Uptycs

CUSTOMER CASE STUDY

> *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*

SaaS Company

Payment Processor Streamlines Threat Detection and Response

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 allows businesses of all sizes to use the company's software to accept online payments and 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 processing solution vendor. The team prioritizes security observability across all their deployment environments with the goal of automating threat detection and response workflows.

0 selected

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	
Process trying to access bash history - T1552 Credential Access for macOS	ATTACK_CREDENTIAL_AC...	builder	Uptycs	ATTA... Bash ... +4	
Process trying to access cron entries - T1053 Execution for macOS	ATTACK_EXECUTION_T10...	builder	Uptycs	ATTA... Execu... +4	
Process trying to access hidden directory - T1564 Defense Evasion for macOS	ATTACK_DEFENSE_EVASI...	builder	Uptycs	ATTA... Defen... +4	
Process trying to access Keychains - T1552 Credential Access for macOS	ATTACK_CREDENTIAL_AC...	builder	Uptycs	ATTA... Crede... +4	
Process trying to access TCC.db File - T1548 Privilege Escalation for macOS	ATTACK_PRIVILEGE_ESCA...	builder	Uptycs	ATTA... Elevat... +4	
Process trying to load/unload kernel modules and extensions - T1547 Persistence for macOS	ATTACK_PERSISTENCE_T...	builder	Uptycs	T1547 ATTA... +4	

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

> *My team is responsible for building the tools that security analysts use to detect and stop bad guys.*
>
> *— Security Engineer*

Solution

Specifically, the threat operations teams wanted to understand how users were behaving and any behavioral changes on the Mac machines used by their remote employees, something they view as a leading indicator of malicious activity within the organization.

They needed a customizable solution that allowed them 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 for their fleet. Now the security engineering team was able to ingest telemetry at scale, investigate stored data as needed, intercept endpoint telemetry in flight, and take action on it within seconds. This speed-to-insight translated directly to risk reduction, a key focus for the security and reliability teams at this organization.

Once the company had visibility into all of their macOS endpoints, they moved on to enhance security for their production server fleet and ensure that they had detection logic that was easily tunable. Using Uptycs for workload telemetry, they pushed queries through Puppet and logs stored in AWS S3 and forwarded to Splunk. The team of high-caliber engineeringcentric professionals focused on building tools to help them understand the spectrum of threats in the wild, and Uptycs helped them to gather the information necessary to write reactive detections and do proactive threat hunting.

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 baddie breaks them for you," said the security engineer. That's why he believes, "You'd better make sure that you've configured your agent properly and added safeguards and response tools in case of emergency."

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

Analyze behavioral changes and anomalies

Uptycs helped the threat operations team set a baseline and define what normal looks like in a system or environment, using a series of queries and analysis. This baseline made it simpler for them to find unusual or unwanted product usage and create a detection for it based on their teams, people, time zones, and work hours.

Detection-as-code automation

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

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