

# Site Blocking



# SITE BLOCKING AT A GLANCE

**In order to avoid word repetition, when we refer to site blocking we also include IP blocking, DNS blocking and the (synonym) “website” blocking.**

**Site blocking is the practice of preventing access to specific websites or online content by individuals or users within a particular region or network.**

**Site blocking is a contentious issue, as it often involves concerns about freedom of expression and censorship. If done correctly it can however be an effective method to curb piracy and protect intellectual property rights.**

**Our main goal (together with our customers) is to discourage and protect users from pirated sites and encourage them to use legitimate ones.**

## INTRODUCTION

Pirated content is everywhere. And the varied ways of accessing it proliferate by the day. This can raise the question of whether trying to block pirate websites is even worth the effort. At Irdeto, we believe it is. Site blocking is a targeted and effective strategy that restricts access to illegal online platforms distributing copyrighted content without authorization. By denying users access to these rogue websites, we disrupt the main sources of piracy, curtailing their ability to profit from stolen content and protecting artists, musicians, filmmakers, and other creators. We strive for migrating users to legal platforms.

# THE GOALS OF SITE BLOCKING

At the request of rights-holders, Internet Service Providers (ISPs) generally use site blocking to prevent consumers from accessing known illegal websites. Through the use of site blocking the expectation is to:

- decrease the number of users that drive traffic towards the pirate host website;
- facilitate and enable the enforcement option of copyright holders and ultimately;
- **to frustrate consumers into using legal alternatives.**

Internationally active cybercriminals are increasingly productive and innovative with phishing campaigns, domain purchases, [video game threats](#), malware, fraud, ransomware, botnets, and of course pirated websites. Through research we see that simultaneously blocking multiple sites is an efficient means of disrupting illicit streaming services. In other words, it requires a comprehensive rather than one-off approach. Site blocking is best combined with our other services outlined in the [Irdeto 5 Step Anti-Piracy program](#).



## KEY BENEFITS

The key benefits of using our comprehensive site blocking solution are:

### **Reduction in Piracy**

Site-blocking makes it more challenging for users to access pirate websites, leading to a decrease in piracy levels. This reduction can translate into increased revenue for content creators and distributors.

### **Improved Consumer Experience**

Pirated content can be of lower quality and may come with various risks, such as malware or unreliable streaming sources. Blocking pirate websites promotes a safer and higher-quality viewing experience for consumers who turn to legal sources.

### **Continuous Coverage**

We provide continuous coverage – we can easily detect once the pirates hop to different IP addresses and URLs ensuring an effective and comprehensive blocking regime resulting in maximum disruption.

### **Easy implementation for ISPs**

We make it easy for ISPs to implement – we work with ISPs to ensure a friction-less deployment process. Irdeto can provide online trainings and assist onsite where needed to ensure the teams are able to execute the blocks in an effective and timely manner.

### **Enhanced Negotiating Power**

Site-blocking can give rights-holders more leverage when negotiating licensing deals with platforms, as they can demonstrate their commitment to protecting their content from piracy.

# OUR APPROACH TO SITE BLOCKING

It is important to take into account the fact that networks are not necessarily bound to a specific jurisdiction. We believe site blocking (on a global scale) can be viewed in two dimensions, namely the legal and administrative aspects and the technical aspects. Through our collaborative network of ISPs, government agencies and global law enforcement partners, Irdeto can help your organization in a comprehensive manner.

The **legal and administrative aspects** that need to be considered are:

## **Administrative/Legislative**

There is a law in place that outlines what can be or can't be done. (There is often a regulator in place to administer and coordinate with all parties involved.)

## **Judicial**

Generally a court compels parties, often ISPs, in the form of an injunction, to perform the site blocks. (The terms and duration vary depending on jurisdiction.)

## **Mutual Agreement**

Through mutual agreement, ISPs and copyright holders/licensees agree on the terms of a blocking regime.

The **technical aspects** involved with site blocking are:

## **Static blocking**

Initial deployments of static blocking regimes can be aimed to block addresses or domains. (An example could be where thepiratebay.org, one of the most popular and prolific piracy websites in history, where site blocking was aimed at specific IP addresses and/or domains.)

## **Dynamic blocking**

Dynamic (or "forward-looking") blocking regimes are an evolution suited for the fluid nature of the internet. (Dynamic blocking allows for flexibility to cover repeated infringements; particularly when a materially similar website becomes immediately available at a different IP address and/or URL upon the execution of the block.)

## **Live blocking**

The latest evolution is aimed to allow repeated blocking of a site during a live broadcast. (In general, blocking regimes under this category allow for new servers to be identified by the rightsholder and/or authorized third parties. A request to start and stop blocking is made and depends on the availability of the live broadcast content on the target website.)

Irdeto strives to provide our [Cyber Services](#) customers with a comprehensive approach that includes not only technical and forensic expertise but investigation and enforcement services as well. Site blocking is only one tool in our broader [anti-piracy toolkit](#).

# HOW TO PREVENT OVER-BLOCKING

The standards set for the blocking of copyrighted material often require a thorough assessment of the infringing website to prevent over blocking. The website in question could be subjected to legal scrutiny and possible legal action. In other words, those sites that could (and should) be blocked by an ISP are often knowingly breaking the law. In short, there needs to be certainty that a site is breaking the law before blocking.

But (often unintended) over blocking can have negative implications with regards to freedom of expression, access to information, and even children's rights. In other words, many sites provide advice and guidance specifically tailored (for example) for young people whereby over filtering or over blocking can have negative consequences. There are legitimate sites and blocking them can be construed as impinging on rights, education, or freedoms. Censorship is an issue that needs to be avoided. It could lead to legal or reputational issues for the entity doing the blocking.

A thorough analysis of website intelligence utilizing WHOIS data, reverse lookup, and other investigative techniques is necessary to positively identify sites for site blocking. Shared IP addresses are often more affordable than dedicated IP addresses, so an infringing site may be sharing an IP with other non-infringing sites. As websites are often dynamic and can change on a moment's notice, continuous scanning, monitoring, and review is required to identify appropriate sites for blocking and to ensure that legitimate services are not affected.

An example of the steps we would take to prevent over blocking are:

- manual validation for each observed IP address;
- reverse IP lookup to identify other domains that might be linked to the same IP address;
- validate if the observed server is used for shared hosting;
- research to conclude that no other services are running on the server, and finally;
- perform frequent checks to validate that the blocked information is only used for illicit streaming and no other purposes.

# WHO IS SITE BLOCKING FOR? IS IT LEGAL?

Any company providing content in the video entertainment and videogame industries could benefit from the Irdeto website blocking solution.

Site blocking is not just for authoritarian governments. In fact, it is normal practice and used worldwide for a variety of reasons including to restrict access to copyright-infringing material, to protect children from obscene content, and often under the auspices to protect national security.

But let's face it. democratic governments also implement extensive filtering regimes with varying degrees of transparency and consistency. And while organizations may want to implement website blocking, it's often not even allowed in their country.

Irdeto helps your organization manage the complex nature of site blocking through a balanced, informed, collaborative, and legal approach. Get in touch to learn how we can implement site blocking for your organization.





Protect. Renew. Empower.

As video entertainment and videogame delivery and consumption evolve, pirates find new ways to circumvent security technologies and steal valuable assets.

Protect your content, brand and investments while meeting premium content security requirements.

## Contact Irdeto

Irdeto is the world leader in digital platform cybersecurity, empowering businesses to innovate for a secure, connected future. Building on over 50 years of expertise in security, Irdeto's services and solutions protect revenue, enable growth and fight cybercrime in video entertainment, video games and connected industries including transport, health and infrastructure. With teams around the world, Irdeto's greatest asset is its people and diversity is celebrated through an inclusive workplace, where everyone has an equal opportunity to drive innovation and support Irdeto's success. Irdeto is the preferred security partner to empower a secure world where people can connect with confidence.