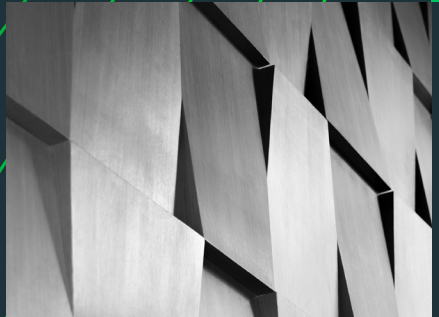
Lookout

SaaS Risk Assessment

Visibility into the risk your SaaS apps present to your data



Assessment Report — Sample

About the Lookout SaaS Risk Assessment

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.

The Customer X Lookout tenant https://Customer X-ms.ciphercloud.eu/ was integrated with the Customer X Google Workspace tenant associated with customer.com and customer.co.uk domains. Using API based integration the Lookout Cloud Security Platform provided insight into User and Content Activity with the platform automatically cataloging content as well as identifying sensitive data and anomalous behavior. This report summarizes the assessment and offers indication for further investigate as part of Customer X's security posture and risk management.

Results Summary

During the assessment period 108.7k files and objects were analyzed as users carried out the following actions: Edit, View, Create, Download, Rename, Add Collaborators, Move, Update Collaborators, Delete, Share, and Restore.

Based on the sample API Access Policies that were deployed to identify sensitive data within Google Workspace, 1.6k violations were observed. Further detail on policy configuration can be found in the Policy Violation section.

238 files were shared with collaborators outside of the registered Customer X domains with a total of 196 unique users being observed. This includes both internal and external users which also covers personal accounts such as Gmail and Hotmail. If identifying the use of sharing files to personal accounts is of interest, creating an API Access Policy to identify collaboration/external sharing with common personal platforms is recommended. Anomalous activity was observed in the form of impossible travel and anomalous download activity. Further details can be found in the Anomalous Activity section.

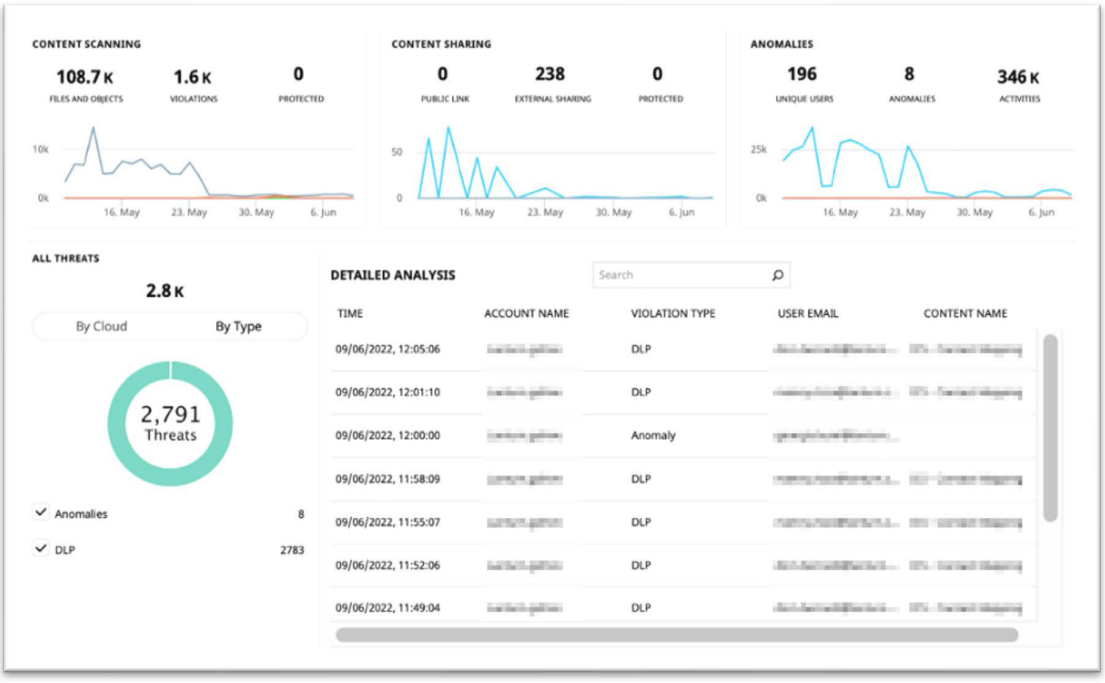


Figure 1: Lookout SaaS Risk Assessment Overview

User Activity

During the assessment, 540 folders were analyzed and a further 24 folders shared. Lookout Audit Activity logs can be used to observe which folders were available internally, externally, and public. Evaluation of the contents of the folders was not carried out as part of the Lookout SaaS Risk Assessment with only folder transactions being observed. For customers who wish to deploy the Lookout Cloud Security Platform across their cloud infrastructure, it is recommended that a Cloud Data Discovery scan is executed in order to analyze contents of folders retrospectively.

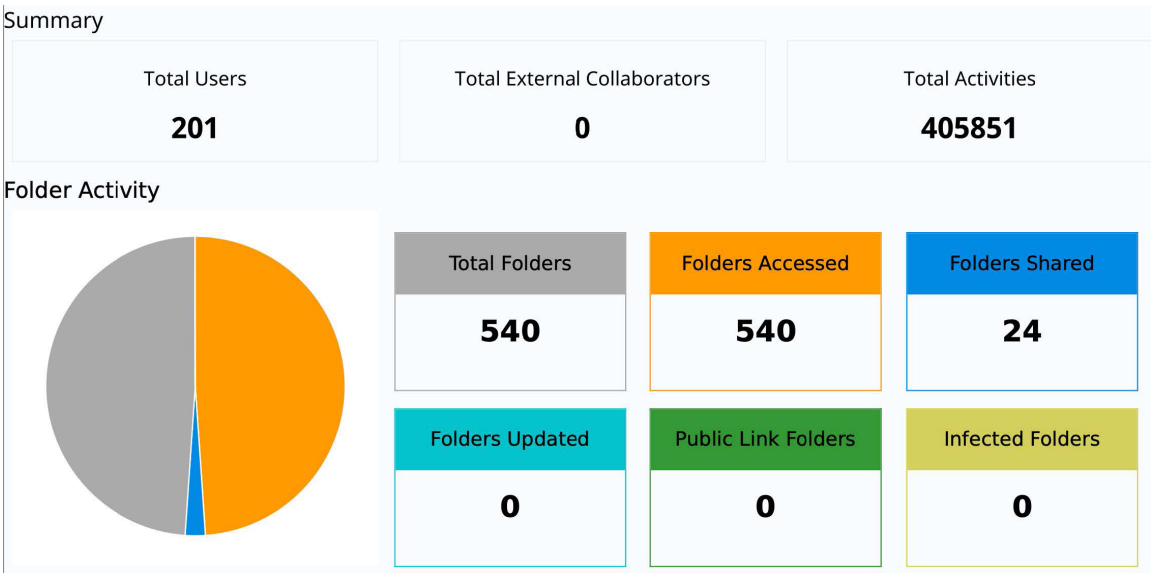


Figure 2: Lookout SaaS Risk Assessment — Analysed Folders

Top 15 Folder Activity Details

User Email	Content Name	Activity	Last Activity
[redacted]	[redacted]	79	June 8, 2022 12:00:00 AM GMT
[redacted]	[redacted]	45	June 9, 2022 12:00:00 AM GMT
[redacted]	[redacted]	42	May 13, 2022 12:00:00 AM GMT
[redacted]	[redacted]	42	June 8, 2022 12:00:00 AM GMT
[redacted]	[redacted]	40	June 8, 2022 12:00:00 AM GMT
[redacted]	[redacted]	38	June 9, 2022 12:00:00 AM GMT
[redacted]	[redacted]	36	June 8, 2022 12:00:00 AM GMT
[redacted]	[redacted]	34	May 19, 2022 12:00:00 AM GMT
[redacted]	[redacted]	34	May 19, 2022 12:00:00 AM GMT
[redacted]	[redacted]	32	June 8, 2022 12:00:00 AM GMT
[redacted]	[redacted]	32	June 6, 2022 12:00:00 AM GMT
[redacted]	[redacted]	31	June 7, 2022 12:00:00 AM GMT
[redacted]	[redacted]	31	June 9, 2022 12:00:00 AM GMT
[redacted]	[redacted]	30	June 7, 2022 12:00:00 AM GMT
[redacted]	[redacted]	30	May 13, 2022 12:00:00 AM GMT

Figure 3: Lookout Risk Assessment — Top 15 Folder Interaction

Top 10 User Activity Details

User Email	Activity	Last Activity
[redacted]	100768	June 9, 2022 12:00:00 AM GMT
[redacted]	36705	June 9, 2022 12:00:00 AM GMT
[redacted]	14400	June 9, 2022 12:00:00 AM GMT
[redacted]	13318	June 9, 2022 12:00:00 AM GMT
[redacted]	9403	June 9, 2022 12:00:00 AM GMT
[redacted]	9390	June 9, 2022 12:00:00 AM GMT
[redacted]	8891	June 9, 2022 12:00:00 AM GMT
[redacted]	8418	June 9, 2022 12:00:00 AM GMT
[redacted]	8331	June 8, 2022 12:00:00 AM GMT
[redacted]	7766	June 9, 2022 12:00:00 AM GMT

Figure 4: Lookout SaaS Risk Assessment — Top 10 User Activity Details

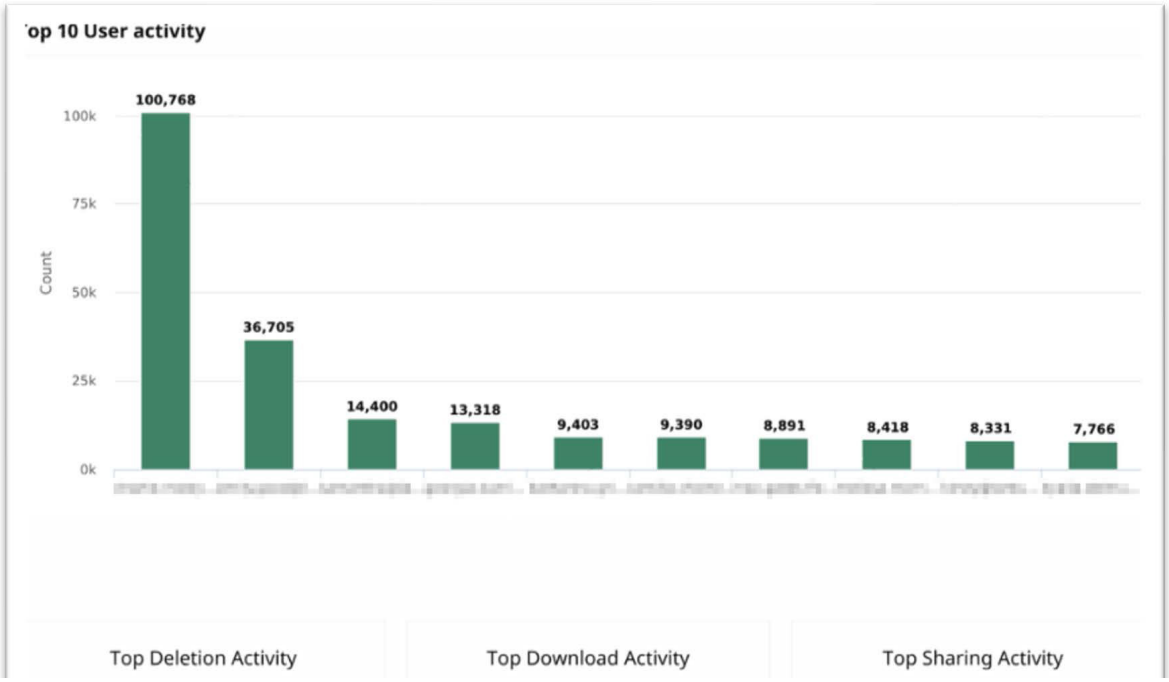


Figure 5: Lookout SaaS Risk Assessment — Top 10 User Activity

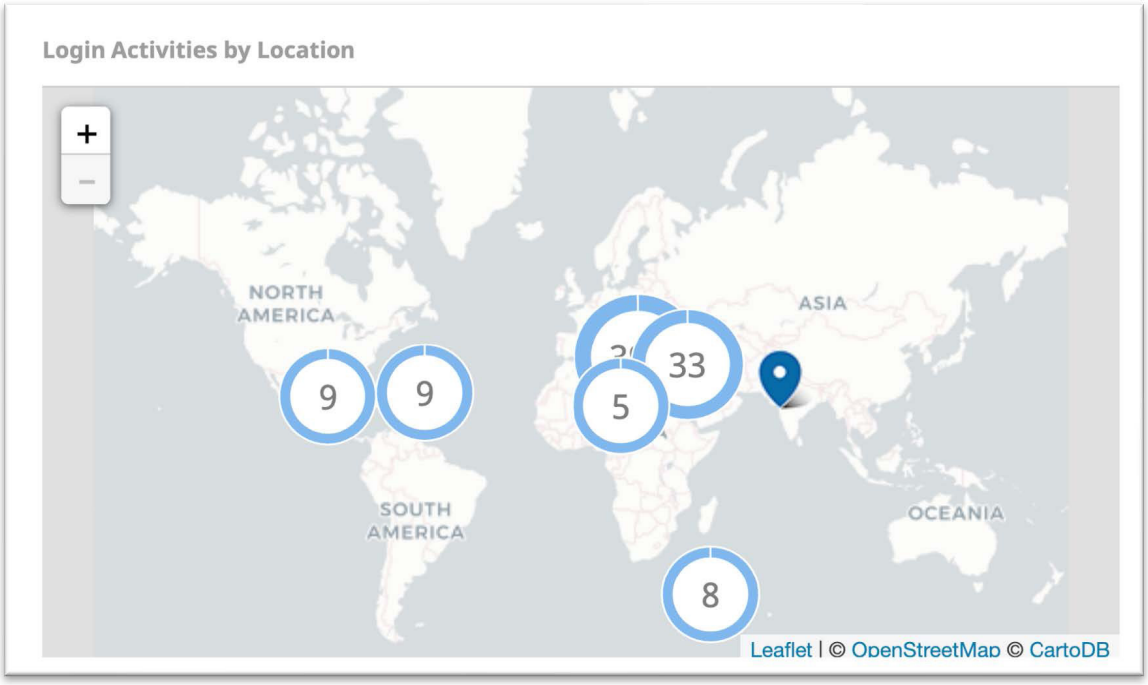


Figure 6: Lookout SaaS Risk Assessment — Login Activity

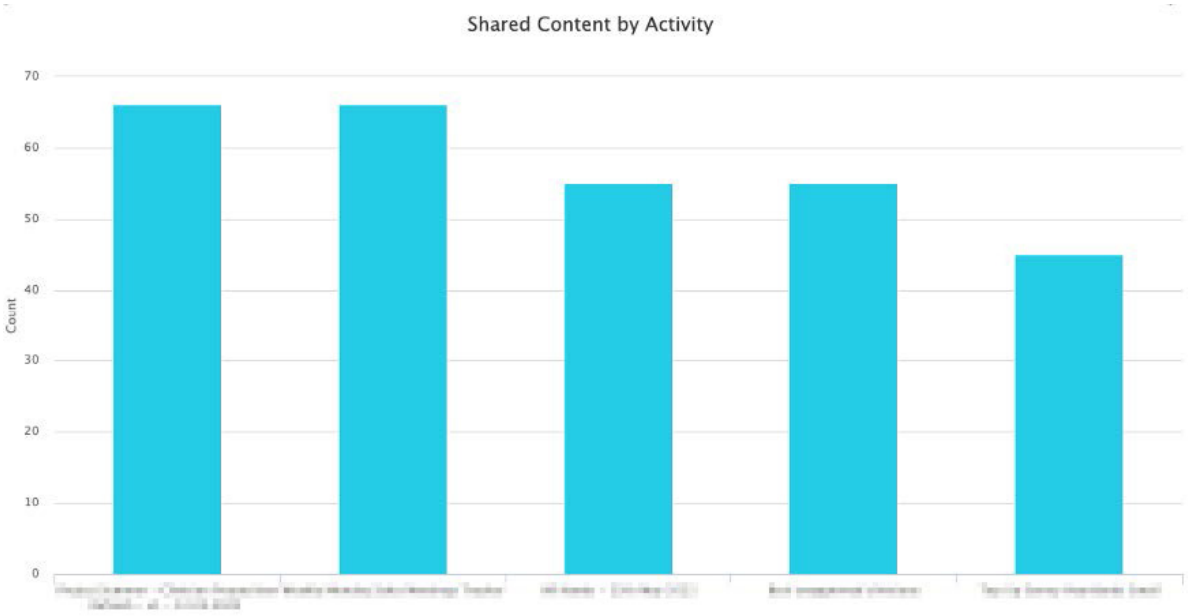


Figure 7: Lookout SaaS Risk Assessment — Shared Content by Activity

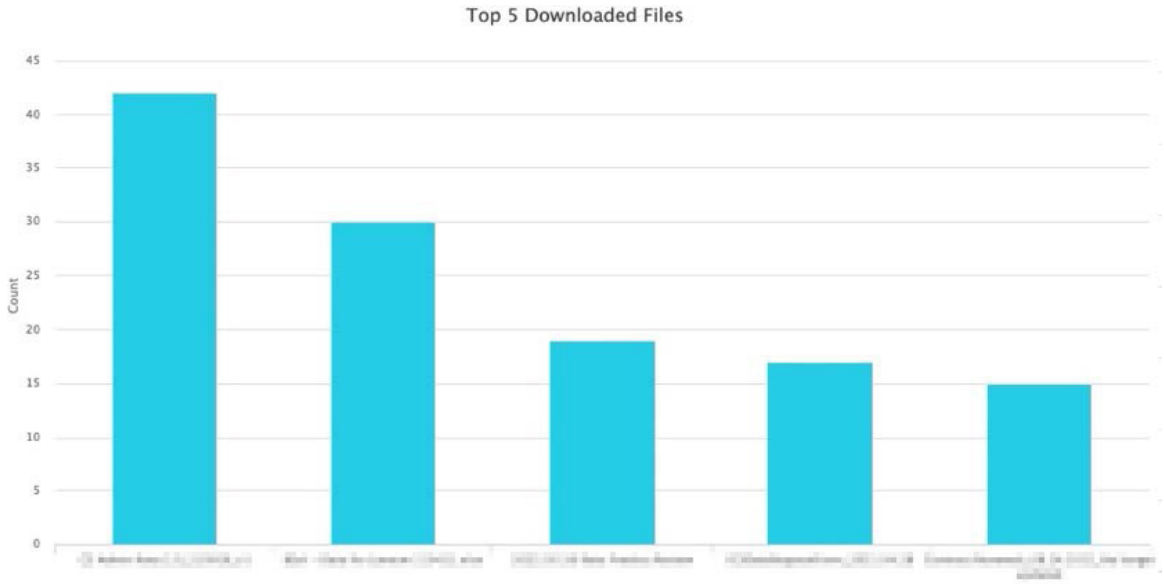


Figure 8: Lookout SaaS Risk Assessment — Top 5 Downloaded Files

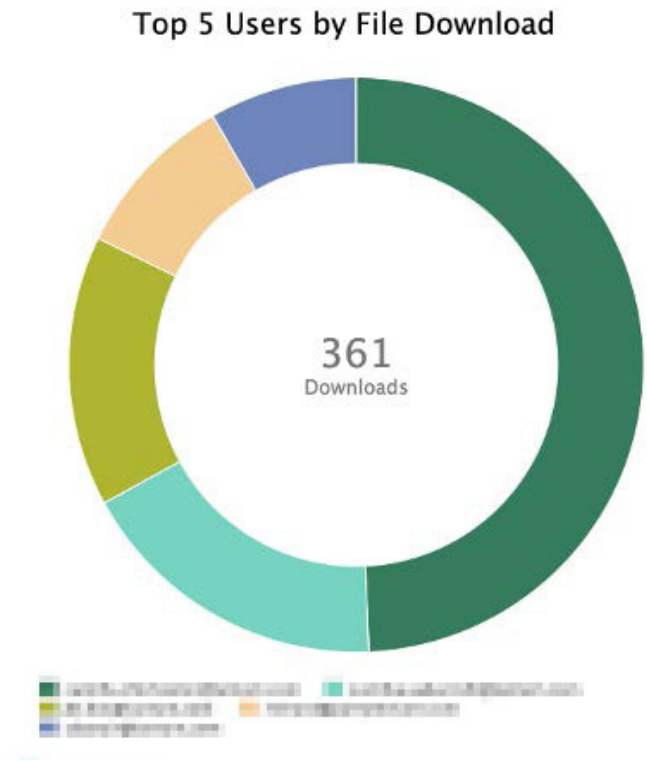


Figure 9: Lookout SaaS Risk Assessment — Top 5 Users by File Download

Policy Violations

During the Lookout SaaS Risk Assessment, all transacted unstructured data is analyzed, scanning both file metadata and content. Each transaction is logged, enabling Customer X to observe user interaction with all content and effectively cataloging content in an information asset tracker.

API Access Policies were implemented to identify content that contained potentially sensitive data or posed a risk to the organization. Each successful detection of sensitive data resulted in a policy violation as shown below. Each API Access Policy was implemented in a 'passive' (Allow and Log) mode and hence causing no user impact during the evaluation. Organizations that deploy the Lookout Cloud Security Platform in an 'active' mode can not only observe violations, but also enforce a wide range of protective measures such as; Allow and Log, Deny, Redact, Mask, Highlight, Watermark, Encrypt, User Coach, Step-up Authentication, Remove Collaborators, Remove Recipients, Remove Shared Link.

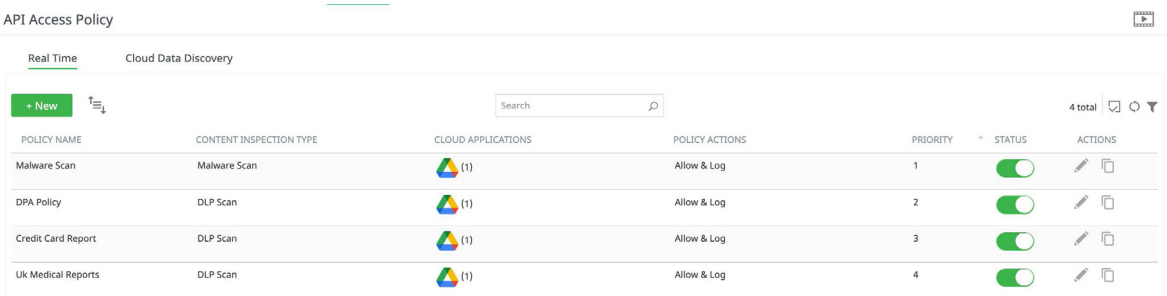


Figure 10: Lookout SaaS Risk Assessment — API Access Policy

The policies implemented for the Customer X Lookout SaaS Risk Assessment were:

- Malware – All content that was introduced to the Customer X Google Workspace tenant was automatically scanned for known threats.
- Access to Medical Records – All content was scanned for UK NHS Numbers and UK National Insurance Numbers using composite rules to reduce false positives. Related keywords were required to be within 500 characters proximity in order for the detection to be considered a positive hit.

The following regular expression was used to identify UK NHS numbers:

- \b(\d{3}[\s\-]?){2}\d{4}\b

The following regular expression was used to identify UK National Insurance numbers:

- \b(?i)[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z (?<!BG|GB|NK|KN|TN|NT|ZZ)(\r?\n?([\t\. -]\r?\n?)?\d{2}) {3}\r?\n?([\t\. -]\r?\n?)?[A-D]\b

UK Data Protection Act – All content was scanned for data that is considered sensitive by the UK Data Protection Act using composite rules to reduce false positives. Related keywords were required to be within 500 characters proximity for the detection to be considered a positive hit.

The following regular expression was used to identify UK National Insurance numbers:

- \b(?i)[A-CEGHJ-PR-TW-Z][A-CEGHJ-NPR-TW-Z] (?<!BG|GB|NK|KN|TN|NT|ZZ)(\r?\n?([\t\. -]\r?\n?)?\d{2}) {3}\r?\n?([\t\. -]\r?\n?)?[A-D]\b

In total, 2,783 policy violations were detected during the Lookout SaaS Risk Assessment, identifying potential threats to sensitive data including UK Medical Records and UK DPA as identified by the DLP rules detailed above.

Credit Card Report — All content was scanned for data that is considered sensitive by the UK Data Protection Act using composite rules to reduce false positives. Related keywords were required to be within 500 characters proximity for the detection to be considered a positive hit.

- The following regular expression was used to identify Credit Card numbers: (?<=^|\s\W|,|"|'|>|\s)\d(?:\d\r?\ n?([\t\. -]\r?\n?)?){11,14}(?<=\d)\d(?=$|\s|,|<|"|'|&|\W\s)

In total, 2,783 policy violations were detected during the Lookout SaaS Risk Assessment, identifying that sensitive data including UK Medical Records and UK DPA as identified by the DLP rules detailed above.

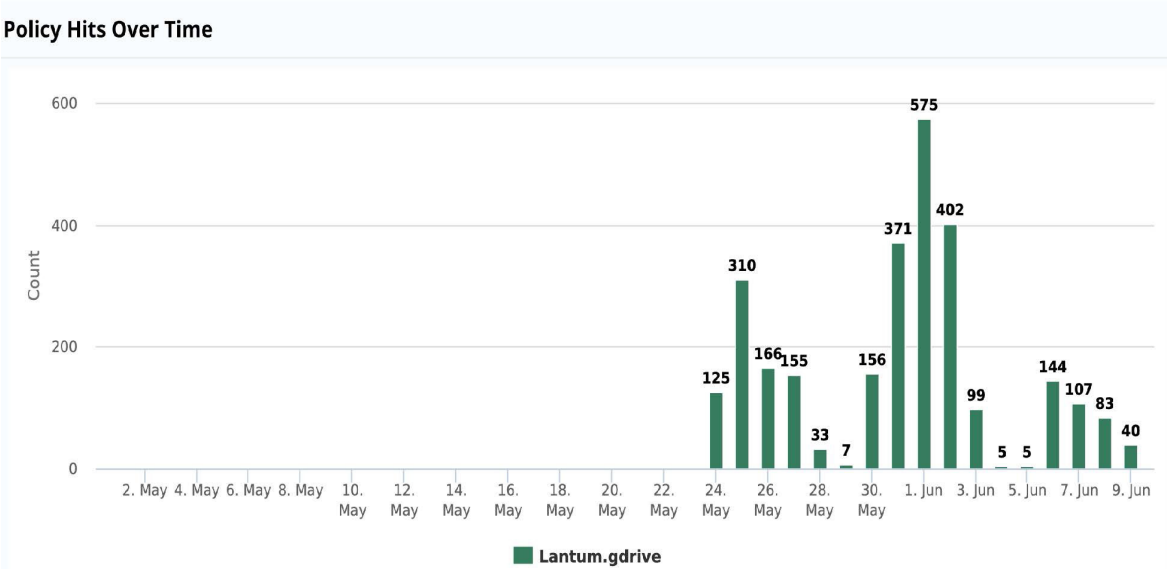


Figure 11: Lookout Risk Assessment — Policy Hits Over Time

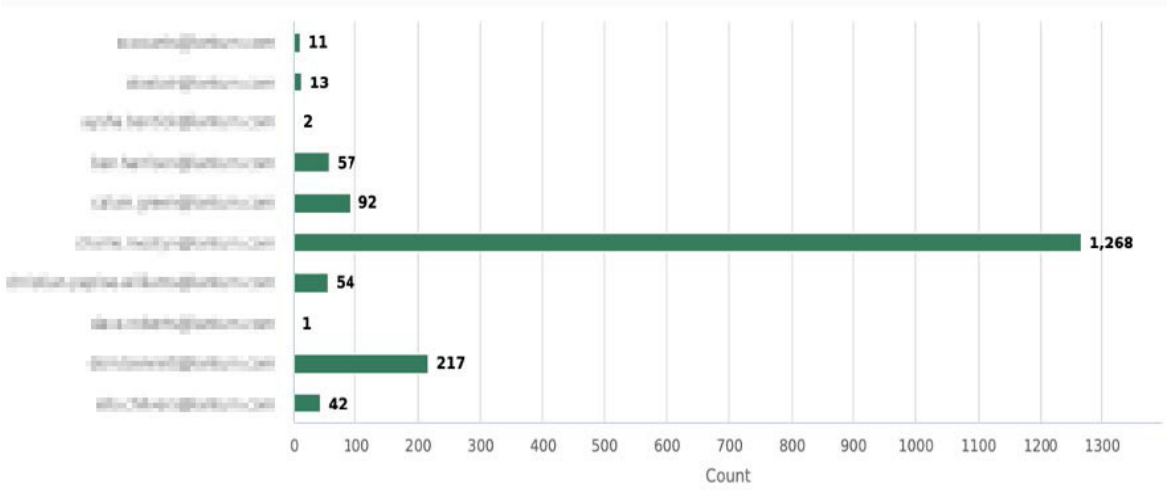


Figure 12: Lookout SaaS Risk Assessment — Policy Hits by User

Figure 13: Lookout SaaS Risk Assessment — Policy Hits by Location

Anomalous Activity

Lookout Cloud Security Platform provides User and Entity Behavioural Analysis (UEBA) using statistical based machine learning to correlate data from user and content activity and identifies anomalous activity, which can be an indication of an insider threat, or potential Malware / Ransomware. The Customer X Lookout SaaS Risk Assessment was configured to observe for Anomalous Activity by Geolocation, Anomalous Downloads by Count, Anomalous Authentications and Anomalous Content Deletes.

6 instances of Anomalous Activity by Geolocation, also known as impossible travel, were observed during the Evaluation. This feature observes for user Login, Logout, Content Create, Delete, Edit, Share, etc. Location associated with an IP address is used to geolocate the activity and observe the distance between the previous activity associated with a user. If the distance exceeds what is possible in the timeframe between the two events, it is flagged as anomalous activity. In instances where the location is incorrect due to a VPN in operation, or the logged IP address is a Point of Presence/Datacentre, exclusions and allow-lists can be created to reduce false positives.

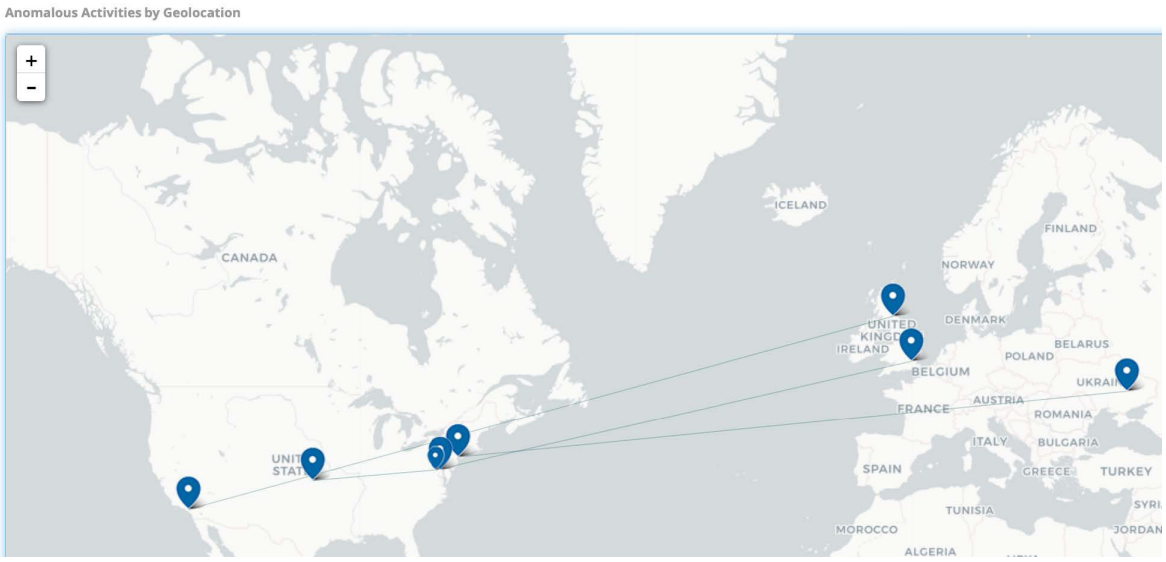


Figure 14: Lookout SaaS Risk Assessment - Impossible Travel

User activity is observed on a rolling basis, maintaining a baseline behavior profile for each user in each onboarded application. This baseline profile is dynamically updated and used to observe for anomalous activity that breaches configured thresholds for the various observed activities.

During the evaluation, two counts of anomalous download activity were observed against two individual users accounts. These activities exceed the acceptable threshold as determined by 'Probability Variation from Peak' (50%) and 'Consecutive Fail Count for Non-Compliance' (3) policies.

The adaptive threshold defines a permitted rate of user activity. The configured threshold can be adjusted based on the user activity rate. Being able to configure a threshold enables a customer to adjust the rate of user activities as needed. If conditions permit, for example, the threshold can be modified to allow a higher rate of activity.

Adaptive threshold configuration evaluates threshold compliance and will allow events up to the defined threshold. The platform also checks the probability of event occurrences after the fixed threshold. If the probability is within the allowed range, the events are allowed.

When the number of consecutive failures exceeds the specified count, the events are considered non-compliant. This can be adjusted up to 20 or down to 1.

There were 2 instances of 'Anomalous Download by Count', indicating an unusual number of downloads for two different users based on their previous download counts.

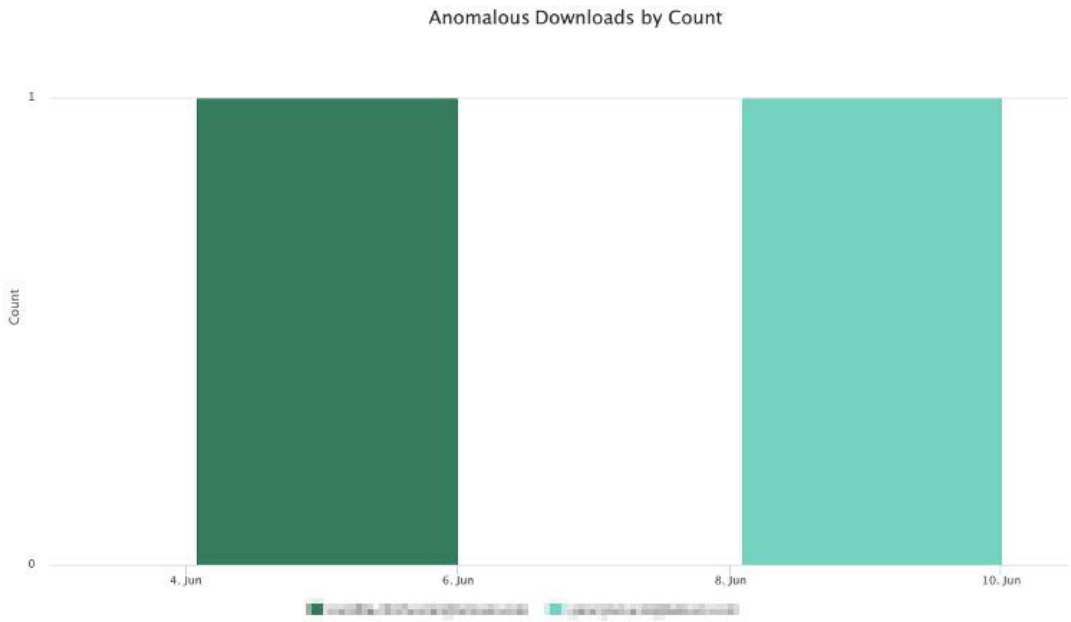


Figure 15: Lookout SaaS Risk Assessment — Anomalous Downloads by Count

Figures 16 and 17 below show the dynamic profile baseline (green) and the anomalous activity (red) that triggered the alerts.

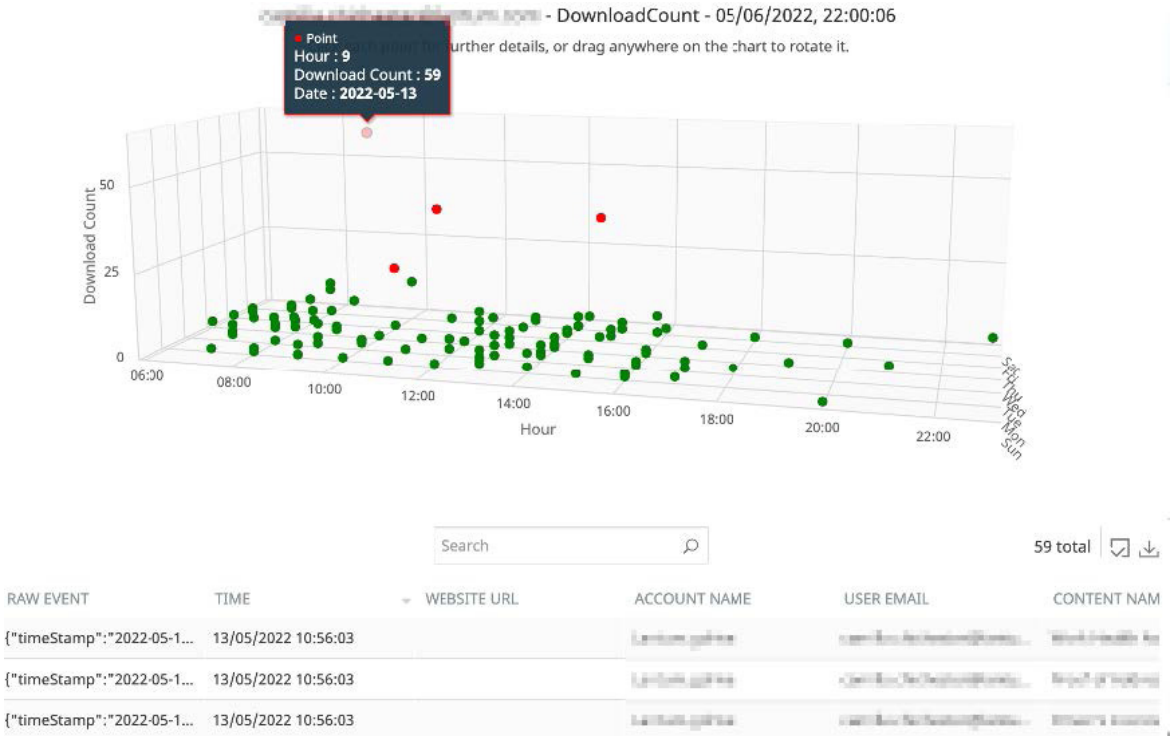


Figure 16: USER1@customerx.com — Anomalous Download

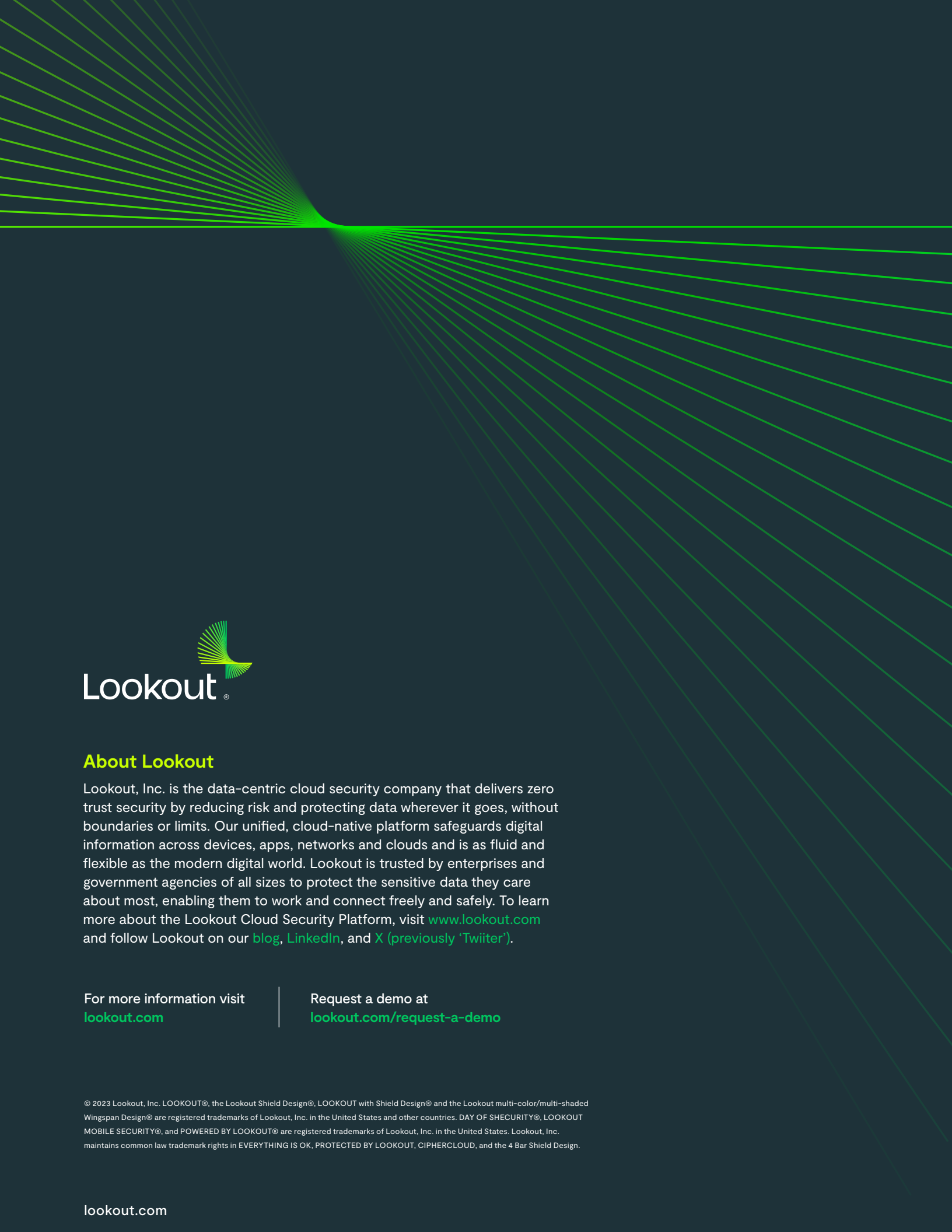
Figure 17: USER2@customerx.com — Anomalous Download

Summary

The Lookout SaaS Risk Assessment offered a limited insight into the capabilities offered by the Lookout Cloud Security Platform with many more features available for evaluation as part of a Proof of Value or live deployment. Additional integrations and configurations enable the platform to provide much richer visibility and control of multiple SaaS, IaaS and private enterprise applications through a single pane of glass with a single policy applied to multiple applications.

Further information can be obtained from your Lookout Account Manager.

To learn more about Lookout's cloud data protection capabilities, visit:
lookout.com/products/cloud-security



Lookout

About Lookout

Lookout, Inc. is the data-centric cloud security 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 X (previously 'Twiiter').

For more information visit
lookout.com

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