SOLUTION BRIEF

Protected API Channels for Mobile Apps

CHALLENGE

Authentication APIs for apps in financial services and other critical industries are getting attacked relentlessly. Threat actors breach accounts through credential stuffing, take down services with high frequency transactions, or otherwise exploit vulnerabilities. Existing solutions, such as Web Application Firewalls, are challenging to administer and only partially resolve the security challenges.

Several pain points result, including:

- Heavy resource requirement to defend against these threats, with significant cost to manage countermeasures, incident response, log storage, customer relationships and regulatory fines.
- Negative end user experience, including unauthorized access, fraudulent charges, account lockouts, password resets and other onerous side effects of security policies

> **Access to mobile app APIs can be restricted to bona fide app users through a secure protocol, greatly reducing risk of fraud and end user friction.**

Traditional mobile app-to-API communication flow creates too much exposure and vulnerability for the authentication servers. A more secure communication channel is required.

SOLUTION

SecureCo's connectivity solution, SecureCo CONNECT, can provide a highly secure software-defined tunnel for API transactions, without exposing the API to discovery and attack.

- Patented Rendezvous methodology creates connections without exposed endpoints – APIs are not publicly accessible other than via SecureCo routing.
- Proprietary routing protocol uses evasion, de-attribution and obfuscation to provide superior protection and interception resistance for the API call, with no perceivable latency.

Benefits

SecureCo's solutions provide practical benefits:

- APIs that are undiscoverable to threat actors are subject to far fewer attacks.
- Fewer security incidents leads to reduced risk of account breach and fraud, and requires fewer resources to defend against and mitigate attacks.
- Improved end user experience with greater account security and less frictional end user security policies.

The practical benefits above yield several positive business outcomes:

- Improved security assurance provides differentiation to attract and retain customers.
- Reduced resource commitment to mitigate attacks could be redirected to more strategic initiatives or otherwise boost profitability.
- Less fraudulent activity.

Copyright 2023 SecureCo, Inc. All rights reserved.

- Client-side SDK is simple to integrate into the mobile application, with security functionality that is invisible to the end user.
- Server-side implementation compatible with security systems, e.g., bot-detection and WAF.

HOW IT WORKS

SecureCo's breakthrough API protection is based on our patented Rendezvous connection methodology. This proprietary approach allows connections to be established with no open inbound ports, as the endpoints establish circuits by reaching out to a random, pre-agreed midpoint in the SecureCo STRATUS cloud delivery platform. In addition, data sent via this method is de-attributed using multi-layer encryption and routed via multiple proxies to hide the source and destination. SecureCo's protocol is obscured by decoy data injection, making it difficult to reverse engineer.

Without the necessity of discoverable inbound ports, firewalls can now be set to block scans that identify connected services. APIs that escape detection avoid downstream security incidents.

SecureCo's networking solutions are high performance, and do not add meaningful latency to data transmission. Data transit is accelerated via the terabit backplane of best-of-breed cloud providers. In some cases, data transit speeds are comparable in performance to that of the customer's ISP unburdened by additional security.

> **It is possible to have it both ways: lower API threat-related fraud and adverse end user experience while reducing administrative overhead.**

Easy to Adopt, Manage and Scale

SecureCo's agent-based solution provides an SDK for mobile app integration, with a server-side virtual appliance installed within the firewall DMZ and in front of load balancers. API call data transit is routed over SecureCo STRATUS, our managed cloud-based delivery platform, which requires negligible customer overhead. The service scales flexibly, drawing upon the resources of cloud services to operate at any volume in any geography.

SECURECO is an elite team of innovators and engineers dedicated to creating the most protected and undiscoverable internet connections possible. We offer a next generation replacement for VPNs and traditional network routing, cloaking data exchange, services and assets to reduce network attack surface. Trusted by some of the world's most demanding cybersecurity customers, we deliver assured, high performance data transit for enterprise and government.

High ROI

For the enterprise-scale customer, a SecureCo implementation saves hundreds of thousands of dollars:

- Reduced Risk of Fraud Mitigation
- Incident Response Overhead Reduction
- Customer Retention Benefits

POC Trial

We offer a 30-day proof-of-concept trial, which is an easy way for prospective clients to assess the ease of implementation, the low cost of management, the high performance and the security benefits. Contact us for a demo today.

secureco

For More Information:

Inquiries, purchasing or evaluation:

https://www.secureco.com/contact/
Email: info@secureco.io
Call: 917-444-5753
Online: www.secureco.com

Copyright 2023 SecureCo, Inc. All rights reserved.