02/23/2022

Uptycs

EDR Competitive Comparison

404 Wyman Street
Suite 357
Waltham, MA 02451

www.uptycs.com

Why to Choose Uptycs Over Traditional EDR

Many organizations are looking for a detection and response solution that meets the changing needs of their modern attack surface. Uptycs is built from the ground up for modern defenders. Here is a list of things to consider when deciding if Uptycs is a better fit for your organization than traditional EDR.

	Product Capabilities	Why it Matters
Platform Support	Uptycs' endpoint capabilities build on the open-source osquery project, which normalizes telemetry from Windows, macOS, and Linux systems. Many organizations have chosen Uptycs for our product's robust support for those platforms.	With Uptycs, you don't have to compromise—you can cover Windows, macOS, and Linux excellently in a single solution.
Richer Telemetry	Both Uptycs and traditional EDR look at processes, HTTP connections, service creation, logins, and other event types. Uptycs goes further with: • Browser extensions • File system files • Configuration files (Augeas lens) • Sudoers list • DNS lookup events • Disk encryption	Organizations use Uptycs to support a broader set of use cases beyond threat detection, such as asset insights and visibility, compliance, vulnerability detection, ad hoc threat hunting, and file integrity monitoring.
Low Footprint	Uptycs has significantly optimized the osquery agent for stability and performance, minimizing the memory, CPU, and disk I/O footprint. On Linux, the agent uses eBPF to non-invasively collect system-level telemetry with very low CPU overhead.	Reliable performance on Linux servers avoids issues for production applications.
Superior investigation And Threat Hunting	Uptycs provides incident responders and threat hunters with a complete record of system activity through our Flight Recorder—even for systems where attack activity did not trigger a detection and was considered benign. Analysts can ask ad hoc questions, browse real-time system activity, and take action (killing processes, deleting files, quarantining machines, and disabling users). This ability to conduct ad hoc real-time and historical investigations for all systems sets Uptycs apart from traditional EDR.	Analysts can quickly answer questions needed to understand the scope, severity, and root cause of an incident.
Sophisticated Custom Detections	Out-of-the-box, Uptycs includes 1,000+ behavioral detections covering the MITRE ATT&CK framework. If you want to augment these rules, you can. Uptycs works transparently, allowing you to easily see how built-in behavioral detections work, create exceptions, and copy that event rule logic as a basis for new custom rules.	With Uptycs, your security engineers can see how a behavioral detection works, which gives them confidence. They can easily copy and customize to fill gaps in coverage.

	Product Capabilities	Why it Matters
Advanced YARA Scanning	Out-of-the-box, Uptycs maintains hundreds of YARA rules to detect 50+ APT toolkits across Windows, macOS, and Linux. Uptycs also enables you to create and deploy custom YARA rules. You can set YARA to scan files and process memory, and any monitored file is scanned by several hundred YARA rules if the content changes, and every process that is launched is scanned by several hundred YARA rules. In addition, any file or process can be scanned ad hoc in real time.	Uptycs lets your team intelligently take advantage of industry-standard YARA rules to identify malware in your environment.
Host Compliance	Only Uptycs provides auditing and compliance support for CIS Benchmarks, FedRAMP, HIPAA, ISO 27001, NIST 800-53, PCI, SOC 2, and DISA STIG. This solution greatly simplifies the task of monitoring and reporting for our customers who are able to confidently answer auditor questions, provide evidence, and streamline remediation workflows.	Uptycs can help you improve your proactive security posture and meeting compliance requirements.
File integrity Monitoring	Uptycs supports file integrity monitoring (FIM) with extreme flexibility to include and exclude folders and files, and only files with certain extensions can be monitored in order to optimize performance. You can configure the solution to run YARA scans against changed files. On Windows, Uptycs can monitor registry paths.	FIM is a security control required by standards such as PCI DSS. In addition, monitoring files is important for threat detection scenarios, such as when an attacker accesses the Keychain file to steal credentials on macOS.
Vulnerability Scanning For Linux	With Uptycs, you can match vulnerability feeds against system telemetry from your Linux fleet to detect software vulnerabilities without burdening host systems. In addition, you can use pre-built queries to identify non-compliant or vulnerable software in your environment, such as Log4j core files.	Uptycs allows your team to scan for vulnerable software in a faster and less invasive manner than traditional scanning solutions.
Historical Exposure To Newly Disclosed Threats	When a new threat emerges, you can query the historical telemetry from your environment to determine if that exploit or behavior was operating in your environment in the past. Many organizations used Uptycs to inventory all of their systems running the vulnerable Log4j library, for example. Uptycs' threat research team also contributes threat books allowing you to scan your historical data against the latest threat intelligence to identify prior infections. Lookback can be extended up to 90 days and you can send telemetry to your own AWS S3 for archival purposes.	With Uptycs, you can quickly report to management on your organization's exposure to newly disclosed threats.