Berkeley
UNIVERSITY OF CALIFORNIA

KOSMOS
GLOBAL ACCESS PROXY

Final Presentation

Cyber 295 | Summer Capstone 2024

Clarence Capio | Garrett Clark | Ruslan Iakupov | Thomas Iannone | Aris Prabhawa

www.kosmosgap.com

KOSMOS

GLOBAL ACCESS PROXY

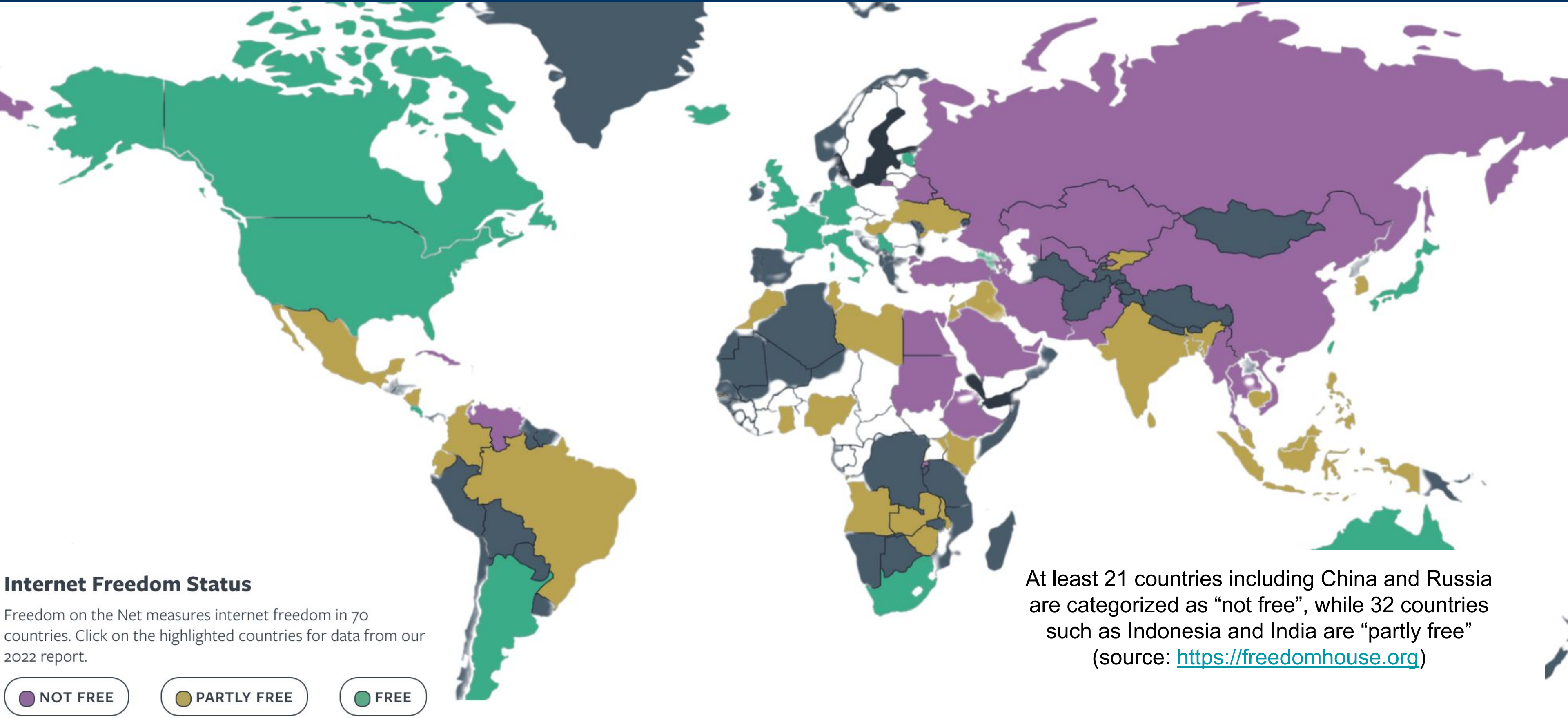
Kosmos is an innovative software solution that enables users worldwide to quickly and securely access the open internet.

Breaking Through Advanced Internet Censorship

From Inspiration to Action

April 25th 2024 UC Berkeley International House guest lecture series

Problem: Over two billions people are isolated from the open internet while modern censorship tools (e.g. DPI) have significantly evolved



Internet Freedom Status

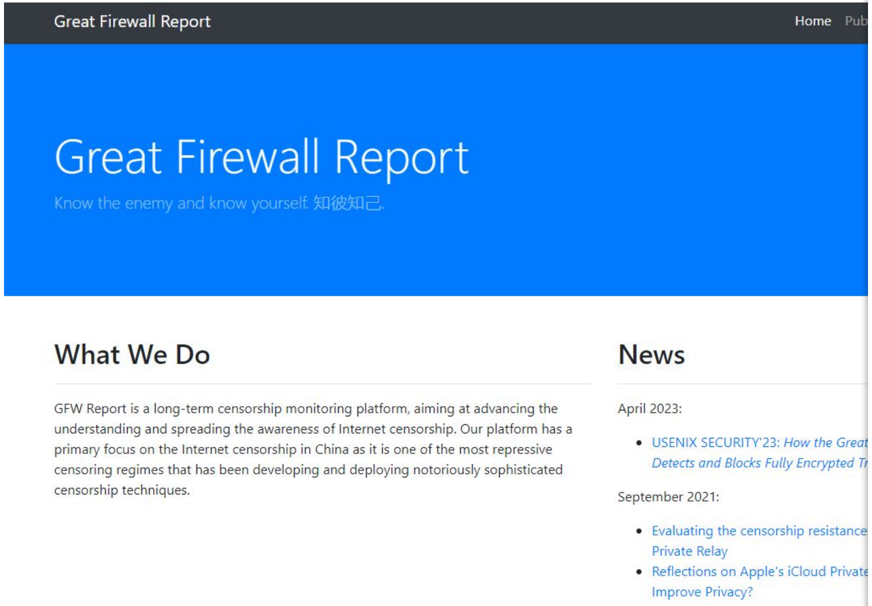
Freedom on the Net measures internet freedom in 70 countries. Click on the highlighted countries for data from our 2022 report.

● NOT FREE ● PARTLY FREE ● FREE

At least 21 countries including China and Russia are categorized as “not free”, while 32 countries such as Indonesia and India are “partly free” (source: https://freedomhouse.org)

Breaking Through Advanced Internet Censorship

From Inspiration to Action



Great Firewall Report

Know the enemy and know yourself. 知彼知己.

What We Do

GFW Report is a long-term censorship monitoring platform, aiming at advancing the understanding and spreading the awareness of Internet censorship. Our platform has a primary focus on the Internet censorship in China as it is one of the most repressive censoring regimes that has been developing and deploying notoriously sophisticated censorship techniques.

News

April 2023:

- USENIX SECURITY'23: *How the Great Detects and Blocks Fully Encrypted Tr*

September 2021:

- Evaluating the censorship resistance Private Relay
- Reflections on Apple's iCloud Private Improve Privacy?

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE
ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL
ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic

Mingshi Wu, *GFW Report*
Jackson Sippe, *University of Colorado Boulder*
Danesh Sivakumar, *University of Maryland*
Jack Burg, *University of Maryland*
Peter Anderson, *Independent researcher*
Xiaokang Wang, *V2Ray Project*
Kevin Bock, *University of Maryland*
Amir Houmansadr, *University of Massachusetts Amherst*
Dave Levin, *University of Maryland*
Eric Wustrow, *University of Colorado Boulder*

Abstract

One of the cornerstones in censorship circumvention is fully encrypted protocols, which encrypt *every* byte of the payload in an attempt to "look like nothing". In early November 2021, the Great Firewall of China (GFW) deployed a new censorship technique that passively detects—and subsequently blocks—fully encrypted traffic in real time. The GFW's new censorship capability affects a large set of popular censorship circumvention protocols, including but not limited to Shadowsocks, VMess, and Obfs4. Although China had long *actively* probed such protocols, this was the first report of *purely passive* detection, leading the anti-censorship community to ask how detection was possible.

In this paper, we measure and characterize the GFW's new system for censoring fully encrypted traffic. We find that, instead of directly defining what fully encrypted traffic is, the

TLS begin with a handshake that comprises plaintext bytes, fully encrypted (randomized) protocols—such as VMess [23], Shadowsocks [22], and Obfs4 [7]—are designed such that *every* byte in the connection is functionally indistinguishable from random. The idea behind these "looks like nothing" protocols is that they should be difficult for censors to fingerprint and therefore costly to block.

On November 6, 2021, Internet users in China reported blockings of their Shadowsocks and VMess servers [10]. On November 8, an Outline [42] developer reported a sudden drop in use from China [69]. The start of this blocking coincided with the sixth plenary session of the 19th Chinese communist party central committee [1,4], which was held on November 8–11, 2021. Blocking these circumvention tools represents a new capability in China's Great Firewall (GFW). To our knowledge, although China has been using passive traf-

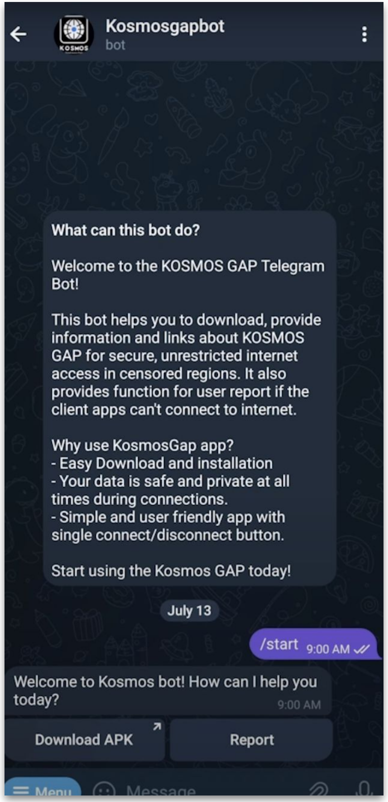
Breaking Through Advanced Internet Censorship

From Inspiration to Action

Breaking Through Advanced Internet Censorship

From Inspiration to Action

Andrei



Kosmosgapbot
bot

What can this bot do?

Welcome to the KOSMOS GAP Telegram Bot!

This bot helps you to download, provide information and links about KOSMOS GAP for secure, unrestricted internet access in censored regions. It also provides function for user report if the client apps can't connect to internet.

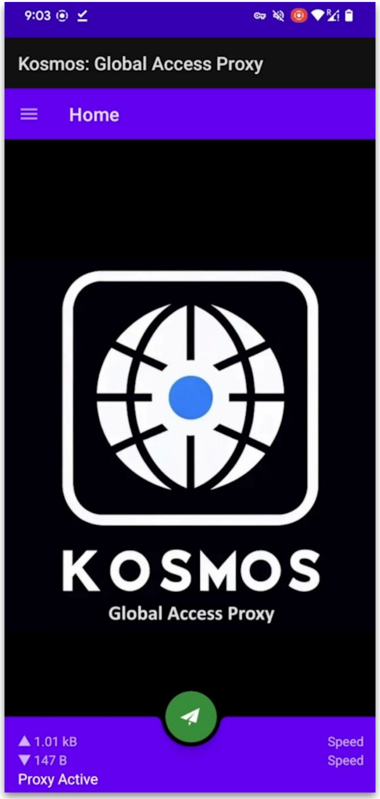
Why use KosmosGap app?
- Easy Download and installation
- Your data is safe and private at all times during connections.
- Simple and user friendly app with single connect/disconnect button.

Start using the Kosmos GAP today!

July 13

/start 9:00 AM

Welcome to Kosmos bot! How can I help you today? 9:00 AM



9:03

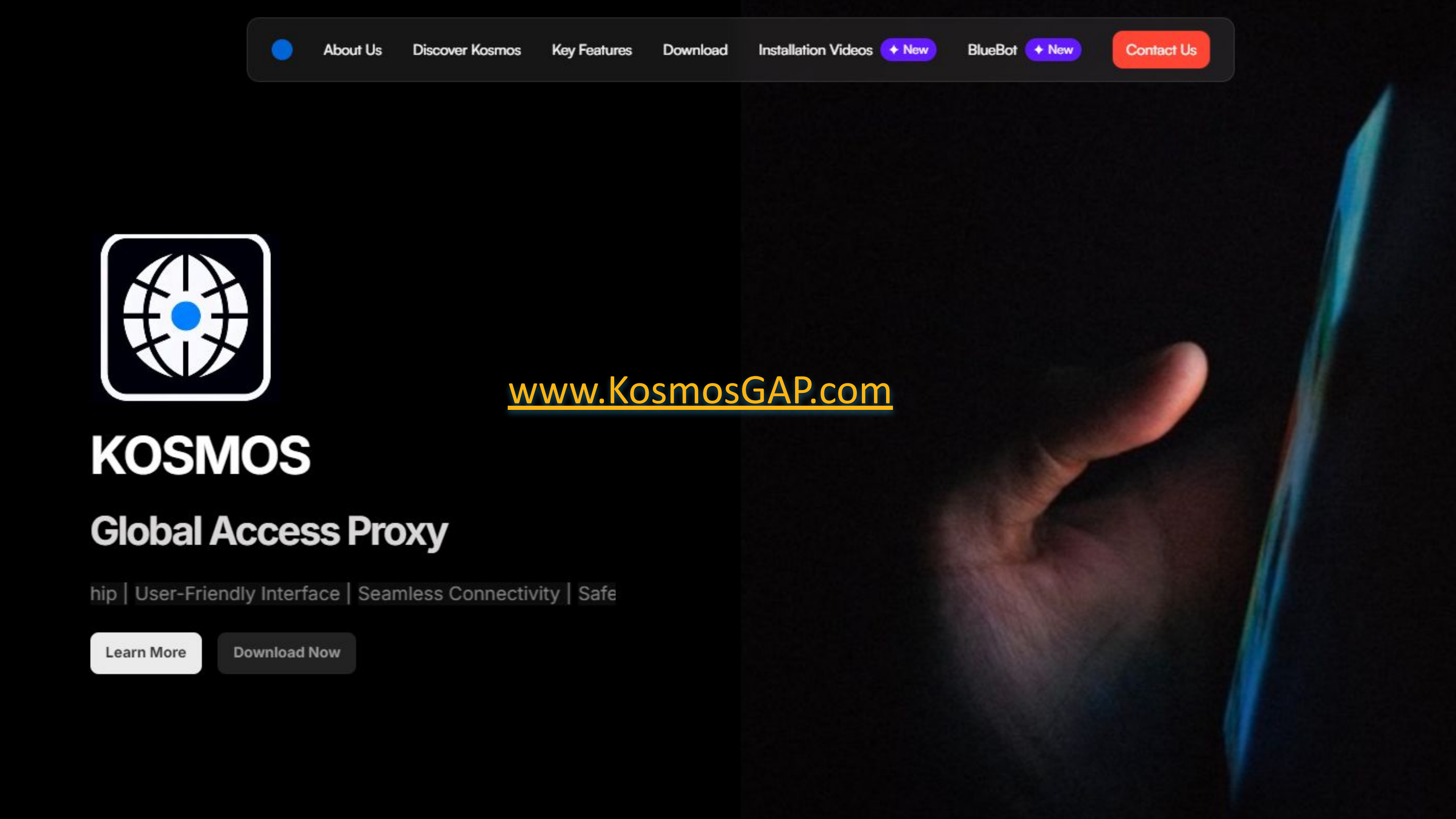
Kosmos: Global Access Proxy

▲ 1.01 kB Speed
▼ 147 B Speed
Proxy Active

facebook

LinkedIn

Discord



www.KosmosGAP.com

KOSMOS

Global Access Proxy

hip | User-Friendly Interface | Seamless Connectivity | Safe

Our Solution: Kosmos Global Access Proxy

Advanced Obfuscation

Kosmos GAP functions differently from a typical VPN. Traffic is indistinguishable from regular HTTPS internet traffic, travelling unnoticed through censorship systems.

Easy to Use

Kosmos GAP makes it easy for users of all technical levels to use our service with clean and intuitive UI while also supported by multi-channel (Web and Telegram bot) customer support for QnA and troubleshooting.

Privacy Protection

Kosmos GAP protects user information by using a stringent no-logs policy and advanced encryption that ensures user data remains confidential and secure.

Secure Communication

Kosmos GAP protects all user interaction and data transmission from interception and unauthorized access with advanced encryption and secure API communication.

KOSMOS vs VPN/TOR

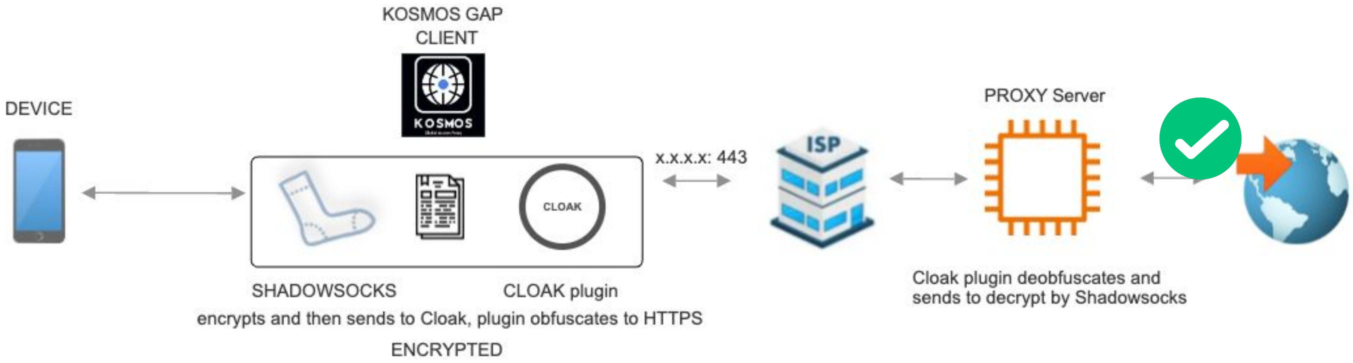
VS

VPN/TOR packets

KOSMOS GAP main components

SHADOWSOCKS fast tunnel proxy bypassing firewalls

CLOAK   pluggable transport, enhances proxy to evade sophisticated censorship and data discrimination



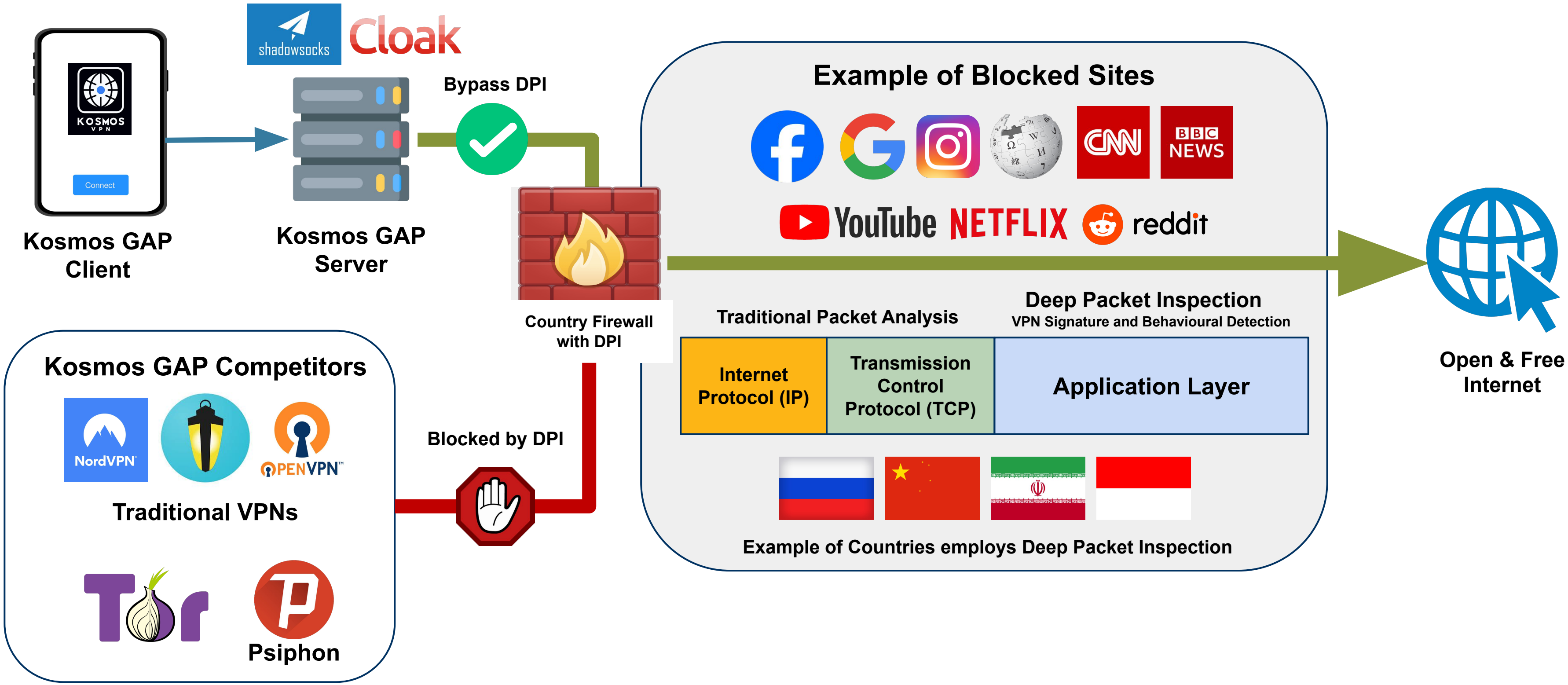
encrypts and then sends to Cloak, plugin obfuscates to HTTPS

ENCRYPTED

Cloak plugin deobfuscates and sends to decrypt by Shadowsocks

Kosmos GAP Technology vs Competition

Kosmos GAP utilizes Shadowsocks and Cloak technology to encrypt connection using SOCKS5 and obfuscate the traffic to make it appear like a normal and legitimate connection to the firewall.



Kosmos GAP Client

Kosmos GAP Server

Bypass DPI

Country Firewall with DPI

Blocked by DPI

Example of Blocked Sites

Traditional Packet Analysis

Deep Packet Inspection
VPN Signature and Behavioural Detection

Internet Protocol (IP)

Transmission Control Protocol (TCP)

Application Layer

Example of Countries employs Deep Packet Inspection

Open & Free Internet

Kosmos GAP Competitors

Traditional VPNs

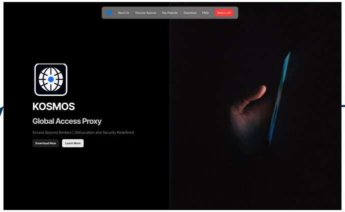
Psiphon

Kosmos Global Access Proxy User Flow

User in internet-restricted country

1

User access Kosmos GAP Website



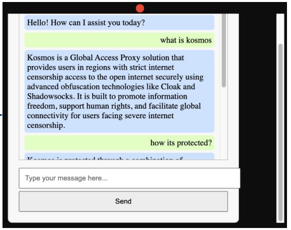
KOSMOS

Global Access Proxy

Access Beyond Borders | Obfuscation and Security Redefined

Kosmos Global Access Proxy Website
Link: https://kosmosgap.com

Ask questions in natural language



Hello! How can I assist you today?

what is kosmos

Kosmos is a Global Access Proxy solution that provides users in regions with strict internet censorship access to the open internet securely using advanced obfuscation technologies like Cloak and Shadowsocks. It is built to promote information freedom, support human rights, and facilitate global connectivity for users facing severe internet censorship.

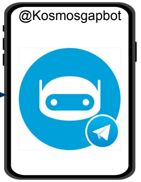
how its protected?

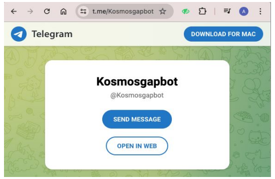
Kosmos GenAI Chatbot website integration

2

Command:
/start, /help, /download, /report, /support

User access Kosmos GAP Telegram Bot





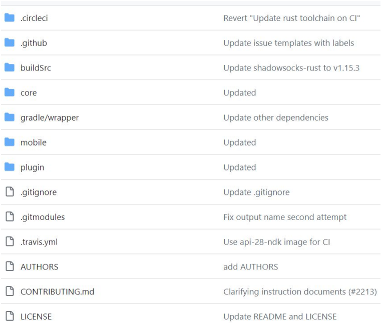
Open t.me/Kosmosgapbot on a website or search @Kosmosgapbot in Telegram application

3

User can access source files

https://github.com/tjiannone/Kosmos

GitHub



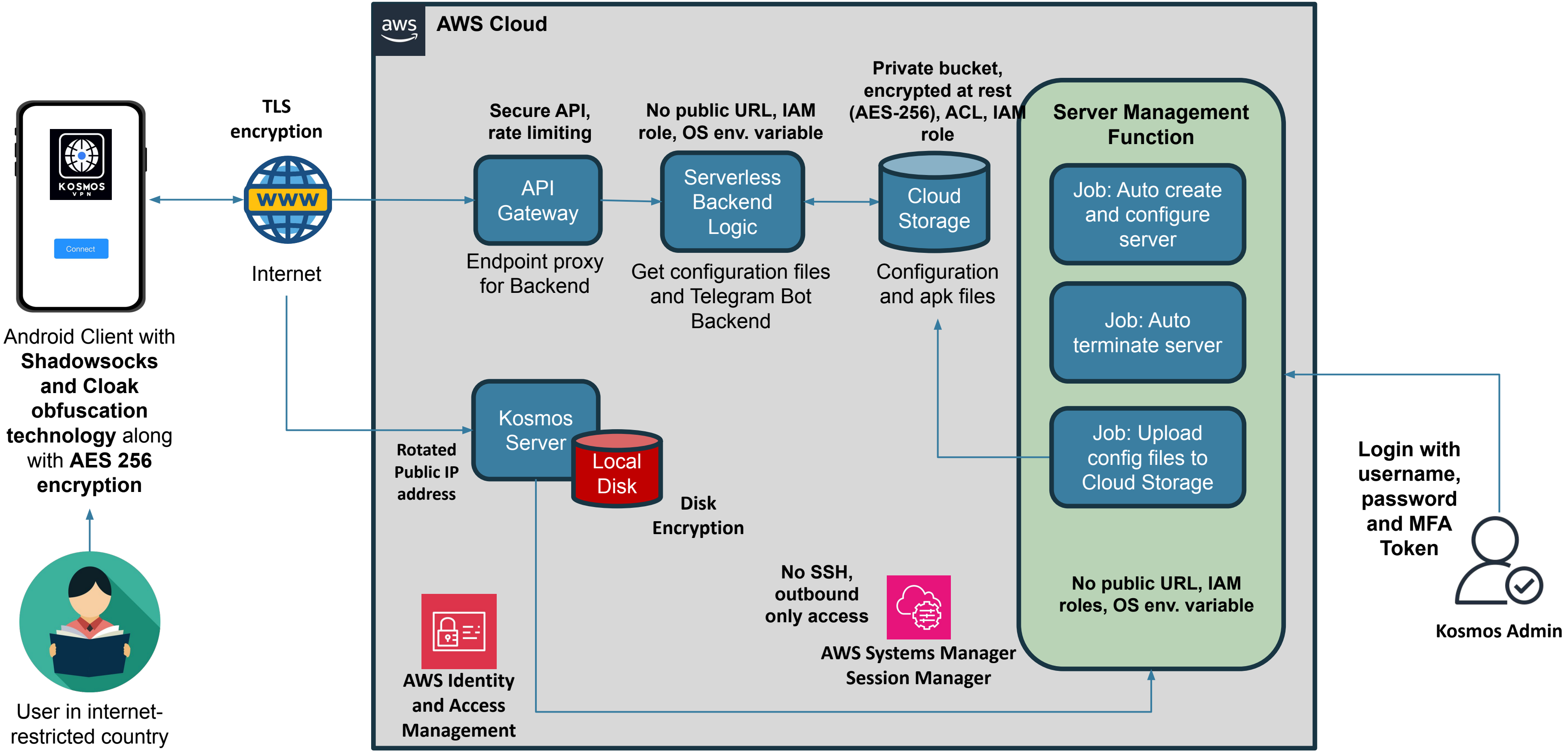
.circleci	Revert "Update rust toolchain on CI"
.github	Update issue templates with labels
buildSrc	Update shadowsocks-rust to v1.15.3
core	Updated
gradle/wrapper	Update other dependencies
mobile	Updated
plugin	Updated
.gitignore	Update .gitignore
.gitmodules	Fix output name second attempt
.travis.yml	Use api-28-ndk image for CI
AUTHORS	add AUTHORS
CONTRIBUTING.md	Clarifying instruction documents (#2213)
LICENSE	Update README and LICENSE

Kosmos GAP Live Demo

Demo: Real Users Interaction in China and Russia

Note: we edited the original user videos by cutting non-essential parts to fit the time limit. The user's IP, latitude and longitude is blurred to protect user privacy.

Architecture/Data Flow Diagram



Android Client with **Shadowsocks and Cloak obfuscation technology** along with **AES 256 encryption**

User in internet-restricted country

TLS encryption

Internet

AWS Cloud

Secure API, rate limiting

API Gateway

Endpoint proxy for Backend

No public URL, IAM role, OS env. variable

Serverless Backend Logic

Get configuration files and Telegram Bot Backend

Private bucket, encrypted at rest (AES-256), ACL, IAM role

Cloud Storage

Configuration and apk files

Server Management Function

Job: Auto create and configure server

Job: Auto terminate server

Job: Upload config files to Cloud Storage

No public URL, IAM roles, OS env. variable

Rotated Public IP address

Kosmos Server

Local Disk

Disk Encryption

No SSH, outbound only access

AWS Systems Manager Session Manager

AWS Identity and Access Management

Login with username, password and MFA Token

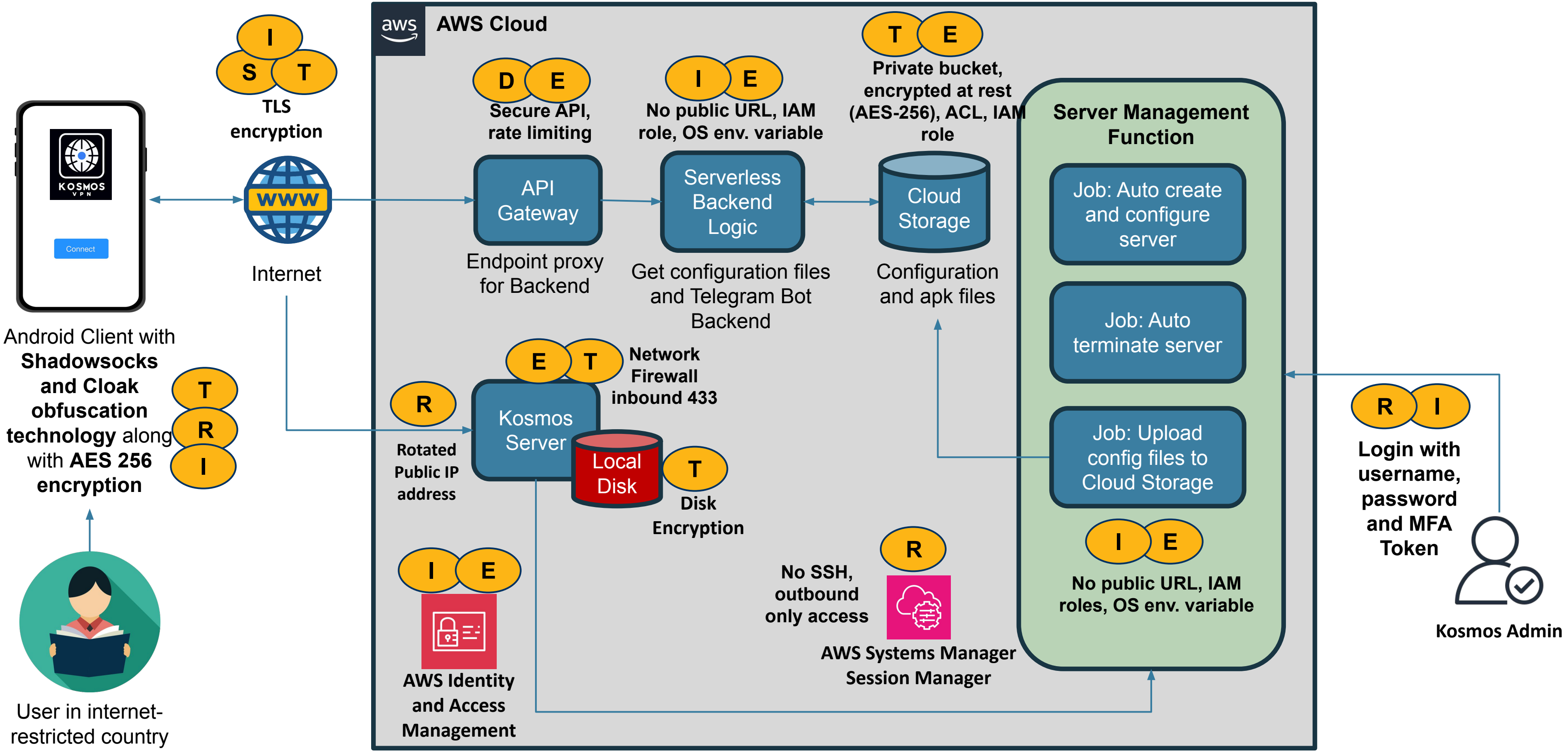
Kosmos Admin

Kosmos GAP Security Approach and Design

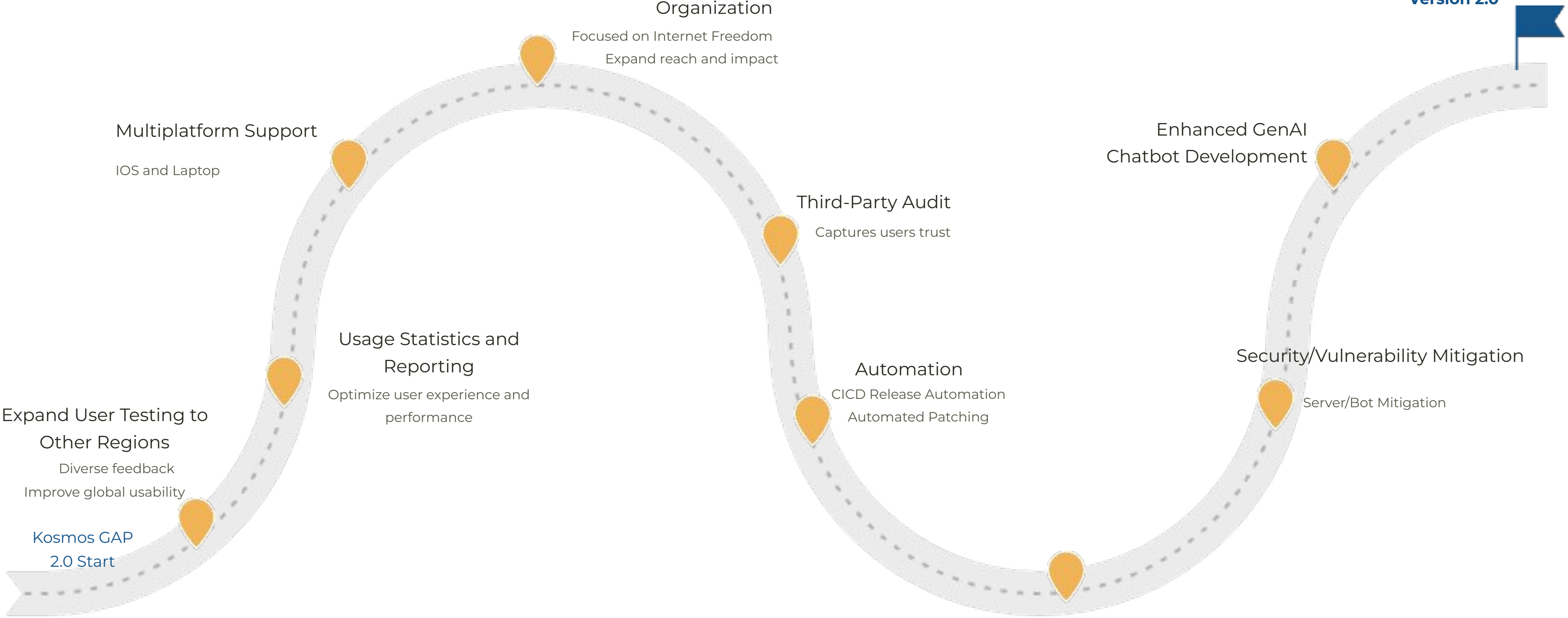
STRIDE is a model for identifying computer security threats developed by Microsoft

STRIDE Category	Threats	Mitigations
Spoofing	Server impersonation Fake TBot	SSL/TLS Future implementation: Server/bot verification
Tampering	Configuration tampering Data tampering in transit	Data encryption: AES 256 and TLS1.3 Open only ports needed, disable any/any inbound and outbound
Repudiation	Action deny	Secure session No logs policy
Information Disclosure	Data leak Configuration exposure Insider threat	Access control MFA Secure data at transit/rest
Denial of Service	DDOS attack Resource exhaustion	AWS DDOS Shield Future implementation: EC2 Auto Scaling mechanism
Elevation of privilege	Privilege escalation Vulnerabilities exploit	Least privilege principle with IAM Future implementation: Automation patching/updates Future implementation: Vulnerability scanning

STRIDE Implementation Diagram


I
S
T
TLS encryption
Internet
KOSMOS VPN
Connect
Android Client with **Shadowsocks and Cloak obfuscation technology** along with **AES 256 encryption**
T
R
I
User in internet-restricted country
AWS Cloud
D
E
Secure API, rate limiting
API Gateway
Endpoint proxy for Backend
I
E
No public URL, IAM role, OS env. variable
Serverless Backend Logic
Get configuration files and Telegram Bot Backend
T
E
Private bucket, encrypted at rest (AES-256), ACL, IAM role
Cloud Storage
Configuration and apk files
Server Management Function
Job: Auto create and configure server
Job: Auto terminate server
Job: Upload config files to Cloud Storage
I
E
No public URL, IAM roles, OS env. variable
E
T
Network Firewall inbound 433
R
Rotated Public IP address
Kosmos Server
Local Disk
T
Disk Encryption
I
E
AWS Identity and Access Management
R
No SSH, outbound only access
AWS Systems Manager Session Manager
R
I
Login with username, password and MFA Token
Kosmos Admin

KOSMOS Product Roadmap - Ver 2.0



Kosmos GAP
2.0 Start

Expand User Testing to Other Regions

Diverse feedback

Improve global usability

Usage Statistics and Reporting

Optimize user experience and performance

Multiplatform Support

IOS and Laptop

Network with Non-Profit Organization

Focused on Internet Freedom

Expand reach and impact

Third-Party Audit

Captures users trust

Automation

CICD Release Automation

Automated Patching

Enhanced Security and Privacy

Containerization with multiple IP addresses

Web App Firewall

EC2 Auto Scaling mechanism
Vulnerability Scanning

Security/Vulnerability Mitigation

Server/Bot Mitigation

Enhanced GenAI
Chatbot Development

Kosmos GAP
Version 2.0

Comprehensive Project and Task Management

Obfuscation Technologies

User-Friendly Access

Excellent Collaboration

Latest technology implementation

Over 36 standup meetings

KOSMOS Servers

COMPLETED 102 JIRA Tasks

13 weekly sprints

User-Friendly Android Client

GenAI Integration

24x7 Follow-the-Sun Development and Support
(Asia → Oceania → West Coast → Midwest)

Achievements

Internet Freedom

Security Implementation

Global Development and Support

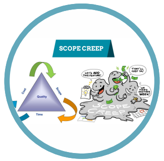
Over 40 hours of meetings

Telegram Bot

Secure API

Latest Encryption Technology

www.kosmosgap.com



Scope Creep

User Recruitment

Project Management, Communication, and Collaboration

Key Challenges and **Lessons Learned**

Setup Complexity for non-technical users

Balancing Security and Usability

KOSMOS
GLOBAL ACCESS PROXY

We empower people worldwide with secure and uncensored internet access, championing digital freedom and privacy through cutting-edge technology and innovation.

Thank you!

Q&A

KOSMOSGAP.COM