UiPath Leverages Reco For Data Exposure Management And Automation

UiPath is a Robotics Process Automation (RPA) company that develops AI technology that mirrors human intelligence. With ever-increasing sophistication, UiPath is transforming how businesses operate, innovate, and compete by automating digital tasks. The UiPath Platform™ accelerates the shift toward a new era of agentic automation—one where agents, robots, people, and models integrate seamlessly to drive autonomy and smarter decision-making.

Before Reco

UiPath ends repetitive tasks for their customers and makes digital transformation a reality through their software robots. As they embarked on their journey to leverage robots to secure their own SaaS environment, they were having difficulty understanding the level of data exposure from numerous shared drives, and exposing critical data to unauthorized access in the process. This is where Reco came in.

The first step was to gain an understanding and manage the level of data exposure from critical SaaS shared drives, including Microsoft OneDrive, Microsoft SharePoint, and Google Drive. This is a common problem for many companies, as over-privileged access increases the risk of data leakage. However, gaining a full understanding of UiPath's SaaS environment was proving impossible with the native Microsoft security tools, notably their Microsoft Sentinel SIEM.

In other words: UiPath has the platform that enables automating the business process to remove access and reduce data exposure risks, and Reco has the ability to inform those robots of where they should go to work.

> ***In order to secure SaaS applications and manage their data exposure, you must first be able to see the full picture,"*** Reco's CEO, Ofer Klein, said. ***"UiPath understood this very fundamental idea, and found Reco's data exposure management to be exactly what they needed for their own automation robots to manage through their SIEM without exposing themselves to more risk***

Data Exposure Management & Automation at Scale

Once Reco was hooked in, UiPath was immediately able to gain visibility into over-privileged data access to exposed files across SharePoint, OneDrive, and Google Drive. Reco's context alerts fed into UiPath's SIEM, and then allowed their automations to appropriately triage and act to reduce their exposure risk. Data owners were automatically contacted and access was removed following the principle of least access. This saved the UiPath team thousands of hours of manpower removing access to critical data files.

This data feed also goes both ways. As UiPath leverages Reco's real-time data access management, Reco also uses UiPath's software automations to reduce exposure automatically by pushing alerts received in Sentinel from Reco to the UiPath platform. The automations can then respond to the alert, and send a notification to Sentinel once fixed.

The Results with Reco

With Reco, UiPath gained context into who has access to the data, its location, as well as who exposed it. This data is crucial to accurately automate remediation without disruptions to the business. This process is now ongoing as Reco sends alerts to Microsoft Sentinel of publicly exposed data located in SharePoint, OneDrive, and Google Drive. UiPath is now gaining more value from their Microsoft Sentinel SIEM as they can centralize logs from tools and tailor the visibility as their environment and business needs grow.

> ***We knew the power and capabilities of our robots, and how they could make our Sentinel SIEM more powerful. By automating the access removal process by passing Reco's contextual detections to our SIEM, we have saved thousands of hours of work, reduced the risk of data exposure across multiple SaaS shared drives, and now continue to reduce data exposure risks. By gaining the intelligence needed to secure our data, we continue toward our constant goal of making digital transformation a reality in this partnership"*** UiPath CIO, Mihai Faur.

As more and more organizations move to SaaS applications for their everyday business needs, getting a full, ongoing view of their data exposure risks has become a foundational piece of their security puzzle. By pairing this with layers of automation, data exposure and access management—a Sisyphean task when done manually—can now be triaged and handled at scale.

About Reco

Reco is an identity centric SaaS security solution. It empowers organizations with full visibility into every app, identity, and their actions to seamlessly prioritize and control risks in the SaaS ecosystem. Their AI based graph technology connects in minutes and provides immediate value to security teams to continuously discover all SaaS applications including sanctioned and unsanctioned apps, associated identities from both humans and machines, their permission level, and actions. Reco uses advanced analytics around persona, actions, interactions and relationships to other users, and then alerts on exposure from misconfigurations, over permission users, compromised accounts, and risky user behavior. This comprehensive picture is generated continuously using the Reco Identities Interaction Graph and empowers security teams to take swift action to effectively prioritize their most critical points of risk.