uptycs

Customer Case Study

Integrated Endpoint and Cloud/Server Workload Protection

> This Uptycs customer is a provider of mobile applications to millions of consumer and enterprise subscribers.

Industry

SaaS

Deployment

- OGreater than 4,000 Linux Servers
- Over 400 MacOS Laptops

Benefits Summary

- Unified Solution for MacOS & Linux
- End-to-End Visibility
- Seamless API Integration
- Security @ Scale

Summary

The customer is a cloud-native company, operating a fleet of Linux servers on AWS for services delivery and a fleet of MacOS laptops for employee productivity. The customer provides a well-known mobile app for Android and iOS. Operating at a scale of over 4,000 servers and over 400 Macs, they were looking to build an in-house security solution based on osquery. After experiencing the challenges of an osquery DIY-solution, they agreed to start a pilot after seeing an Uptycs demo and went into production after the pilot. The modules and functionality provided by the Uptycs Security Analytics Platform met their Linux server security visibility and MacOS endpoint detection requirements. Additionally, the customer was able to focus its limited internal resources on securing the MacOS fleet and AWS servers, rather than building an in-house solution.

Challenge

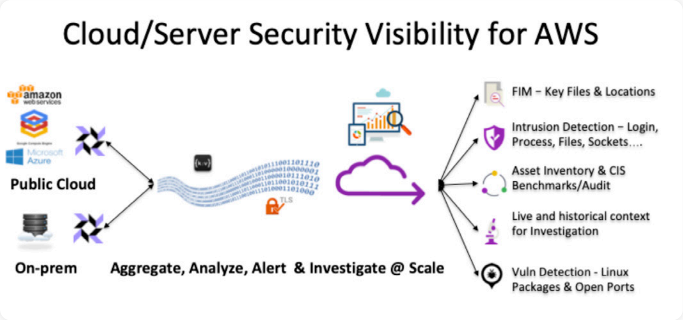
The customer's anti-virus deployment was not giving them sufficient security visibility on their MacOS fleet. On their servers, they were reliant on sys logs, audit and scripts to scrape and forward data into a log-aggregation-based SIEM. Being a true cloud-native organization, the IT and the technical operations teams collaborated on a universal endpoint agent, a common backend aggregation, and a single console for security visibility. API-based integration into their existing workflows and slack integration collaboration were key attributes of the desired solution. Finally, after experimentation with OSSEC (HIDS agent), they decided to standardize on osquery, focusing on root-kit detection, compliance/audit capabilities, and FIM support.

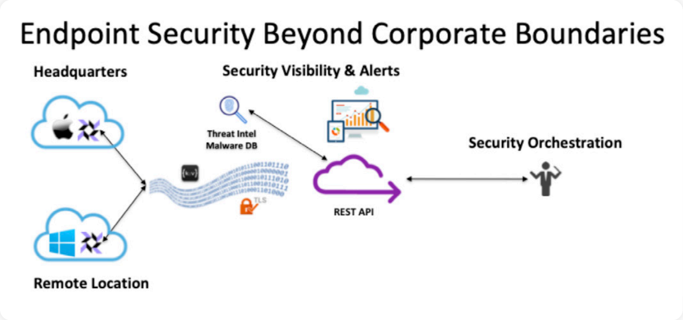
Modules

- Uptycs Core
- Uptycs Detection
- Uptycs Investigation
- Uptycs FIM
- Uptycs Flight Recorder
- Uptycs Audit & Compliance

Why Uptycs?

- **Comprehensive:** Universal Open-source Agent - Osquery
- **Scale:** Endpoint Detection Network (EDN)
- **Visibility:** Streaming Analytics
- **Context:** Purpose-built flight recorder
- **Open:** API-First approach
- **Standards:** SQL-powered analytics


Cloud/Server Security Visibility for AWS
amazon web services
Microsoft Azure
Public Cloud
On-prem
Aggregate, Analyze, Alert & Investigate @ Scale
TLS
FIM – Key Files & Locations
Intrusion Detection – Login, Process, Files, Sockets….
Asset Inventory & CIS Benchmarks/Audit
Live and historical context for Investigation
Vuln Detection - Linux Packages & Open Ports



Solution

The customer worked with Uptycs to finalize osquery as the agent of choice. To get there, Uptycs ported OSSEC XML-based rules for rootkit detection to SQL-based query packs, developed higher fidelity FIM detection in osquery by leveraging kernel-based audit for richer context (e.g., who/what changed a file) vs. the OSSEC file-systembased inotify detection. The Uptycs Core module provided the scale to connect, manage and ingest data from thousands of Linux and MacOS endpoints at scale. To make this happen, Uptycs partnered with Apple and Microsoft to provide a signed osquery-agent package to ease and simplify deployment with JAMF (MacOS) and SCCM. Uptycs also provided a fully packaged DEB image with certificates and secrets preprovisioned for rapid deployment via AWS AMI and Chef (Linux). This reduced agent configuration, management and deployment from many weeks down to a few hours. The Uptycs Detection, Uptycs FIM, Uptycs Flight Recorder and Uptycs Investigation modules were configured for end-to-end security visibility into the customer server and endpoint fleets.

Impact & Results

Immediately after deployment, nothing is as assuring as knowing the Uptycs solution is busy at work detecting potential threats. In the case of this customer, within a short time they saw laptops downloading malicious payloads from an IP address with a known bad reputation.

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.