SW LABS

Product Review | Intrigue

Produced by SW Labs, a Security Weekly Resource

CyberRisk ALLIANCE

SecurityWeekly

SC MEDIA

About

Contents

Company background

Intrigue is the brainchild of Jonathan Cran, who formerly held various product and research roles at Rapid7, BugCrowd and Kenna Security. Cran has been quietly working on Intrigue for several years. In November 2020, he made the move to working on Intrigue full time and founded Intrigue as a company in Austin, Texas. On April 13, 2021, Intrigue announced a $2 million seed round led by LiveOak Venture Partners. Along with this funding, new pricing and a roadmap have also been announced (details below).

SW Labs Product Review | Intrigue

Product summary

While some ASM products left us wondering where the details were and other products buried us in discovered assets with no prioritization, Intrigue strikes a solid balance between the two. If you want details, down to the raw data used to discover an issue, Intrigue has that. If you have three minutes before your next board meeting and need to know where your orgs stand, this tool has your back there as well.

We're reviewing the Professional Edition of Intrigue here, but it's worth mentioning that there is also an Enterprise Edition for organizations that need to monitor more than 5,000 external assets. The Enterprise Edition removes the 5,000-asset cap and provides a higher level support plan.

A free, open-source Community Edition (also known as Intrigue Core) exists for those on a tight budget or any organization that have a hard "no SaaS" rule when it comes to security products (which seems increasingly rare). This option can be useful for technically savvy folks that only need to run the occasional one-time collection. For example, penetration testers and other consultants that don't require monitoring, ticketing integration, teams and other enterprise features.

Target market: Intrigue will work well for mid-to-large enterprises that don't have the time, skills or resources to perform regular reconnaissance manually on their own assets. While the automation helps to monitor and manage exposed assets, it doesn't replace the recon role on the security team. Someone experienced in understanding and managing the findings is still necessary to manage the tool and its output.

Time-to-value: As a SaaS product, there's no heavy lifting to get the product up and running. Creating collections (which allow you to logically group results) takes seconds. Expect a few hours before initial results show up and up to a few days for more comprehensive results. The only real deployment work is creating alerts, integrating with external ticketing and communications tools and inviting other team members. All told, this should be less than an hour's worth of work.

Maintaining value: For a mid-sized Enterprise (hundreds, not thousands of exposed assets), expect to initially spend 8-16 hours digging through the initial results on first use. Once everything is sorted, expect to spend 2-4 hours per week to review new findings as they trickle in. This is ideal work for a junior analyst.

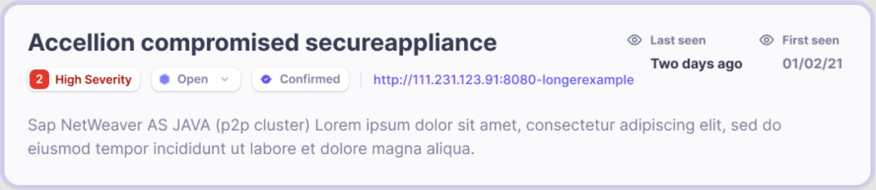
Total cost: For the Professional Edition, the subscription cost is $15,000 annually. In a mid-sized enterprise (100-2,000 employees), we've estimated four hours of junior analyst time, two hours of analyst time and one hour of senior analyst time to do the initial analysis of Intrigue results and configuration of the tool. Based on our average salary estimates, this labor totals $302.87. For ongoing analysis work, we've estimated two hours of junior analyst time per week, which totals $3,499.60 per year. The total cost to use this product every year, including product cost and labor comes to $18,802.47.

Strengths: Intrigue is a newcomer in this market, making this an ideal time for early customers and investors to weigh in, provide feedback and help shape the future product. Even for an early release, Intrigue is more than capable for production use. Intrigue is one of only two ASM vendors in this space with flexible alerting features.

Weaknesses: As an early product just following a major release, some features aren't yet available or fully baked. Plenty of room for improvement with regards to asset attribution. This is a challenge all ASM vendors struggle with and is one of the main tasks analysts will undertake when maintaining Intrigue's findings.

Conclusion: A solid choice from a relative newcomer that is just getting started.

Deployment and configuration



Accellion compromised secureappliance

2 High Severity | Open | Confirmed | http://111.231.123.91:8080-longerexample

Last seen: Two days ago

First seen: 01/02/21

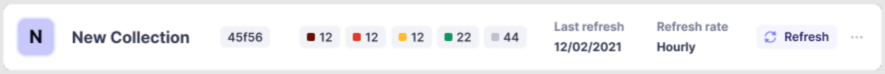
Sap NetWeaver AS JAVA (p2p cluster) Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Figure 1 – Excluding third party assets

Each Collection has its own individual settings. While the ability to manage notifications at the Collection level is ideal, the lack of an option to manage multiple Collections, er… collectively, means a dozen Collections will require repeating the same configuration process a dozen times.

Aside from creating the initial collections and notification settings, there isn't much to configure. That's a good thing – a good ASM product shouldn't require a ton of settings management or dial-twisting.

Usage



N New Collection 45f56 ■ 12 ■ 12 ■ 12 ■ 22 ■ 44

Last refresh: 12/02/2021

Refresh rate: Hourly

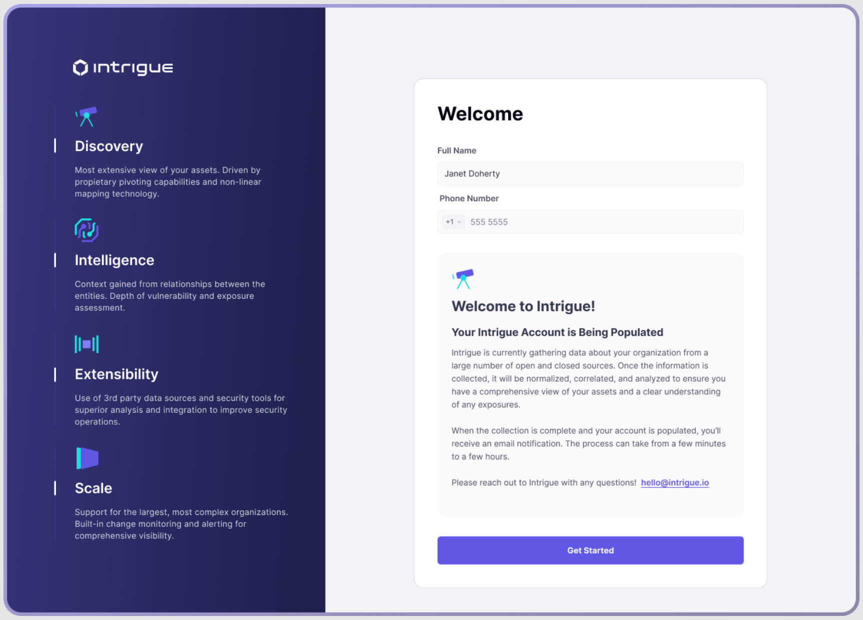
Figure 2 – Excluding third party assets

Getting initial results should take less than an hour, even for large organizations. Once collections have been configured, it can take up to 48 hours for collection to complete. While Intrigue does have pre-scanned collections on tens of thousands of companies (that can be queried with an additional license), for most customers, collection will run on-demand.

The initial view we're presented with is the Issues tab, which makes sense. If you want to maximize your time using this tool, Issues will automatically show you the most critical findings, across all your collections by default. From here, you can filter on one or more collection, on issue status (like a ticketing system, the options are open, in progress or closed), severity or confidence. That las filter option indicates whether the finding is confirmed or if it can't be fully verified. This is reminiscent of some vulnerability management vendors, which also separate findings into 'potential' and 'confirmed' categories. For example, if Intrigue finds dev.acme.com, it will create a low severity finding called "Development System Identified" and labeled as "potential."

The Entities tab is a list of all the individual attack surface elements discovered for a given collection. Entities are further broken down into 16 types, which include AWS S3 Buckets, DNS records, Email Addresses, IP Addresses, GitHub Accounts, SSL Certificates and many more. Finally, the Collections tab can be used to create and manage collections. Collections aren't limited to your organization, either — they can be used to monitor third parties as well. This tab also includes a summary for each collection. The summary includes the raw number of entities and a breakdown of issues by severity.

Click on any of the Collections to manage the seed values that fuel the discovery engine or to configure notifications.



Discovery

Most extensive view of your assets. Driven by propietary pivoting capabilities and non-linear mapping technology.

Intelligence

Context gained from relationships between the entities. Depth of vulnerability and exposure assessment.

Extensibility

Use of 3rd party data sources and security tools for superior analysis and integration to improve security operations.

Scale

Support for the largest, most complex organizations. Built-in change monitoring and alerting for comprehensive visibility.

Welcome

Full Name
Janet Doherty

Phone Number
+1 555 5555

Welcome to Intrigue!

Your Intrigue Account is Being Populated

Intrigue is currently gathering data about your organization from a large number of open and closed sources. Once the information is collected, it will be normalized, correlated, and analyzed to ensure you have a comprehensive view of your assets and a clear understanding of any exposures.

When the collection is complete and your account is populated, you'll receive an email notification. The process can take from a few minutes to a few hours.

Please reach out to Intrigue with any questions! hello@intrigue.io

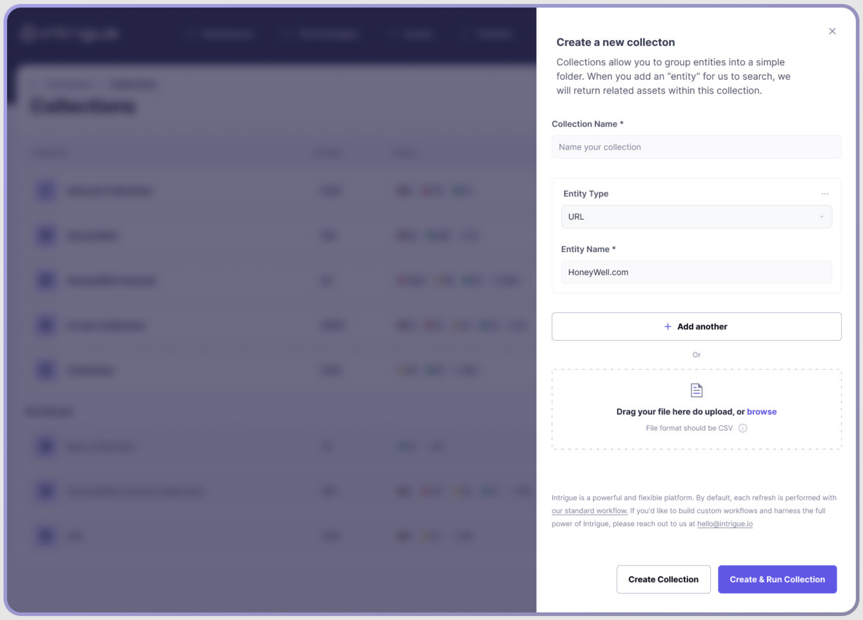
Figure 3 – Excluding third party assets

Getting into the details

As with all ASM products we're testing (aside from the open-source projects), Intrigue is a SaaS application. All the technical, gritty details of collecting data are handled behind the scenes. The benefit, as with any SaaS app, is very little setup time.

Registering for an account is the same as any other SaaS application. A welcome message invites the operator to start a collection on the domain tied to the registration email. (Note: though this screenshot is from the previous Intrigue UI, the process remains the same.)

What results is a grouping of attack surface data Intrigue refers to as a Collection. Each collection can be tied to a team, allowing for some access control between teams that manage different portions of an organization's assets.



Create a new collecton

Collections allow you to group entities into a simple folder. When you add an "entity" for us to search, we will return related assets within this collection.

Collection Name *

Name your collection

Entity Type

URL

Entity Name *

HoneyWell.com

+ Add another
Or
Drag your file here do upload, or browse
File format should be CSV

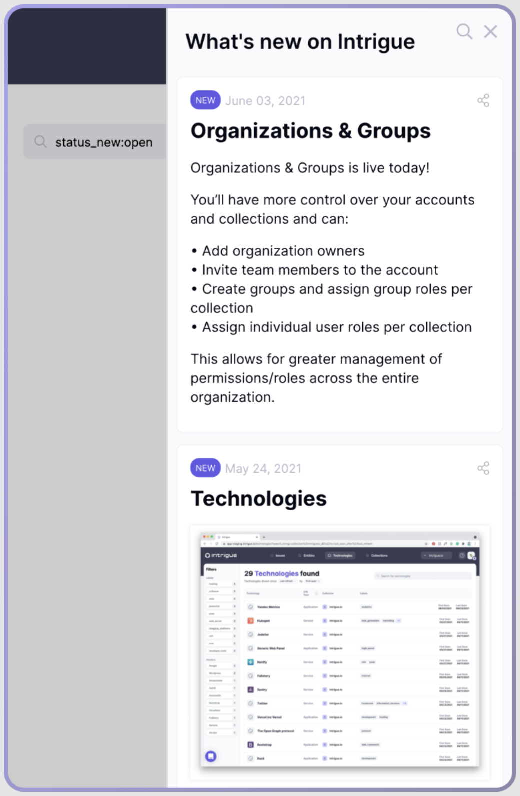
Intrigue is a powerful and flexible platform. By default, each refresh is performed with our standard workflow. If you'd like to build custom workflows and harness the full power of Intrigue, please reach out to us at hello@intrigue.io

Figure 4 – Excluding third party assets

While the examples in these screenshots show collections based on domains, collections can also be based on IP addresses, subdomains, name servers, network blocks, Github accounts or even just a company's name. Collections can be added in bulk using a simple, two-column CSV format (type, value).

Intrigue will send an email once the initial collection is complete (notification via webhook or Slack channel is also an option). Following this initial collection, additional notifications will be sent whenever new assets are discovered or existing assets change.

Having tested these tools using CyberRisk Alliance properties, this is an example notification for the SC Media collection Slack integrated alert.



status_new:open

What's new on Intrigue

NEW June 03, 2021

Organizations & Groups

Organizations & Groups is live today!

You'll have more control over your accounts and collections and can:

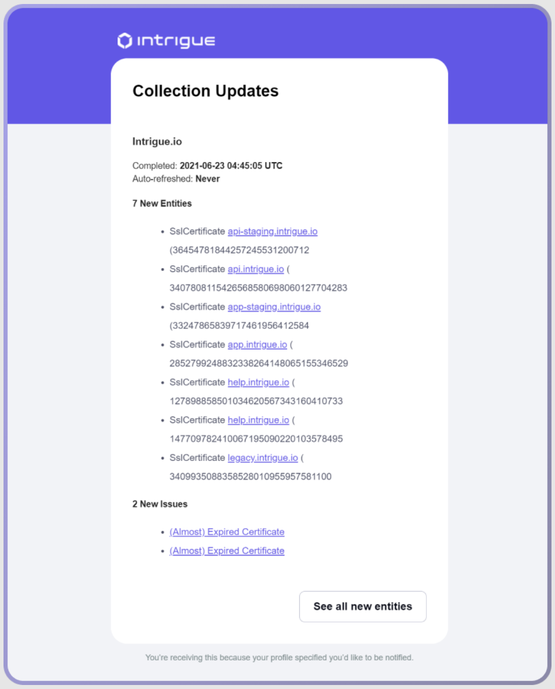
- Add organization owners
- Invite team members to the account
- Create groups and assign group roles per collection
- Assign individual user roles per collection

This allows for greater management of permissions/roles across the entire organization.

NEW May 24, 2021

Technologies

Figure 5 – Excluding third party assets



Collection Updates

Intrigue.io

Completed: **2021-06-23 04:45:05 UTC**
Auto-refreshed: **Never**

7 New Entities

- SslCertificate api-staging.intrigue.io (364547818442572455312007l2
- SslCertificate api.intrigue.io (340780811542656858069806012770428 3
- SslCertificate app-staging.intrigue.io (332478658397174619564l2584
- SslCertificate app.intrigue.io (285279924883233826414806515534652 9
- SslCertificate help.intrigue.io (127898858501034620567343160410733
- SslCertificate help.intrigue.io (147709782410067195090220103578495
- SslCertificate legacy.intrigue.io (340993508835852801095595758110 0

2 New Issues

- (Almost) Expired Certificate
- (Almost) Expired Certificate

You're receiving this because your profile specified you'd like to be notified.

Figure 6 – Excluding third party assets

Performance

While technical performance isn't a focus of this round of ASM product reviews, it's worth noting that Intrigue did discover some significant findings we were unaware of, regarding outdated components of web application platforms. The breadth and depth of findings matched other similar tools we tested. False positives were few and easily managed.

As ASM products mature, two performance metrics seem worth tracking: the completeness of discovery results and how quickly changes can be detected.

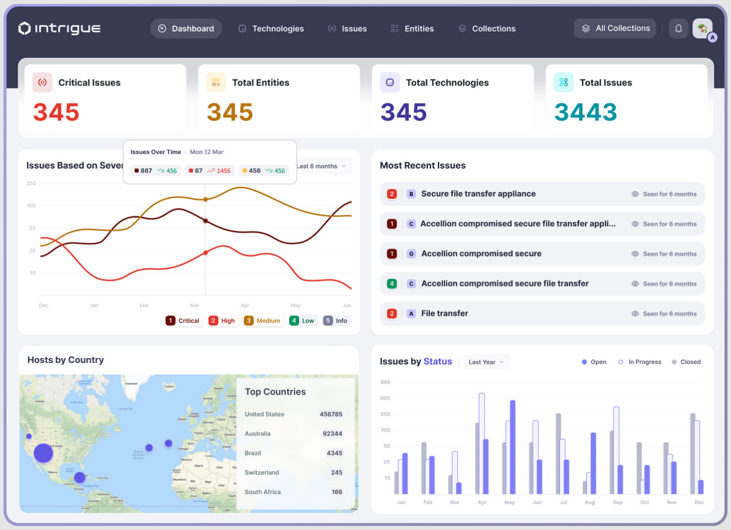
Roadmap

According to Intrigue, following the major release in mid-April 2021, a number of features will be added in the short term. It should be noted that a number of these existed in the previous release, so much of this is likely front-end and UX work, not new development from scratch.

Some of these features include:

- Tagging
- Team and Group Management
- Inclusion of vulnerabilities and typosquats to the Issues tab
- Export any search results
- Ability to search by technologies (e.g., show all entities running JQuery)
- Improved email notifications

Following is an example of what the new dashboard will look like (currently, the Dashboard and Technologies tabs are missing.)



Most Recent Issues

2 B Secure file transfer appliance — Seen for 6 months
1 C Accellion compromised secure file transfer appli... — Seen for 6 months
1 G Accellion compromised secure — Seen for 6 months
4 C Accellion compromised secure file transfer — Seen for 6 months
2 A File transfer — Seen for 6 months

Top Countries

United States	456785
Australia	92344
Brazil	4345
Switzerland	245
South Africa	166

Figure 7 – Dashboard

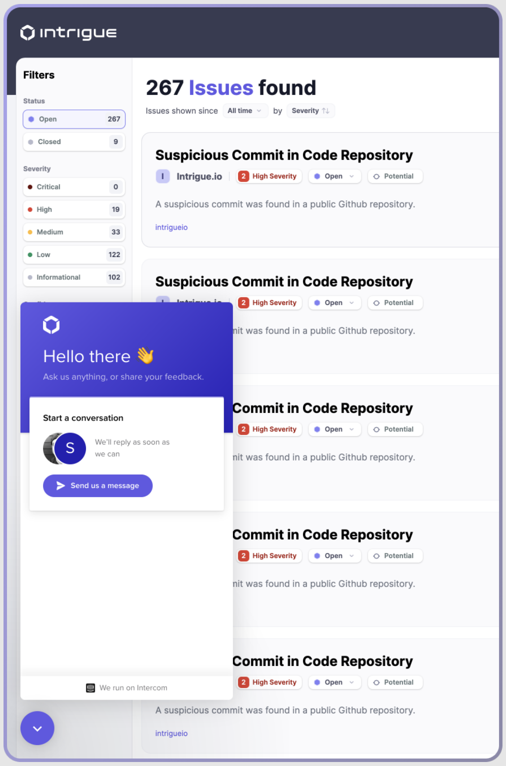
Support

Intrigue has a multi-faceted support model that scales to different customer sizes and needs. Traditional enterprise phone and email support is available, but for folks that prefer chat, there is an in-app chat option (see screenshot) and a Slack-based community forum.

Claims

The Intrigue tagline is "Know What You Own, What It's Running, and What It's Exposed To". The website goes on to say, "Intrigue provides you with a comprehensive view of your environment and actionable intelligence to mitigate risk."

Conclusion: Spot on, Intrigue's messaging says what it does and doesn't exaggerate capabilities or methods.



267 Issues found

Issues shown since All time by Severity

Status	
Open	267
Closed	9

Severity	
Critical	0
High	19
Medium	33
Low	122
Informational	102

Suspicious Commit in Code Repository
Intrigue.io | 2 High Severity | Open | Potential
A suspicious commit was found in a public Github repository.
intrigueio

Suspicious Commit in Code Repository
2 High Severity | Open | Potential
…nit was found in a public Github repository.

Commit in Code Repository
2 High Severity | Open | Potential
…nit was found in a public Github repository.

Commit in Code Repository
2 High Severity | Open | Potential
…nit was found in a public Github repository.

Commit in Code Repository
2 High Severity | Open | Potential
A suspicious commit was found in a public Github repository.
intrigueio

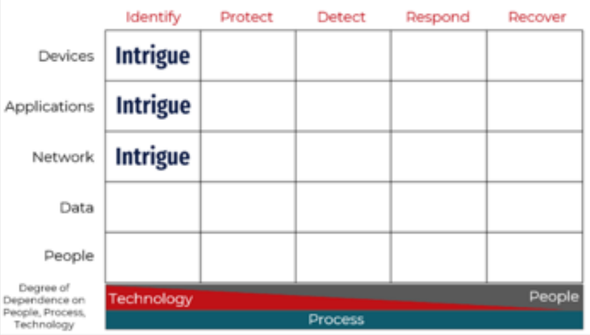
Hello there 👋
Ask us anything, or share your feedback.

Start a conversation
We'll reply as soon as we can

Figure 8 – Excluding third party assets.

Security Program Fit

Intrigue, like other products focused on discovering vulnerabilities and misconfigurations, fits solidly within the Identify column of the Cyber Defense Matrix.



	Identify	Protect	Detect	Respond	Recover
Devices	Intrigue				
Applications	Intrigue				
Network	Intrigue				
Data					
People					

Degree of Dependence on People, Process, Technology
Technology
People
Process

Figure 9 – Excluding third party assets.

SW Labs Product Review | Intrigue

Conclusion

Intrigue is a promising platform that is as capable as platforms with a two or more-year head start. Currently, Intrigue's engine is much more capable than its newly updated (and much more attractive) front-end. Based on past development speed, we doubt it will take more than a few months for the front end to catch up with the back end. Despite some temporarily missing features, it remains one of the most capable and usable ASM products on the market today.