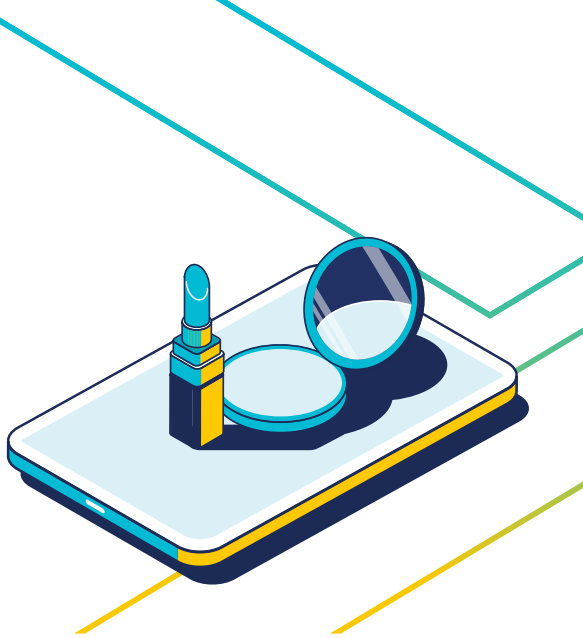
CEQUENCE

Case Study

American Multinational Cosmetic Company Adopts a Defense in Depth Approach to Application Security



API Applications Power Their Business

One of the world's largest multinational cosmetics companies has been in business for the last 77 years with a worldwide footprint in more than 150 countries. This cosmetics company owns a diverse portfolio of brands that are distributed internationally through both digital commerce and retail channels. Supporting this business is a set of 240 API applications that distribute their goods across suppliers, channels, and consumers.

Though supported by various software teams around the world, these application groups have no unified management that would enable the security team to easily track and coordinate the security posture of each of these applications that support the company's business operations.

No Real API Protection

More concerning, this cosmetic company's entire set of applications had no real API protection, making them vulnerable to a devastating cyber-attack that could exploit their organization, adversely impacting customers, brand image, and revenue.

The Cequence Unified API Protection (UAP) solution was introduced to the cosmetics firm's fraud team, which included managed service components that supported API protection, web application firewall (WAF), and distributed denial of service (DDoS) services. Deployed together, this delivered a defense-in-depth approach to application security across all of their applications.

The Results

Through the Cequence UAP platform and managed services, the security team was able to achieve an application security defense-in-depth approach that provided comprehensive security to defend their entire application portfolio:

- **Complete API Inventory:** Through API Sentinel, they obtained continuous discovery of their API inventory, immediately surfacing newly deployed APIs, ensuring they could constantly monitor for changes.
- **Compliance Enforcement:** API Sentinel provided full API compliance, governance, and best practices, ensuring they could identify and remediate high-risk APIs that posed an immediate threat to their organization.

Customer Profile

A multinational cosmetics company that is a manufacturer and marketer of makeup, skincare, fragrance, and hair care products that are sold in over 150 countries worldwide. Founded in New York in 1946, it has over 62,000 employees that support its operations worldwide. It has an annual worldwide revenue of over US$15 billion per year.

Goals

- **API Inventory:** Continuous and complete discovery of all APIs within the organization.
- **API Compliance:** Ensure that each API endpoint complies with OpenAPI specifications, governance and security best practices.
- **Real-time Mitigation:** Deploy an inline API protection solution that can block API attacks in real time with a low false positive rate.
- **DDoS Protection:** Defend against distributed denial of service (DDoS) attacks that could render an application completely inaccessible to its end-users.

- **Real-time Detection and Protection:** Deployed a real-time security solution that was able to detect and block targeted API attacks that aim to exploit their mission-critical applications.
- **DDoS Protection:** Enforced an extra layer of DDoS protection that blocked large-scale network attacks that aimed to disrupt their business operations.
- **Web Protection:** A WAF with a core rule set (CRS) that ensured they received up to date OWASP API Security Top 10 protection against common web exploits such as injection, cross-site scripting, and remote file inclusion (RFI).

What They Achieved

The security team acheived the following:

- **Discovered APIs:** 2,344 new API endpoints that were completely unmanaged with no OpenAPI specification or API protection.
- **Shadow APIs:** 4,801 shadow API endpoints that were not included in the OpenAPI specification file on the server.
- **Published APIs:** 1,662 API endpoints that were fully managed and had an OpenAPI specification file on the server.
- **High-Risk APIs:** 3,311 API endpoints that contained security risks. Of this number, 6 API endpoints contained security issues that required immediate remediation.