uptycs

PayNearMe

Payments Technology Company PayNearMe Tames Asset Management with Uptycs

"The pre- and post-Uptycs worlds are vastly different regarding visibility and the security comfort level of our fleet."

Sean Todd
Chief Information Security Officer

Company
PayNearMe

Champion
Sean Todd, CISO
Princeton Baker,
Enterprise Security Engineer

Laptop Fleet:
macOS and Windows productivity endpoints

Cloud Environment:
AWS

PayNearMe Handles Billions of Dollars of Electronic Payments Annually

PayNearMe develops technology that drives better payment experiences for businesses and their customers. The platform helps businesses increase customer engagement, improve operational efficiency, and drive down the total cost of accepting payments. Originally launched in 2009 to process cash payments through retail stores, PayNearMe now processes billions of dollars annually via all major payment types—cards, ACH, cash and mobile-first payment methods including Apple Pay, PayPal, Venmo, and Google Pay.

Uptycs Helps Manage Assets

Maintaining a clean and consistent computing environment is critical for a financial services company. Thorough laptop hygiene on productivity laptops used by the PayNearMe workforce is under the purview of Chief Information Security Officer Sean Todd. "When this was a smaller company, it was easy to manually keep tabs on the laptops," he says. "As we grew, it became difficult to keep track of all our devices, especially with people operating in different locations. We needed a technology solution to help manage our assets."

"As head of security for a financial services company, I'm personally liable for anything that goes wrong security-wise. Having Uptycs to assure me that things are going right helps me sleep better at night."

Sean Todd
CISO

Security Challenges

- Visibility into laptop configurations was low and couldn't scale to support more devices
- Need to support a number of regulations and industry standards (e.g., PCI, CIS, SOC)
- Want to use osquery but not run it themselves
- Need deep information for incident response

Uptycs Security Results

- Uptycs Inventory and Insights management screen provides deep information at a glance
- The time to respond to compliance audits is minimized
- Uptycs's support of osquery enables gathering extensive data and running custom queries on it
- Custom queries and data correlation shorten the time to respond to incidents

Unlike many security tools that use a proprietary method for gathering and exposing security telemetry, osquery is an open source instrumentation framework for Windows, OS X (macOS), and Linux. It exposes an operating system as a high-performance relational database. SQL queries can be written to explore OS data such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events, and file hashes. Uptycs extended this approach by taking osquery to cloud infrastructure, Kubernetes, and identity and SaaS providers.

"Uptycs looked like a good solution based on its inclusion of osquery," says Todd. "Even as an early stage security company at the time we adopted it, Uptycs had the interface that we needed. It's not just a shiny dashboard—its technical layer lets us write and run SQL queries against our laptop fleet in near real time."

Uptycs Exposes More Useful Data Than Competitors

Enterprise security engineer Princeton Baker is a regular Uptycs user as he cares for the laptop fleet. "I'm using the tool at least three or four times a day to verify compliance configurations and respond to alerts," he says. "We distribute our laptops with certain configurations. If something changes, or if someone turns off a firewall, we receive alerts. If we are alerted about malicious or unapproved software, we can locate exactly where that resides within the device file structure. Other vendors might not report these issues in a timely manner, if they even report them at all."

Baker speculates, "My daily activities would be harder without Uptycs. It would take up most of the week just to do simple compliance checks." Todd concurs. "I was at the company before we implemented Uptycs. Every time Apple would send out a macOS update, it took a month of asking each user, 'Did you update yet?' I had no way of verifying that updates were actually done."

Baker appreciates that Uptycs provides the ability to run queries on the data they already have and to gather additional data based on those same queries. For him, the most valuable feature is the Uptycs Inventory and Insights screen showing assets under management. "I can see everything at a quick glance," Baker says. "I see the OS version, where the user is located, if the system name has changed, if there are new assets that aren't being accounted for, or if there is a random asset that shouldn't be there. It's all I need to keep track of our assets."

> ***"A lot of vendors collect data from the endpoints but don't provide access to run queries on it which limits our ability to manage our fleet. Uptycs gives us access to all the data so we can write our own queries and answer questions that arise."***
>
> **Princeton Baker**
> Enterprise Security Engineer

Todd cites another important aspect of having the asset information. "A big thing today in the security industry is a software bill of materials (SBOM). What's included in each app? Having the list of browser plugins, homebrew things and apps installed—all of that data gives us a new level of asset inventory that's becoming increasingly more critical."

Faster Incident Response

Incident response is a primary Uptycs use case. "Perhaps someone downloads something suspicious, or a malicious program has been run," says Baker. "We can run a query to find whatever it is. It's easy to correlate data if you have an asset that's contacted a malicious site. Then you've learned that external IP address with the potential malicious software or downloaded file. Given this kind of information, Uptycs enables us to respond to incidents faster."

Without Uptycs, Baker says he'd be dependent on end users to report that something is wrong; he'd have to then run a manual investigation process that is cumbersome and time consuming.

Easing Compliance Efforts

Uptycs is proving its worth when it comes to privacy, risk and compliance at PayNearMe. "We often won't get every piece of evidence auditors want ahead of time," says Todd.

> ***"In the middle of an audit, I might be asked for an exported list of all laptops. I'll randomly pick ten and need to know, 'Is the firewall turned on?' 'Is the password enabled?' Being able to run such queries quickly always impresses our auditors."***
>
> **Sean Todd**
> CISO

Extending Uptycs to AWS and Kubernetes Containers

PayNearMe's applications are hosted on AWS. The company is just getting into the realm of Docker containers and microservices, and as it does so, it's working toward integrating Uptycs into its server infrastructure as well as its laptops. "We've plugged Uptycs into a couple of demo containers," says Todd. "I'm hoping it can help us validate that every container is performing correctly, especially pertaining to regulations and industry standards we have to adhere to."

An Uptycs advantage is that the same product can run on endpoints as well as in the cloud. It's easy to deploy in any environment and yields more telemetry data than other security solutions.

PayNearMe has conquered its laptop management challenges. Now it's onto the cloud to maintain control of the k8s containers.

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