uptycs

DATA SHEET

CNAPP for Hybrid Cloud

On Guard. On Cloud. On Loop.

Traditional posture management is a valuable step, but it's only the beginning. A Unified Cloud Security solution requires real-time response, moving beyond risk prioritization to real-time protection and prevention.

Uptycs CNAPP empowers enterprises with our “On Guard, On Cloud, On Loop” approach. By blending insights and signals from runtime, cloud control plane, identities, and application-level activity across the software development pipeline, we surpass traditional agentless and image scanning methods. This enables us to detect, protect, and prevent real-time threats, vulnerabilities, and risks in your hybrid cloud environment.

Operationalize fixes and prevention policies at cloud speed, from build time to runtime, with best-in-class integrations, exception management, and customizable rules and policies. With Uptycs, your hybrid cloud security is always on guard, on loop, and forever protecting every workload.

Unified Risk Prioritization and Prevention Across Your Hybrid Cloud

Uptycs empowers teams with a single data model that unifies security insights from runtime workloads, identities, cloud infrastructure, Kubernetes, and your software development pipeline. This comprehensive view enables you to prioritize risk and prevent malicious threats across every layer of your cloud security journey, from build time to runtime.

Discover & Monitor

Inventory Assets from Pipeline to Runtime

See with context everything you build and deploy in the cloud from pipeline to runtime.

Detect & Respond

Unify Risk Management and Remediation

Focus on the threats and risks that matter with insights that correlate runtime and historical data in real time.

Prevent & Harden

Strengthen Posture & Compliance Guardrails

Fortify your security and compliance posture with preventative guardrails.

Why Uptycs?

Uptycs is rewriting the rules of cloud security, merging cutting-edge CNAPP technology with unparalleled flexibility to safeguard your cloud on loop.

Unparalleled Scalability

Grow without limits. Embrace the cloud's expanse as Uptycs scales with you, from hundreds to millions of workloads, ensuring your journey is secure at every step.

Deep Visibility Into Every Asset

Uptycs collects real-time telemetry via eBPF from every attack surface across your hybrid cloud fleet from processes to network/file activity, and even software catalog and packages. This telemetry is stored continuously for historical lookups, providing complete visibility for compliance audits, threat hunting, and continuous risk prioritization.

Go Beyond Real-Time Threat Detection

Stay ahead of threats. Uptycs spots malicious behavioral patterns and outliers in your environment all mapped to the MITRE framework to protect against modern threats. We go beyond detection by enabling you to attribute and establish provenance to code level activity for faster root cause analysis.

Powerful Response and Prevention Actions

With Uptycs Protect, stop malicious threats such as cryptominers and malware proactively across millions of workloads. Prevent malicious artifacts from being deployed into your runtime. Create bulk remediation policies for fleet level management.

Insightful Forensics

Forensics made simple. Uptycs combines real time and historical data to transform complex investigations into clear insights, enabling you to understand and explain security outcomes.

Customized for Your Cloud

Your cloud, your rules. With broad hybrid and multi-cloud support, Uptycs' customizable platform means your security fits your needs perfectly, as unique and dynamic as your cloud environment.

Benefits

Unified Security
Uptycs consolidates cloud security into a single platform, eliminating complex integrations and simplifying operations.

Always-on Protection
A continuous security loop ensures comprehensive threat detection, response, and prevention across your hybrid and multi-cloud environment.

Scalable Safeguards
Uptycs seamlessly adapts to your needs with robust scalability, versatile workload security, and integrated software pipeline protection, ensuring your cloud security grows with your business.

Uses Cases

Workload Protection

- **Versatile Workload Security:** Uptycs protects a broad variety of technologies, including container runtimes, self-managed platforms, managed container orchestration services, and serverless technologies.
- **Uptycs Sensor or Agentless Scans:** Start with instant agentless coverage for cloud and container security, then add the Uptycs Sensor for deeper telemetry, enhanced runtime protection, and quicker remediation.
- **Rich Security Telemetry:** That goes beyond basic events to include file system files, Augeas lenses, 4NS lookups, sudoers lists, and disk encryption.

Posture Management

- **Identify Access Monitoring:** Continuous monitoring secures cloud resources by detecting unauthorized access, preventing misuse, identifying permission gaps, and enforcing least privilege access.
- **Customizable Checks:** Create your own checks to address unique security needs in your development lifecycle and cloud environment, ensuring comprehensive coverage.
- **Streamlined Remediation:** Get notified of issues through integrations with third-party tools and receive guided remediation steps to ensure best practices are followed across development and cloud environments.

Detection & Response

- **Threat Detection Correlation:** Utilize real-time threat detections that map data plane threat information to the MITRE ATT&CK framework, correlating threats with vulnerabilities, environmental context, and cloud infrastructure misconfigurations.
- **Attack Path Visualization:** Secure cloud workloads with full attack path visibility across hosts, VMs, containers, Kubernetes clusters, and serverless functions.
- **Security Graph:** Combine data from diverse sources, like host/container vulnerabilities and open ports.
- **Remediation Actions:** Perform real-time actions, such as quarantining a host, killing or pausing processes, managing user accounts, and executing scripts, either manually or through automated processes.

Asset Management

- **Instant Discovery:** Identify cloud assets in real-time without the use of a sensor, ensuring an up-to date inventory of both ephemeral and persistent cloud assets.

Risk & Compliance Management

- **Cross-Cloud Compliance:** Map multiple compliance standards to a single policy across clouds and provide customization for specific security objectives. Utilize industry best practices, such as the AWS Well-Architected Framework and NIST-based hardening checks to improve security posture.
- **Out-of-box Compliance Support:** Customizable template support for CIS benchmarks, HIPAA, ISO 27001, NIST, PCI, and SOC 2 ensure compliance within cloud infrastructure and workloads.
- **Risk Prioritization:** Prioritize security findings across your hybrid cloud workloads (VMs, containers, clusters, and serverless), and cloud infrastructure (databases, data stores, object storage) through exposure scanning, full attack path analysis, and correlation of security signals.
- **Audit Efficiency:** Uptycs simplifies audits with 13 months of historical data readily available and Ask Uptycs for easy querying of both real-time and historical information.

Vulnerability Management

- **Unified Visibility:** A single, intuitive dashboard offers a centralized view of vulnerabilities across your entire environment, including applications, systems, and cloud workloads.
- **Alert Prioritization:** Uptycs Smart Indicators prioritize vulnerabilities based on factors such as the presence of malware and secrets, CVSS scores, EPSS scores, the asset's significance as a business critical resource, and more.
- **Metrics Reporting:** Track key performance metrics, such as average close time and scan coverage, to continuously monitor and improve vulnerability management and support audit reporting.
- **Exception Management:** Add CVEs to an exception list with time frames to ignore the vulnerability.
- **Automated Ticketing:** Closed-loop ticketing system integrations automate vulnerability workflows, routing issues to the appropriate teams for faster remediation.

Software Pipeline Security

- **Automated SDLC Scanning:** Scan images across CI/CD pipelines and registries for vulnerabilities, misconfigurations, malware, and secrets, ensuring your code is always at its safest.
- **Unified Security Posture Checks:** Uptycs continuously monitors security posture across the software pipeline, including branch protection rules, code scanning alerts, and registry misconfigurations, ensuring proactive mitigation of supply chain attacks.
- **Full Image Provenance and Integrity:** Visualize and inspect security from image build to runtime, enabling investigations to easily trace back to the image source, identify PR-related vulnerabilities, verify image signing, and seamlessly evaluate security posture.
- **Policy-Driven Guardrails:** Image security policies allow security teams to define guardrails and checks within the software development process, maintaining development velocity while safeguarding the integrity of deployed images.

uptycs

Uptycs never stops innovating so you can secure in your hybrid cloud and software pipeline. Create with confidence! Uptycs is the leading cloud security platform for large hybrid cloud environments. We extend security visibility from development to runtime, ensuring consistent protection and compliance across the application infrastructure. That's why enterprises like PayPal, Comcast, and Nutanix rely on Uptycs to secure the development ecosystems they use to build their applications and run their workloads.

Many CNAPP solutions lack the comprehensive data necessary to manage and prioritize risk effectively. With Uptycs, data is power! We provide deeper context effortlessly, enabling you to focus on what truly matters. While other CNAPPs may inform you if a vulnerable workload is exposed to the internet, they often fall short in identifying vulnerable packages currently running or those from three weeks ago, and whether and how you were breached. Uptycs can.

Uptycs unites teams to optimize security operations, ensure compliance, and accelerate remediation across cloud workloads, containers, Kubernetes, and software pipelines—all from a single security console, policy framework, and data lake. Elevate your cybersecurity with Uptycs.

On Guard. On Cloud. On Loop.

Learn more at Uptycs.com