Solution Brief

6 SaaS Discovery Methods + 1 Only Grip Does

Solution Brief

Business-Led IT Drives Technology Spending

The pace of business today requires companies to move quickly and adapt to changing market conditions. When the pandemic occurred, companies adapted quickly to a digital-first go to market model, and SaaS played a critical role in helping companies accelerate the transition. The increasing use of SaaS is expected to continue, and companies are expecting to shift more of their IT budget to SaaS spending over the coming years.

The adoption of SaaS during the pandemic is a great example of business-led IT helping companies become more agile and adapting to market conditions quickly. For most SaaS applications, the only thing needed is an email address, which can be upgraded to a low cost subscription when needed. Over time, employees can have hundreds of SaaS accounts, and we often see that during our proof of value engagements where we see many employees with 100+ SaaS accounts. Many are dormant or unused, but they may contain sensitive or confidential company information or data that should be secured also known as SaaS security.

SaaS Discovery: How Many SaaS Apps are Employees Using?

As employees use more SaaS, there is a need for companies to identify and know what applications are being used and who is using them. This becomes especially important when there is employee turnover so that IT/security can ensure that all access to corporate and business-related SaaS applications are deprovisioned or at least locked so the former employee loses access.

The need to know how much SaaS is in a company goes beyond just IT and security. Groups such as finance, human resources, and business managers all benefit from knowing how much SaaS is in their organization. Each of these groups have different objectives, they naturally adopt tools that help them accomplish their functional objectives. Finance is concerned with costs and budgets, so they look for tools that help lower subscription costs. The flexibility to use the app of choice affects employee morale, so human resources wants to know which apps are being used to let people have options. Business managers want to attract high performing talent, and they want people to know that they will be using the most efficient tools to help their teams be more productive.

Read more about SaaS Security: What is SaaS Security?

The Best SaaS Discovery Method

Because SaaS is no longer just an IT/security problem, there are multiple products on the market that are attempting to help companies discover and manage SaaS usage. Each product has a unique approach but uses one of seven standard discovery methods listed below. There are pros and cons to each of the methods. So to address the shortcomings, Grip has created a new discovery method that no other product in the industry uses.

7 SaaS Discovery Methods

1. CASB
2. API
3. Browser plugin
4. Expenses/Accounts Payable
5. Web Proxy
6. Single Sign On (SSO)
7. Grip's Method

CASB

Cloud access security broker (CASB) products were initially designed to "broker" the connections between an endpoint device and SaaS service. They are typically used to detect and control access to SaaS services and collect data by analyzing network traffic, data from an endpoint agent, or both. Since the CASB has access to the network connection, it is able to detect SaaS quickly.

The challenge with CASBs is the sheer volume of data that is generated. They are similar to web proxies, but since they were designed to identify SaaS, the data is easier to analyze. However, it is not always easy to distinguish a regular website vs. a SaaS site, so there are a high volume of alerts that need to be triaged by security analysts and false positives are common. Similar to a proxy, because it relies on network and endpoint data, CASBs are only effective for managed devices or when the device is on the corporate network.

Read more about CASBs: Pros and Cons of CASB for SaaS Security.

API

API discovery uses SaaS vendor provided API connections to discover users and usage. Many SaaS security companies use this method to also identify misconfigurations, vulnerabilities, or misuse of SaaS applications by users. Depending on the application, APIs may also be used to complete the remediation.

The downside to API SaaS discovery is that it requires setup and integration by IT, and it may require a more expensive enterprise license. This method also does not work well for new SaaS discovery and only works well for SaaS that has been identified. API SaaS integration is increasingly used to help understand configurations or other risks within the application. Because of the integration required, APIs are not very useful for inventorying all the SaaS apps being used by employees.

Agent or Browser plugin

Agents or browser plugins can be deployed to monitor or track new SaaS applications. Data can be gathered from an agent or plugin already deployed on each company device. This data can then be analyzed to identify SaaS application usage. Similar to other agent based solutions, the data from this approach can be overwhelming and result in a high number of false positives. This approach also only works for managed devices and would not work when an employee uses SaaS on their personal device.

Expenses/Accounts Payable

Integration with expense or accounting systems can help identify SaaS applications where the user has purchased a subscription. This is particularly useful for managing costs and reducing subscription costs by aggregating users to qualify for a volume discount or consolidate overlapping SaaS vendors. Some vendors who offer this type of product will also negotiate subscription prices with SaaS vendors as a value added service.

Using expense or accounting information to detect SaaS, however, is only useful for SaaS where the employee is paying for a subscription. Most SaaS applications have a free tier or a freemium model, and this approach would completely be unaware of those SaaS applications. Nearly every SaaS application does not require any sort of payment initially, and these would be completely invisible to this detection method.

Web Proxy

Web proxy products are deployed to secure employee Internet traffic by analyzing the website destinations. Based on a risk assessment of the site being visited, the proxy can restrict access, for example blocking known phishing or malware sites. SaaS discovery can be done using the data from a web proxy, but this is not their core functionality, and it requires extensive analysis and manual work.
With a reliance on network traffic, web proxies are not effective when the SaaS application is being used on a personal device or when the device is not connected to the corporate network. Many web proxies also require endpoint agents, and some vendors do have compatibility issues between their endpoint agent and some SaaS applications.

Single Sign On (SSO)

SSO is a good way to track and monitor SaaS usage and manage access to known applications. It provides a centralized access and control mechanism for the company to govern sanctioned SaaS applications.
SSO can become very expensive when it comes to SaaS governance. Most enterprise SaaS applications require an SSO license, which can be 3X the cost of a non-SSO license. In addition, it is only useful for known SaaS applications that have been integrated with the SSO product. It cannot help detect applications that employees are accessing outside of SSO.

Read more about SSO: 5 Reasons Your SaaS is not Connected to SSO

Grip's Method

Taking a step back and understanding the problem of SaaS discovery, Grip has developed a method that has the advantages of all the other discovery methods without the downsides. The Grip detection method involves a 15 minute deployment and delivers the following key features:

- Detects SaaS usage from any device (managed or unmanaged)
- Detects SaaS usage regardless of network connectivity (managed or unmanaged)
- Deprovisions SaaS access with one click for one employee or any number of employees
- No agent or browser plugin required
- No web proxy integration required
- No firewall integration required
- No SSO required
- No expense or accounting system integration required

The discovery method is extremely powerful and effective. During most proof of value engagements, Grip's platform discovers on average 5X more SaaS applications than a CASB. We often hear in meetings with CISOs, "This works like magic." It is not magic, but it is innovative technology. To learn more about Grip's SaaS Discovery method sign up for a FREE SaaS risk assessment today or download our SaaS security eBook.