uptycs

Customer Case Study

Cloud/Server Workload Protection Supporting FedRAMP Certification

This Uptycs customer is a major SaaS-based customer relationship management services provider.

Company
SaaS Company

Deployment
- Greater than 500 Linux servers for the initial FedRAMP deployment

Benefits Summary
- Unified solution for security and compliance
- Rapid FedRAMP enablement
- End-to-End Visibility
- Operational Simplicity

Summary

The customer was in need of a security and compliance solution to support their FedRAMP certification for delivering a dedicated SaaS platform to a large Federal Government agency. Within a three-month window of engagement, the **Uptycs Security Analytics Platform** provided the necessary functionality to meet the criteria established by the auditors for FedRAMP certification. Specifically, the solution addressed Intrusion Detection, Auditing, Linux CIS Benchmarks, and over 25 key controls for FedRAMP compliance and certification. With Uptycs-provided security and compliance controls in place, the customer was able to go into production in a timely manner to deliver services to the Federal Government agency.

Challenge

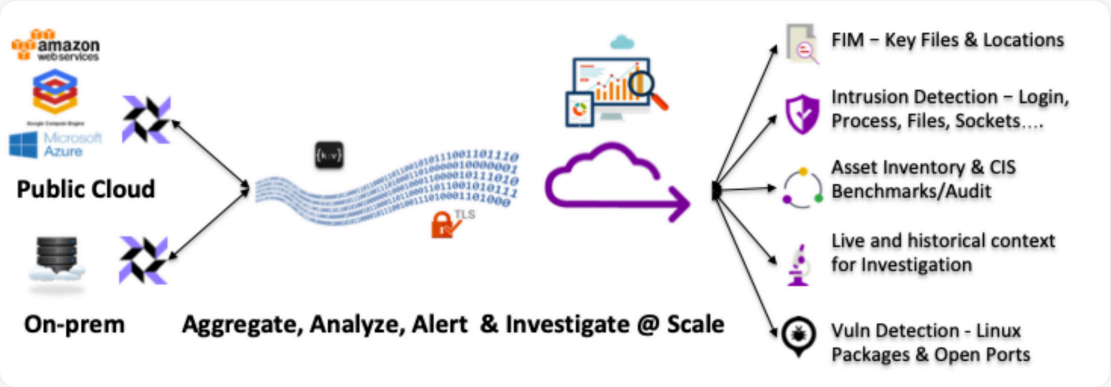
The customer provides a popular SaaS-based software integration services platform. The customer won a contract from the Federal Government to provide its dedicated SaaS platform to one of its large agencies. The Federal Government mandated that the customerprovided SaaS platform be delivered from a specialized AWS GovCloud VPC along with audit certification for FedRAMP compliance. With a significant contract at stake and a short timeline, the customer had to stand up solutions for endpoint detection, ad-hoc auditing and investigation, and to demonstrate FedRAMP specific controls. Finally, the entire solution had to work in the confines of an AWS GovCloud environment isolated from the Internet.

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



Solution

The customer had familiarity with FedRAMP standards and was looking to Uptycs to provide a unified solution for security and compliance to achieve certification from their FedRAMP auditors. First, the **Uptycs Security Analytics Platform** was instantiated in the customer's AWS GovCloud-based VPC. The customer then worked with Uptycs to operationalize the **Uptycs Core** module to connect, manage and ingest data from all Linux server endpoints at scale. The **Uptycs Detection** and **Uptycs FIM** modules were configured to provide intrusion and malicious activity detection to establish baseline security support for FedRAMP certification. The **Uptycs Flight Recorder** and **Uptycs Investigation** modules then provided real-time visibility along with the ability to rewind history to audit the state of thousands of servers at any arbitrary time in the past. Uptycs supplied query-packs, along with customized Augeas lens, that provided a structured data and historical evidence collection mechanism to enable over 25 different FedRAMP specific Linux server controls.

Impact and Results

The customer was able to secure and comply with the FedRAMP standards in a short window of three months. The Uptycs Security Analytics Platform security and compliance controls gave FedRAMP auditors the necessary confidence to certify the customer's solution toward FedRAMP Ready status. This enabled the customer to close a multi-million dollar contract with the Federal Government, get into production, and realize revenue in a timely manner.

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