Third-Party API Security with Vorlon

SPONSORED BY

A SANS First Look

Written by **Jason Jordaan** | May 2024

Introduction

Modern organizations are often complex ecosystems. With increased usage of cloud-based Applications as a Service, more and more organizations are making use of third-party services to provide specific functionality to support their overall information systems architecture. These systems are often integrated into organizational information systems through specific APIs.

Not only do these third-party services store and process organizational data that an organization is still accountable for in terms of data protection, but the APIs used can potentially expose other systems within an organization to risk. The adage, "You can delegate responsibility, but you cannot delegate accountability," very much rings true. Just because you are making use of a third-party application, that doesn't mean your organization can simply pass the accountability to the third-party vendor for your data and systems.

In this SANS First Look, we examine Vorlon, a platform that enables proactive security of your third-party application ecosystem. Vorlon has the ability to detect and respond to third-party application security incidents and to ensure compliance with laws, regulations, and rules when it comes to third-party API risks.

The First Look

The first thing we noticed is Vorlon's user interface is clean and neat. We feel that it is important to be able to find what you need easily, which can be achieved with Vorlon's very intuitive and functional interface. Vorlon has researched the APIs of various third-party application vendors to understand how they work and what data is available from them. At the time of this paper, it can monitor approximately 70 popular third-party apps (and growing). Most of these apps would be considered "business critical" because they are likely to house or have access to sensitive information.

Using Vorlon is very intuitive. You start by selecting what applications you want to monitor from a catalog and then provide Vorlon authorization to connect to that app. This allows Vorlon to observe how that app is communicating with other apps and systems in your information system. It identifies the data used by those apps as well as the secrets that app uses (OAuth, API keys, and so forth). It ingests logs automatically, parses out the data, provides alert correlation rules, alerts when a rule is matched, and provides step-by-step responses for each type of alert.

Vorlon is not monitoring the vendor application in general, but is monitoring one's instance of the application, as well as connections from well over 1,000 fourth-party applications. For example, if you have a Salesforce.com tenant, Vorlon monitors this and identifies other known applications connecting to your Salesforce tenant in addition to unknown and unidentified applications. When Vorlon identifies unknown or unidentified applications, these are added to a backend database and identified for appropriate future identifications. There are three core areas where Vorlon really shines: compliance and data protection, visibility into third-party APIs, and threat detection and incident response.

Compliance and Protecting Your Data

Using third-party apps means essentially trusting these apps with your data. Vorlon provides a clear understanding of what compliance standards a particular app must meet, and provides risk scoring for that particular app. This allows an organization to make clearly informed risk management decisions regarding the use of that app (see Figure 1).

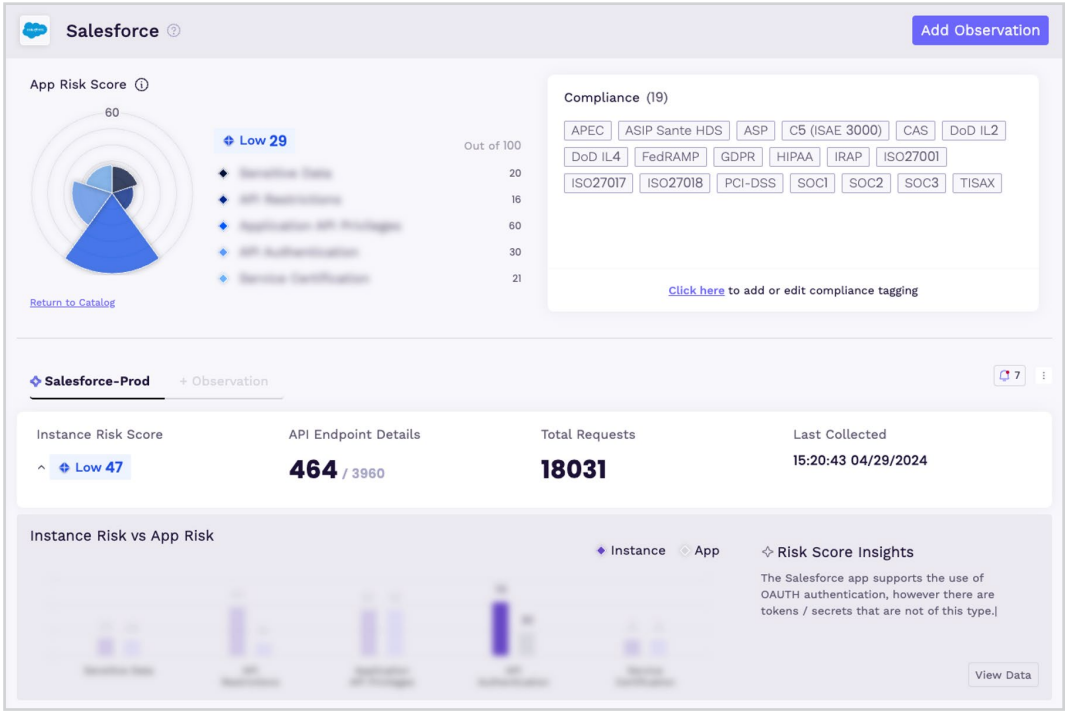

Figure 1. Vorlon Risk Scoring

Vorlon also allows you to see exactly what data—particularly what sensitive data—is being used by a given app. Knowing what data is being used is a crucial part of being able to protect it. The advantage of having Vorlon continuously monitoring your data in third-party applications is that it allows you to always stay up to date with the data you share with the application, while your vendors keep changing their APIs, providing a point-in-time versus near-real-time view.

What we really appreciate is that Vorlon also monitors itself. As a third-party app, it provides insight into what it does from a compliance perspective. This transparency is much appreciated. Vorlon also provides detailed logging of everything done within the platform, further enhancing transparency.

Visibility of Your Third-Party API Ecosystem

One of the things Vorlon does impressively is provide a comprehensive insight into the third-party API ecosystem an organization is using. Not only does it provide details of each application, it also shows the relations and interactions between them (see Figure 2).

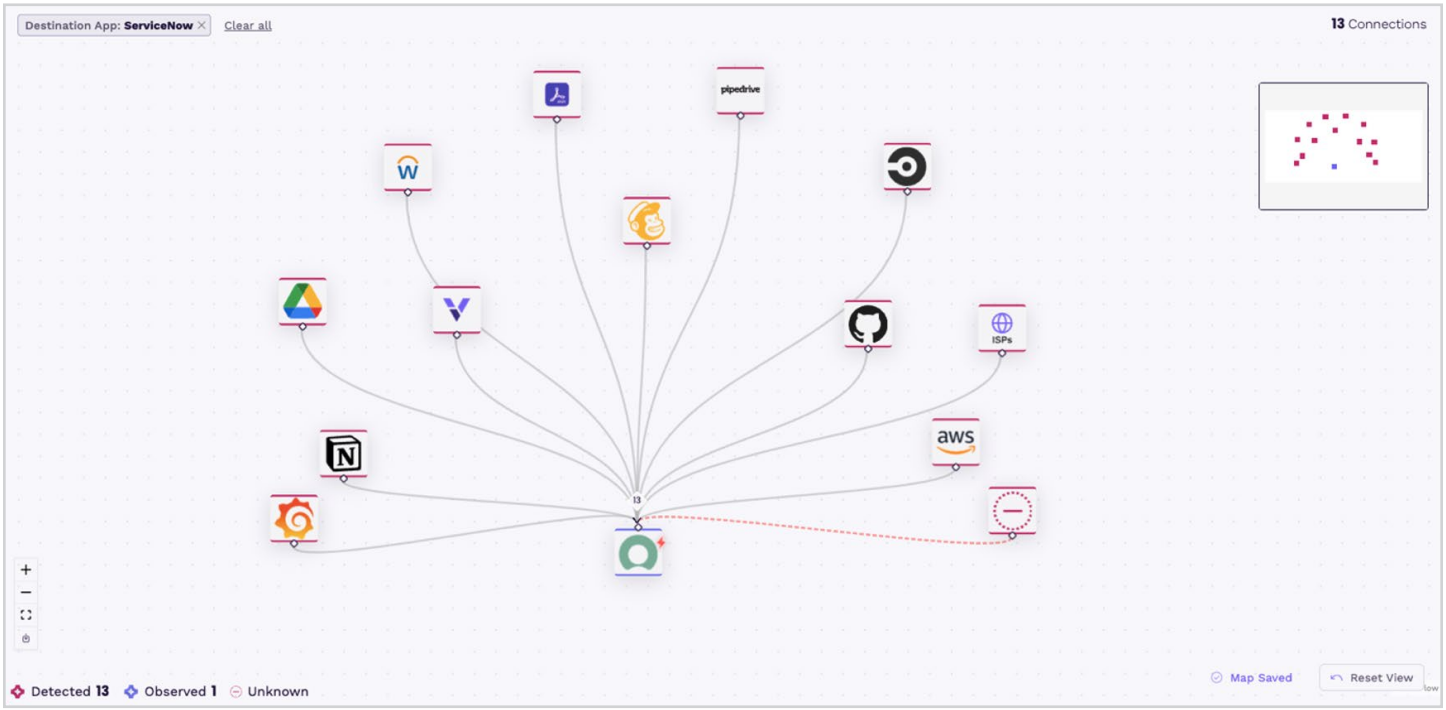

Figure 2. View of a Third-Party API Ecosystem

By monitoring the interactions and communications, Vorlon can see what type of data is being shared, allowing the platform to observe when applications have access to excessive sensitive data. What is also important to bear in mind is that the application in the observed application is not actually exposed or visible to Vorlon. Vorlon's real-time monitoring of all API traffic, both to and from, allows a clear picture of what data is being pulled by the app and essentially to whom the app is talking.

Also impressive is the visual map of the app ecosystem that clearly identifies areas of concern and alerts for an organization to act upon.

Threat Detection and Incident Response

Vorlon does an impressive job of detecting potential threats related to third-party apps based on developed rules and behavioral anomalies. When a potential threat or risk has been identified within Vorlon, an alert is sent (see Figure 3). In addition, Vorlon is customizable and can connect to your current security applications and implemented process to raise alerts or take actions, for example, with your existing SIEM, SOAR, or ITSM.

The alert clearly identifies the potential threat with sufficient detail to allow a user to make an informed decision regarding how to respond to it. Vorlon also provides step-by-step recommendations about how to remediate. As digital forensics practitioners and incident responders, we are often put in the position of having to make recommendations about how to respond to a security incident, and we must consider how our response actions impact the overall organization. Vorlon provides a useful capability in this regard. If we must essentially revoke a secret used by an app to address the immediate incident, Vorlon identifies what other apps also make use of the same secret within the ecosystem, so you can immediately see what other apps within the ecosystem would be exposed to a supply-chain attack or might be impacted by revoking the secret. This allows security teams to make an informed risk management decision.

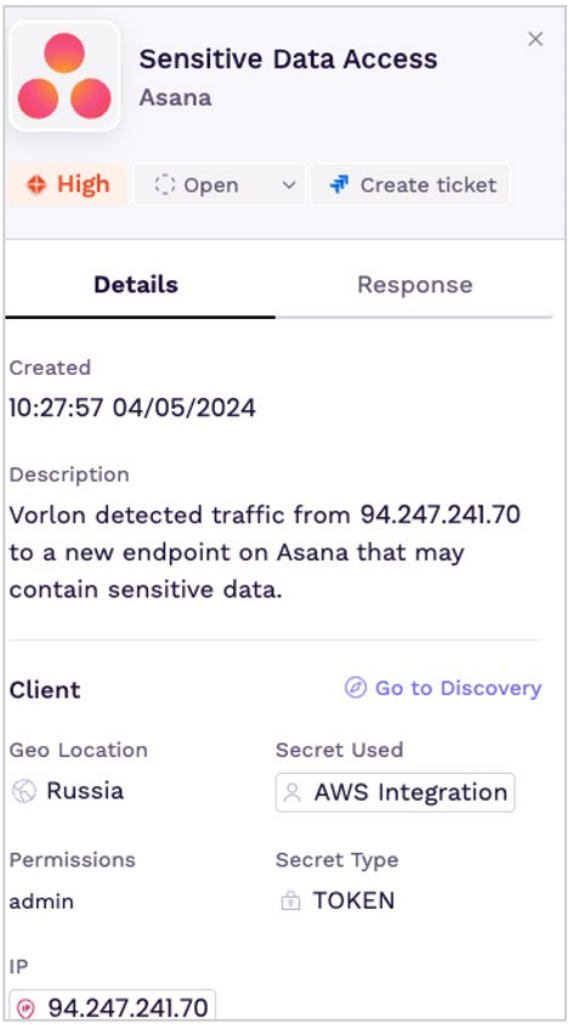

Figure 3. Vorlon Alert

Takeaways

Vorlon is an impressive platform that provides much needed security visibility to organizations using third-party apps and their APIs, while at the same time providing real-time monitoring and alerts. It provides many useful features for an organization, from managing compliance and risk within their third-party application ecosystem to identifying security risks and empowering an organization to appropriately respond to and remediate risks.

Sponsor

SANS would like to thank this paper's sponsor:

vorlon