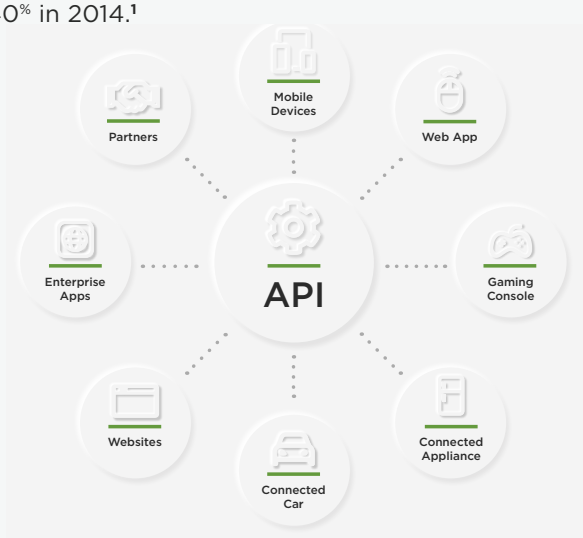
digital.ai™

Solution Brief

The rise of API threats due to modern app development

The advent of API-based services provides developers the ability to create mobile and web-based apps faster with seamless user experiences.

The adoption of API-based application development can clearly be seen in the dramatic shift in internet traffic — 83% of current traffic is API related, compared to 40% in 2014.[1]



Not all API traffic is legitimate

White traffic — legitimate traffic used to conduct business comprising a majority of all API traffic.

Black traffic — clearly dangerous traffic, usually directed at a web server to break through layers of network security. Common attack vectors are bots using brute force techniques (e.g., DDoS attacks) or more focused automated credential stuffing attacks.

Grey traffic — likely dangerous traffic, but on the surface it appears legitimate. Grey traffic is hard to recognize because it can utilize stolen, legitimate account IDs and tokens to gain access.

Why modern apps and APIs are so vulnerable

Any app published publicly can be vulnerable to reverse engineering and follow-on attacks because of poor code-level security and coding mistakes. A major source of API identity-based attacks can be attributed to mobile and web apps that unwittingly expose API secrets, including URLs, tokens, encryption keys, and login credentials. Unfortunately, lapses in mobile and web app security that expose organizations to risk are more common than should be tolerated.

- **74%** Organizations which experienced material cyber-attack because of compromised apps[3]
- **100%** Websites compromised by Magecart lacked source code protection[4]
- **97%** Mobile apps tested lacked any form of binary protection[5]
- **25%** Apps contained hard-coded API URLs, API keys, and other API secrets[5]
- **80%** Executed weak communication encryption methods[5]
- **60%** Did not mask database parameters or SQL queries[5]

Application-level security breaches enable secondary attacks against APIs because the information embedded in application code can provide a road map to the way APIs work.

According to Gartner, by 2021 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the UI.[2]

[1] *Akamai State of the Internet Security Report, Retail Attacks and API Traffic, Volume 5 Issue 2, 2019*

[2] "API Security: What You Need to Do to Protect Your APIs," Gartner, August 28, 2019

[3] Cost of a Data Breach Report 2019, Ponemon Institute and IBM Security

[4] In Plain Sight II: On The Trail of Magecart, Aite Group, August 2019

[5] In Plain Sight: The Vulnerability Epidemic in Financial Mobile Apps, Aite Group, April 2019

[6] OWASP API Security Top 10

In the new API Security Top 10, OWASP states:

By nature, APIs expose application logic and sensitive data such as Personally Identifiable Information (PII) and because of this have increasingly become a target for attackers.[6]

How to mitigate API attacks

Existing network security solutions address some issues with black traffic but have a clear gap when trying to address issues with grey traffic. In order to secure APIs, security professionals need to verify whether traffic using account IDs and tokens is actually legitimate. But if an application has been reverse engineered and API secrets uncovered, black traffic can be made to look legitimate all the while executing a follow-on attack using compromised API secrets.

Digital.ai Application Protection secures APIs on the client side

Protect mobile and web apps at the code level to prevent discovery of API details.

- Static and active binary and source code protections to prevent reverse engineering that could expose API information
- Encryption of data and keys to protect sensitive information from being intercepted
- Detects if an application and its contents are being targeted — in real-time — to notify the business and automatically trigger defense measures

Digital.ai in-app firewall helps prevent data exfiltration

To add another layer of web app security to existing network and authentication defenses, Digital.ai designed an in-app firewall that allows protected web apps to only connect to authorized APIs stopping the exfiltration of customer data from browser web forms.

Benefits of Digital.ai Application Protection

All of Digital.ai's protection capabilities are designed to prevent threat actors from reverse engineering app code and uncovering embedded information that can be used to conduct follow-on attacks against back office systems. Digital.ai Application Protection can also be integrated into today's rapid DevOps environments without slowing down your CI/CD processes.

One of the key capabilities integrated into all Digital.ai protection solutions is the ability to provide an understanding of the threat posture of any mobile or web app from the moment it's published.

From understanding how many jailbroken and rooted devices your mobile apps are running on — to instantly knowing if any code is being tampered with — Digital.ai App Aware (formerly Arxan) allows an organization to quickly understand the threat environment its apps are running in. This capability is an integral part of all Digital.ai's protection solutions and delivers real-time field level intelligence about the status of all protected apps — and the APIs embedded within.

Digital.ai threat data can feed into existing SIEM, BI, WAF, or fraud prevention platforms, helping to enrich known user data and provide a more complete picture of what, where, and who is attacking your apps. Digital.ai gives organizations the ability to automatically respond to threats by shutting accounts down, having apps disable functionality or access, and updating code before attacks can successfully breach back office systems.

Inside-out app protection

Digital.ai provides comprehensive, app-level security to protect against a range of threats or to enforce enterprise app governance — expanding the corporate perimeter of trust. Digital.ai provides a broad range of patented security capabilities to protect applications in the wild, such as a dynamic app policy engine, code hardening, obfuscation, white-box cryptography and encryption, and threat analytics.

About Digital.ai

Digital.ai enables enterprises to focus on outcomes instead of outputs, create greater business value faster, and deliver secure digital experiences their customers trust. The Digital.ai Value Stream Platform seamlessly integrates all the disparate tools and processes across the various value streams, uses data and AI/ML to create connective tissue between them, and provides the real-time, contextual insights required to drive and sustain successful digital transformation. With Digital.ai, enterprises have the visibility they've been seeking to deliver value, drive growth, increase profitability, reduce security risk, and improve customer experience.

Learn more at Digital.ai

©2020 Digital.ai is a trademark of Digital.ai Software, Inc.