Datasheet

uptycs

Uptycs for Endpoints

Security Observability For Productivity And Server Endpoints

> *"After a thorough evaluation by our security engineering team, Uptycs was deployed on a large scale as a key component of our security posture. The Uptycs platform provides a broad set of security capabilities with instant endpoint and asset visibility that powers detection and response as well as compliance and governance."*
>
> **Leo Li**
> Vice President, Comcast Security

Introduction

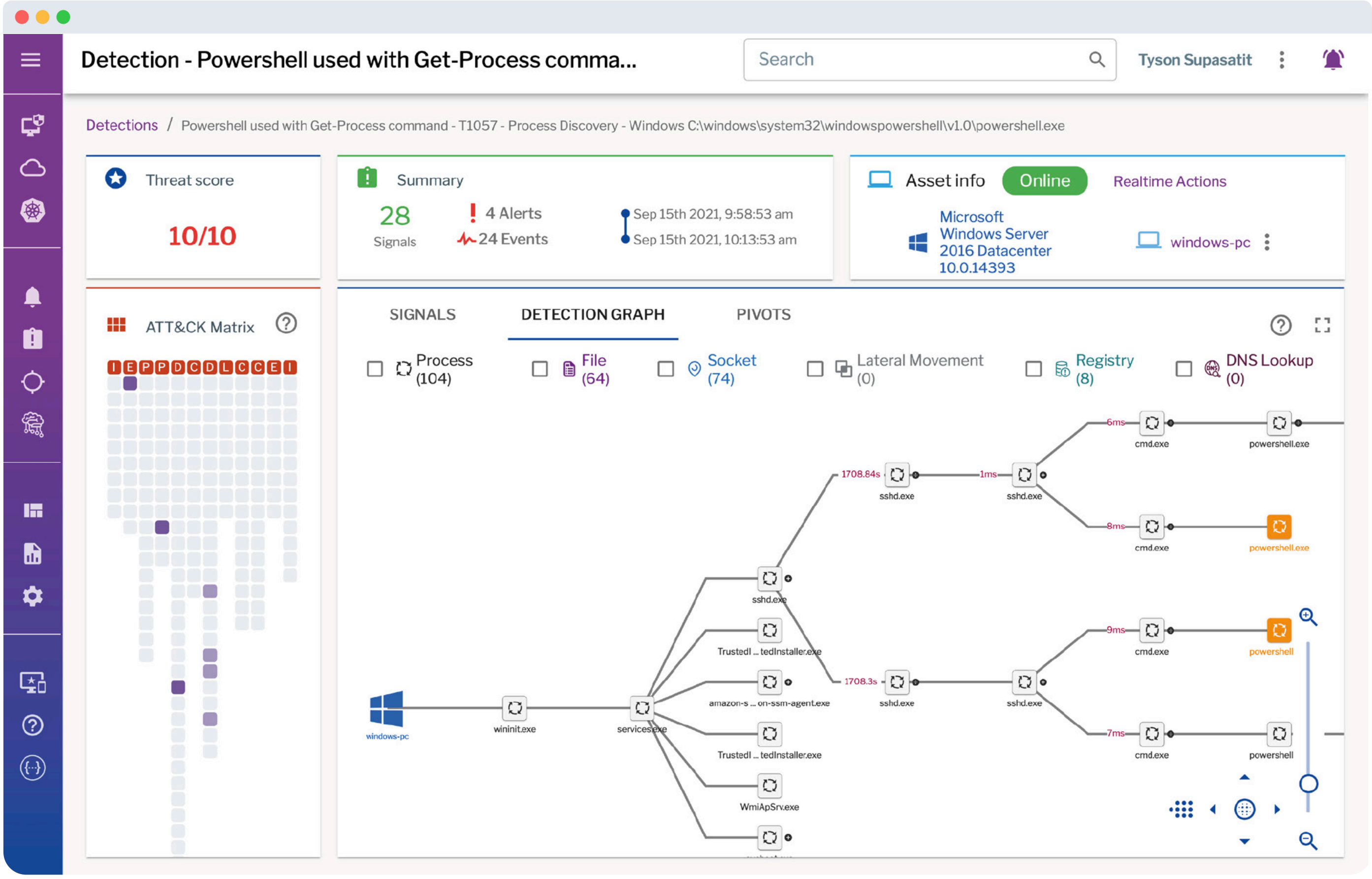
Uptycs provides you with unprecedented visibility across your endpoint fleet for threat detection and response, asset inventory and insight, audit and compliance, and more. Uptycs helps you protect all of your productivity and server endpoints.

Security Observability At Scale

The Uptycs platform is built for large-scale collection and analysis of security telemetry, with a SaaS backend that applies Lambda streaming analytics to billions of points of telemetry each day gathered from our lightweight agents and collectors. Within seconds of an event, Uptycs correlates it with other signals and fires a single, high-quality detection. In addition, Uptycs automatically gathers relevant artifacts (files, socket connections, etc.) and generates pivot queries for investigation. After the real-time analysis, telemetry is stored for historical baselines, reports, and queries.

Best-In-Class EDR For All Platforms

As remote working has become the norm, securing employees' laptops and workstations is more important than ever. Uptycs detects and correlates observed MITRE ATT&CK behaviors across macOS, Windows, and Linux endpoints (including for those running Graviton processors). Uptycs offers advanced EDR capabilities including file integrity monitoring, the ability to run YARA rules against live memory and files, file and process memory carving to extract malicious payloads, application allowlisting, and binary authorization and blocking.



Detection - Powershell used with Get-Process comma...

Detections / Powershell used with Get-Process command - T1057 - Process Discovery - Windows C:\windows\system32\windowspowershell\v1.0\powershell.exe

Threat score 10/10

Summary: 28 Signals; 4 Alerts; 24 Events; Sep 15th 2021, 9:58:53 am – Sep 15th 2021, 10:13:53 am

Asset info: Online; Microsoft Windows Server 2016 Datacenter 10.0.14393; windows-pc

□ Process (104) □ File (64) □ Socket (74) □ Lateral Movement (0) □ Registry (8) □ DNS Lookup (0)

Uptycs provides excellent coverage for the MITRE ATT&CK framework with hundreds of behavioral rules describing tactics and techniques for macOS, Windows, and Linux.

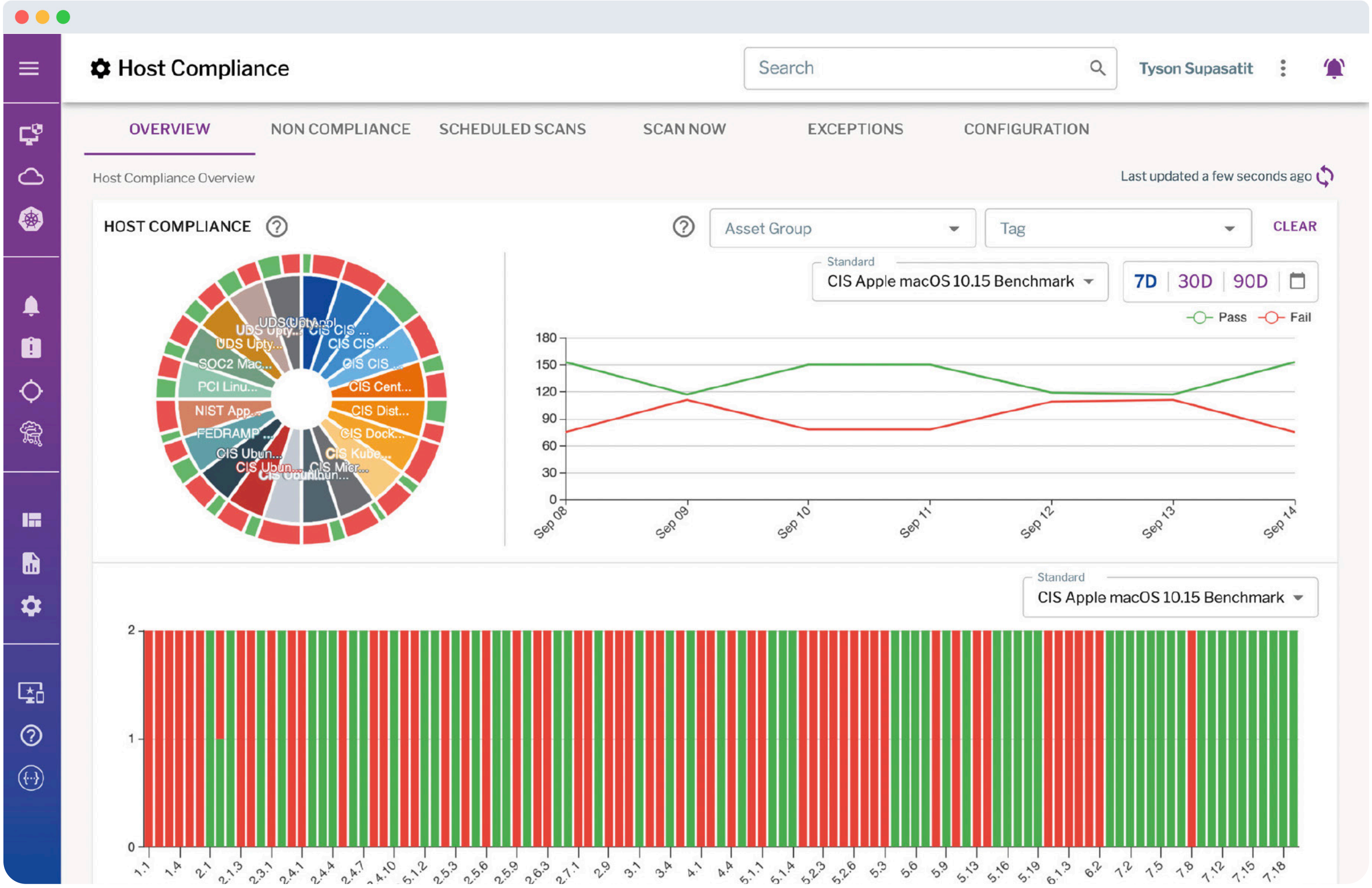
Go Beyond The Endpoint With XDR Scenarios

Uptycs also extends the types of detection scenarios possible, correlating endpoint telemetry with telemetry from other relevant data sources, such as cloud infrastructure, Kubernetes systems, SaaS applications, and identity providers. This type of extended detection and response (XDR) capability is increasingly important as your attack surfaces multiply.

Proactively Harden Your Endpoint Attack Surfaces

Uptycs provides much more than traditional EDR. Security, compliance, and IT operations teams also rely on Uptycs to proactively identify and remediate risk through:

- Asset insight and inventory
- Detection of vulnerable software packages
- Robust support for audit and compliance



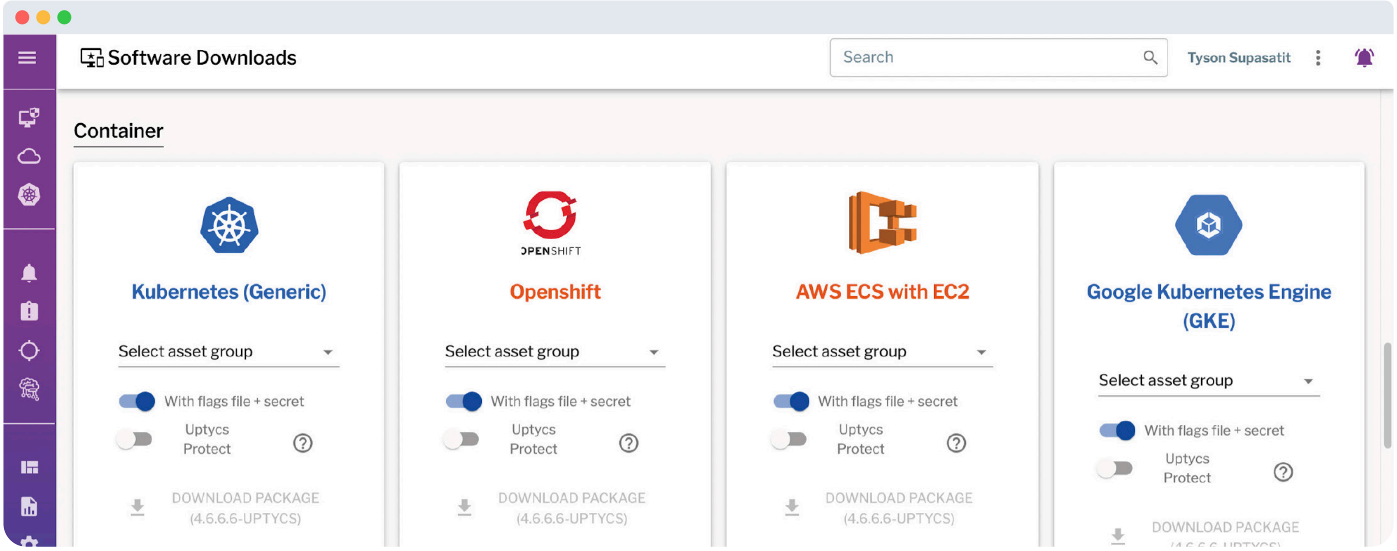
Uptycs supports a number of compliance standards including CIS Benchmarks, HIPAA, ISO, NIST, PCI, SOC 2, and STIG.

Remediation and Blocking

The Uptycs Protect add-on gives users the ability to safely remediate and block malicious or non-compliant activity on the endpoint. CSIRT teams and incident responders can take action when they observe real-time attack activity, and security teams can remediate issues without having to wait for IT Operations.

Why Uptycs?

- **Agent performance:** Uptycs has made a number of improvements to the osquery agent, resulting in significantly better performance and stability. The agent typically consumes less than 4% CPU.
- **Scalable:** The Uptycs solution has been proven in large enterprise environments, operating safely in fleets of more than 300,000 servers in a single deployment.
- **Platform support:** Uptycs supports macOS, Windows, and a broad selection of Linux distributions, including those running on AWS EC2 Graviton instances.
- **Flexible:** Uptycs is highly extensible, allowing your to meet unique organizational needs with custom detections, monitoring policies, dashboards, etc.
- **Integration:** Uptycs offers a robust API that enables you to make the most of the solution, integrating with your existing security infrastructure (SIEM, SOAR, CMDB, etc).



Uptycs supports managed container deployments in the cloud such as ECS, EKS, and GKE.

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