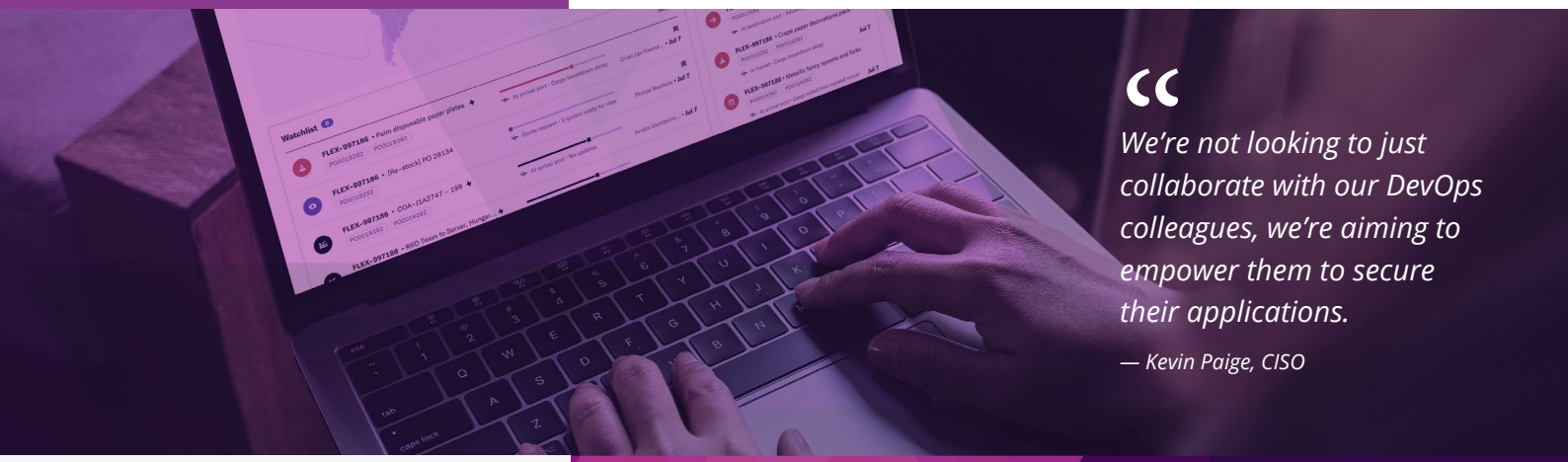
Uptycs

CUSTOMER CASE STUDY



> *We're not looking to just collaborate with our DevOps colleagues, we're aiming to empower them to secure their applications.*
>
> *— Kevin Paige, CISO*

flexport.

Flexport Empowers DevOps Teams with Security Observability

Deployment

- 12 AWS accounts
- 1,500 endpoints including laptops and AWS-hosted server workloads

Benefits Summary

- Improved cloud security posture
- Security observability for multiple teams
- Risk assurance for clients

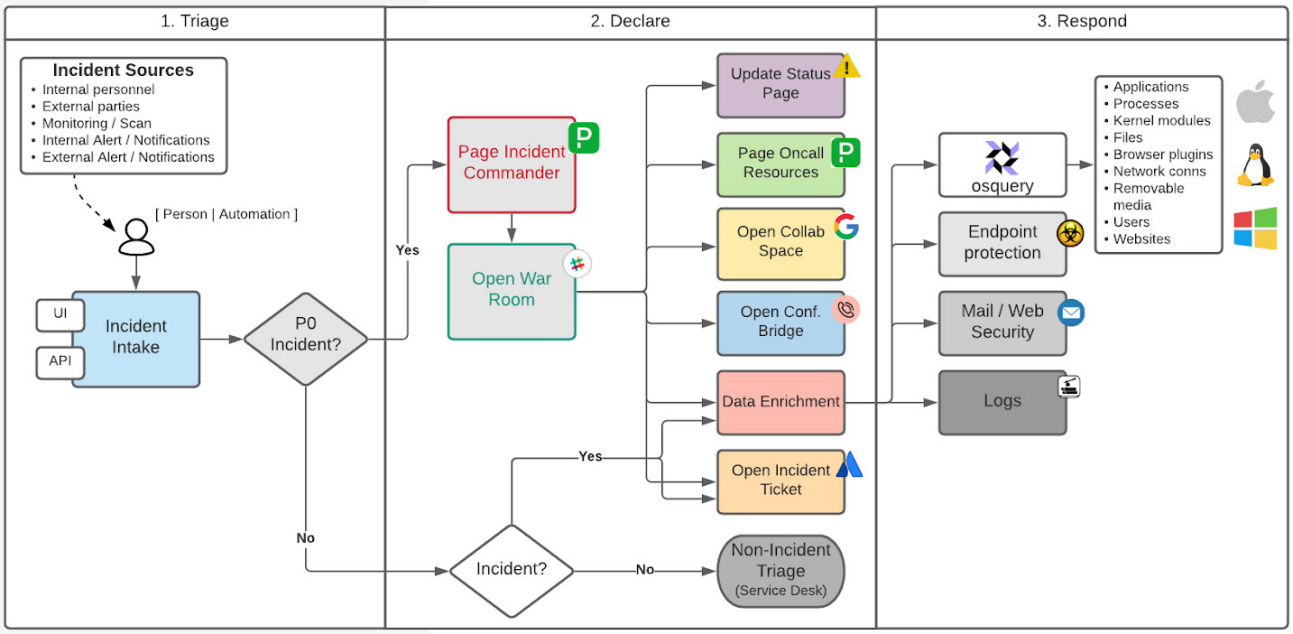
Flexport is the platform for global logistics. Companies of all sizes—from emerging brands to Fortune 500s—use Flexport technology to optimize their supply chain and deliver for customers anywhere in the world.

Challenge

Flexport has big goals. A leader in logistics, the company is building a technology platform to make global trade easy for everyone. That means working with a number of partners in the broader freight ecosystem—and ensuring that everything is highly secure.

That's why Flexport CISO Kevin Paige is thinking outside of the box. "We're not looking to just collaborate with our DevOps colleagues, we're aiming to empower them to secure their applications."

To this end, Flexport replaced its incumbent cloud security posture management (CSPM) product with the Uptycs Cloud-Native Security Analytics Platform because it provided holistic visibility across multiple AWS accounts and serves as a basis for broader security observability.



The Uptycs Security Analytics Platform is an integral part of detection and investigation workflows at Flexport.

> *The security team at Flexport owns the Uptycs deployment, but the solution is providing value to the entire organization.*
>
> *— Kevin Paige, CISO*

Solution

The goal is to provide developers with a "golden pathway" for building and deploying code securely, with the flexibility to deviate when needed in a safe manner. When something goes wrong, alerts are directed to the application owners, along with context, so that they know how to remediate relevant issues.

"Uptycs collects a vast amount of real-time telemetry from our infrastructure and workloads and makes it available for analysis immediately," says Taylor Merry, Director of Security Operations at Flexport.

Uptycs integrates with Flexport's AWS accounts to ingest telemetry data from CloudTrail, EC2, S3, and other resources. As it streams into the Uptycs cloud platform, the data is analyzed in flight so that Merry's team can easily see the asset and resource inventory across AWS accounts, what resources failed specific CIS Benchmark checks, and vulnerable configurations.

Flexport also uses Uptycs for its macOS and Windows fleets, aggregating telemetry from developers' laptops for audit, detection, and investigation. Flexport is expanding visibility into DevOps by deploying Uptycs agents to its Linux server workloads running as EC2 instances and containers on ECS and deploying an Uptycs sensor for EKS telemetry. This deployment adds security telemetry from inside the workloads themselves, such as resource utilization, processes running, and network connections, and telemetry from the orchestration layer.

"With Uptycs, we can gather security telemetry from attack surfaces across our entire ecosystem and have it normalized and accessible through SQL tables," explains Merry. "This enables our analysts and application owners to quickly answer questions that span different domains without having to find the right person to ask or collecting more entitlements to find those answers themselves. Access to this data in one place unlocks context that enables better alerting and incident response. For example, if a security group on an EC2 instance is listening on port 22 for 0.0.0.0., that's not a concern if it's not exposed to the Internet. But with visibility inside the host, we can also check to see if the SSH is also running on the endpoint. That ability to quickly get context is key."

> *For so many issues, our answer is 'Go to Uptycs.*
>
> *— Taylor Merry, Director of Security Operations*

Impact and Results

Unified visibility in a single tool

When security staff have a single tool to cover a variety of areas, it improves productivity, says Merry. "For so many issues, our answer is 'Go to Uptycs.' This improves efficiency because we can consolidate knowledge in fewer tools. Our security operations analysts can focus on one toolset and interface," he explains.

Improved cloud security posture

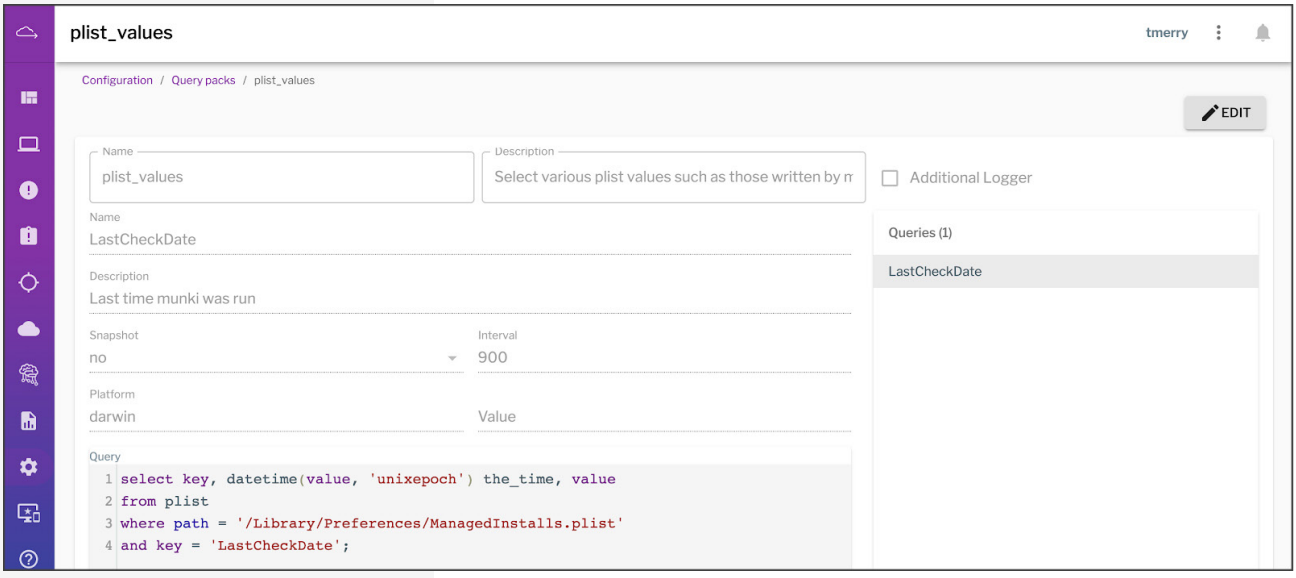
With Uptycs, Flexport can quickly identify and remediate vulnerabilities in their cloud infrastructure and applications. The security operations team automates workflows so that issues are sent to the right individuals and teams, with the right contextual information needed to remediate fast.

"Uptycs gives us broad visibility across our assets, so we know what is out there and how it is being used. We can understand what controls to put in place to protect those assets," explains CISO Paige.

Security observability for multiple teams

Besides the security operations team, multiple teams at Flexport use Uptycs to get answers. Cloud infrastructure engineers get cloud asset inventory and configuration information, compliance teams provide reports to auditors, and service desk staff answer questions about laptops and workstations.

"The security team at Flexport owns the Uptycs deployment, but the solution is providing value to the entire organization" says Paige.



Here's one example of how the IT team at Flexport uses Uptycs. This query gathers the execution times for the software update process on endpoints.

Developers and IT staff at Flexport have read-only access to Uptycs, allowing them to answer questions about the configuration of AWS resources or analyze how their workloads operate in production without direct console access to those systems.

Risk assurance for clients

Flexport is able to answer client questions about security because Flexport teams can easily assess compliance posture for infrastructure and workloads (in real time and for specific periods of time in the past). If a customer asks how something is done, Flexport has the capability of showing them with concrete evidence.

"Our goal is to become the most trusted supply chain partner," says Merry. "We want our clients to be excited about our platform, but also have confidence that they can entrust us with sensitive information."

About Uptycs

Uptycs provides the first unified, cloud-native security analytics platform that enables both endpoint and cloud security from a common solution. The solution provides a unique telemetry-powered approach to address multiple use cases—including Extended Detection & Response (XDR), Cloud Workload Protection (CWPP), and Cloud Security Posture Management (CSPM). Uptycs enables security professionals to quickly prioritize, investigate, and respond to potential threats across a company's entire attack surface.

Want to learn more?

A free trial of Uptycs can be requested at www.uptycs.com/free-trial