uptycs

Solution Brief

Uptycs System Insight, Visibility, and User Behavioral Monitoring

Uptycs System Insight, Visibility, and User Behavioral Monitoring offers organizations a unified solution to gain deep visibility, manage assets, and monitor insider risk across hybrid cloud, on-premise, and containerized environments, providing real-time insights and advanced security controls to safeguard their critical infrastructure.

Simplifying Security for Complex Hybrid Cloud Environments

As enterprises grow and adopt hybrid cloud infrastructures, the complexity of managing and securing their environments increases exponentially. Uptycs is the leading cloud-native application protection platform (CNAPP) designed to help organizations maintain robust security and compliance across their diverse ecosystems. Whether you are managing workloads in public or private clouds, on-premise data centers, or distributed devices, Uptycs provides deep visibility and actionable insights—all from a single, centralized platform.

With Uptycs, enterprises can gain real-time system insights, establish behavioral baselines, and take decisive actions to mitigate risks. By integrating asset management, user behavior monitoring, and anomaly detection into one solution, Uptycs enables proactive risk management and ensures organizations maintain a strong security posture, regardless of their environment's complexity.

In today's interconnected and increasingly complex IT environments, having comprehensive visibility and control over assets is essential for preventing operational inefficiencies and insider risk. Uptycs empowers companies to:

- **Enhance Security Posture:** With real-time monitoring and anomaly detection across users, systems, and containers, Uptycs allows organizations to identify and address unusual behavior that could lead to insider risks or compliance violations.
- **Centralized Insights:** By consolidating asset, behavioral, and system data into one platform, Uptycs streamlines asset management and compliance reporting for improved operational efficiency.
- **Support for Diverse Workloads:** Uptycs is designed to secure environments ranging from traditional on-premise data centers to complex multi-cloud infrastructures and containerized workloads.

This solution is ideal for:

- Enterprises managing hybrid cloud and multicloud environments, needing consistency across their security operations
- Organizations running mission-critical applications in VMs, containers, or Kubernetes clusters that require tight operational control and compliance.
- Teams seeking to monitor and mitigate insider risk across their entire infrastructure, including public cloud resources, on-premises workloads, and unmanaged assets..

Uptycs Benefits

Uptycs delivers a comprehensive solution that transforms asset management and operational efficiency in complex IT environments.

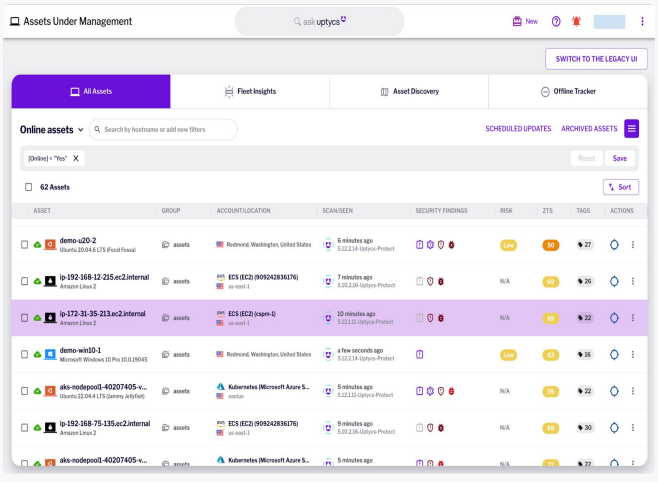
- **Unified Asset Management:** Manage your entire asset portfolio, including hardware, software packages, images,software licenses, certificates, and containers, with ease.
- **Visibility Across Environments:** Get detailed insights into user behavior, system processes, and network activity, giving your security team full situational awareness across cloud and on-premise assets.
- **Anomaly Detection and Behavior Modeling:** With Uptycs' built-in behavior modeling, identify deviations from established user and system baselines in real time.
- **Advanced Forensics and Debugging:** Interactively engage with live hosts,VMs and containers, and gather forensic artifacts to pinpoint the root cause of issues, improving response times and enhancing operational reliability.
- **Faster, More Effective Remediation:** Act swiftly in response to security, operational or performance issues by quarantining hosts, rebooting systems, or applying patches across thousands of assets with bulk remediation capabilities.
- **Zero Trust Security:** Strengthen your security posture with Zero Trust principles, ensuring that every device, user, and process is continuously validated for confirming to enterprise defined best practices.

Seamless Kubernetes and Cloud Integration: Uptycs provides comprehensive visibility and control across Kubernetes clusters and public cloud environments, ensuring secure, scalable operations for modern, containerized workloads.

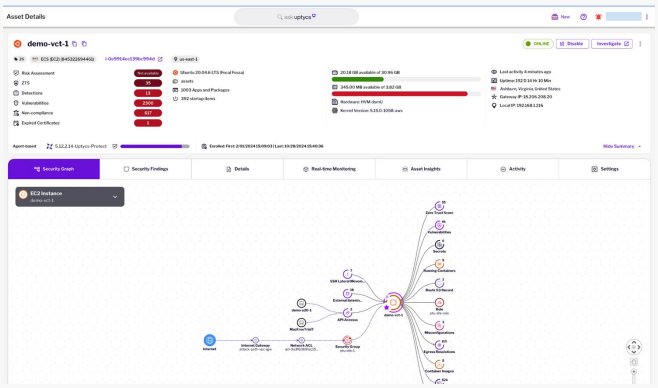
Comprehensive Asset Management and Discovery

Uptycs offers a unified platform to manage assets, track inventory, and monitor user and system behavior, giving organizations enhanced visibility and control over their environment.

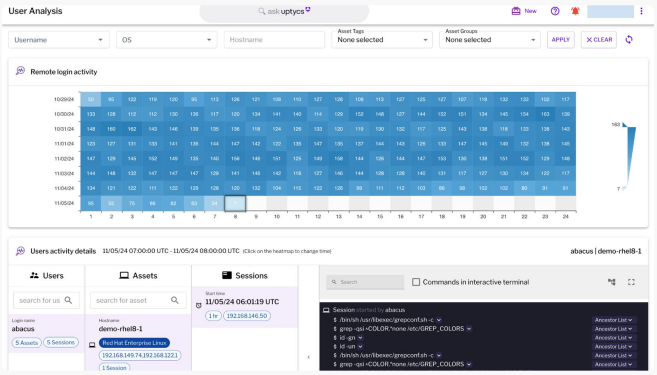
- **Asset Inventory and Reporting:** Uptycs allows you to maintain a comprehensive inventory of your hardware, operating systems, packages, and services across your infrastructure. The platform also offers software cataloging and license tracking capabilities, helping to ensure compliance and optimize resource allocation.
- **Certificate Discovery:** Easily track expired and active certificates, ensuring security and compliance.
- **SBOM:** The integration of SBOM (Software Bill of Materials) ensures visibility into the components of software running in your environment. Uptycs provide upto date SBOM for hosts, containers and images.
- **Unmanaged Asset Discovery:** Uptycs identifies and manages previously undiscovered assets such as printers, IoT devices, and mobile phones, enhancing visibility across your enterprise footprint.



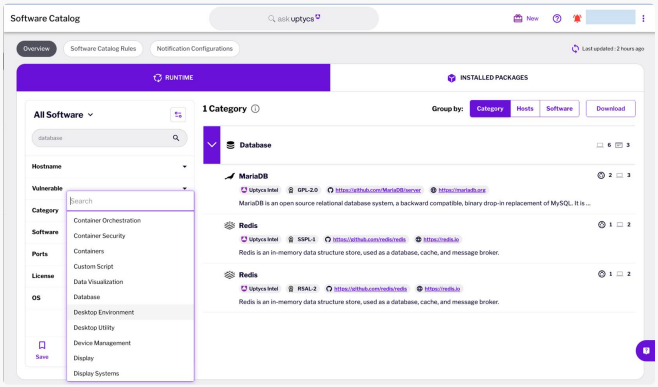
All assets under management



Individual asset details including full security posture



Track all user behavior and identify outlier behavior



Complete Software Catalog including licensing and vulnerabilities in the software

User and System Behavior Monitoring

Uptycs leverages real-time insights into user and system activities to establish baselines and detect anomalies that could indicate insider risk or operational inefficiencies.

- **User Behavior Monitoring:** Track user activity with detailed insights into logins, processes launched, files accessed, and socket connections made. Uptycs builds behavioral baselines to detect deviations, ensuring enhanced protection against insider threats.
- **Anomaly and Outlier Detection:** Uptycs develops baseline models for users, VMs, hosts, and containers, identifying anomalous activities that could signal insider risk or unusual system performance. This functionality is supported by over 2,000 detection rules, continuously monitoring for irregular behaviors.

Forensics, Debug, and Diagnostics

Uptycs offers powerful forensic capabilities, enabling real-time investigation and debugging.

- **Live Diagnostics:** Interact with hosts, VMs, and containers to examine live system states, review running processes, and inspect opened files. Uptycs supports file and memory carving. The carved files and memory can be downloaded for analysis by forensic investigation tools.
- **Performance Monitoring:** Automatically gather performance metrics when certain thresholds are breached, such as CPU usage exceeding 85%, and quickly identify which processes are responsible for excessive resource consumption.

Remediation and Patch Management

Uptycs accelerates remediation efforts, minimizing potential operational inefficiencies.

- **Host Quarantine and Management:** Manage assets by quarantining hosts or VMs, rebooting/shutting down compromised systems.
- **Run Custom Scripts:** Run custom scripts across a single host or entire fleet within minutes to remediate issues, gather data for offline analysis. Access all your servers, VM's containers from one central console, no need for remote login.
- **Software Patch Management:** Update or install software to optimize performance and ensure your systems are running the most secure versions.

User and System Behavior Monitoring

Uptycs leverages real-time insights into user and system activities to establish baselines and detect anomalies that could indicate insider risk or operational inefficiencies.

- **User Behavior Monitoring:** Track user activity with detailed insights into logins, processes launched, files accessed, and socket connections made. Uptycs builds behavioral baselines to detect deviations, ensuring enhanced protection against insider threats.
- **Anomaly and Outlier Detection:** Uptycs develops baseline models for users, VMs, hosts, and containers, identifying anomalous activities that could signal insider risk or unusual system performance. This functionality is supported by over 2,000 detection rules, continuously monitoring for irregular behaviors.

Disk Scanning and Content Search

Uptycs offers the ability to scan entire disks for sensitive content or patterns, ensuring critical data is secure across your fleet.

Secret and Pattern Detection: Search for secrets or other important patterns in files across your infrastructure, identifying potential vulnerabilities or operational inefficiencies before they happen.

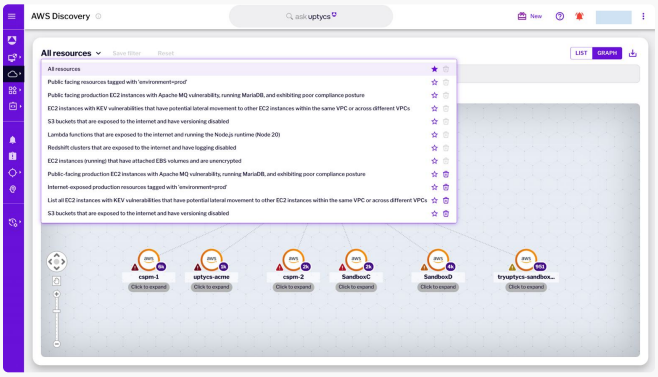
Zero Trust Networking

Uptycs supports Zero Trust Networking (ZTN), providing a security score for each device to help manage the level of access a particular device has to enterprise applications.

Public Cloud Discovery and Monitoring

Gain comprehensive visibility into your public cloud environment with Uptycs.

- **Resource Discovery:** Discover all resources in your cloud infrastructure, report across regions, and monitor changes in real time to ensure operational consistency.
- **Identity Monitoring:** Uptycs provides insights into roles, policies, and permissions, ensuring that permissions are right-sized and excessive permissions are flagged.

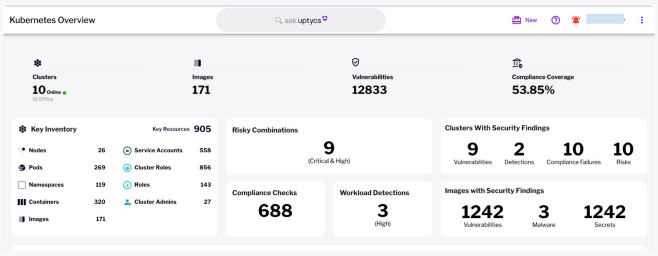


Cloud Discovery

Kubernetes Visibility and Image Management

Uptycs offers unparalleled visibility into Kubernetes environments and container image management.

- **Kubernetes Visibility:** Track the inventory of clusters, namespaces, pods, and containers. Monitor service accounts and access policies for a comprehensive operational stance.
- **Image Management:** Uptycs inventories container images in registries, helping ensure compliance and operational efficiency across your containerized environments.



Kubernetes visibility

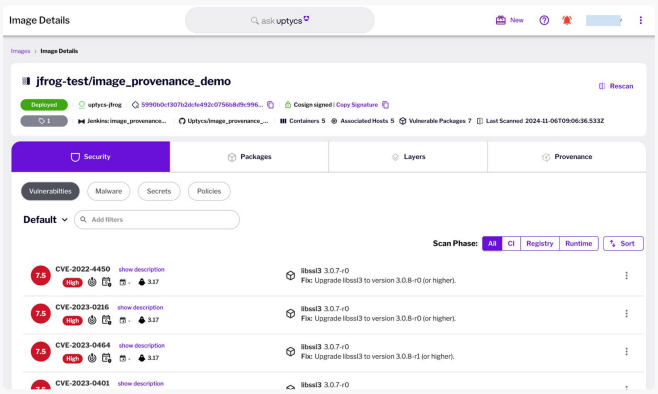
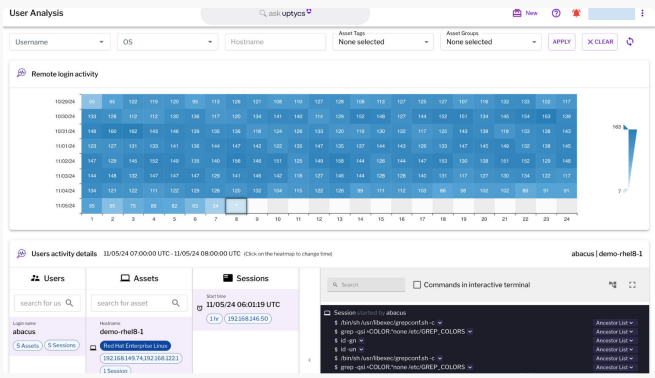


Image details - security posture, layers and provenance

Endpoint Overview



Track all user behavior and identify outlier behavior

Conclusion

Uptycs' robust platform offers unparalleled visibility and control over your infrastructure, enabling organizations to streamline asset management, enhance security posture, execute remediation actions and mitigate operational inefficiencies across complex infrastructures. Whether managing assets in hybrid clouds or monitoring user behavior, Uptycs delivers the insights and tools needed for a secure and compliant environment.

Success Stories

"I would not want to do security anywhere without this level of visibility"

Steve Shedlock
Incident Response Team Lead SEI

uptycs

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.

Secure Everything from Dev to Runtime

See Uptycs in action