Cequence

VOTE for API Security

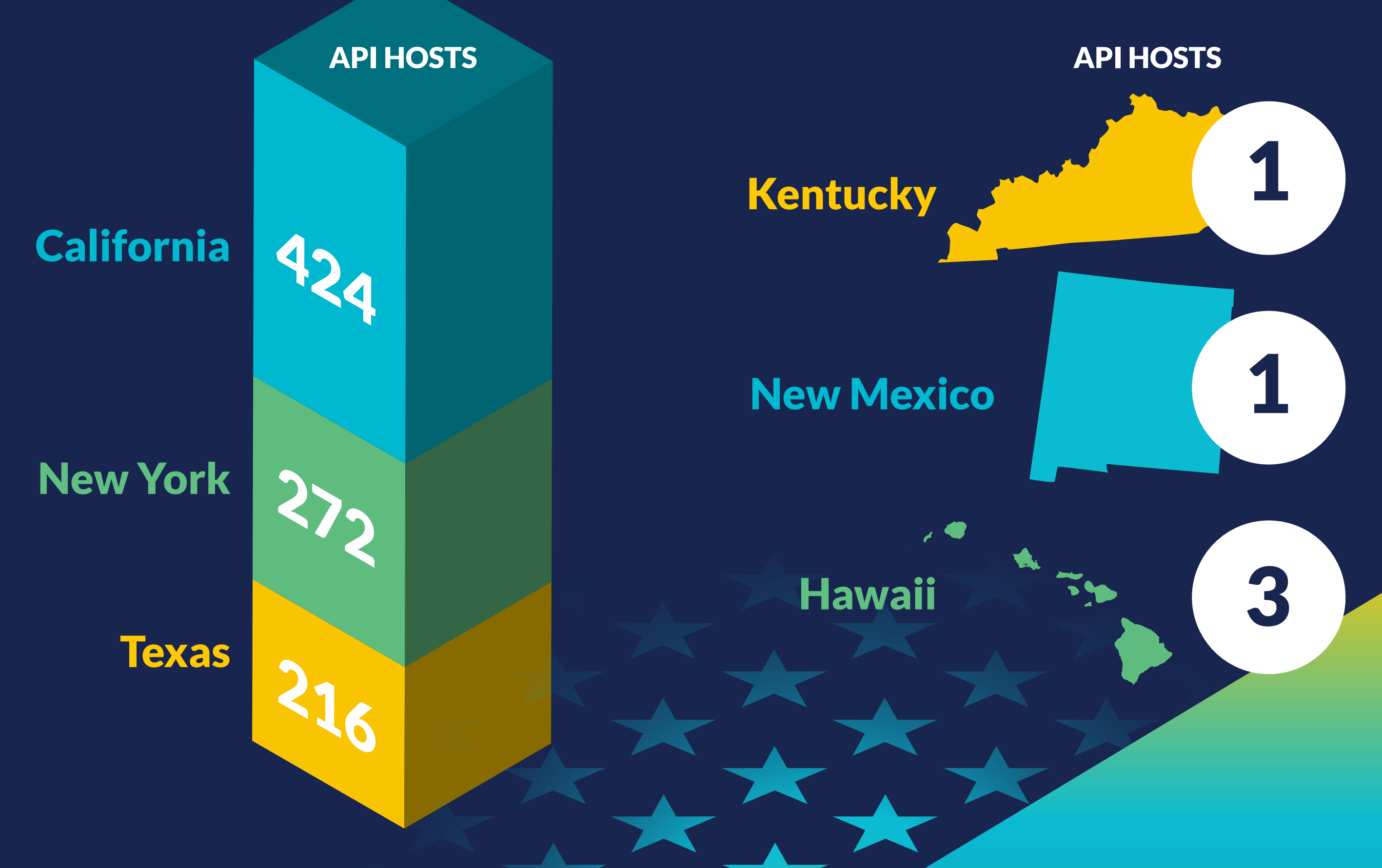
Which States Are Leading the Charge?

As we head to the polls this election season, it's crucial to understand where our nation's API security stands. This infographic highlights the states with the most robust and the most vulnerable API infrastructures, shedding light on the risks and best practices in API management. Let your voice be heard—not just at the ballot box, but in ensuring our digital landscapes are secure!

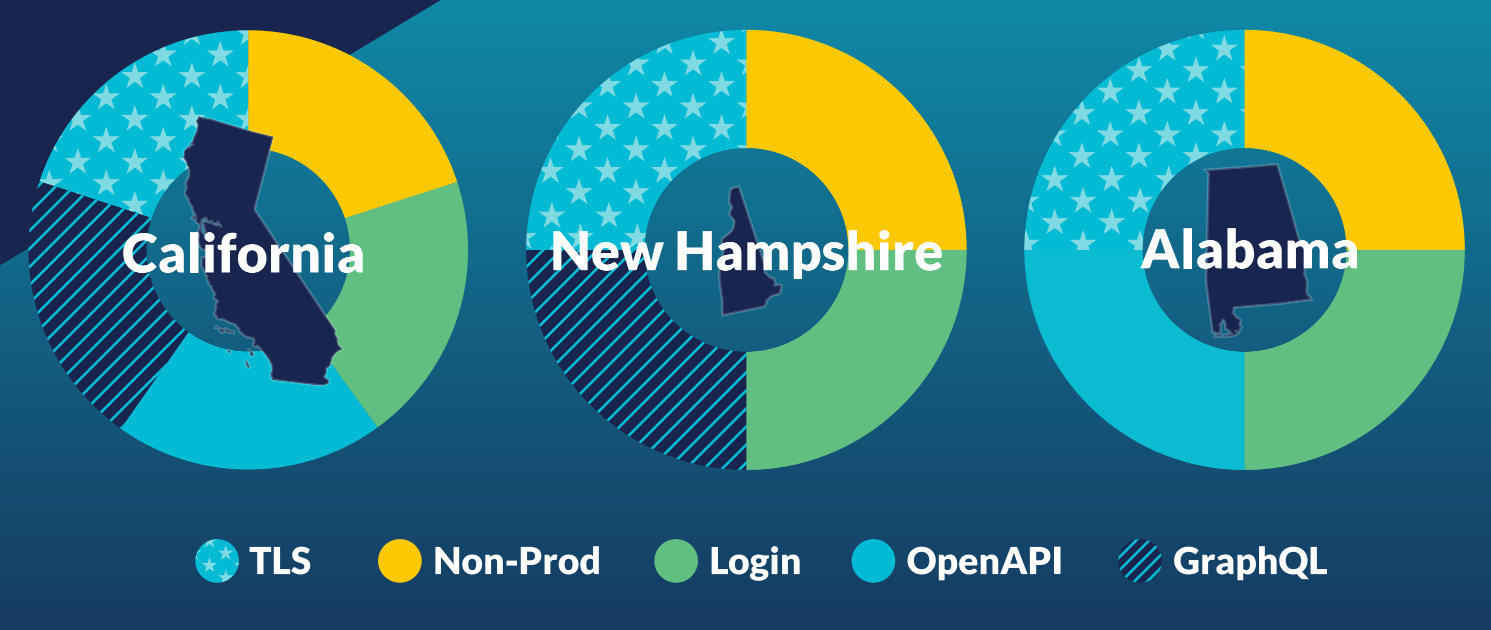
States with the Lowest Risk

States with the Most API Hosts

States with the Least API Hosts



States with the Most Security Findings



Top 3 Security Findings

- Transport Layer Security (TLS) Risks
- Login Risks
- Non-Prod Risks

Top 3 Hosting Providers

1. Amazon Web Services
2. Google Cloud Platform
3. Microsoft Azure

Top 3 Edge Providers

1. Cloudflare
2. Akamai
3. Fastly

Top 3 Gateway Providers

1. AWS API Gateway
2. Azure API Management
3. Google Cloud Endpoints

Cast Your Vote for a Secure Future

In the landscape of risk, there's a virtual tie between Democratic- and Republican-led states, much like the split we often see in elections. Just as voters are divided, so too are states when it comes to cybersecurity risks. **But per our predictions, Democratic-led states pull slightly ahead in cybersecurity readiness.** This is a reminder for all of us to exercise our rights—whether it's casting a vote or practicing cybersecurity best habits, our voices and actions shape a safer, more resilient world. Let's get out there, be it for the ballot box or the digital battlefield, and make a difference!

Democrats are the predicted winners!

METHODOLOGY

To determine the security landscape of APIs across the United States, we analyzed key metrics related to API hosting, provider distribution, and security findings. Each state was evaluated against a predefined algorithm that assesses risk based on factors like the ratio of API hosts to all hosts, the diversity of hosting providers, and the presence of security vulnerabilities. This comprehensive approach enables us to identify areas needing improvement and celebrate those leading in API security.

Security Best Practices Checklist

To mitigate risky behavior and enhance security, we recommend that government and public sector organizations consider the following best practices to protect sensitive data:

1 Restrict API Exposure
Limit sensitive data access via APIs and enforce strict access controls.

2 Minimize Provider Dependencies
Consolidate third-party services and audit them for security compliance.

3 Utilize Mature Cloud Providers
Choose reliable cloud providers and monitor configurations for vulnerabilities.

4 Limit Gateway Diversity
Use no more than three gateway types to simplify oversight and security policies.

5 Ensure API Gateway Coverage
Manage at least two-thirds of APIs with a centralized gateway and check configurations for compliance.

6 Verify Encryption Practices
Regularly audit encryption methods and address vulnerabilities immediately.

7 Secure Non-Production Environments
Isolate these environments from public access and monitor for exposed endpoints.

8 Protect Login Endpoints
Use multi-factor authentication (MFA) and strong password policies.

9 Safeguard API Specifications
Keep specifications private and review documentation to exclude sensitive info.

10 Restrict GraphQL Endpoint Exposure
Limit exposure of GraphQL endpoints, implementing rate limiting and authorization checks.

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai