

Welcome to your KYND ON guide

See, understand, and manage cyber risks easier and quicker than ever before with the help of KYND ON

With new threats appearing every day, it's no longer a question of if an organization will face a cyberattack – it's when.

Luckily, KYND ON has you covered. KYND ON is a powerful cyber risk management platform that provides continuous monitoring and will alert you to new and potential risks as they arise.

This guide addresses some of the key questions about using KYND ON to identify and mitigate the key cyber vulnerabilities posing a risk to your organization.



How does the KYND ON analysis work?

KYND delivers a comprehensive cyber risk assessment using just one of your organization's registered domains. This non-intrusive analysis examines over 280 risk indicators across domain configuration, email security, and exposed services. Plus, KYND delves into your internal security practices through a set of questions, requiring no special access or involvement from your organization.

The results are clearly presented using a simple traffic light system, making it easy for you to understand your cyber risk at a glance.

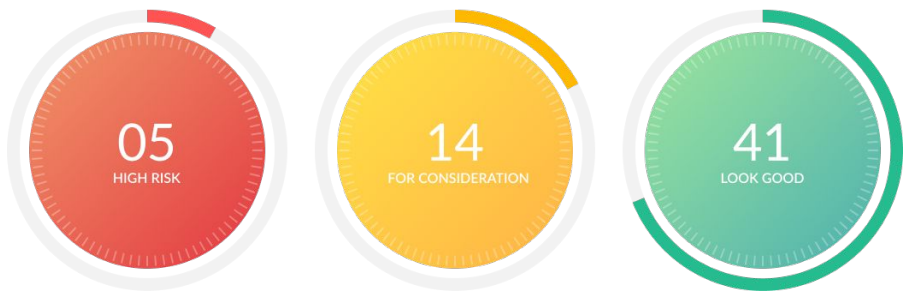


What does KYND look for?

KYND is looking for any instances of exposed services or critical software vulnerabilities we can identify. These are risks that would significantly increase your organization's exposure to cyberattacks.

KYND scans a single URL to uncover exposed services, critical vulnerabilities, and connected assets. The non-invasive Risk Report checks more than 280 cyber risk factors, including domain registration, email security, and internet-facing services.

Your cyber risk overview



When you log into your KYND ON portal, you'll instantly get a clear, traffic light-style view of your cyber risk – so you know exactly where you stand at a glance. The dial numbers represent the risk factors that KYND has discovered.

RED: Marked as “High risks”, these are the risks that KYND believes will cause business interruption if not addressed.

AMBER: Marked as “For consideration”, these are the risks that KYND believes may cause possible business interruption if not addressed.

GREEN: Marked as “Look good”, these risks appear not to carry an immediate risk based upon the information KYND has access to.

Your priorities

Essential Actions

!

Advisable Actions

Your priorities

These are the cyber risks usually considered by others when making decisions about your organization.

See your priorities

▲ There are 6 advisable issues to be resolved

KYND has compiled the identified risks that external parties – such as insurers, investors, or procurement teams – are likely to assess during insurance, investment, or due diligence decisions.

Your internal security

Assess your organization's internal security measures to ensure you have the necessary procedures and policies in place for robust cyber resilience.

As you respond to the questions, KYND will pinpoint any associated risks and feature them in your Risk Report.

✓

✓

Your internal security

Review your internal security practices to make sure you are always resilient against cyber attacks.

Manage your risk posture

▲ There are questions you need to answer



Your domains

These are the things associated with your Internet addresses (aka. your Internet domains).

 domains found

Manage

Your domains

This section lists the domains you provided at registration, plus others KYND has linked to your organization. Maintaining control of these domains is critical – losing any could seriously disrupt your business operations.

Mail security risks

This section checks for email addresses without SPF, DKIM, or DMARC protection, leaving them open to spoofing. Without these safeguards, your organization is at high risk of impersonation attacks targeting staff, customers, and partners.



Mail security risks

Check whether your email can be spoofed

 There are items to check

Manage



Data breach risks

Be alerted to breaches in your databases, helping you to comply with GDPR

 You haven't set up any credentials yet

Manage

Data breach risks

As an option, KYND continuously monitors secret synthetic identities in your databases, alerting you to potential data leaks so you can act quickly. A data breach occurs when sensitive information is accessed or exposed without authorization.

Phishing and malware

This section checks if any of your domains or subdomains are linked to phishing or malware. These threats can trick users into sharing sensitive data or infect their devices to cause harm or exploit systems.



Phishing & Malware

Check that your websites aren't hosting dangerous content

 Everything is secure and up to date

See risks

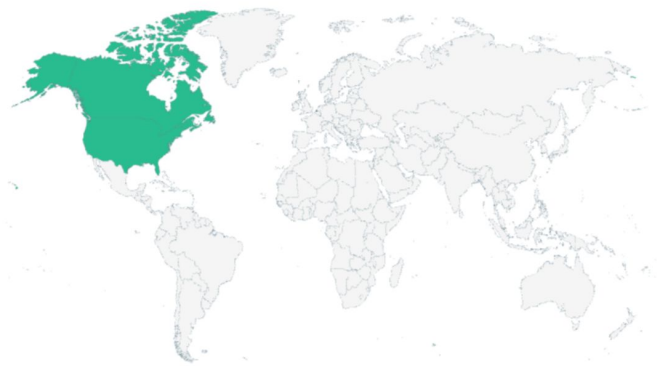
Your service locations

On this map, you can see all the international locations your Internet services are running from so you can check and ensure there are no unexpected surprises.

Your service locations

We have visualized all the locations your Internet services are running from so you can check there are no surprises.

41 services in undefined



Got questions?

If you have any questions about your KYND ON findings, easily get in touch with our friendly team by either sending us an email at info@kynd.io or tapping the  icon in your KYND ON dashboard. Visit kynd.io/kynd-on-guide for more details.

