uptycs

flexport.

Flexport Empowers DevOps with Unified CNAPP and XDR

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

Company
Flexport

Champion
Kevin Paige, CISO

Taylor Merry, Director
of Security Operations

Computing Environment
- 80 AWS accounts
- 600 Amazon ECS containers and 4,800 Amazon EC2 instances
- 3,600 macOS, 600 Windows, and 240 Amazon WorkSpace endpoints

Challenge

Flexport has big goals. A leader in freight forwarding and supply chain management, the company wants to build a technology platform that will make global trade more efficient. 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."

Solution

Flexport replaced its incumbent cloud native product with Uptycs. Uptycs has helped the company provide developers with a "golden pathway" for building and deploying code securely, with the flexibility to deviate in a safe manner when needed.. When something goes wrong, alerts are directed to application owners, along with context, so 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 Uptycs, the data is analyzed in flight so Merry's team can easily see the asset and resource inventory across AWS accounts, as well as which resources failed specific CIS Benchmarks, or have vulnerable configurations.

Flexport also deployed Uptycs agents to its Linux server workloads running as Amazon EC2 instances and containers on Amazon ECS. This deployment adds security telemetry

Challenges

- Empower developers to secure their applications
- Consolidate tooling for better security visibility and productivity
- Show customers and auditors evidence of how Flexport protects sensitive data

Uptycs Results

- Uptycs provides developers with a "golden pathway" for building and deploying code securely
- Having a single tool to cover a variety of areas improves their productivity
- Uptycs creates easy, comprehensive reports to show customers and auditors

coming from inside the workloads, such as resource utilization, running processes, and network connections.

Flexport has deployed Uptycs agents to its macOS and Windows fleets to gather telemetry from developers' laptops for audit, detection, and investigation on those machines—including 240 virtual desktops running on AWS WorkSpace.

"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 multiple domains. 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 workload, we can also check if SSH is also running on the endpoint. That ability to quickly get context is key."

Benefits

Unified CNAPP and XDR

When security staff has 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 with 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 its cloud infrastructure and applications. The security operations team automates workflows so issues are sent to the right individuals and teams, with corresponding contextual information needed for fast remediation.

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

Security visibility for multiple teams

In addition to security operations, 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.

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 having direct console access to those systems.

Risk assurance for clients

Flexport is able to answer client questions about security because its teams can easily assess compliance posture for infrastructure and workloads, both in real time and historical states via Uptycs Flight Recorder. If a customer asks how something is done, Flexport can show them the evidence. "Our goal is to become the most trusted supply chain partner," says Merry. "We want our clients to be excited about our platform and have the confidence that they can entrust us with sensitive information."

About Uptycs

Uptycs, the first unified CNAPP and XDR solution, 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