

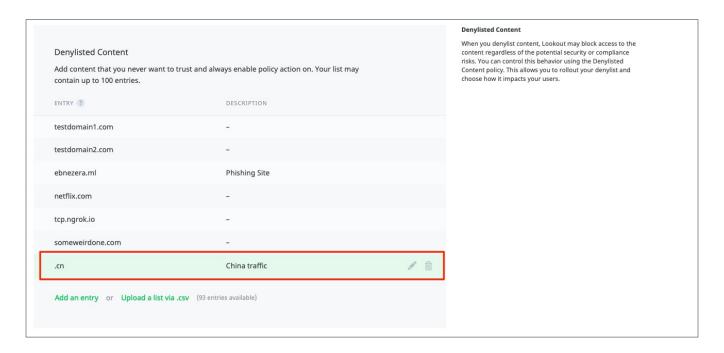
Lookout Keeps Data Safe from China

In today's security conscious climate where government and corporate cyber espionage is becoming a norm, countries and organizations worldwide waste little time debating whether a risky mobile application or websites belonging to specific domains should be banned — regardless of their popularity. With security and data privacy at the center of public and private sector conversations, these issues typically come about when an app is found to have concerning data collection and handling practices.

The Lookout Cloud Security Platform enables any organization to minimize the risk of data being shared with apps, domains, and IPs that communicate with locations in China. Organizations can implement security policies in Lookout Mobile Endpoint Security to mitigate the risk of mobile data being leaked through apps or websites using Chinese domains.

Block traffic to China based domains

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



As a result, any domain ending in *.cn that is accessed from a browser or within mobile apps for data sharing will be blocked. Since the 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.

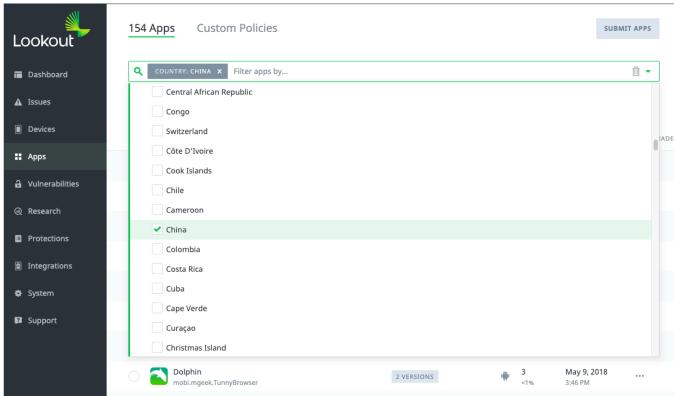
This can be extended to any Android, iOS or ChromeOS device, including unmanaged & BYO devices.

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.



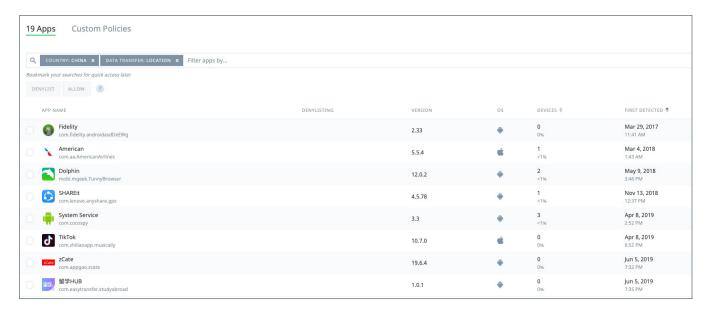




They can research each individual app and see what countries they're sending data to and even what type of data is being sent.



You can combine these queries for more complex actions, such as understanding which apps are sending location data off of the device while also communicating with China.



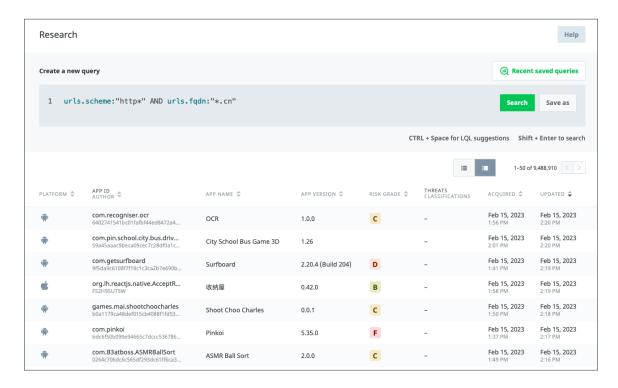
Using this information, IT admins can add apps to your denylist, which marks any devices containing the app as out of compliance. On some managed devices, admins can also use any MDM to block the app from being installed.

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

With Lookout's advanced research capabilities, admins can dive into Lookout's entire corpus of over 180 million apps to find which ones are sending data to China.

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.



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



Lookout is authorized and trusted by Public Sector agencies





















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

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

© 2023 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, SCREAM, the 4 Bar Shield Design, and the Lookout multi-color/multi-shaded Wingspan design.