uptycs

Datasheet

Uptycs vs. Traditional XDR Solutions

Traditional XDR solutions struggle to aggregate, correlate, and analyze massive amounts of security telemetry, provide complete cloud visibility, and identify and stop threats underway. 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 Cabability	Why it Matters
Agent consolidation across macOS, Windows, cloud workloads, and Linux—including IBM AIX, Linux on Z, and more	Many customers replace multiple agents with Uptycs. It provides threat detection, response and forensics, vulnerability scanning, security hygiene, compliance, asset management, and more in a single solution for macOS, Linux, Windows, cloud workloads, and containerized environments.	Within a single console you can manage the security posture of your modern attack surface. Teams manage and learn fewer tools, and can answer more questions in one place. Of course, tool consolidation also means cost effectiveness.
Agent performance	Uptycs has significantly optimized its osquery-based agent for stability and performance, minimizing the memory, CPU, and disk I/O footprint. On Linux, the agent uses eBPF to noninvasively collect system-level telemetry with very low CPU overhead.	Reliable performance on Linux servers avoids issues for production applications, including HPC (high-performance computing) and HPCaaS environments.
FIPS compliant agent	Uptycs provides FIPS compliant (Federal Information Processing Standards) versions of its agent when installed on a FIPS compliant host. Uptycs will validate that a FIPS capable OpenSSL is installed and that your endpoint is correctly configured to FIPS before initializing and connecting to the Uptycs Cloud.	Better data security, risk management, and increased trust from clients and partners.

Uptycs Advantage	Product Cabapilities	Why it Matters
Modern, scalable architecture	Uptycs normalizes your security data close to its collection point, then streams it up into your Uptycs Detection Cloud—your security data lake that's part of your Uptycs subscription. Uptycs adeptly handles the massive volume, variety, and velocity of security and IT data emanating from your modern attack surface.	Enjoy centralized control of your security data, instantly access the correlated insights you care about most, and take decisive action. Uptycs is a future-proof security solution that can evolve with your needs.
Deeper, purposeful, rich security data	Both Uptycs and traditional EDR look at processes, sockets, files, DNS, HTTP connections, service creation, logins, and other event types. Uptycs goes further with: • YARA scanning of files and memory • Scanning for secrets • Forensics support • Configuration files discovery (Augeas lens) • Device Zero Trust Score Computation • Performance monitoring • Discovery of hosts/devices in the neighborhood and port scanning	You can use Uptycs to support a broader set of use cases beyond threat detection, such as cyber asset inventory, compliance, vulnerability management, ad hoc threat hunting, and file integrity monitoring (FIM).
Host compliance	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 so you can confidently answer auditor questions, provide evidence, and streamline remediation workflows.	Uptycs can help you improve your proactive security posture and meet compliance mandates.
File integrity monitoring (FIM)	Uptycs supports file integrity monitoring with extreme flexibility such as the ability to include/exclude folders, files, and file extensions. You can configure Uptycs to run YARA scans against changed files. On Windows, Uptycs can monitor registry paths.	Focus on what matters and support threat detection scenarios, such as when an attacker accesses the Keychain file to steal credentials on macOS

Uptycs Advantage	Product Cabapilities	Why it Matters
Vulnerability scanning for Linux, Windows and macOS	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 prebuilt queries to identify non-compliant or vulnerable software in your environment, such as log4j-core files. Uptycs prioritizes the vulnerabilities using environmental factors (Uptycs Smart Indicators), for example, is a vulnerable shared library currently open and in use by a process, is a process listening on a vulnerable port, is a binary from a vulnerable package currently running.	Uptycs lets your team scan for vulnerable software in a faster and less invasive manner than traditional scanning solutions. Prioritize which vulnerability on which host, image, container, lambda function to fix first by taking into consideration the environment in which the vulnerability was detected. Vulnerable packages that are not used are deprioritized.
Advanced YARA rule-based scaning	Out of the box, Uptycs maintains hundreds of YARA rules to detect 250+ 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.
Uptycs Threat Research Team	Uptycs Threat Research Team conducts real-time research across multiple threat intel feeds and platforms and uses this information to fortify your defenses. This includes direct delivery of threat books into your Uptycs instance to scan for current and prior vulnerabilities and infections.	Uptycs helps ensure your organization is on top of imminent threats. As soon as a new malware is reported, Uptycs pushes threat books to each customer, threat books scan the historical data for presence of IoC's and IoB's associated with the malware just reported.

Uptycs Advantage	Product Cabapilities	Why it Matters
Sophisticated custom detections	Out of the box, Uptycs includes over 1,800 behavioral detections covering the MITRE ATT&CK Framework. You can augment these rules by customizing or writing your own rules. 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 • Create custom detections as code using Sigma	With Uptycs, your security engineers can see how a behavioral detection works, which also gives them the confidence to easily copy and customize the detection to fill gaps in coverage.
Superior investigation and threat hunting	Uptycs provides incident responders and threat hunters with a complete record of system activity through our Flight Recorder (going back up to 13 months)—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, even if it occurred up to 13 months ago. Start with simplistic yet powerful tools and dive deeper with complex queries using standard SQL or detection rules written in Uptycs YAML or in Sigma.
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. Lookback up to 90 days, and send telemetry to your AWS S3 or cold storage system for archival purposes.	With Uptycs, you can quickly report to management regarding your organization's exposure to newly disclosed threats.

Uptycs Advantage	Product Cabapilities	Why it Matters
Sophisticated custom detections	Out of the box, Uptycs includes over 1,800 behavioral detections covering the MITRE ATT&CK Framework. You can augment these rules by customizing or writing your own rules. 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 • Create custom detections as code using Sigma	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 or detection rules written in Uptycs YAML or in Sigma.
Superior investigation and threat hunting	Uptycs provides incident responders and threat hunters with a complete record of system activity through our Flight Recorder (going back up to 13 months)—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 or detection rules written in Uptycs YAML or in Sigma.
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. Lookback up to 90 days, and send telemetry to your AWS S3 or cold storage system for archival purposes.	With Uptycs, you can quickly report to management regarding your organization's exposure to newly disclosed threats.
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 Cabapilities	Why it Matters
Prompt remediation (manual and automated)	Following a detection, alert, threat hunt, or investigation, Uptycs enables prompt remediation by giving you the ability to quarantine the host, kill processes, block the offending IP address and port, delete files, disable users, delete registries, run scripts (localized diagnosis), and carve files (including process binaries). These actions can be manually instrumented or automated via alerts based on triggers. For example, upon detecting data exfiltration you can automatically trigger a blocking action (against dropbox, a USB drive, etc.). Bulk remediations allow you to run a script against thousands of assets.	Faster threat eradication and containment, both for external and internal/insider threats. Limit legal, reputational, and operational damage.
Unified endpoint and cloud security	Uptycs unifies XDR and CNAPP (cloud-native application protection) under a single UI and data model. Get centralized control of your security data, consistency across environments, and a more complete picture of software supply chain visibility. Detect malware and vulnerabilities on your developers' laptops and reveal any suspicious behavior as they move code in and out of repositories and into the cloud.	Secure digital transformation to drive better business results.

About Uptycs

Attackers don't think in silos and neither should your security. Uptycs, the first unified CNAPP and XDR platform, protects the developer laptops that build your applications to the cloud workloads that run them—all from a single console and data lake. Uptycs helps drive DevSecOps excellence, bringing teams together to master threat operations, meet compliance mandates, and reduce risk across clouds, containers, and endpoints. Take back control of your security data, get the correlated insights you care about most, and take decisive action.

Shift up your cybersecurity with Uptycs. Learn how at: Uptycs.com

uptycs