CEQUENCE SECURITY

CUSTOMER CASE STUDY

Large Mobile Phone Carrier Discovers Thousands of Unmanaged and Insecure APIs

New Solution, API Spyder, Enables the Security Team to Get Full Visibility into their API Attack Surface and Secure it

One of the nation's largest mobile phone carriers with over 100 million wireless subscribers has been trying to get a complete understanding of its entire API footprint. API applications play a critical role in helping to support and manage their large nationwide network. The security team wanted to ensure that they had complete visibility into all APIs regardless of where they were deployed, to ensure that they had complete oversight and control.

The carrier's security team had been using Cequence's products API Sentinel and Bot Defense, part of our Unified API Protection solution, to protect their mission-critical API applications; however, the team was concerned if their existing count of API's was accurate. The Cequence account team introduced them to our new offering, API Spyder, also part of our Unified API Protection solution to help them obtain a complete discovery of their entire API attack surface, including all APIs regardless of where they were hosted.

THE RESULTS

API Spyder provides the customer with complete visibility of their attack surface

After running API Spyder, the security team's assumption was confirmed. There were thousands of unmanaged APIs that existed that the team had no visibility into and therefore no control over. API Spyder crawled through their entire public-facing APIs regardless of where they were hosted, building out their entire API footprint.

With API Spyder the security team was able to discover the following:

- **Complete API Footprint:** Obtain a complete API footprint of all API servers regardless of where they were hosted.
- **Automated Discovery:** Through API Spyder, they avoided the manual process of discovering and maintaining a list of external-facing API servers. The process of maintaining a complete list of APIs was laborious, never-ending, incomplete, and error-prone.
- **Continuous Discovery:** API Spyder provided a dashboard that ensured that if a new API application were developed, they would be immediately notified, ensuring that it would be secured.
- **No Security Blind Spots:** They now were able to surface any potential unprotected API applications that could serve as backdoor into their environment.
- **3rd-Party Risk:** They were able to ensure that OpenAPI specification files used by 3rd-party API integration partners were secure and not exposed publicly.

CUSTOMER PROFILE

One of the nation's largest mobile phone carriers with over 100 million wireless subscribers.

Goals

- Obtain a complete attack surface report of all API servers regardless of where they were hosted
- Discover if their understanding of the existing API server inventory was accurate
- Remediate any security issues on any API that could serve as a backdoor into their environment

What They Achieved

Full API server Discovery: Discovered over 1000 API servers that were not actively protected by any API security solution.

- **Non-production Servers:** Discovered that over 18% of their overall servers were exposed to non-production servers with no API security enabled.
- **Log4J Vulnerable Servers:** Despite a rigorous patching program, they had discovered that over 5 API applications with the Log4J vulnerability were not patched.
- **SSL Issues**: Over 30% of their API servers had SSL security issues such as invalid or expired certificates, potentially enabling a MITM (man-in-the-middle) attack.
- **Exposed Files:** They discovered over 107 files that could expose private keys that could be used to gain access to mission-critical business information.