DORA

API Compliance Checklist

For CISOs and Security Managers

equixly

API Compliance: DORA

Compliance requirements sometimes seem like an additional load on already-burdened security and development teams. However, they're simply a standardized acknowledgment of what every organization must do to ensure the security of its information systems and networks, including APIs.

APIs are integral to contemporary information environments. An application or digital system can only be imagined with a heavy reliance on application programming interfaces. As an example, *2023 State of API Security: A Global Study on the Reality of API Risk* stated that the 1629 surveyed organizations from over 100 countries relied on as many as 501–2,500+ APIs.

These numbers underscore the fact that strong and resilient information environments greatly depend on strong and resilient APIs. And strong and resilient APIs are compliant APIs.

DORA stands for Digital Operational Resilience Act. The more formal name is Regulation (EU) 2022/2554.

DORA is a cybersecurity regulation applying to financial entities operating on the territory of the European Union. Its objective is to consolidate digital operational resilience measures for the finance sector across the EU.

To attain this goal, DORA sets strict requirements regarding:

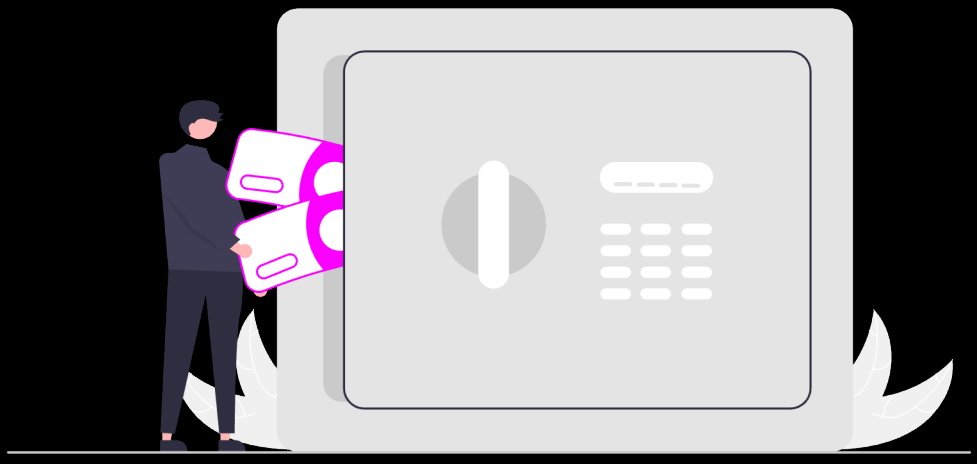
- ICT (information and communication technology) risk management
- Incident reporting and notifying
- Digital operational resilience testing
- Sharing of information and intelligence on cyber threats and vulnerabilities
- ICT third-party risk management
- Contractual arrangements between ICT third-party services and financial entities
- Establishing and executing the Oversight Framework for critical ICT third-party services
- Supervision and enforcement as well as cooperation between authorities regarding DORA

Who Does DORA Apply To?

As already noted, DORA is a sector-specific regulation—it applies exclusively to financial entities. However, this is too general and requires a further explanation of who precisely is subject to the DORA requirements.

The list of financial entities affected by DORA is lengthy. It includes 21 types of organizations and persons:

1. Credit institutions
2. Payment organizations
3. Account information service providers
4. Electronic money institutions
5. Investment companies
6. Crypto-asset service providers and issuers of asset-referenced tokens
7. Central securities depositories
8. Central counterparties
9. Trading venues
10. Trade repositories
11. Managers of alternative investment funds
12. Management companies
13. Data reporting service providers
14. Insurance and reinsurance undertakings
15. Insurance, reinsurance, and ancillary insurance intermediaries
16. Institutions for occupational retirement provision
17. Credit rating agencies
18. Administrators of critical benchmarks
19. Crowdfunding service providers
20. Securitization repositories
21. ICT third-party service providers



One caveat: Additional conditions apply to 2, 4, and 6, so if your organization falls within those three types, refer to DORA, Article 2, for further clarification.

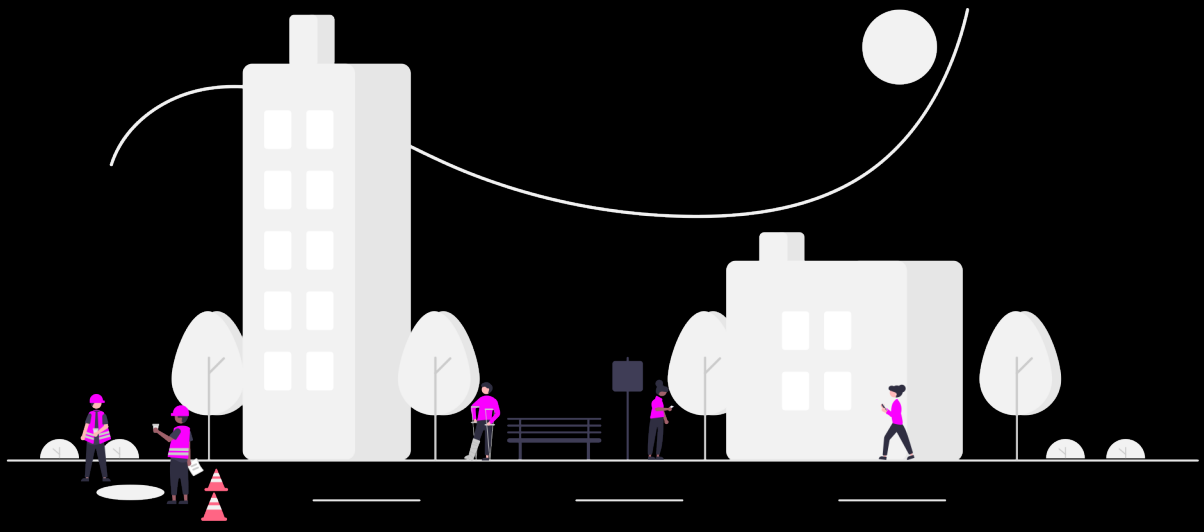
Also, keep in mind that some financial entities may be of a type covered by DORA but still be outside DORA's scope. More specifically, the regulation does not apply to:

- Managers of alternative investment funds covered by Directive 2011/61/EU, Article 3(2)
- Insurance and reinsurance undertakings covered by Directive 2009/138/EC, Article 4
- Institutions for occupational retirement provision operating pension schemes that do not exceed 15 members overall
- Insurance, reinsurance, and ancillary insurance intermediaries that belong to the categories of micro, small, or medium-sized enterprises as defined in EU recommendation 2003/361, Article 2

In addition, exempted from DORA are the following two types of entities:

- Post office giro institutions
- Natural or legal persons covered by Directive 2014/65/EU, Articles 2 and 3

It is worth noting that DORA also affects non-EU financial entities as long as they operate on EU territory.



DORA and NIS2

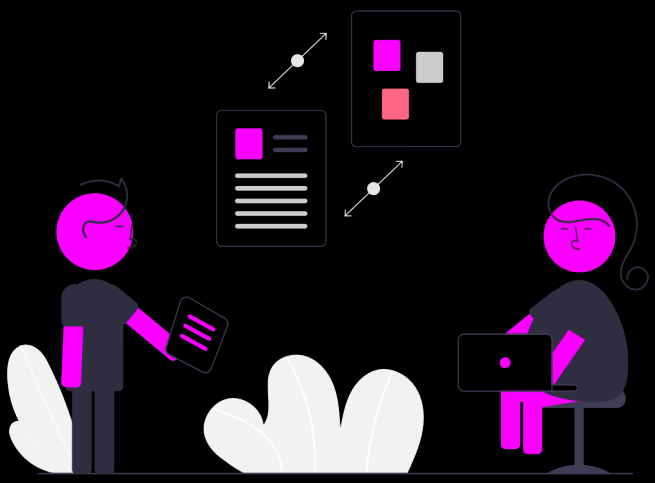
The DORA recitals and articles contain multiple references to NIS2, that is, Directive (EU) 2022/2555. Moreover, an entire DORA article, Article 47, is dedicated to the structures and authorities established by NIS2. That makes it crystal clear that DORA and NIS2 have a strong relationship.

Both legal provisions aim to harmonize financial entities' cybersecurity efforts. Nevertheless, as a sector-specific regulation, DORA provides tighter, more specific measures and, hence, leads to a higher level of harmonization than NIS2.

DORA is *a lex specialis* in relationship to NIS2, meaning it takes precedence in matters directly related to the finance sector.

However, DORA's precedence does not make NIS2 irrelevant for financial entities. It simply means they should avoid duplicating technical and organizational measures by giving DORA an advantage in matters where the requirements overlap (instead of following both).

Still, since NIS2 is broader in scope and regulates issues that DORA does not cover, financial entities' practices must also be consistent with NIS2 requirements. For example, financial supervisors are obliged to share information on security incidents with the authorities and single points of contact established by NIS2 and in accordance with the directive.

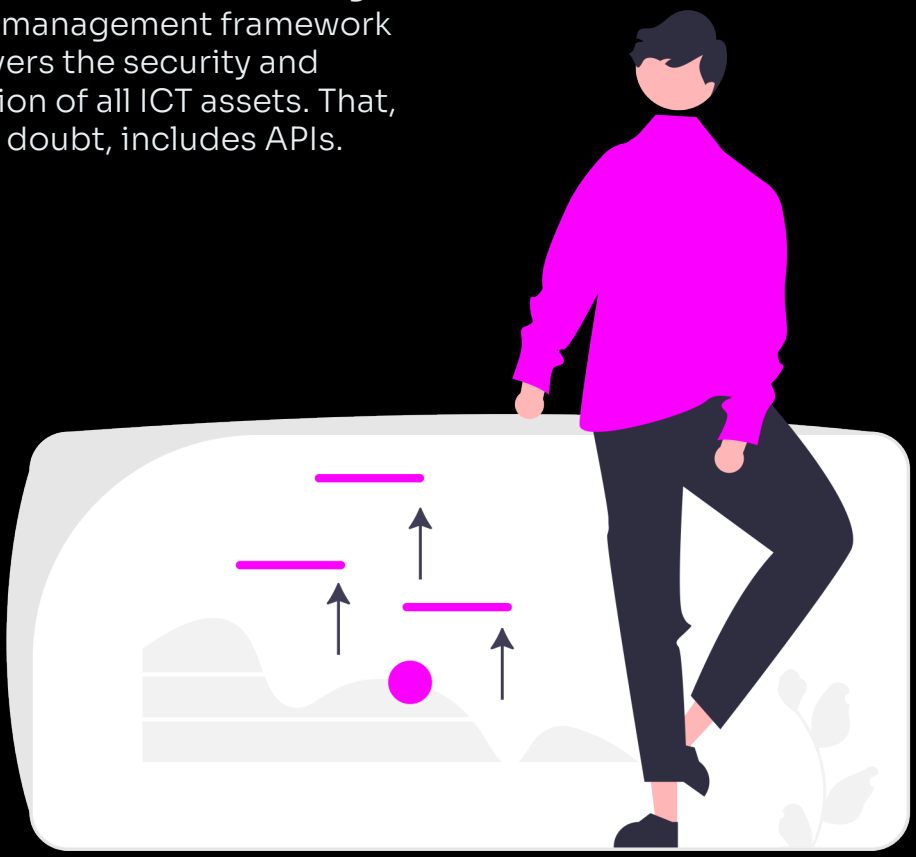


DORA
Compliance Checklist for APIs

1. Establish an ICT Risk Management Framework with Special Consideration for APIs

DORA, Chapter II, requires financial entities to establish a well-documented and thorough ICT risk management framework that covers the security and protection of all ICT assets. That, without doubt, includes APIs.

Considering how prevalent APIs are and how common API security incidents and cyberattacks have become, API security must play a prominent role in your framework. That means recognizing API's unique nature and treating API security as a separate subject irreducible to web application security.



DORA
Compliance Checklist for APIs

2. Create a Risk Management Body that Understands the Pivotal Role of APIs

DORA also mandates that financial entities establish a management body responsible for implementing their ICT risk management frameworks.

Some of the management body's responsibilities include:

- Creating policies for high data security standards and business continuity
- Assigning clear risk management roles and duties inside the organization
- Determining the risk tolerance level of the financial entity
- Allocating budget for advancing the entity's digital operational resilience
- Taking account of third-party ICT providers
- Establishing reporting channels
- Providing security awareness and digital operational resilience training
- Continuously gaining up-to-date knowledge and skills related to ICT risk management

It is difficult to imagine a financial entity's high risk tolerance without proper attention to the APIs in its information environment. APIs are the connective tissue between different systems, applications, and data sources, making strong API security imperative.

For this reason, the members of management bodies must clearly understand the inner workings of their organization's digital systems in relation to APIs and ensure that this knowledge is available to the rest of the employees, especially developers and security professionals.

As a result, it is only natural to allocate a separate budget or at least sufficient material means for securing critical APIs.

DORA
Compliance Checklist for APIs

3. Use Appropriate Purpose-Built API Solutions

DORA requires financial entities to deploy appropriate tools to ensure the security and protection of their ICT systems. Applied to APIs, that means using purpose-built security solutions instead of over-relying on WAFs (web application firewalls) and gateways.

The API security tools market is nascent but quickly developing. OWASP (Open Worldwide Application Security Project) differentiates between three general categories covered by API security tools:

- API security posture
- API runtime security
- API security testing

Research the possibilities carefully and choose an API security solution that best fits your environment, not the most popular and marketed one.

4. Conduct API Risk Assessment

Proper security risk management requires identifying API risk sources and conducting API risk and vulnerability assessments. The most recent OWASP Top 10 API Security Risks should be the starting point for your API security risk and vulnerability assessment process.

API risk assessment should not be a one-time affair. You must assess your APIs for risk regularly and continuously, including after every significant change.

In the process, you must identify all information assets and processes, including those coming from third parties. Inventorying assets and APIs must be integral to this process. It goes without saying that you should update your API inventory upon every change in your API landscape, such as when your organization retires an API, develops a new one, or updates an existing one.

DORA
Compliance Checklist for APIs

In addition, you should collect information on in-the-wild vulnerabilities, threats, incidents, and cyberattacks and evaluate the potential impact they can have on your organization's digital operational resilience.

5. Continuous API Security Monitoring and Threat Detection

Continuous API security monitoring and threat detection are a must.

Employ API security solutions that help you detect anomalous behavior and real-time cyberattacks on your APIs. API monitoring and detection tools that integrate smoothly within your existing workflows and send automated alerts to staff members so they react promptly and prevent major incidents are highly recommended.

6. Implement Strong API Data Security Mechanisms

DORA puts a strong emphasis on protection against:

- Data impairment, corruption, breach, and loss
- Compromised data authenticity and integrity
- Unauthorized data access
- Lack of data availability
- Poor data administration

Taking into account that APIs play a fundamental role in data exchange and most of the highly publicized API cyberattacks, such as the Optus security incident, have ended in data breaches, you must take great care to ensure that:

- Your APIs do not expose excessive data or leak data in other ways
- You know which API endpoints operate with sensitive data (data classification) and fortify their defense

DORA
Compliance Checklist for APIs

Your API data protection efforts should focus on implementing robust authentication and authorization, considering that the two most frequent and severe API security vulnerabilities involve precisely these two.

For practical guidelines on implementing proper authentication and authorization, refer to the OWASP API Security Top 10 entries on Broken Object Level Authorization, Broken Authentication, Broken Object Property Level Authorization, and Broken Function Level Authorization.

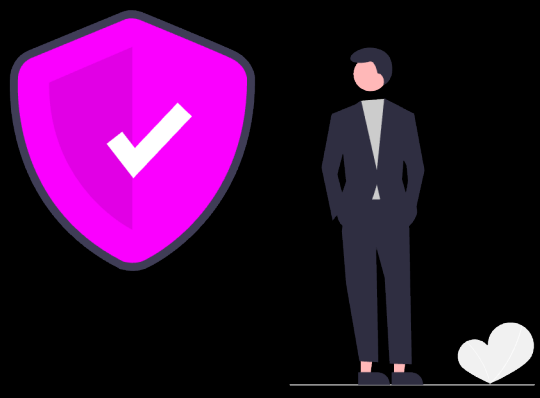
sure that API security takes up a significant portion of your security training program. Security professionals, developers, and management must all be properly informed about what is at stake when API security is neglected.

In addition, organizations must stay current and follow the development of new technologies and their impact on APIs, both positive and negative. For instance, while AI can elevate API security testing to another level, threat actors can also use it to improve and streamline API reconnaissance.

7. API Security Training

DORA makes ICT security awareness and digital operational resilience training mandatory. This training must include senior management as well as technical staff. Interestingly, DORA prescribes that security training should also include third parties when possible.

The number of API cyberattacks is growing in parallel with the number of APIs in use, so make



DORA
Compliance Checklist for APIs

8. Develop an Incident Management Process that Includes API Security Incidents

Your organization must develop incident response procedures in the form of an incident response plan, and APIs must be part of it.

Preparations for handling API incidents should include:

- Simulating API-specific attacks
- Assigning incident response roles
- Establishing appropriate communication channels

Ensure that additional strengthening measures are taken after API weaknesses are detected in simulations as well as in the aftermath of actual incidents.

To avoid penalties, you must report major API incidents to higher management and relevant external authorities without unnecessary delays.

9. Conduct Regular and Frequent API Security Testing

DORA dedicated an entire chapter to digital operational resilience testing, signaling its critical role in financial entities' cyber resilience.

Since digital operational resilience testing plays a key role in both risk assessment and incident handling, the regulation requires financial entities to develop a digital operational resilience testing program.

Your program needs to include diverse types of API security and software testing, such as:

- Automated and manual API penetration testing
- API vulnerability scanning
- API source code review
- Open-source analysis

In addition, since DORA requires advanced testing in the form of threat-led penetration tests (TLPTs), critical APIs should be included in this type of testing too.

DORA
Compliance Checklist for APIs

But keep in mind that here, the emphasis is on “advanced,” which implies that TLPT is different from standard penetration testing.

Regular and frequent standard penetration tests are not just feasible but highly recommended. That applies especially to automated pentesting precisely due to it being automated and boosted by artificial intelligence and machine learning. In contrast, as extremely time-consuming and resource-intensive, and on top of that, conducted in live environments, frequent TLPTs are neither attainable nor recommended by DORA.

As a final note, you must include API security testing in both development and production and ensure that it leads to a high rate of accuracy in vulnerability detection, as well as risk prioritization and remediation.

10. Keep Track of Third-Party APIs

As DORA roughly states, third parties are an integral part of ICT risk, which is why financial entities must pay special attention to third-party risk management. And to ensure all-encompassing third-party risk management, you must make third-party APIs part of your security program.

Keeping track of third-party APIs in your information environment is a highly recommended practice because they can be the weakest link in the ICT supply chain. To ensure high visibility, make sure to:

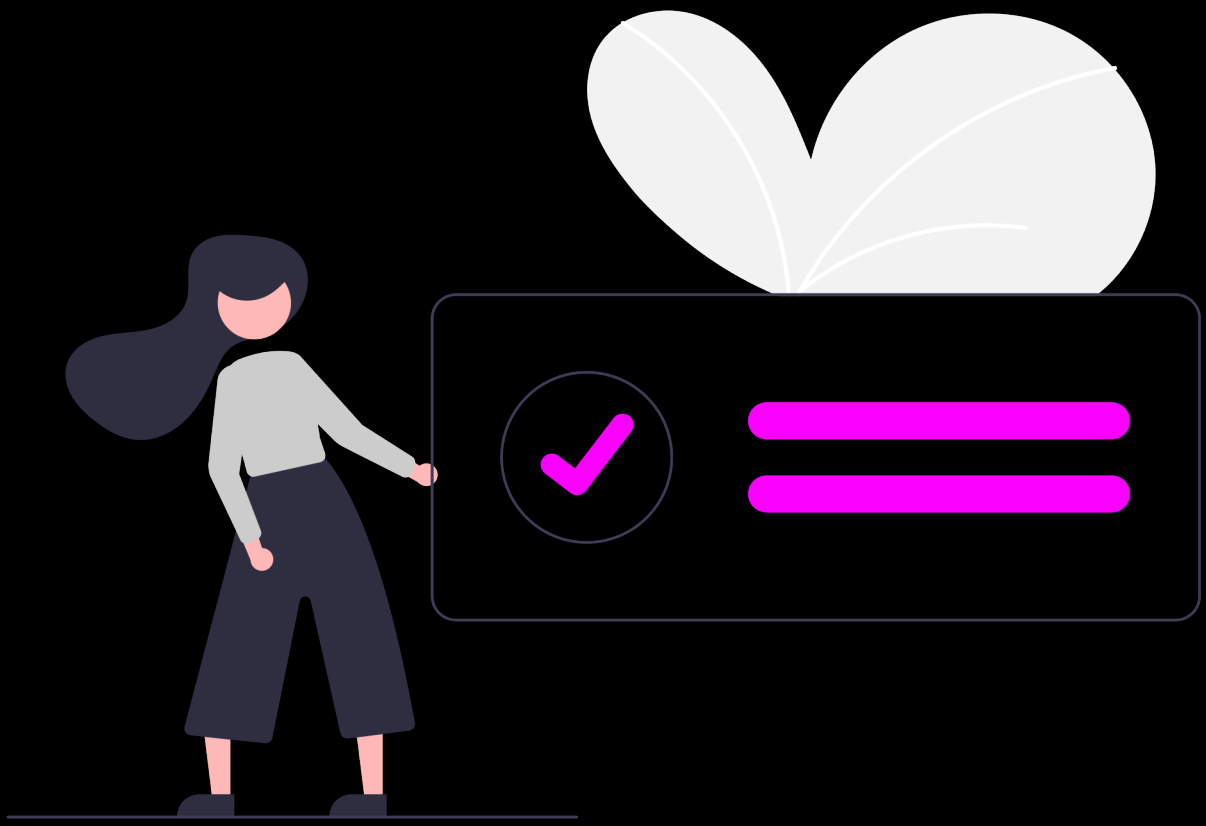
- Maintain a list of third-party APIs
- Update the list as the APIs change
- Note when the original vendor retires them, or you no longer use them for other reasons

Conclusion

DORA is a new directive whose goal is to harmonize cybersecurity measures in the EU's finance sector and elevate its cyber resilience to a higher level. It overlaps with another recent regulation, NIS2, but it takes precedence in matters directly applicable to financial entities.

DORA's scope is generally simple to understand. However, certain subtleties must be considered when deciding whether this set of compliance requirements affects your organization.

Due to APIs' omnipresence and pivotal role in today's applications and digital systems, financial entities must take proper steps to secure both the third-party APIs they use and their own APIs, from including them in their cybersecurity risk management and incident handling programs to deploying purpose-built API security solutions.



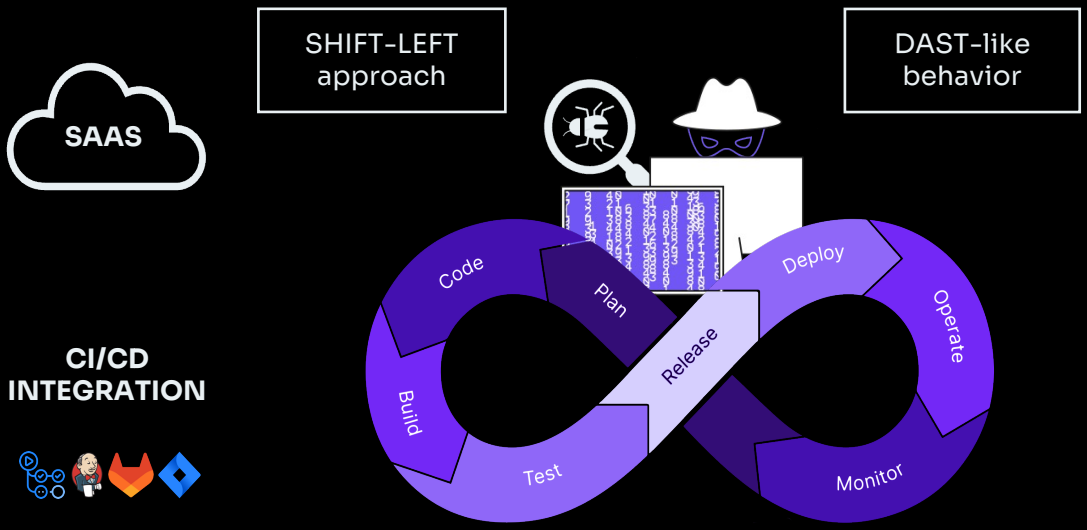
What is Equixly?

Equixly is an AI-driven, API Penetration Testing platform that delivers timely, actionable feedback and helps keep track of the details of thousands of your APIs, empowering decision-makers, as well as developers and security professionals. It alleviates pain points where there are budget and time restrictions and fills gaps where there's a staffing void and missing expertise.

As primarily an automated penetration tester or virtual ethical hacker, Equixly uses the same principles of work as ethical hackers, probing APIs and attacking them just like a hacker would. Why? To discover vulnerabilities and oversights and inform you before threat actors find them, bringing chaos to your cosmos.

Since the team behind Equixly knows that the context determines whether an API action is legitimate, Equixly goes further than testing only for common API vulnerabilities. On top of testing for the OWASP Top 10 API Security Risks, it also searches for subtle context indicators that point to barely perceptible business logic flaws or omens for the birth of a new zero-day.

In addition, Equixly is built for continuous security testing in development, makes shadow and zombie API discovery possible, and helps mend security weaknesses that may occur after significant software updates.

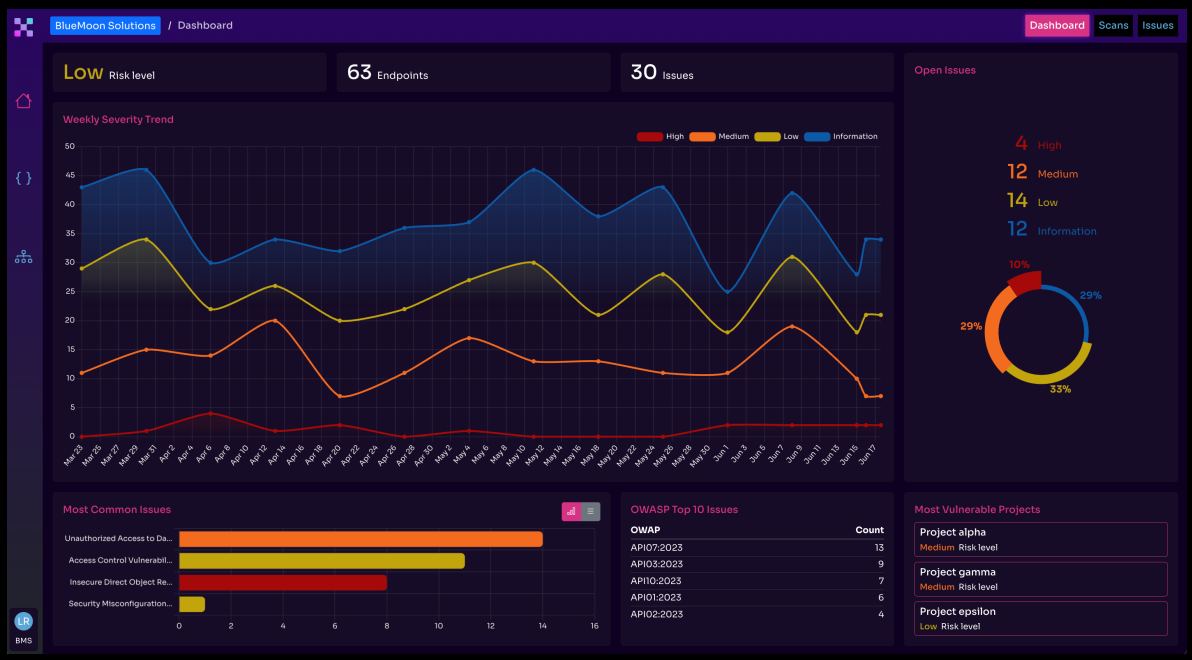


Why Equixly?

Manual testing is time-consuming and limited, both in scope and scalability. Equixly's platform harnesses the power of machine learning to execute hundreds of appropriate API attacks automatically.

Comprehensive penetration tests are not run often. Equixly can be run at any time during the SDLC, for example, each time a feature is released or updated. That enables addressing vulnerabilities early, reducing risk & the costs of later-stage remediation.

Addressing all the security vulnerabilities at once can be overwhelming. Equixly is a paradigm shift. Addressing security concerns during development not only helps secure the code but also offers actionable learnings, enhancing an organization's overall API security maturity.



Equixly's SaaS Dashboard

Contact us

MEET US

Equixly – Local Office

Via Evangelista Torricelli, 8/A

37135 Verona, Italy

Equixly – HQ

Via del Tiratoio, 1

50124 Florence, Italy

WRITE US

General questions

info@equixly.com

Sales Team

sales@equixly.com

VISIT US

Website

https://equixly.com/

Blog

https://equixly.com/blog/

CALL US

Book a meeting

https://meet.equixly.com/