Customer Case Study

uptycs

Payment Processor Streamlines Threat Detection and Response

> *"We can detect really, really fast: 0.7 seconds from execution to Uptycs detection, and 1.6 seconds from execution to case management alert."*
>
> **Security engineer**

Company

SaaS company

Deployment

- Over 2,000 macOS workstations
- 15,000 Ubuntu Linux servers on AWS

Benefits Summary

- Security observability at scale
- Analyze behavioral changes or anomalies
- Detection-as-code automation

This global financial services and software as a service (SaaS) company builds economic infrastructure for the Internet. It enables businesses of all sizes to use its software to accept online payments. And it provides application programming interfaces (APIs) that web developers use to integrate payment processing into their websites and mobile applications.

Challenge

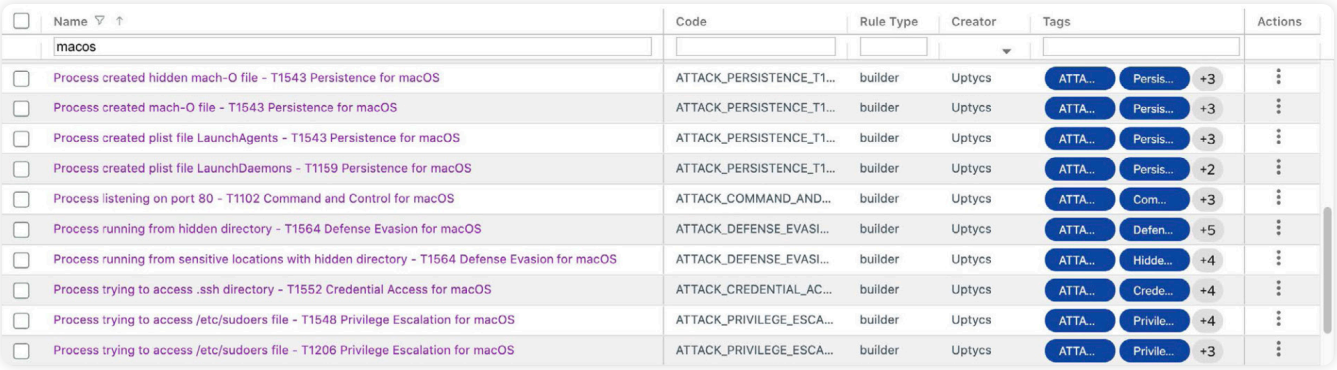
As a fast-growing organization processing billions of dollars in transactions, risk reduction is of paramount importance to this payment solution vendor. Its team prioritizes security observability across all of their deployment environments with the goal of automating threat detection and response workflows.

Solution

The threat operations teams wanted to understand how users were behaving observe behavioral changes on Macintosh machines used by remote employees—which they view as a leading indicator of malicious activity.

They needed a customizable solution to proactively hunt for threats, create custom detection rules, and orchestrate their internal response. Uptycs provided visibility into all 2,000 macOS endpoints, enabling them to detect intrusions, monitor vulnerabilities, and track configuration compliance. Now the security engineering team cloud to ingest telemetry at scale, investigate stored data as needed, intercept endpoint telemetry in flight, and take action within seconds. Such speed-to-insight translates directly to risk reduction, a key focus for the company's security and reliability teams.

Once the company had visibility into all of its endpoints, it sought to enhance security for its production server fleet to it had easily-tunable detection logic. Using Uptycs for workload telemetry, it pushed queries through Puppet and logs stored in AWS S3 it then forwarded to Splunk. Its team of engineering-centric pros built tools to help them understand the threat spectrum in the wild, and Uptycs helped it gather the required information to write reactive detections and do proactive threat hunting.



Name	Code	Rule Type	Creator	Tags	Actions
macos					
Process created hidden mach-O file - T1543 Persistence for macOS	ATTACK_PERSISTENCE_T1...	builder	Uptycs	ATTA... Persis... +3	
Process created mach-O file - T1543 Persistence for macOS	ATTACK_PERSISTENCE_T1...	builder	Uptycs	ATTA... Persis... +3	
Process created plist file LaunchAgents - T1543 Persistence for macOS	ATTACK_PERSISTENCE_T1...	builder	Uptycs	ATTA... Persis... +3	
Process created plist file LaunchDaemons - T1159 Persistence for macOS	ATTACK_PERSISTENCE_T1...	builder	Uptycs	ATTA... Persis... +2	
Process listening on port 80 - T1102 Command and Control for macOS	ATTACK_COMMAND_AND...	builder	Uptycs	ATTA... Com... +3	
Process running from hidden directory - T1564 Defense Evasion for macOS	ATTACK_DEFENSE_EVASI...	builder	Uptycs	ATTA... Defen... +5	
Process running from sensitive locations with hidden directory - T1564 Defense Evasion for macOS	ATTACK_DEFENSE_EVASI...	builder	Uptycs	ATTA... Hidde... +4	
Process trying to access .ssh directory - T1552 Credential Access for macOS	ATTACK_CREDENTIAL_AC...	builder	Uptycs	ATTA... Crede... +4	
Process trying to access /etc/sudoers file - T1548 Privilege Escalation for macOS	ATTACK_PRIVILEGE_ESCA...	builder	Uptycs	ATTA... Privile... +4	
Process trying to access /etc/sudoers file - T1206 Privilege Escalation for macOS	ATTACK_PRIVILEGE_ESCA...	builder	Uptycs	ATTA... Privile... +3	

Uptycs applies streaming analytics to endpoint telemetry to detect real-time threats.

Impact and Results

Security at scale

"When you're operating at scale, it's arguably just as likely that you break your own systems as a bad actor breaks them for you," says the security engineer. "You'd better make sure you've configured your agent properly and added safeguards and response tools in case of emergency."

The security engineering team worked with IT operations and reliability teams to ensure Uptycs provided the information to meet requirements for threat modeling while minimizing the risk of altering the production infrastructure. Uptycs empowered this FinTech company to ingest telemetry at scale, take action on telemetry in flight, and keep its payments systems safe through proactive threat hunting.

Analyze behavioral changes and anomalies

Uptycs helped the threat operations team set a baseline to define what normal looks like in its systems and environment by using a series of queries and analysis. This makes it simpler for it to find unusual or unwanted product use. It was then able to create reactive detections based on the company's teams, people, time zones, and work hours. This is one way in which Uptycs helps the security teams perform proactive threat hunting.

Detection-as-code automation

Using Uptycs, Python, and SQL, the security operations team simplified and codified its detection strategy, and build a framework that incorporates automation, metrics, reliability, and threat intelligence. The visibility across all endpoints and baseline information on environments empowers it to correlate, augment, and confirm Uptycs findings with other tools to scale the entire security program with programmable detections.

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