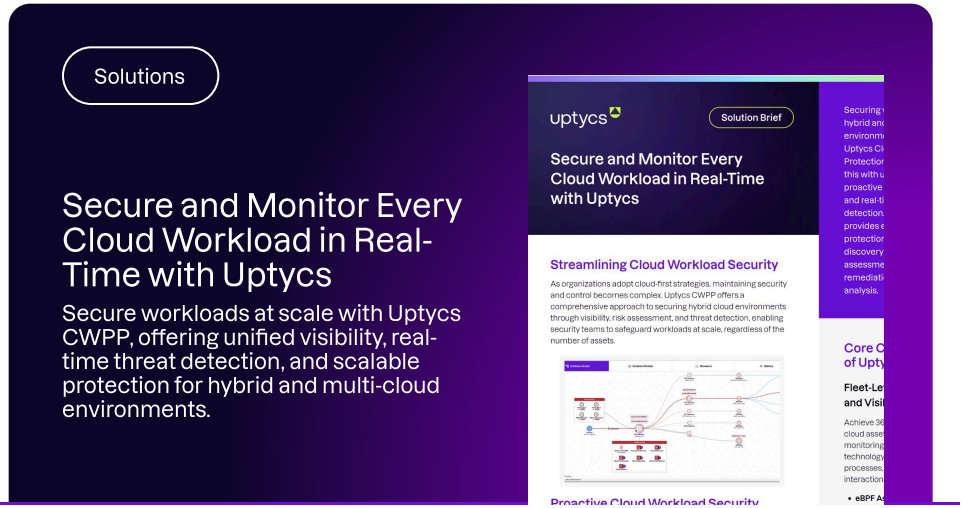
Runtime Protection and Behavioral MonitoringAt its core, runtime protection enables

- At its core, runtime protection enables CWPP to detect and neutralize threats in real time, providing defenses against advanced attacks like fileless malware, crypto-miners, and container escapes. Behavioral monitoring identifies unusual patterns, such as overprivileged user activity or unexpected service interactions, and raises alerts for immediate action.

© 2024 All Rights Reserved

Server Workload EDR, Threat Detection, and Anti-Malware Scanning

- CWPP's EDR capabilities monitor processes, file activity, and network traffic to detect malicious behaviors across workloads. In addition, CWPP enables vulnerability shielding and optional anti-malware scanning to comply with regulatory requirements.



04 The Benefits of Having a CWPP

CWPP solutions provide numerous benefits to organizations aiming to secure hybrid and multi-cloud environments. These include:

- **Shared Responsibility Support:** CWPP helps bridge gaps in the shared responsibility model by protecting workloads from attacks that bypass cloud vendor defenses.
- **Unified Visibility:** CWPP consolidates visibility across cloud, hybrid, and on-prem workloads, reducing blind spots that attackers may exploit.
- **Proactive Threat Mitigation:** With real-time detection and response, CWPP ensures incidents are addressed immediately, minimizing potential damage.
- **Cost Efficiency:** Lower upfront costs, reduced hardware dependencies, and minimized operational overheads contribute to improved resource utilization and scalability.

© 2024 All Rights Reserved

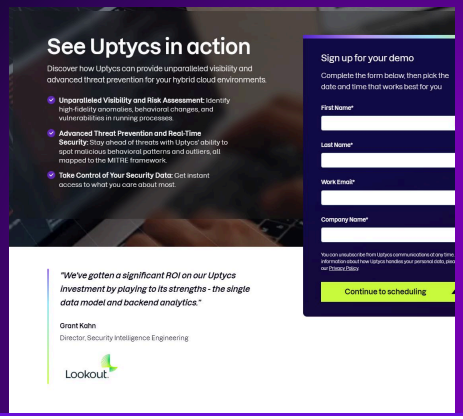
- **Compliance Assurance:** Continuous compliance assessments safeguard sensitive data and streamline reporting across regulatory frameworks.

By addressing these needs, CWPP tools improve overall security posture, enhance operational efficiency, and ensure compliance with regulatory requirements.

Demo

See Uptycs in action

Find and remove critical risks in your modern attack surface - cloud, containers, and endpoints - all from a single UI and data model. Let our team of experts show you how.



05 CWPP Implementation Steps

To implement an effective cloud workload protection program, Gartner recommends that security and risk management leaders take the following steps:

- **Design for Visibility and Control:** Architect solutions that provide continuous visibility and control over workloads, regardless of their location or size.
- **Adopt Zero-Trust Security Principles:** Use execution models like default-deny and runtime behavioral monitoring to eliminate unnecessary risk.
- **Integrate with DevSecOps Pipelines:** Embed security into CI/CD workflows to protect workloads during development and runtime.
- **Require API-Driven Functionality:** Enable automation through robust API integrations to streamline security operations.
- **Support Agentless Scenarios:** Account for runtime environments where deploying CWPP agents is impractical, enabling scalable, lightweight protection.

© 2024 All Rights Reserved

06 The Future of CWPP – and the Links to CSPM & CNAPPs

As cloud environments grow increasingly complex, the future of CWPP lies in its integration with other cloud security tools. For example, CWPP works alongside:

- **Cloud Security Posture Management (CSPM):** Ensuring workloads are securely configured.
- **Cloud Infrastructure Entitlement Management (CIEM):** Managing permissions at scale.

Together, CWPP, CSPM, and CIEM converge into cloud-native application protection platforms (CNAPP), enabling end-to-end security for modern cloud infrastructures. CNAPP simplifies the security stack by unifying threat detection, workload monitoring, and policy enforcement across dynamic, multi-cloud environments.

CWPP remains a cornerstone of this approach, providing essential tools for visibility, proactive detection, and workload protection—a vital step for securing today's evolving cloud workloads.

© 2024 All Rights Reserved

07 Learn more about cloud security and CWPP:

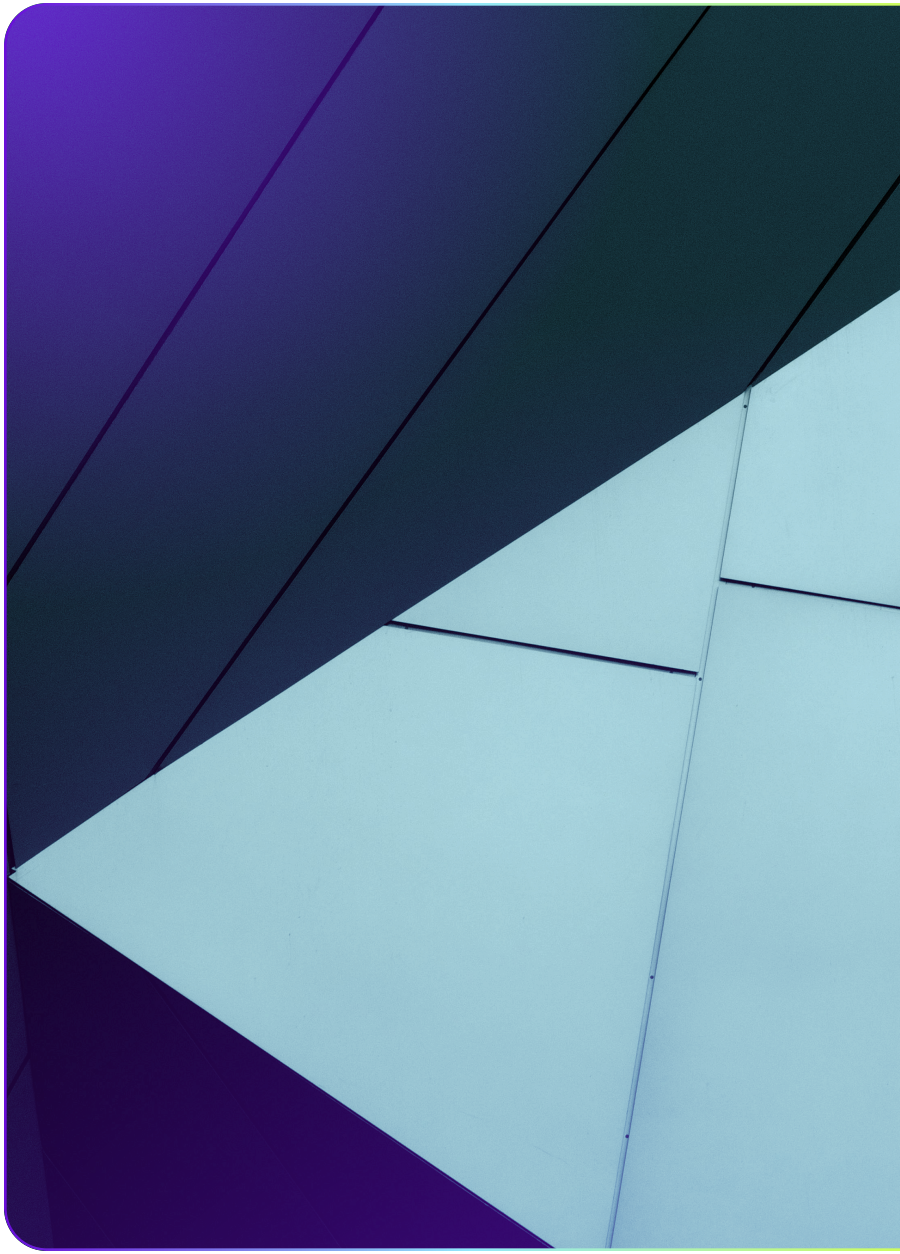
- Cloud Workload Security: What You Need to Know **(Cloud Security Alliance)**
- Cloud workload protection platform security benefits, features **(TechTarget)**
- Cloud Native Security White paper **(Cloud Native Computing Foundation)**

Read more about Cloud Security and Best Practices.

Guide

Cloud Security Fundamentals

10 questions to guide your strategy and secure your attack surface



© 2024 All Rights Reserved

Uptycs is dedicated to leading security innovations in hybrid cloud environments, ensuring robust protection and enabling our customers to innovate safely and efficiently. Included in the 2024 CNAPP Market Guide, Uptycs provides comprehensive security solutions that bridge the gap from code to cloud. Our platform excels in Cloud Workload Protection (CWPP), Vulnerability Management, Cloud Security Posture Management (CSPM), Detection & Response, Software Pipeline Security, XDR, and Risk & Compliance. Trusted by leading enterprises like PayPal and Comcast, Uptycs transforms potential vulnerabilities into fortified security, ensuring your digital environments are safeguarded from development through runtime.

Secure Everything from Dev to Runtime

Learn more at Uptycs.com