INFO SHEET

DNS Content Filtering

Stay Safe, Stay Productive. Block Threats at the Source.

Ransomware is a nightmare. Protect your company and employees by blocking access to malicious websites that could result in downtime, data loss, reputation damage as well a serious hit to your bottom line.

It takes just one bad click by an employee to bring your company to a halt. Over 85% of ransomware attacks are aimed at small to medium size firms. Furthermore, users that spend time on unproductive websites can cost your company precious time and be a drain on your Internet bandwidth.

What is DNS Content Filtering?

DNS Content Filtering is a technology that blocks access to harmful or inappropriate websites by controlling how devices connect to the internet. DNS, or Domain Name System, acts like the internet's phonebook, translating website names (like www.example.com) into the numerical addresses computers use. DNS filtering works by intercepting these requests and checking them against a list of known malicious or unwanted sites. If a site is flagged as dangerous—such as one hosting ransomware, phishing scams, or other online threats—the connection is blocked, keeping your network and users safe. It's a proactive way to ensure secure and productive internet use for your business.

Why FirstLight?

No need to manage multiple vendors—FirstLight is your single source for both Internet access and online protection for your business. Our DNS filtering solution comes pre-configured, making implementation effortless. Best of all, exceptional service and support from the FirstLight team is just a phone call away whenever you need us.

INFO SHEET

Benefits of FirstLight's DNS Content Filtering

Block malicious websites

It feels good knowing there's a line of defense between your users and the hackers that want to hurt your business. DNS filtering blocks and filters unwanted access to websites, website-based security attacks, malware and more.

Nip unacceptable user behavior in the bud

With DNS Content Filtering, the use of Acceptable Use Policies (AUP) will monitor or block AUP violations ensuring not only network security but can help curb unproductive and wasted time online by your users

Be in the know

Proactivity is key when the stakes are high. You'll receive email-based security alerts in real-time so that you're always in the know if a problem should arise.

Power in visibility

Maybe you don't want to know? But if you do, you'll gain access to a dashboard offering an enterprise-wide view of all your online activity and the websites that were blocked activity.

Preconfigured & ready to protect

No setup required. FirstLight's DNS Content Filtering comes with the best practices in content filtering that will begin protecting you right away. For those that want a little more control and access, you'll be able to use the portal to easily create and manage your white and black lists to your specific requirements.

Grow with ease

You shouldn't need to reinvent your existing services when your organization fluctuates in need or size. The cloud-based nature of FirstLight's DNS Content Filtering makes scaling easy.

Ongoing support

You don't have to go at it alone. FirstLight will implement the service and provide you everything you need to begin protecting your company right away. And of course, the FirstLight team is always there for you for ongoing support or assistance.