Uptycs Vulnerability Management

Empower security teams with comprehensive risk-based vulnerability management, including detection, prioritization, and remediation across your hybrid cloud – from development ecosystem to runtime.

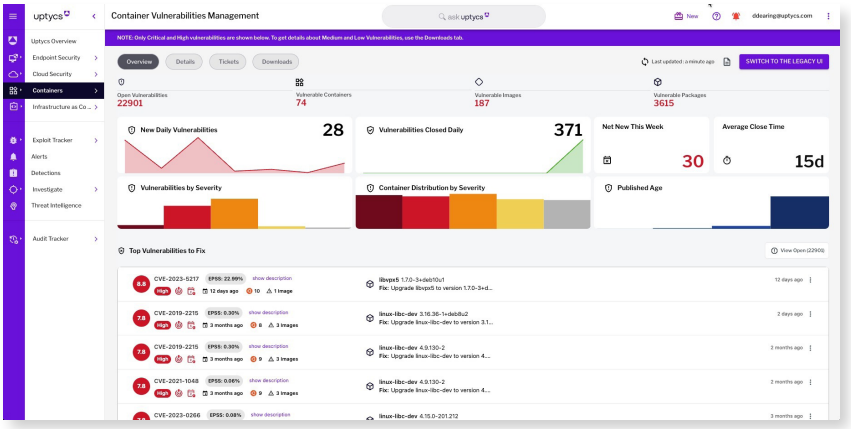
Managing vulnerabilities is painful, especially across complex hybrid clouds and fast-moving software pipelines. Stop struggling with disjointed security tools and workflows.

Uptycs unifies visibility across your developer ecosystem and runtime environment to help you focus on what truly matters. Through a single security console and policy framework, you can efficiently identify, prioritize, and remediate vulnerabilities. Automate risk analysis, taking into account asset criticality, active vulnerabilities, and real-time threat intelligence for exploits.

Get the runtime visibility that other solutions can't deliver. While most CNAPPs (Cloud Native Application Protection Platform) can determine if a vulnerable workload is exposed to the internet, they often lack visibility into other runtime risks, such as:

- Process listening on a vulnerable port
- Binary from a vulnerable package that is running
- Vulnerable jar file currently in use by a process

And once detected, you can quickly remediate with automated workflows or follow curated step-by-step guidance.



Uptycs Benefits

- Flexible Deployment: Utilize run-time sensors for vulnerability scanning in hybrid clouds and software pipelines, optionally complemented by agentless scanning for deployment flexibility.
- Simplified Management: Eliminate coverage gaps, detect vulnerabilities, assess relevant exploits, utilize transparent risk scoring, and leverage curated remediation guidance—all from a single security console.
- Comprehensive Coverage: Prioritize and address your most critical vulnerabilities seamlessly, from the developer ecosystem that builds and deploys your applications to the cloud workloads that run them.

> "Uptycs enables us to make risk-based decisions based on the full picture, like whether a system with a vulnerability is exposed to the internet or not without having to boil the ocean. It's what everyone should be doing."
>
> **Chris Castalado, CISO, Crossbeam**

Unified Management

Simplify vulnerability management with seamless visibility and reporting:

Centralized Dashboard: A single, intuitive dashboard offers a centralized view of vulnerabilities across your entire environment, including applications, systems, and cloud workloads.

Asset Inventory: Instantly discover images in registries, cloud resources, and application workloads, along with all their vulnerabilities and misconfigurations, in your hybrid cloud environment.

Built-in Compliance: Leverage built-in, customizable support for industry compliance frameworks such as PCI-DSS, HIPAA, GDPR, SOC 2, 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 user specified 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.

Developer Ecosystem Protection

Catch vulnerabilities early to mitigate risk before they reach production:

Automated SLDC Scanning: Scan images across CI/CD pipelines and registries for vulnerabilities, misconfigurations, malware, and secrets, ensuring your code is always at its safest.

Prioritized Alerting: Uptycs Smart Indicators prioritize vulnerabilities based on factors such as the presence of malware and secrets, ZTS (Zero Trust Score) rating, CVSS scores, EPSS scores, Uptycs Risk Score, changes in asset location, exposure to the Internet, the asset's significance as a business-critical resource, and more.

Policy Controls: Customizable policy controls for vulnerabilities, secrets, and malware enable security and development teams to prioritize fixes and establish remediation guidelines.

Advanced Correlation, Remediation, and Investigation

Correlate threats and vulnerabilities for rapid remediation:

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: Graphically identify vulnerabilities, misconfigurations, and other potential attack vectors to prevent lateral movement, privilege escalation, unauthorized access, and more.

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.

Runtime Investigation: Utilize YARA rules to scan and carve files and processes in real-time.

Broad Coverage and Flexible Deployment Options

Tailor your security to adapt to evolving cloud environments, both now and in the future:

Hybrid Cloud Support: Uptycs provides scanning capabilities across a wide array of environments, including public clouds (AWS, Azure, GCP), private cloud, containers, Kubernetes, and software pipelines.

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.

Versatile Workload Security: Uptycs protects a broad variety of technologies, including container runtimes, self-managed platforms, managed container orchestration services, and serverless technologies.

Kubernetes Clusters	Amazon EKS, Google GKE, Azure AKE, Red Hat OpenShift, VMware Tanzu, Unmanaged (on-Prem or Cloud)
Self Managed Container Types	Amazon ECS and Fargate, Google GCE, Azure Container Service, and any containers running in VMs or bare metal
Container runtimes	Docker, CRI-O, Containerd
Registry Scanning	JFrog Artifactory, Amazon ECR, Google GCR, Azure ACR, Private Docker Registry (cloud and on-prem)
CI Pipeline Scanning	Jenkins, GitHub Actions, GitLab, AWS Codebuild, Travis CI
Operating Systems	AIX, Alma Linux, Alpine Linux, Amazon Linux, Arch Linux, CBL-Mariner, CentOS, Container OS, Debian GNU Linux, Fedora, Flatcar, macOS, Maven, openSUSE Leap, Oracle Linux, Photon OS, Rocky Linux, SUSE Linux Enterprise Server, Ubuntu, Windows
Programming Language Support for App Level Vulnerabilities	Go, Java, Python, Ruby, Rust

About SRC

At SRC Cyber Solutions LLP , we provide Next Generation , Highly Automated , User - Friendlyand scalable solution . Our robust solutions include Comprehensive Email Security , Automated Patching and Endpoint Management , Asset Risk Visibility and Management with Policy Enforcement (ARM), Third - Party Data Flow Security solutions, Agentless Micro Segmentation, Endpoint, Management, and, Compliance Platform and an Online Gamified Simulation Platform for Cyber Security Training attacks . Additionally , we provide a Cloud - Native Application Protection Platform (CNAPP) solution to ensure comprehensive security across cloud - native applications.

SRC CYBER SOLUTIONS LLP

uptycs

www.srccybersolutions.com | +91 120 232 0960 /1 | sales@srccybersolutions.com