Data XD: Discover | Monitor | Secure APIs
API Security Gaps Lead to Data Breaches

By Year 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise applications- **Gartner Report ID G00342236**

OWASP API Security Top 10

1. Broken Object Level Authorization
2. Broken Authentication
3. Excessive Data Exposure
4. Lack of Resource & Rate Limiting
5. Broken Function Level Authorization
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Asset Management
10. Insufficient Logging and Monitoring

Limitations of Existing Tools

Lack API Discovery
- Manual API spec creation/update
- Incomplete, not updated
- Not automatically verified against actual traffic

Lack Deep API Tracking
- No object level data tracking
- No function level behavior tracking
- Cannot correlate assignments
- Overall lack API spec

You Cannot Protect the Invisible

Capital One

The Issue: CapitalOne Insider Data Leak
Stolen access credentials, Aug, 2019 Undetected Data Exfiltration Using S3 API: Lack of Resource & Rate Limiting, Broken Function Level Authorization, Security Misconfiguration | **100M+ Records, 6+ Months**

The Solution: Deep Data DR
Enables targeted Detection and rapid Response to API data structure level anomalies

You Cannot Protect the Unknown

T··Mobile

The Issue: T-Mobil Nothing to Discover Shadow APIs:
T-Mobile Private API Exposed, May, 2018:
Injection, Improper Asset Management
20M Records, 12+ Months

The Solution: Discover 360
CloudVector Micro-Sensors discover all APIs, establishing a structured data blueprint that enables Deep Data DR

Data XD: Discover | Monitor | Secure APIs
API Security Gaps Lead to Data Breaches

By Year 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise applications- **Gartner Report ID G00342236**

OWASP API Security Top 10

1. Broken Object Level Authorization
2. Broken Authentication
3. Excessive Data Exposure
4. Lack of Resource & Rate Limiting
5. Broken Function Level Authorization
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Asset Management
10. Insufficient Logging and Monitoring

You Cannot Protect the Invisible
You Cannot Protect the Unknown

The Issue: CapitalOne Insider Data Leak
Stolen access credentials, Aug, 2019 Undetected Data Exfiltration Using S3 API: Lack of Resource & Rate Limiting, Broken Function Level Authorization, Security Misconfiguration | **100M+ Records, 6+ Months**

The Solution: Deep Data DR
Enables targeted Detection and rapid Response to API data structure level anomalies

The Issue: T-Mobil Nothing to Discover Shadow APIs:
T-Mobile Private API Exposed, May, 2018:
Injection, Improper Asset Management
20M Records, 12+ Months

The Solution: Discover 360
CloudVector Micro-Sensors discover all APIs, establishing a structured data blueprint that enables Deep Data DR

Limitations of Existing Tools

Lack API Discovery
- Manual API spec creation/update
- Incomplete, not updated
- Not automatically verified against actual traffic

Lack Deep API Tracking
- No object level data tracking
- No function level behavior tracking
- Cannot correlate assignments
- Overall lack API spec

Gartner: Adopt a Continuous Approach to API Security: Discover, Monitor, and Secure Use a Distributed Enforcement Model to Protect APIs Across Your Entire Architecture, Not Just at the Edge

Data XD: Discover | Monitor | Secure APIs

API Security Gaps Lead to Data Breaches

By Year 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise applications- **Gartner Report ID G00342236**

OWASP API Security Top 10

1. Broken Object Level Authorization
2. Broken Authentication
3. Excessive Data Exposure
4. Lack of Resource & Rate Limiting
5. Broken Function Level Authorization
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Asset Management
10. Insufficient Logging and Monitoring

You Cannot Protect the Invisible You Cannot Protect the Unknown

DISCOVER
MONITOR
SECURE

The Issue: CapitalOne Insider Data Leak

Stolen access credentials, Aug, 2019 Undetected Data Exfiltration Using S3 API: Lack of Resource & Rate Limiting, Broken Function Level Authorization, Security Misconfiguration | **100M+ Records, 6+ Months**

The Solution: Deep Data DR

Enables targeted Detection and rapid Response to API data structure level anomalies

The Issue: T-Mobil Nothing to Discover Shadow APIs:

T-Mobile Private API Exposed, May, 2018:
Injection, Improper Asset Management
20M Records, 12+ Months

The Solution: Discover 360

CloudVector Micro-Sensors discover all APIs, establishing a structured data blueprint that enables Deep Data DR

Limitations of Existing Tools

Lack API Discovery

- Manual API spec creation/update
- Incomplete, not updated
- Not automatically verified against actual traffic

Lack Deep API Tracking

- No object level data tracking
- No function level behavior tracking
- Cannot correlate assignments
- Overall lack API spec