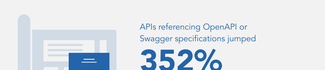
CEQUENCE SECURITY

APIs: Developer **Tool** of Choice. **#1 Target** for Malicious Use.

Today, software is eating the world and **APIs ARE TAKING THE BIGGEST BYTE**. Modern cars, every mobile app we use, our favorite shopping site, and our finance management all rely on APIs to deliver an engaging user experience. For these same reasons, threat attackers love APIs. So much so that Gartner predicts that by 2022, API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications.

APIs: **The Development Tool of Choice**

14.4B of the 21.1B application requests were **API-based.**



70%

USAGE PATTERNS OBSERVED FROM JUNE TO DECEMBER 2021

Much like blood tests uncover illnesses, **health monitoring APIs** used for solving system problems and known to expose too much information **saw usage skyrocket**

941%

APIs referencing OpenAPI or Swagger specifications jumped

352%

signaling increased adoption, but their public nature can provide an API attack blueprint.

GraphQL — THE HOT NEW API TECHNOLOGY

saw usage shoot up

133%

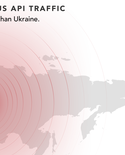
TOO OFTEN, NEW TECHNOLOGY ADOPTED (TOO) QUICKLY CAN **INTRODUCE SECURITY RISKS**

USER AUTHENTICATION, LOGIN or **ACCOUNT REGISTRATION WORKFLOWS** continue to be one of the primary API use cases, growing by

95%

APIs **EXPOSING SENSITIVE DATA** like payment (PCI) or personally identifiable information (PII) **INCREASED BY 87%** emphasizing the continued need for strong security and privacy in API development.

Public-facing APIs linked to internal or non-production applications **grew by 44%**, reminding enterprises to monitor internal applications to prevent inadvertent API exposure.



APIs: **#1 Target for Malicious Use**

of all blocked traffic was **API-BASED**

ATTACK PATTERNS OBSERVED

CONTENT SCRAPING, commonly caused by competitive snooping of product or technical information, was up

178%

resulting in wasted compute resources and cost overruns.

ACCOUNT TAKEOVERS, often the precursor to fraud, data loss or system compromise, increased 62%

MALICIOUS TRAFFIC originated from around the world with the top **10 COUNTRIES** shown in the map

58% — 86%

10x MORE MALICIOUS API TRAFFIC came from **RUSSIA** than Ukraine.

Protect Your APIs While **Empowering** Your Developers with Cequence Security

Organizations that rely on APIs to power their businesses trust Cequence Security to deliver the most comprehensive API Security Platform on the market. The Platform has proven to be effective in preventing unintended data leakage, outline fraud, business logic attacks and exploits, which helps our F500 customers remain resilient in today's ever-changing business and threat landscape. Cequence is the only API Security Platform vendor that unifies runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving online attacks.

SCHEDULE YOUR CEQUENCE API SECURITY PLATFORM DEMO:

CEQUENCE.AI/DEMO

CEQUENCE SECURITY

100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086, 1-650-437-6338, info@cequence.ai, www.cequence.ai

DATA SOURCE: CEQUENCE IS A LEADER IN API SECURITY AND THIS DATA WAS COLLECTED BETWEEN JUNE 1, 2021 AND DECEMBER 31, 2021 FROM F500 FINANCIAL SERVICES, RETAIL AND TELECOM ORGANIZATIONS.