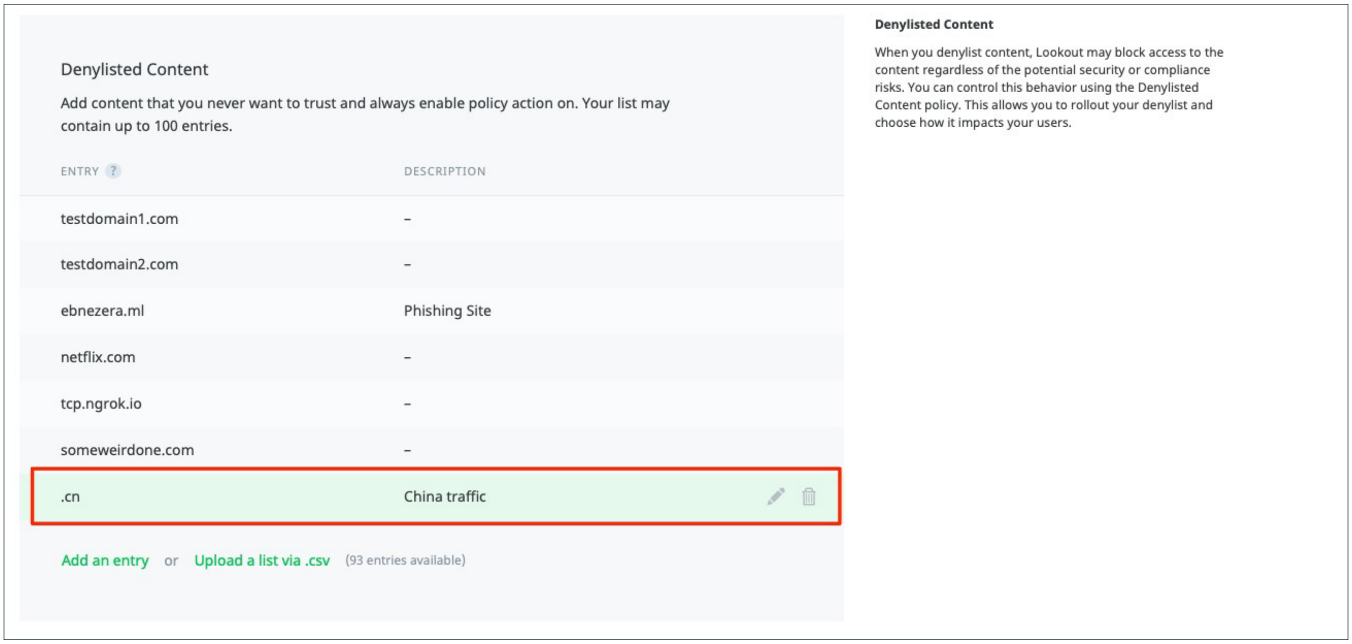
Keep Your Data Protected from Adversarial Nation States and Governments

With security and data privacy at the center of public and private sector conversations, enterprise and government organizations look to each other for guidance on best practices. Mobile applications can have risky or concerning data collection and handling practice, and with adversarial Nation States using mobile apps and domains to collect sensitive user information, countries and organizations worldwide should waste little time debating whether a risky mobile application or website should be banned — regardless of its popularity.

Lookout enables you to minimize the risk of data being shared with apps, domains, and IPs that communicate with locations like China, which may be risky for your business. Whether you have apps that are installed on devices with modern operating systems like iOS, Android and Chromebooks, or if your users are connecting to public websites that have domains listed in these countries, Lookout helps protect data that is being leaked or shared through these apps and websites.

Block mobile traffic to geographic domains

Leveraging Lookout's configurable Phishing and Content Protection engine, organizations can block all traffic to specific domains, including top level domains like .cn or .ru that belong to a specific country. In the Lookout console, admins can configure denylisted content to include country top level domains you wish to block.



Denylisted Content

Add content that you never want to trust and always enable policy action on. Your list may contain up to 100 entries.

ENTRY ?	DESCRIPTION
testdomain1.com	–
testdomain2.com	–
ebnezera.ml	Phishing Site
netflix.com	–
tcp.ngrok.io	–
someweirdone.com	–
.cn	China traffic

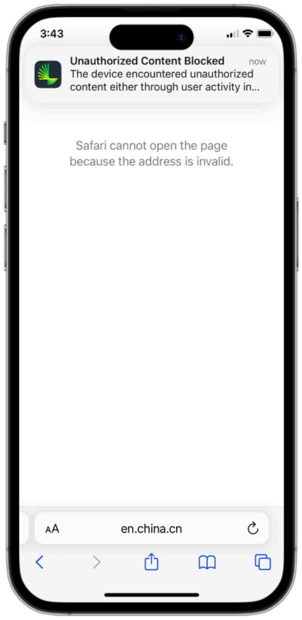
Add an entry or Upload a list via .csv (93 entries available)

Denylisted Content

When you denylist content, Lookout may block access to the content regardless of the potential security or compliance risks. You can control this behavior using the Denylisted Content policy. This allows you to rollout your denylist and choose how it impacts your users.

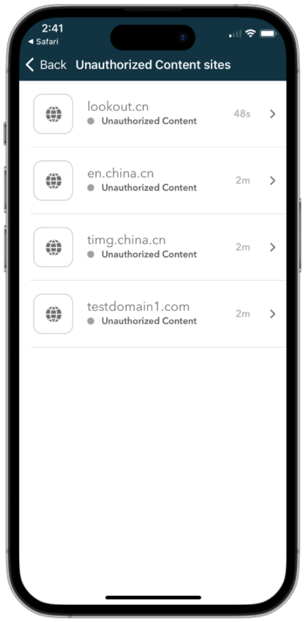
As a result, any browser or app-based communication with domains ending in *.cn* will be blocked. Since denylist policies are defined at the DNS level, they will extend to every app on the device, not just corporate apps or links in specific browsers. This includes background traffic like API traffic or communication to command and control servers hosted at *.cn* domains.

This can be extended to any managed, or unmanaged, or BYO devices running modern operating systems such as Android, iOS or ChromeOS.



Unauthorized Content Blocked now
The device encountered unauthorized content either through user activity in...

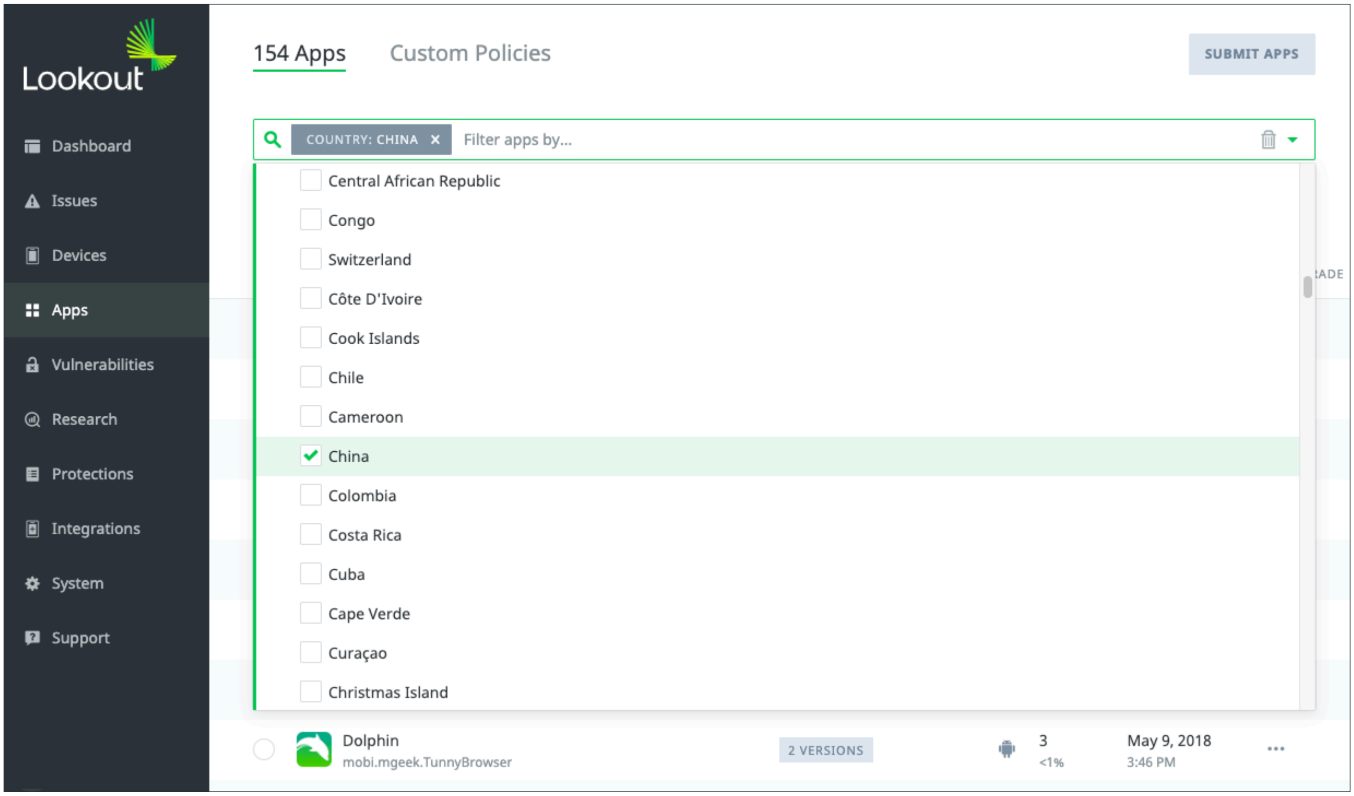
Safari cannot open the page because the address is invalid.



lookout.cn	Unauthorized Content	48s
en.china.cn	Unauthorized Content	2m
timg.china.cn	Unauthorized Content	2m
testdomain1.com	Unauthorized Content	2m

Reactively block apps that send data to China

There are over 9 million mobile apps in Lookout's corpus of security telemetry that send data to China. In order to block any apps that might already be in the mobile fleet from communicating with Chinese domains or IPs, Lookout admins can first search across their protected device fleet to determine which apps on their devices send data to China.



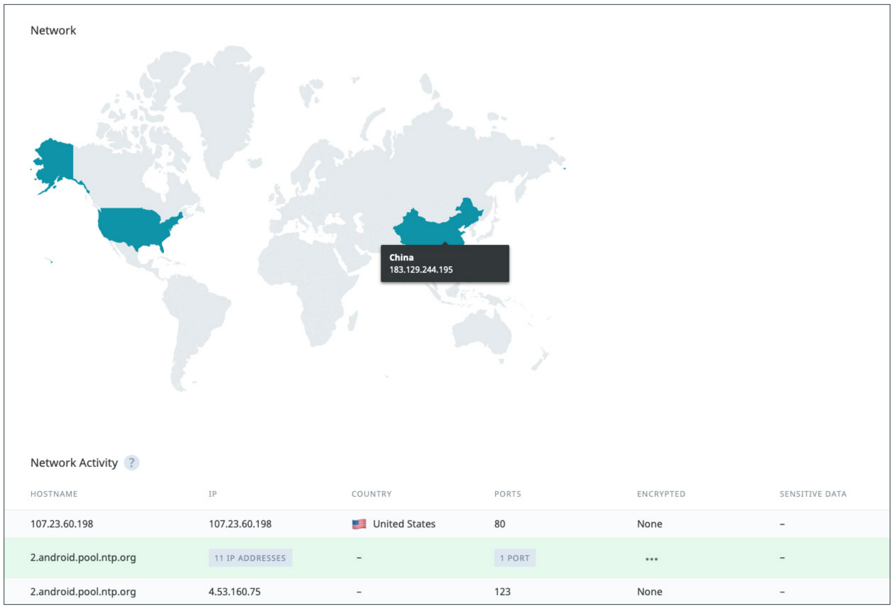
COUNTRY: CHINA ✕ Filter apps by...

□ Central African Republic
□ Congo
□ Switzerland
□ Côte D'Ivoire
□ Cook Islands
□ Chile
□ Cameroon
☑ China
□ Colombia
□ Costa Rica
□ Cuba
□ Cape Verde
□ Curaçao
□ Christmas Island

Dolphin mobi.mgeek.TunnyBrowser	2 VERSIONS	3 <1%	May 9, 2018 3:46 PM	•••

They can drill down into each individual app and see what countries they're sending data to and even what type of data is being sent. Lookout will also provide an app grade based on the domains the app communicates with, its alignment to the OWASP top 10 mobile risks, reputation of its developers, permissions it requests, and more.

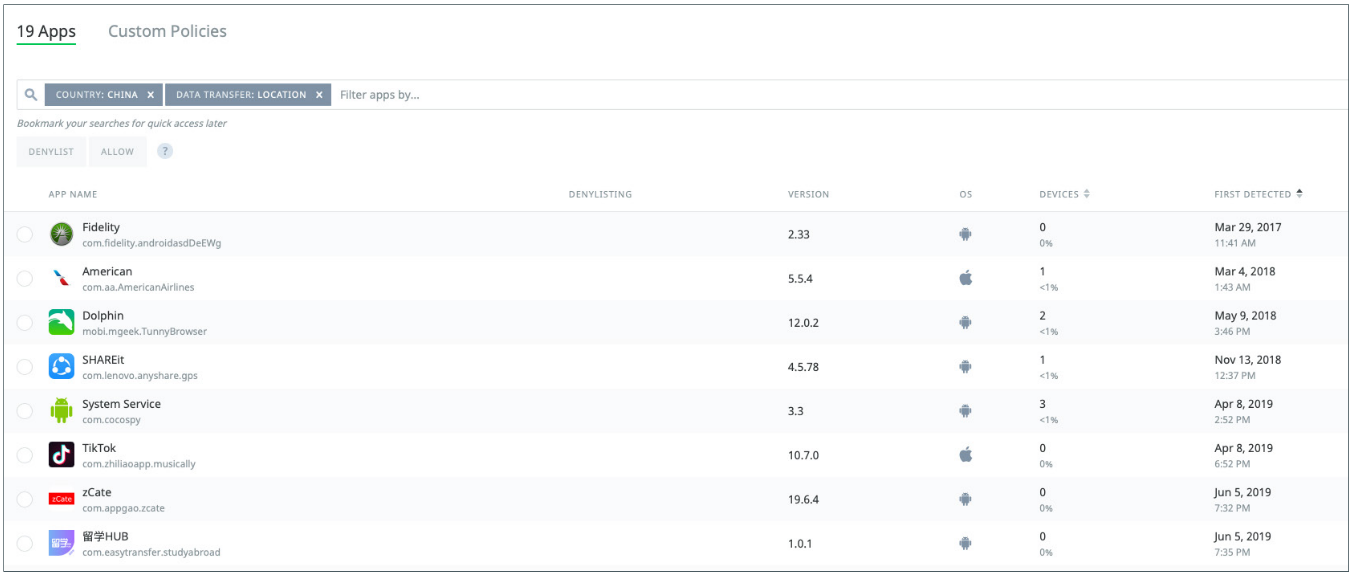
You can combine these queries to carry out more granular research of your existing apps, such as understanding which mobile apps are sending location data off of the device while also communicating with China.



Network

Network Activity ?

HOSTNAME	IP	COUNTRY	PORTS	ENCRYPTED	SENSITIVE DATA
107.23.60.198	107.23.60.198	🇺🇸 United States	80	None	–
2.android.pool.ntp.org	11 IP ADDRESSES	–	1 PORT	•••	–
2.android.pool.ntp.org	4.53.160.75	–	123	None	–



COUNTRY: CHINA × DATA TRANSFER: LOCATION × Filter apps by...

Bookmark your searches for quick access later

APP NAME	DENYLISTING	VERSION	OS	DEVICES	FIRST DETECTED
Fidelity com.fidelity.androidasdDeEWg		2.33	🤖	0 0%	Mar 29, 2017 11:41 AM
American com.aa.AmericanAirlines		5.5.4		1 <1%	Mar 4, 2018 1:43 AM
Dolphin mobi.mgeek.TunnyBrowser		12.0.2	🤖	2 <1%	May 9, 2018 3:46 PM
SHAREit com.lenovo.anyshare.gps		4.5.78	🤖	1 <1%	Nov 13, 2018 12:37 PM
System Service com.cocospy		3.3	🤖	3 <1%	Apr 8, 2019 2:52 PM
TikTok com.zhiliaoapp.musically		10.7.0		0 0%	Apr 8, 2019 6:52 PM
zCate com.appgao.zcate		19.6.4	🤖	0 0%	Jun 5, 2019 7:32 PM
留学HUB com.easytransfer.studyabroad		1.0.1	🤖	0 0%	Jun 5, 2019 7:35 PM

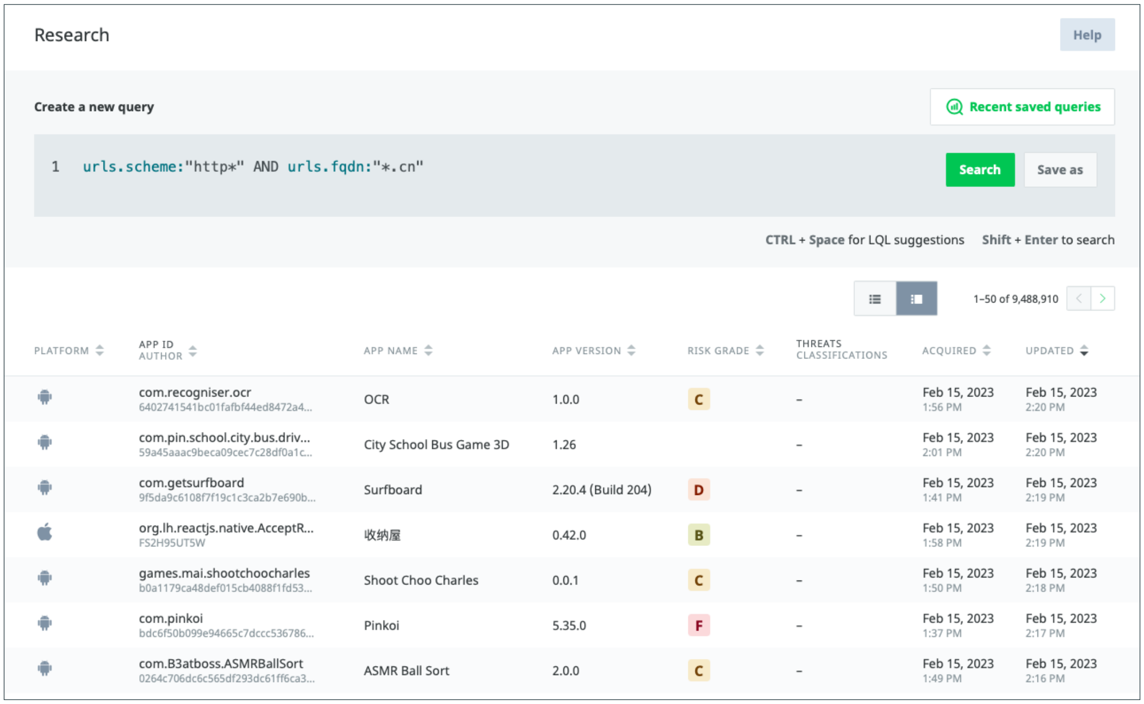
Using this information, IT admins can denylist these apps, which marks any devices containing the app as out of compliance. End users will then receive an alert on their device and be instructed on how to remove the apps in question. To ensure employees actually remove the risky apps, admins can block that device from accessing work apps until the issue is resolved. On some managed devices, admins can use any MDM to block the app from being installed in the first place.

This capability can be extended to managed Android & iOS devices and additionally to unmanaged or BYO Android devices. Unfortunately, because of how iOS is architected, it is not possible to get an iOS app inventory on unmanaged iOS devices. However, to ensure full coverage against this risk, admins can implement the top level domain denylist in order to protect unmanaged iOS devices.

Proactively research apps that are sending data to China

In addition to gaining insight into risky apps that already exist within the protected fleet, admins can leverage Lookout's advanced research console to dive into Lookout's entire corpus of over 180 million apps to find which ones are sending data to China. With the information they find, they can create policies to proactively denylist all of these apps before they even have a chance to be installed on an employee's device.

They can then analyze those apps and gain deep insights into the exact data these apps can access, where they're sending it, what code libraries are in use, and what URLs, domains, and IP addresses the apps are communicating with. Admins can search for apps regardless of whether they are present in your fleet of devices.



```
urls.scheme:"http*" AND urls.fqdn:"*.cn"
```

PLATFORM	APP ID AUTHOR	APP NAME	APP VERSION	RISK GRADE	THREATS CLASSIFICATIONS	ACQUIRED	UPDATED
	com.recogniser.ocr 6402741541bc01fafbf44ed8472a4...	OCR	1.0.0	C	–	Feb 15, 2023 1:56 PM	Feb 15, 2023 2:20 PM
	com.pin.school.city.bus.driv... 59a45aaac9beca09cec7c28df0a1c...	City School Bus Game 3D	1.26		–	Feb 15, 2023 2:01 PM	Feb 15, 2023 2:20 PM
	com.getsurfboard 9f5da9c6108f7f19c1c3ca2b7e690b...	Surfboard	2.20.4 (Build 204)	D	–	Feb 15, 2023 1:41 PM	Feb 15, 2023 2:19 PM
	org.lh.reactjs.native.AcceptR... FS2H95UT5W	收纳屋	0.42.0	B	–	Feb 15, 2023 1:58 PM	Feb 15, 2023 2:19 PM
	games.mai.shootchoocharles b0a1179ca48def015cb4088f1fd53...	Shoot Choo Charles	0.0.1	C	–	Feb 15, 2023 1:50 PM	Feb 15, 2023 2:18 PM
	com.pinkoi bdc6f50b099e94665c7dccc536786...	Pinkoi	5.35.0	F	–	Feb 15, 2023 1:37 PM	Feb 15, 2023 2:17 PM
	com.B3atboss.ASMRBallSort 0264c706dc6c565df293dc61ff6ca3...	ASMR Ball Sort	2.0.0	C	–	Feb 15, 2023 1:49 PM	Feb 15, 2023 2:16 PM

Admins can use these capabilities to proactively research unknown threats and block applications before they end up in their environment.

CONTACT SALES

About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, 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