uptycs

Solution Brief

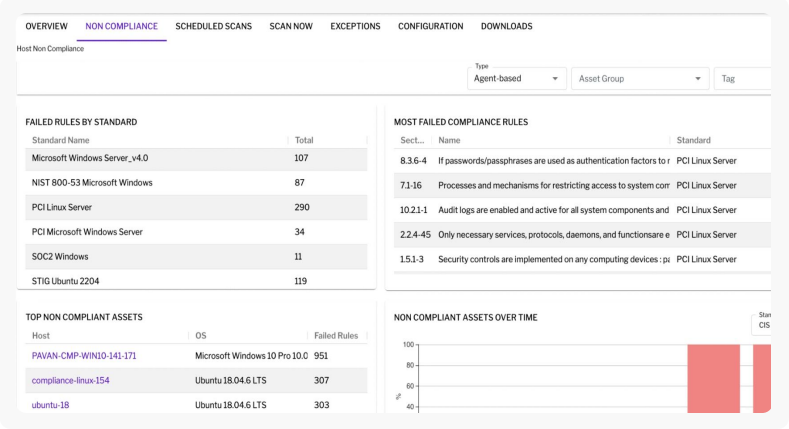
Ensure Continuous File Integrity Monitoring and Threat Detection with Uptycs

Maintaining file integrity is essential for upholding security standards and regulatory compliance. Uptycs File Integrity Monitoring (FIM) provides real-time alerts and continuous oversight of changes to critical files and directories. This proactive approach allows organizations to detect and respond to threats like ransomware attacks, unauthorized modifications, and privilege escalations quickly. By delivering comprehensive file monitoring and integrated threat intelligence, Uptycs ensures businesses can protect sensitive data and maintain strong security postures against emerging threats.

What We Do

What Uptycs FIM Offers

- **Real-Time File Auditing:** Instantly alerts on file changes, attributing modifications to specific users or processes, while scanning for malware with YARA rules.
- **Complex Threat Detection:** Correlates file changes with broader security data to detect threats like unauthorized logins and ransomware.
- **Policy-Driven Compliance Monitoring:** Ensures regulatory compliance (e.g., PCI-DSS, HIPAA) with tailored monitoring that flags compliance risks early.



How We Do It

Secure and Protect Your Most Essential Files

Uptycs continuously monitors file changes, with real-time alerts for incident response teams. Integrated YARA scanning and forensic analysis allow rapid threat detection and remediation for threats like ransomware.

Comprehensive Visibility and Control

- **Real-Time Monitoring:** Track critical files, including password databases and app configurations, with immediate alerting via eBPF sensors.
- **YARA-Based Scanning:** Scan files for over 700 malicious toolkits, with customizable rules.
- **Forensics and Querying:** Perform instant queries and historical analysis for suspicious file activities.

Threat Analysis and Root Cause Attribution

- **Event Correlation:** Uptycs correlates file changes with broader security data, facilitating immediate root cause analysis and enabling swift identification of potential threats.
- **Integrated Malware Detection:** Utilizing YARA scanning and threat hunting capabilities, Uptycs detects and blocks processes attempting to modify critical files, effectively mitigating malware risks.
- **SIEM Integration:** Forward FIM alerts to SOC teams for comprehensive threat visibility.

Compliance and Data Integrity

- **Policy-Based Monitoring:** Define file monitoring policies to meet compliance standards like PCI-DSS and HIPAA.
- **Unified Auditing and Reporting:** Access dashboards for streamlined compliance reporting.
- **Custom Exceptions:** Tailor exclusions based on file path or process names across asset groups.

Monitor and Protect Your Files

Uptycs FIM offers continuous monitoring, real-time alerts, and compliance reporting, enabling swift detection of threats and protection of critical data across hybrid environments. Security teams gain instant insight into unauthorized changes, supporting quick responses and compliance.

Beyond monitoring, Uptycs FIM correlates file changes with broader security signals to detect complex threats, such as ransomware or privilege escalations. Customizable policies allow teams to tailor monitoring for sensitive files, while seamless integration with tools like Slack and JIRA streamlines incident response, providing comprehensive visibility and control.

Success Stories

> "Uptycs was deployed on a large scale as a key component of our Security posture."
>
> **Comcast**
> Vice President IT Security

> "I would not want to do security anywhere without this level of visibility"
>
> **Steve Shedlock**
> Incident Response Team Lead SEI

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.

uptycs

Secure Everything from Dev to Runtime

See Uptycs in action