

## Datasheet

# Cequence Unified API Protection for Telecoms

## Protecting Global Telecommunications Organizations Against API Attacks

### Introduction

As a pioneering early adopter of technology, the telecommunications industry was among the first to embrace APIs and microservices to further business goals, like reducing cost and transaction friction, increasing visibility, and providing customers with compelling new services. Today, internal carrier services like billing, account management, and payments, along with external integration with third-party service providers like Apple, Netflix, Hulu, etc. all depend on APIs. To ensure uninterrupted business success, security teams must prevent the misuse and abuse of these business-critical services.

### API Security Challenges

Today's security teams face numerous challenges when it comes to protecting critical APIs and applications from cyber attacks. First, APIs are routinely developed and deployed by disparate teams at lightning speed across numerous cloud providers, creating a "fog of war" that shrouds security team visibility. Discoverable by attackers, these unmanaged and unprotected APIs often contain critical vulnerabilities that can lead to exploited applications and data breaches.

Second, security and development teams do not have a clear and consistent picture of the security posture of their APIs across their application footprint. Understanding where a critical vulnerability, sensitive data exposure, or business logic flaw can be exploited empowers security teams to work with development teams to pinpoint areas of security risk for immediate remediation.

Third, API applications are under constant attack with attackers seeking to find any opportunity to exploit an application and in turn, compromise your organization. The ability to detect and block attacks as they occur can prevent organizations from experiencing fraud, data exfiltration, and business disruption.

Security leaders are now asking three fundamental questions:

1. How many APIs do I have?
2. What risks do my APIs pose?
3. Are my APIs under attack?

### The Ideal Solution: Unified API Protection

To address these security challenges, a security solution must provide a complete discovery of your entire API attack surface that includes both external and internal APIs, understands your API risk posture pinpointing where you need to remediate critical security vulnerabilities, and provides real-time protection that blocks API attacks before they reach your application.

The solution should provide the following capabilities:

- **DISCOVER** Identify all external and internal APIs, ensuring you have visibility into the complete API attack surface of your organization.
- **COMPLY** Ensure that APIs comply with API specifications, security test requirements, and governance best practices.
- **PROTECT** Detect and block API threats in real time that target your APIs and applications, with minimal false positives.

The Cequence Unified API Protection solution provides exactly that.

### Telecom Use Cases



Block Payment  
Fraud



Mitigate SIM  
Swaps



Reduce CPNI  
Leakage



Manage API  
Risk



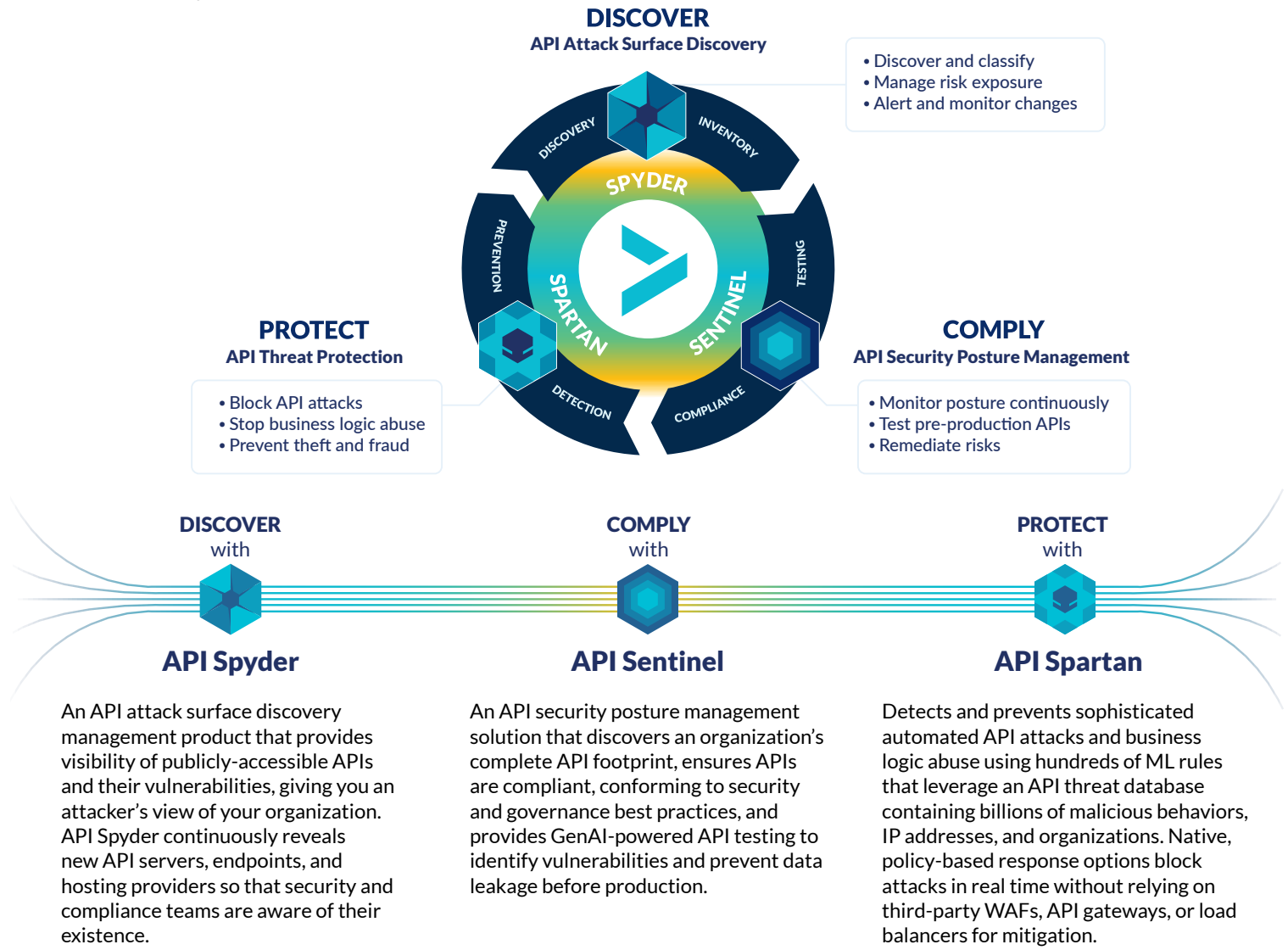
Prevent MSISDN  
Activation Fraud



Protect Hype  
Sales

# The Cequence Unified API Protection Solution

The Cequence solution is the only security offering that addresses all phases of your API security lifecycle, discovers your entire API attack surface, eliminates unknown and unmitigated API security risks, and protects your APIs from cyber attacks that lead to data loss, fraud, and business disruption.



The Cequence Unified API Protection solution enables customers to continuously reap the competitive and business advantages of secure, ubiquitous API connectivity. The Cequence solution results in attack futility, failure, and fatigue for even the most relentless of attackers. It significantly improves visibility and protection while reducing cost, minimizing fraud, data loss, non-compliance, and business disruption. Learn more at [www.cequence.ai](http://www.cequence.ai).

## Protecting Top Global Telecommunication Brands

**\$10T** Business value protected

**8B** Daily API transactions secured

**3B** User accounts safeguarded

