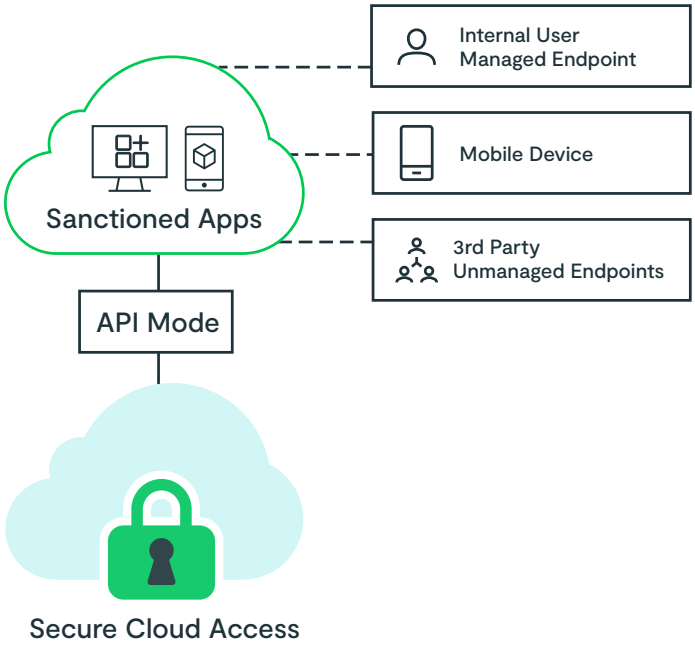
Lookout SaaS Risk Assessment

Overview

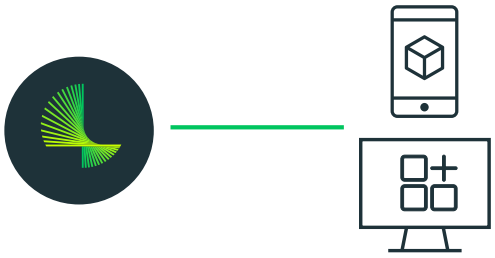
Every day your employees upload, download and share corporate data from your approved SaaS applications. This can create ongoing risk through data leakage, unauthorized sharing, regulatory violation or malware incursion. The Lookout SaaS Risk Assessment provides granular visibility into the actions taken by your users, allowing you to identify blind spots and open risks

How does it work?

The Lookout SaaS Risk Assessment provides an audit of an existing cloud service to identify your level of ongoing risk. Lookout provides a dedicated cloud native tenant which connects via API to one of your SaaS applications, for example Office365 or Google Workspace.
The deployment is passive, simple to activate and quick to give results. Once connected, the Lookout Security Platform will scan the connected SaaS repository, monitor ongoing usage of the SaaS app, and will identify any malware, data leakage or compliance violations. After two weeks, the tenant is decommissioned and an executive summary is provided, highlighting discovered risks. Experience shows that anomalous user behavior and sensitive data exposure has been identified in as little as 90 minutes.



Dedicated Lookout CASB tenant, integrated with your SaaS app via API-mode



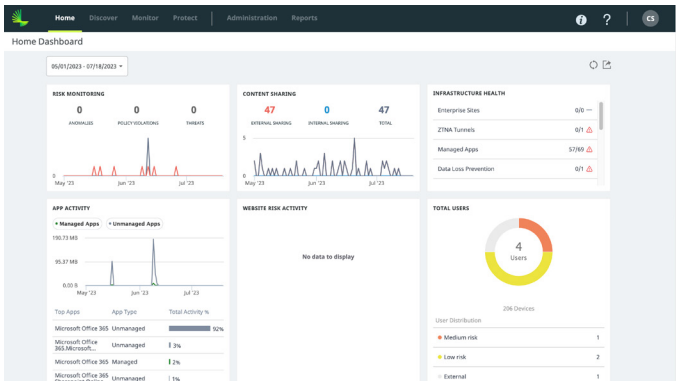
Get fast eye-opening results with API mode

- Simple Configuration - no new infrastructure required
- Complete visibility into user interactions, anomalies, sharing & collaboration and DLP violations
- Fast implementation
- Initial results within 10 mins for first live data in console
- Full summary provided

What are the pre-requistes?

In order to run a Lookout SaaS Risk Assessment you will need to have a corporate instance of a SaaS app supported by Lookout - Office365, Google Workspace, Box, Dropbox, salesforce, etc. You will also need to sign an NDA with Lookout and provide a service account with read-only privileges to allow API access to your SaaS application from the Lookout Security Platform.

1. Customer & Lookout sign a mutual NDA.
2. Lookout provides a dedicated tenant on the Lookout Security Platform.
3. Customer has to approve an API connection for Lookout to the SaaS application to be monitored.
4. Lookout will work with the customer to create up to five policies.
5. Over a two week period, Lookout will scan for violations according to the pre-configured policies. During this time, customer access to the Lookout console is provided, to monitor activity and events.
6. After two weeks, the tenant will be decommissioned and an executive summary provided to the customer.



Data Handling and Privacy

No customer data is collected or stored by Lookout. The assessment is based on metadata that includes user IDs and activity. All data resides in a dedicated tenant that is only accessible by the customer and the Lookout operations team. After the two weeks, the tenant will be decommissioned.

About Lookout

Lookout, Inc. is the endpoint-to-cloud cybersecurity company that delivers zero trust security by reducing risk and protecting data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards digital information across devices, apps, networks and clouds and is as fluid and flexible as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit **lookout.com**

Request a demo at **lookout.com/request-a-demo**