Datasheet

uptycs

Uptycs vs. Traditional EDR or XDR Solutions

404 Wyman Street
Suite 357
Waltham, MA 02451
www.uptycs.com

Uptycs vs. Traditional EDR or XDR Solutions

Uptycs is built from the ground up to analyze a wealth of telemetry at scale and meet multiple security controls in one solution. Here is a list of things to consider when deciding if Uptycs is a better fit for your organization than traditional solutions.

Uptycs Advantage	Product Cababilities	Why it Matters
Agent consolidation across macOS, Linux, and Windows	Many customers replace multiple agents with Uptycs. It provides threat detection and response, vulnerability scanning, security hygiene, compliance, asset management, and more in a single solution for macOS, Linux, and Windows.	Within a single console you can manage the security posture of your entire laptop and server fleet. Your teams need to manage and learn fewer tools, and can answer more questions in one place. Of course, tool consolidation also means cost effectiveness.
Purposeful, rich security 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	You can 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 (FIM).
Scalability	Experience exceptional scalability with Uptycs XDR, designed to effortlessly adapt to your organization's growth and evolving infrastructure. Our cloud-native architecture ensures seamless performance and comprehensive protection, meeting the demands of diverse environments and accommodating increased data volumes, endpoints, and workloads as needed.	Scalability and adaptability make Uptycs an ideal choice for businesses seeking a future-proof security solution that can evolve with their needs.

Uptycs Advantage	Product Cababilities	Why it Matters
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 an attacker's activity didn't trigger a detection and was considered benign. This ability to conduct ad hoc, real-time and historical investigations for all systems sets Uptycs apart from traditional EDR or XDR.	Quickly answer questions needed to understand the scope, severity, and root cause of an incident. Start with simplistic yet powerful tools and dive deeper with complex queries using standard SQL.
Sophisticated custom detections	Out of the box, Uptycs includes over 1,500 behavioral detections covering the MITRE ATT&CK Framework. You can augment these rules if you like. Uptycs works transparently, enabling you to: • See how built-in behavioral detections work • Create exceptions to rules • Copy event rule logic as a basis for new custom rules	With Uptycs, your security engineers can see how a behavioral detection works, instilling confidence in them. They can easily copy and customize it to fill gaps in coverage.
Advanced YARA rule-based scanning	Out of the box, Uptycs maintains hundreds of YARA rules to detect 50+ APT toolkits across macOS, Linux, and Windows. Uptycs also lets you create and deploy custom YARA rules used to scan process binaries and process memory. Also, monitored files are scanned with several hundred YARA rules, with events being raised immediately following a match. 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, with considerably higher degrees of effectiveness than the signature-based approach used by antivirus tools.
Preemptive blocking	Uptycs permits process and DNS blocking to be instrumented on specific hosts—or across your fleet— through blocking policies based on file hash, executable path, certificate, or YARA rule match.	Stop malicious processes before they cause further damage, thus reducing risk across your assets.

Uptycs Advantage	Product Cababilities	Why it Matters
Prompt remediation (manual and automated)	Following a detection, alert, threat hunt, or investigation, Uptycs enables prompt remediation by quarantining the host, killing processes, blocking the offending IP address and port, deleting files, disabling users, deleting registries, running scripting (localized diagnosis), and carving files (including process binaries). These actions can be manually instrumented or automated via alerts based on trigger conditions.	Speed threat eradication and containment, both for external and internal/insider threats. Limit legal, reputational, and operational damage.
Host compliance	Only Uptycs provides auditing and compliance support for CIS Benchmarks, DISA STIG, FedRAMP, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2. This greatly simplifies the task of monitoring and reporting for customers who can confidently answer auditor questions, provide evidence, and streamline remediation workflows.	Uptycs can help you improve your proactive security posture and meet compliance requirements.
File integrity monitoring (FIM)	Uptycs supports file integrity monitoring with extreme flexibility to include/exclude folders, files, and specific file extensions can be monitored 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, e.g., 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 lets your team scan for vulnerable software in a faster and less invasive manner than traditional scanning solutions.

Uptycs Advantage	Product Cababilities	Why it Matters
Historical visibility	When a new threat emerges, you can query your environment's historical telemetry to determine if that exploit or behavior was operating there in the past. For example, many organizations have used Uptycs to inventory all of their systems running the vulnerable log4j library. Uptycs' threat research team also contributes threat books that let you scan and compare your historical data with the latest threat intelligence to identify prior infections. Its Lookback feature can be extended up to 90 days, and you can send telemetry to your AWS S3 for archival purposes.	With Uptycs, you can quickly report to management regarding your organization's exposure to newly disclosed threats.
Agent performance	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.

About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

Shift your cybersecurity up with Uptycs.

uptycs