

www.uptycs.com

CONTINUOUS ENDPOINT, CONTAINER, AND CLOUD COMPLIANCE WITH UPTYCS



Uptycs 

- 3** Introduction
- 4** A new approach to security compliance and risk assurance is needed
- 5** Uptycs solves key compliance reporting problems
 - Flexibility to meet complex requirements
- 7** Live and historical queries for gathering evidence
- 8** Examples of how Uptycs helps fulfill compliance control requirements
 - File integrity monitoring (FIM)
 - Software inventory
- 9** Intrusion detection
 - Vulnerability scanning
 - Malware detection
 - Disk encryption
- 10** Scanning Wi-Fi networks on a quarterly basis
 - Data processing governance, aka DLP-lite
 - Insecure protocols and ciphersuites on web servers
- 11** Technical advantages of Uptycs over traditional compliance tools
 - Agent performance
- 12** SaaS platform
 - Compliance for cloud and container environments
 - Cloud infrastructure compliance
- 13** Container and Kubernetes compliance
- 14** User-driven security
- 15** Integrating Uptycs with your existing reporting and analytics systems
 - Additional Uptycs use cases
- 16** Conclusion



INTRODUCTION

Imagine having a solution that lets you assess your compliance posture across your on-premises and cloud environments in a single place, at the press of a button. It works across your entire endpoint fleet—macOS, Linux, and Windows workstations and servers—as well as your containers and cloud infrastructure.

Imagine that, instead of taking hours to run a new compliance check, you had the data you needed immediately, served up with insights into which assets need attention most urgently. This solution not only meets your organization's compliance reporting needs, but also provides ad hoc reporting to answer auditors' questions about real-time and historical security posture. You finally have the tools needed to gain compliance, stay compliant, and spend more time focusing on strategic initiatives.

All this is possible with the Uptycs Security Analytics Platform, which provides continuous compliance for endpoints, server workloads, containers, and the cloud. Uptycs makes security telemetry—across all your modern attack surfaces—easily understandable and accessible so you can get the answers you need, quickly.

This paper highlights how you can use Uptycs to implement, monitor, and report on policies for endpoint and cloud compliance. Uptycs offers a highly scalable, more performant, and on-demand way to report on compliance and answer ad hoc audit questions, compared to traditional compliance solutions. In addition, Uptycs meets a number of other security and compliance needs including cloud and container compliance, file integrity monitoring, software auditing, and behavioral detection.



A NEW APPROACH TO SECURITY COMPLIANCE AND RISK ASSURANCE IS NEEDED

The stakes are higher than ever for cybersecurity risk governance and compliance, both in terms of avoiding costly penalties and being able to assure your customers. Yet, at the same time, compliance has never been more difficult for IT teams as regulations continue to evolve, the scale of their endpoint and server fleets grow, and organizations adopt new cloud technologies.

Traditional compliance tools are not up to the task, because they typically use a relational database that makes extracting information from hosts and compiling the reports a slow process. If the feed fails and a report isn't completed, that may cause an embarrassing delay as senior leadership will need to wait while you try to run the report again: connecting to the endpoints, fetching the data, and evaluating the policies. With this traditional architecture, it's virtually impossible to run a report on tens of thousands of hosts in a single day.

In addition, new cloud environments and industry requirements add to the number of standards that compliance teams are responsible for monitoring. You may be subject to PCI, HIPAA, or GDPR, depending on the type of data your company handles, or your company's cloud service may need to meet SOC 2 or FedRAMP standards in order to win contracts. The addition of cloud environments means that your organization will need to implement the relevant CIS Benchmarks developed specifically for those environments. In the past several years, The Center for Internet Security (CIS) has worked with cloud providers on benchmarks for AWS, Azure, and GCP.

Adding to this complexity is the fact that every environment is unique. You need flexibility in your monitoring and reporting to accommodate different operating systems and the criticality of data (whether a server is Internet-facing or handles PII, etc.), not to mention the special needs of different business units.

Cybersecurity compliance can feel like a necessary evil, and traditional ways of managing it have become more cumbersome than helpful. Security and compliance teams need a solution that is fast, lightweight, scalable, and customizable.

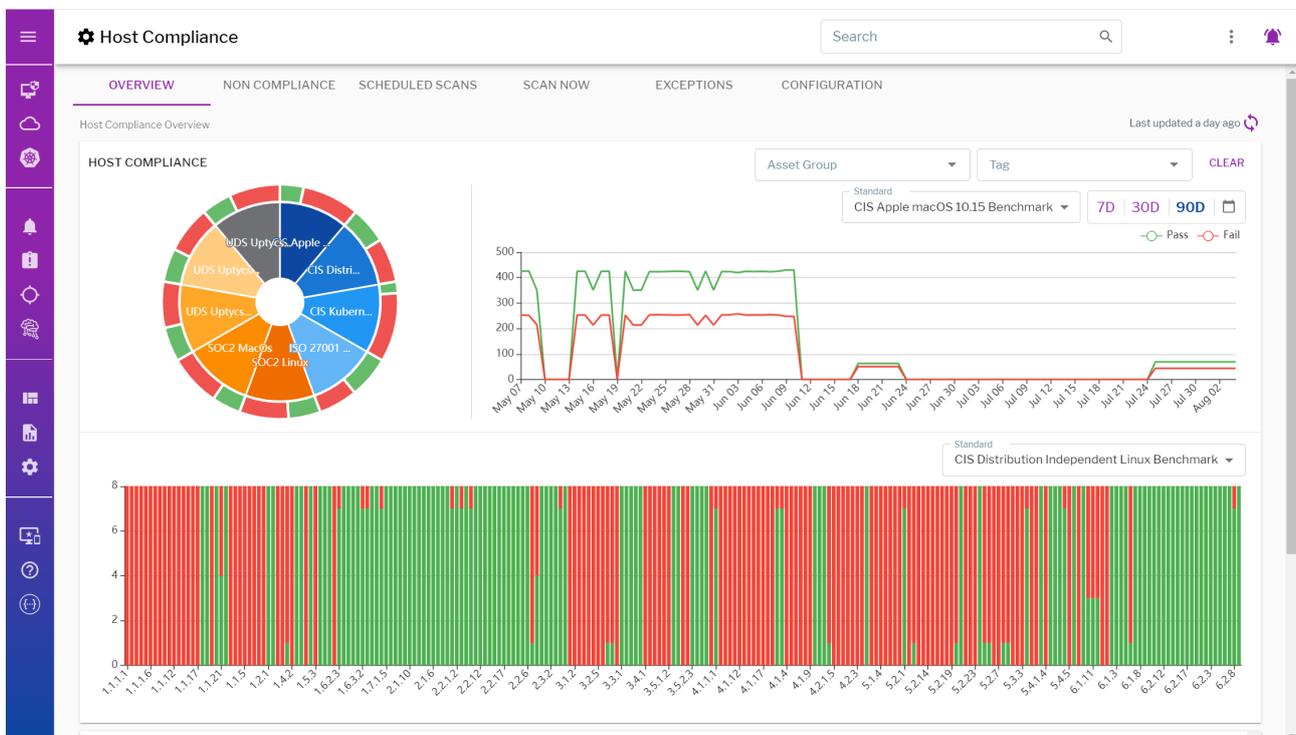


UPTYCS SOLVES KEY COMPLIANCE REPORTING PROBLEMS

For compliance teams that are stressed out with their growing burdens, Uptycs offers a much-needed new approach to security auditing and compliance. Uptycs gathers a wealth of telemetry from hosts regarding processes, installed software packages, and file changes. This information is stored and made immediately available for query and reports, and can also be used to meet specific compliance requirements, like file integrity monitoring. Uptycs offers the broad coverage and flexibility needed today by security compliance and risk assurance teams.

FLEXIBILITY TO MEET COMPLEX REQUIREMENTS

With Uptycs, compliance teams can easily support new requirements that are unique to their organizations. The asset grouping and tagging functionality allows you to get a high-level view of the compliance posture of your organization as a whole, or a particular business unit. For any group of assets, you can see the percentage of checks that are passing and their compliance posture over time, so you can quickly assess whether or not you're meeting your goals. This flexibility makes Uptycs ideal for monitoring compliance in complex environments that are running many different types of assets subjected to various requirements.



Uptycs allows compliance managers to easily track compliance across the organization or specific groups of machines.

Uptycs supports reporting for common regulatory standards, like the CIS Benchmarks, but sometimes organizations want to tailor these checks to meet their own security goals. For example, setting passwords to rotate every two weeks instead of 30 days. These types of customizations to standards are easy to implement in Uptycs through parameterization, whereby the user can modify parameters of the checks.

CIS Configurations							
Name	OS	OS Version	Framework	Version	Checks	Actions	
CIS_Apple_macOS_10.15_Bench	Darwin	10.15	CIS	1.1.0	114		
CIS_CentOS_Linux_6_Benchmark	Linux	6	CIS	3.0.0	242		
CIS_CentOS_Linux_7_Benchmark	Linux	7	CIS	2.2.0	222		
CIS_Distribution_Independent_L	Linux	any	CIS	2.0.0	237		
CIS_Docker_Benchmark_v1.2.0	Linux	any	CIS	1.2.0	94		
CIS_Kubernetes_Benchmark_v1.	Linux	any	CIS	1.5.1	87		

Uptycs offers CIS Benchmark checks for Windows, MacOS, Linux, AWS, Docker and Kubernetes.

CIS

Description
Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters. Ensure that a special character is part of the password policy on the computer

Rationale
The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

Command
Perform the following to ensure the system is configured as prescribed: , , 1. Run the following command in Terminal: , , , pwpolicy -getaccountpolicies | egrep "1 special" , , , 2. Verify the value returned , , Password must have at least 1 special character , , Password must have at least 1 special character

Parameterization
Enabled

Parameters

```
{
  "all_of_pwpolicy_check":
  [{"category": "min_complex_chars", "operator": "EQUAL_OR_GREATER", "expected_result": "2"}],
  "update_path": "/usr/bin/pwpolicy"
}
```

SAVE **CANCEL**

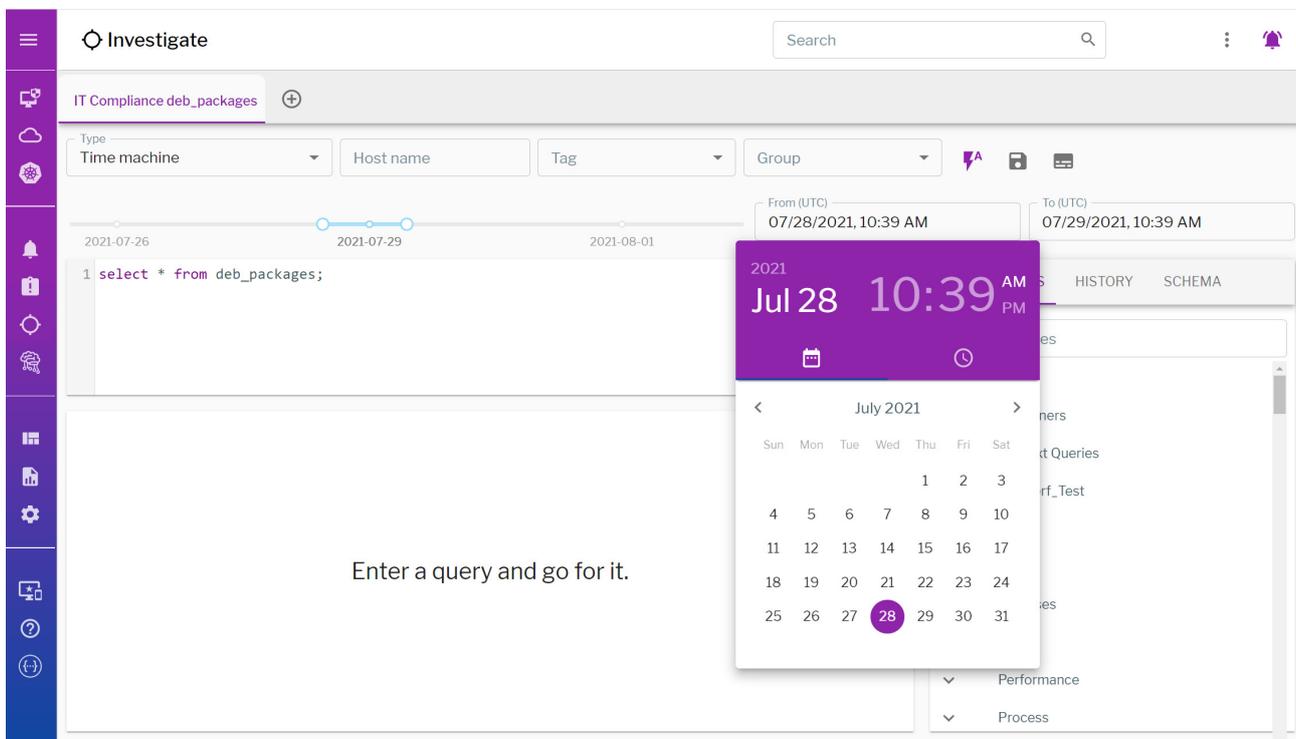
With Uptycs, you can adjust parameters for compliance checks to meet the specific requirements of your organization. Here, the number of special characters required for user passwords has been changed from 1 to 2.

SUPPORTED STANDARDS:

- CIS Benchmarks
- HIPAA
- And more to come!
- SOC 2
- NIST 800 Series
- FedRAMP
- ISO 27001
- PCI-DSS
- DISA STIG

LIVE AND HISTORICAL QUERIES FOR GATHERING EVIDENCE

Uptycs also offers the ability to run ad hoc live and historical queries to answer very specific questions that come up from internal and external groups. With the Time Machine feature, you can jump back to a specific point in time to see the configuration state and other details of an asset for evidence gathering. For example, you can run a query to show the compliance posture of a particular asset three months ago. With the ability to run queries against historical state, you can easily obtain the evidence needed to satisfy an auditor's questions.



The screenshot shows the Uptycs Investigate interface. At the top, there is a search bar and a menu icon. Below the search bar, the page title is "Investigate". The main content area is titled "IT Compliance deb_packages" and includes a "Time machine" dropdown menu. Below the dropdown, there are fields for "Host name", "Tag", and "Group". A timeline slider is visible, showing dates from 2021-07-26 to 2021-08-01. A query input field contains the text "1 select * from deb_packages;". Below the query input, there is a large text area that says "Enter a query and go for it.". A calendar overlay is shown, displaying the month of July 2021, with the 28th highlighted. The time is shown as 10:39 AM. The interface also includes a sidebar with various icons and a bottom navigation bar.

Uptycs enables you to retroactively check if software on a set of machines was up to date during a specific time period.

EXAMPLES OF HOW UPTYCS HELPS FULFILL COMPLIANCE CONTROL REQUIREMENTS

Organizations can use Uptycs for more than just reporting. With the event and alerting functionality, you're able to implement key security controls needed to meet compliance requirements. In fact, the breadth of system telemetry that Uptycs gathers makes it an extremely versatile tool for meeting a wide variety of control requirements across multiple regulatory standards. Some examples are given below.

FILE INTEGRITY MONITORING (FIM)

File integrity monitoring is a core requirement for any device that is subject to PCI DSS and SOC 2 standards. For example, PCI Requirement 11.5 requires "a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files." Uptycs' FIM capabilities enable you to keep an audit log of file modifications, track specific application files that should not change outside of change-management processes, and monitor specific operating system files which are often modified by malware. Events include contextual information including machine name, host IP, file path modified, action taken, process ID, process name, and the user account that modified a given file.

SOFTWARE INVENTORY

Knowing which software packages you have installed is essential to maintaining a strong security posture. Software inventory is No. 2 on the list of CIS Critical Controls for a good reason! However, maintaining an up-to-date software inventory is difficult, especially with the array of software types on workstations and servers: regular applications, third-party package managers, app stores, and browser extensions, to name a few. Typically, getting a holistic look at installed software requires looking at an equally wide variety of information sources.

You can simplify software inventory with Uptycs, automating the collection of needed data so that it is immediately available to answer questions. For example, if you receive news about a critical vulnerability in a particular Chrome browser extension, or intelligence about malware targeting a particular PDF reader, you will be able to easily discover which assets in your environment have the vulnerable software installed.

Furthermore, you can use Uptycs to allowlist or blocklist software packages.

Read more:

- [Osquery tutorial: Gathering software inventory](#)
- [Osquery tutorial: Assessing Chrome extension permissions](#)
- [Using osquery to monitor third-party system extensions for IT compliance](#)

INTRUSION DETECTION

Intrusion detection is covered by PCI-DSS (Requirement 11.4) and SOC 2 CC6.6, with the latter specifying “logical access security measures to protect against threats from sources outside its system boundaries.” Uptycs offers a method of host-based intrusion detection as it observes every port that is opened on the host and every network connection established, comparing IP addresses, domains, and JA3 signatures against updated threat intelligence sources.

VULNERABILITY SCANNING

SOC 2 CC7.1 requires “detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.” With the Uptycs Vulnerability Detection capability, we continuously ingest information about your asset inventory, including software packages and asset configuration, alongside vendor-provided security bulletins, CVE’s and other known sources of vulnerabilities, and correlate them to surface any identified vulnerabilities within your environment. Since this process is continuous, you’ll always be up to date with the latest vulnerabilities and will have immediate insight into which assets need your attention.

MALWARE DETECTION

SOC 2 CC6.8 requires “controls to prevent or detect and act upon the introduction of unauthorized or malicious software.” Uptycs uses multi-method malware detection to be able to spot and alert you to malicious activity. With third-party file reputation database integration, live YARA scanning for signatures at process launch, on-demand YARA scanning of files, process/memory and related carving, and YARA scanning triggered by FIM, any malware that’s made its way into your system will be detected almost instantly so you have time to react accordingly.

DISK ENCRYPTION

Over its lifespan, there’s a **1 in 10 chance that a laptop will be stolen**, according to the physical device security provider, Kensington. Disk encryption is one way to keep sensitive data out of the hands of thieves, and Mac and Windows operating systems have made disk encryption easy to use. Uptycs makes it easy to check if systems in your environment have full-disk encryption turned on.

SCANNING WI-FI NETWORKS ON A QUARTERLY BASIS

PCI-DSS 11:1 requires organizations to take an inventory of their managed Wi-Fi networks every quarter. Usually, this involves an IT staff member roaming around the campus with a laptop seeking out access points. Instead, organizations can configure Uptycs to gather this information automatically every week from laptops (using the Wi-Fi Survey function available in macOS, for example).

DATA PROCESSING GOVERNANCE, AKA DLP-LITE

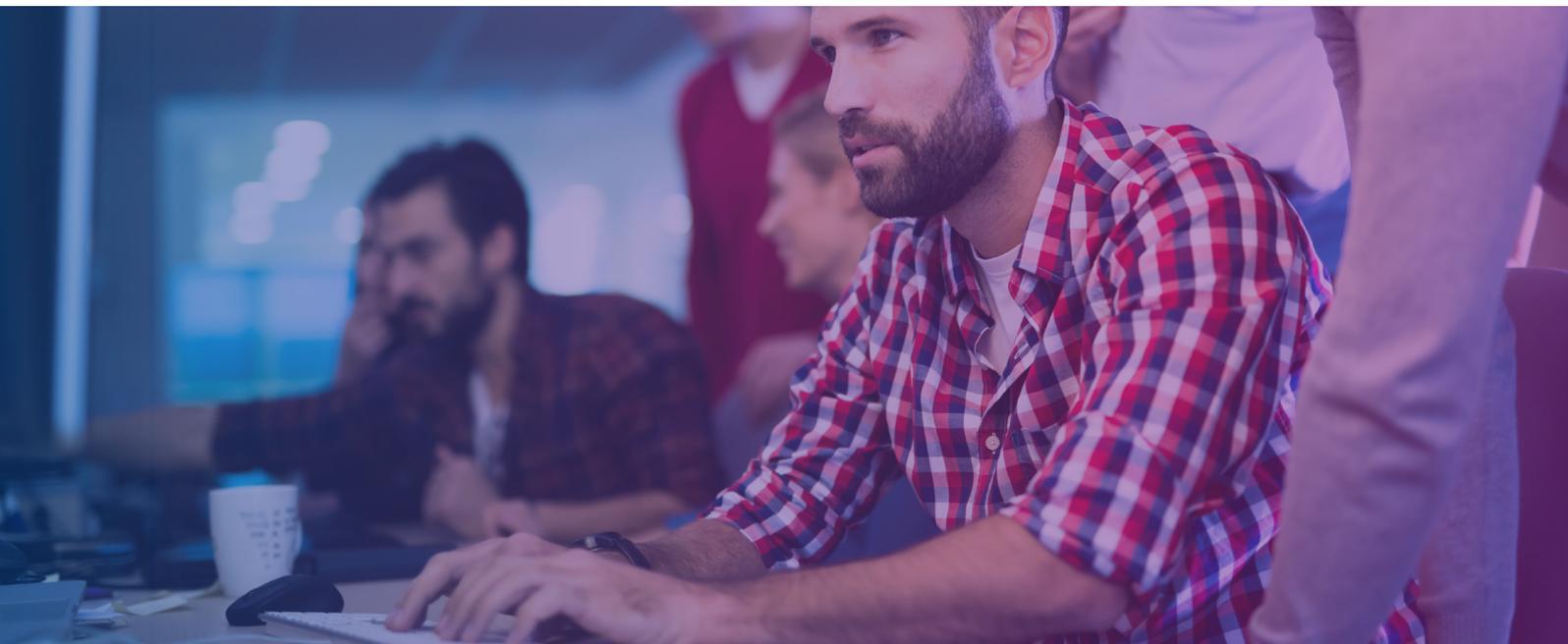
GDPR requires that companies govern how customer data is processed—a very vague injunction that many interpret as requiring some type of data loss protection (DLP) solution. Because Uptycs has access to file information on endpoints, you can use it to approximate DLP for relevant systems by applying YARA rules to files and searching for sensitive information, like social security numbers, and monitoring when files are moved on and off USB drives.

INSECURE PROTOCOLS AND CIPHERSUITES ON WEB SERVERS

Some compliance standards, such as [NIST 800-52](#), prohibit the use of insecure protocols and ciphersuites, such as SSLv3, on web servers in your environment. Uptycs helps you to identify web servers and parse those machines' configuration files using Augeas lenses to determine if they are using the compliant protocols and ciphersuites. You can also use curl (built into the Uptycs agent) to find certificate information, such as the serial number, issuer organization, SHA fingerprint, and expiry date. With this data collected, you can easily attest to compliance when an audit occurs.

Read more:

- [Using Augeas with osquery: How to access configuration files from hundreds of applications](#)



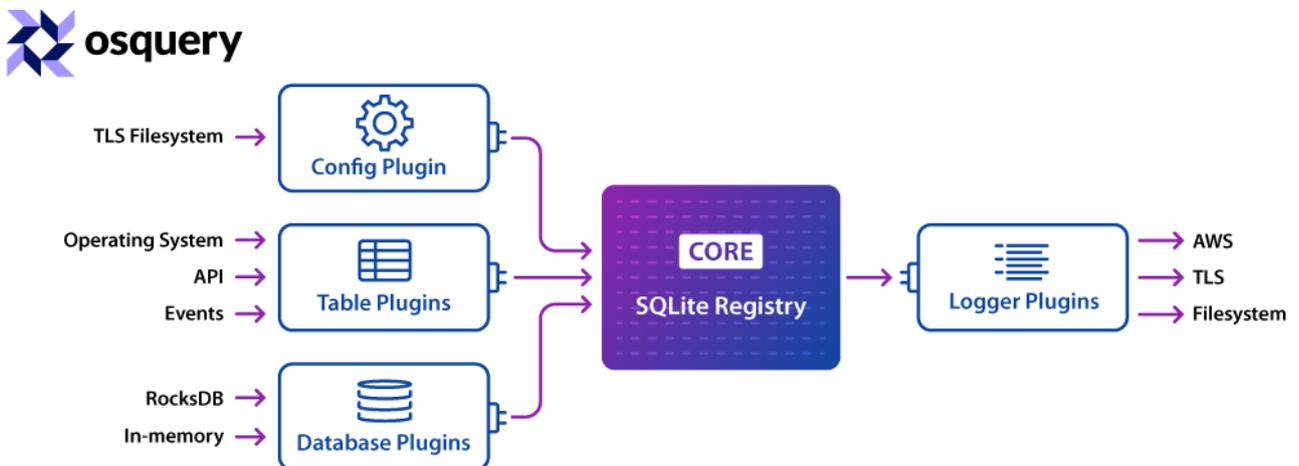
TECHNICAL ADVANTAGES OF UPTYCS OVER TRADITIONAL COMPLIANCE TOOLS

AGENT PERFORMANCE

The Uptycs platform is built to stream endpoint telemetry to a SaaS backend (an on-premises option is available), avoiding many of the performance issues associated with traditional compliance solutions.

For endpoints, Uptycs deploys an optimized osquery-based agent on Linux, macOS, and Windows systems, collecting system information like configurations, file changes, installed software packages, user activity, and more. Scheduled queries gather this information in the background and send it to the Uptycs SaaS backend through HTTPS. This means that data is always at the ready for reporting, and reports can be run in a fraction of the time required by traditional compliance tools.

The Uptycs agent utilizes virtual tables and a RocksDB datastore that is optimized for write operations. It includes a Watchdog service that limits resource consumption and can automatically terminate long-running queries.



For cloud infrastructure, Uptycs leverages our proprietary cloudquery to normalize, ingest and analyze data from your cloud environment. Cloudquery can be deployed as an osquery extension or Docker container, on-premises or in the cloud, and can be configured to fetch data from one or more cloud providers. In a typical deployment you'll have one instance of cloudquery in each cloud provider account. This makes data transfer faster and cheaper as the incoming data will not leave the perimeter of the cloud deployment.

SAAS PLATFORM

The Uptycs platform is available as a SaaS or on-premises solution. The SaaS offering dramatically simplifies deployment and management; Uptycs has been deployed for hundreds of thousands of endpoints in a matter of days. Customers typically use Ansible, Chef, Puppet, or other automation software to quickly deploy the agent to their workstations and servers.

As an on-premises solution, Uptycs functions exactly the same. The only difference is that you'd have your own servers, and staff to maintain them, which can be more difficult to manage overall. Not all organizations' security policies permit them to use SaaS, though, which makes the on-premises offering an option for meeting FedRAMP compliance.

COMPLIANCE FOR CLOUD AND CONTAINER ENVIRONMENTS

Most organizations operate a hybrid environment spanning on-premises data centers and public cloud environments. Uptycs enables continuous compliance of both your server workloads and cloud infrastructure.

CLOUD INFRASTRUCTURE COMPLIANCE

Uptycs ingests telemetry from the cloud service provider control plane to help ensure that your cloud services are configured according to standards such as SOC 2, the CIS AWS Foundations Benchmark, and the CIS GCP Foundations Benchmark.

Section / Control	Resources	Pass	Fail	Score	Pass %
1. Identity and Access Management					
CIS_AWS_1.1 : Avoid the use of the "root" account (Scored)	3	3	0	<div style="width: 100%; background-color: green;"></div>	100
CIS_AWS_1.2 : Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)	7	4	3	<div style="width: 57%; background-color: green;"></div>	57
CIS_AWS_1.3 : Ensure credentials unused for 90 days or greater are disabled (Scored)	7	4	3	<div style="width: 57%; background-color: green;"></div>	57
CIS_AWS_1.4 : Ensure access keys are rotated every 90 days or less (Scored)	7	7	0	<div style="width: 100%; background-color: green;"></div>	100
CIS_AWS_1.5 : Ensure IAM password policy requires at least one uppercase letter (Scored)	3	1	2	<div style="width: 33%; background-color: green;"></div>	33
CIS_AWS_1.6 : Ensure IAM password policy require at least one lowercase letter (Scored)	3	1	2	<div style="width: 33%; background-color: green;"></div>	33
CIS_AWS_1.7 : Ensure IAM password policy require at least one symbol (Scored)	3	0	3	<div style="width: 0%; background-color: green;"></div>	0
CIS_AWS_1.8 : Ensure IAM password policy require at least one number (Scored)	3	0	3	<div style="width: 0%; background-color: green;"></div>	0
CIS_AWS_1.9 : Ensure IAM password policy requires minimum length of 14 or greater (Scored)	3	0	3	<div style="width: 0%; background-color: green;"></div>	0
CIS_AWS_1.10 : Ensure IAM password policy prevents password reuse (Scored)	3	0	3	<div style="width: 0%; background-color: green;"></div>	0
CIS_AWS_1.11 : Ensure IAM password policy expires passwords within 90 days or less (Scored)	3	0	3	<div style="width: 0%; background-color: green;"></div>	0
CIS_AWS_1.12 : Ensure no root account access key exists (Scored)	3	3	0	<div style="width: 100%; background-color: green;"></div>	100

Uptycs enables companies to simplify asset and resource inventory in the cloud, as well as ensure compliance with standards such as SOC 2 and the CIS Foundations Benchmarks for AWS and GCP.

In the same way you get at-a-glance breakdowns of your host and asset compliance posture, you're able to quickly determine which cloud resources are failing compliance checks and where you should focus your remediation efforts.

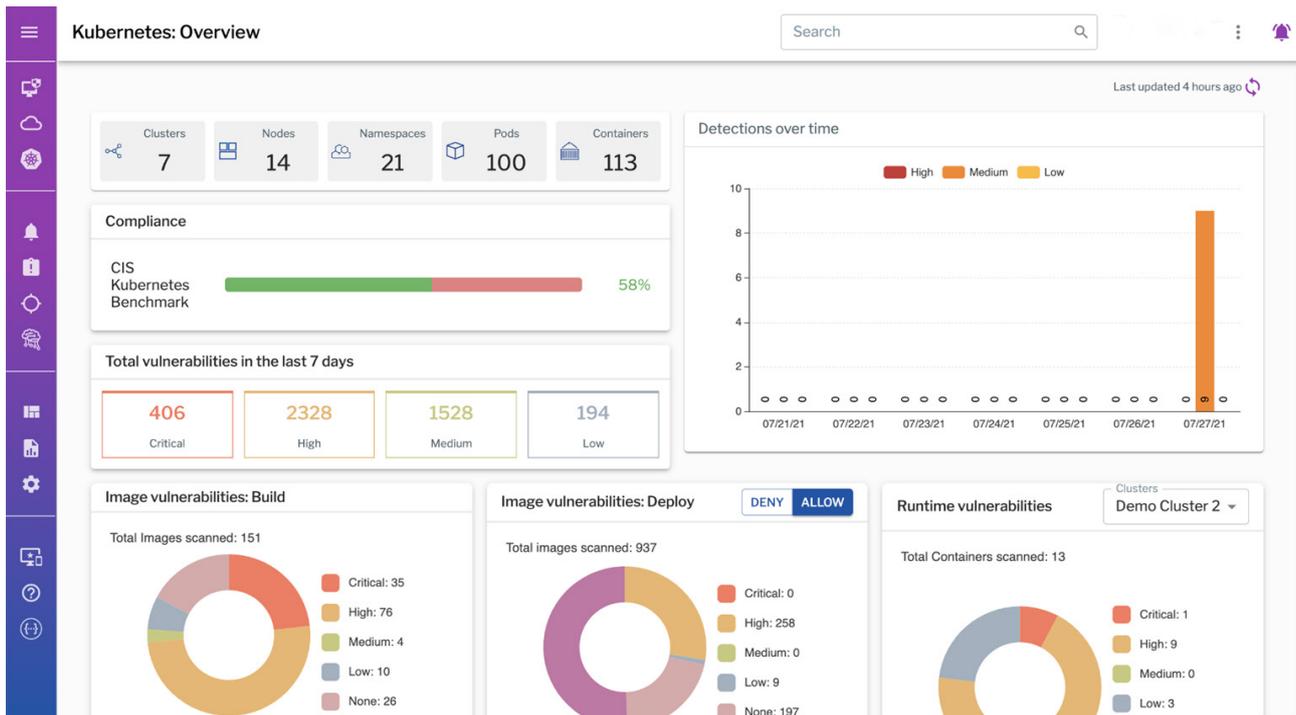


The Cloud Compliance Overview dashboard provides quick insight into your cloud compliance posture.

The level of compliance support Uptycs can offer for public cloud environments boils down to the Shared Responsibility Model: In PaaS environments, the Cloud Service Provider manages the majority of the control plane and they are responsible for ensuring compliance requirements are met for that portion. The customer is still responsible for the compliance of the data plane, and that's where Uptycs can assist. In IaaS environments, the security responsibility falls almost entirely on the customer, with the exception of the physical servers, storage, and network hardware needed to run the service. In this case, the majority of the control plane is managed by the customer which leaves them responsible for meeting compliance requirements, and this is where Uptycs can assist.

CONTAINER AND KUBERNETES COMPLIANCE

The Uptycs agent is well-suited to workloads in the cloud, including workloads running in container services such as AWS Elastic Container Service (ECS) and managed Kubernetes environments such as AWS Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS), and Google Kubernetes Engine (GKE). Uptycs collects information from both the workload itself and the Kubernetes orchestration layer. This streaming telemetry enables customers to continuously assess their compliance with standards such as the CIS Benchmarks for Docker and Kubernetes.



Uptycs analyzes telemetry from your Kubernetes systems to continuously monitor compliance against the CIS Benchmark for Kubernetes.

For containers, Uptycs is able to gather a wealth of system telemetry for ingestion, analysis and storage, to give you instant insight into the relationships among nodes, containers, and images in your deployment. Where applicable, you'll be able to dig into the details of specific systems and check their compliance posture against the CIS Benchmarks for Linux and Docker.

Additionally, Uptycs stores data even after a container is decommissioned. This allows auditors to get data and answer questions about historical activity like executed commands, network connections, and API events.

USER-DRIVEN SECURITY

User-driven security is a new approach to endpoint compliance that enlists employees in securing their own devices. Most employees want to do their part in keeping company assets secure—user-driven security empowers them to do so.

With Uptycs' user-driven security, administrators implement security policies for employee workstations while a Slack integration works with users to remediate issues. "Otto M8" is a friendly security chat bot on Slack that prompts device owners to fix issues, providing step-by-step guidance on how to update their device configurations according to policy.

Along with improved visibility into device security for administrators, Uptycs' user-driven security subtly improves employee security awareness. Each security alert not only provides instructions, but also context as to why this issue is important from a security perspective.

Read more:

- [Uptycs 15-Minute demo: Mac and user-driven security](#)
- [Why you need to embrace user-focused security](#)

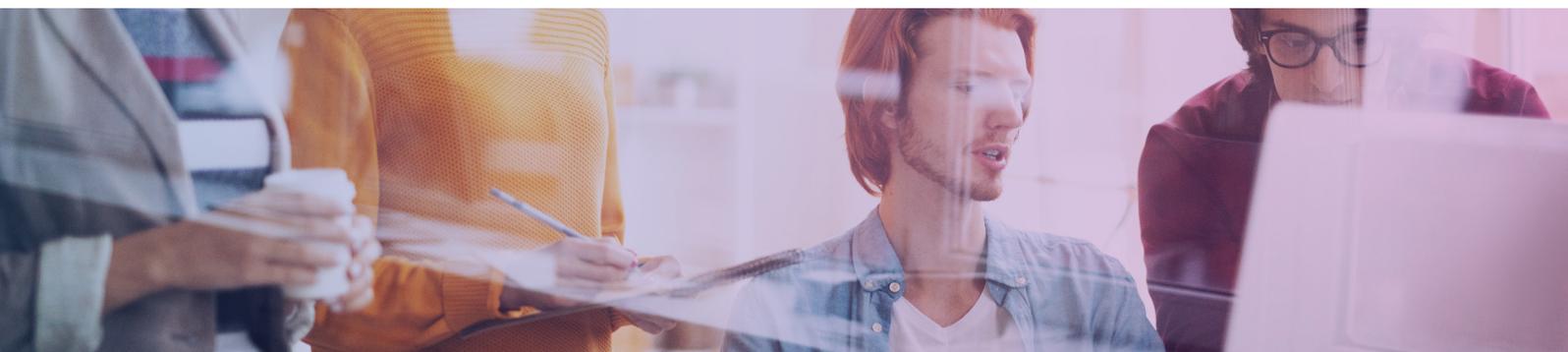
INTEGRATING UPTYCS WITH YOUR EXISTING REPORTING AND ANALYTICS SYSTEMS

No technology solution will provide much value if it doesn't work with your existing systems and workflows. Uptycs offers generous APIs so that your organization can get the most out of the solution:

- Create tickets in ServiceNow or other ITSM platforms for remediating misconfigurations
- Send compliance and audit evidence to business analytics and reporting tools
- Feed behavioral detections to a SIEM platform for alerting and correlation with other data

ADDITIONAL UPTYCS USE CASES

In addition to IT compliance, many organizations use Uptycs to enhance their cybersecurity posture and provide visibility to IT operations teams. Because the Uptycs platform provides flexible access to telemetry from endpoints and cloud environments, various teams can quickly answer questions that come up in the course of threat detection, incident response, IT asset inventory, and other important use cases. Uptycs offers role-based access control so that members of various teams can access the information that is relevant to their jobs.



The screenshot displays the Uptycs detection interface for a specific alert. The top navigation bar shows the title "Detection - Process using tar utility on hidden directory - ..." and a search bar. Below the navigation, the interface is divided into several sections:

- Threat score:** 10/10
- Toolkit Data:** DELTA68
- Summary:** 60 Signals, 14 Alerts, 46 Events. Timestamps: Jun 16th 2021, 1:50:46 pm and Jun 16th 2021, 2:05:46 pm.
- Asset info:** Online, Ubuntu 18.04.5 LTS (Bionic Beaver), user: uncle.
- ATT&CK Matrix:** A grid showing the MITRE ATT&CK framework with a path highlighted in red.
- DETECTION GRAPH:** A complex flowchart showing the sequence of events leading to the alert. It includes categories like Process (139), File (111), Socket (28), Lateral Movement (1), Registry (0), and DNS Lookup (0).

Security analysts can quickly understand the context of alerts, with the ability to drill down into suspicious activity and answer critical questions.

CONCLUSION

By providing continuous compliance capabilities, Uptycs simplifies evidence gathering and reporting for compliance, saving time for your IT staff and ensuring that the business moves forward on solid footing. The wide-ranging endpoint telemetry made accessible in Uptycs facilitates a number of IT audit and compliance use cases, including file integrity monitoring, software inventory, vulnerability detection, and enforcing policies on workstations and servers. The platform can be deployed at scale in a matter of days, providing continuous visibility into IT compliance posture.

Special thanks to Kuntal Mukherjee of Comcast, whose *Endpoint compliance at your "fingertips"* presentation at osquery@scale 2021 provided many ideas and examples for this white paper.



