Consortium DNS is a low latency cloud-based DNS filtering solution. Use domain history and threat intelligence to prevent traffic from malicious, dormant, and newly active domains.

Protecting Your Users From Malicious Web Content with Cloud-based DNS Threat Defense

A strong indicator of a modern malware attack is usually linked to a recently registered domain name. Consortium DNS allows our customers to instantly identify suspicious recently registered domains and block the connections before the malware can execute.

Consortium utilizes Farsight’s live feed of dormant domains that are currently active along with new domains never before observed and blocks them for 48 hours. This allows domain categorization and reputation sites time to properly categorize threats to your organization and protects users from domain-based phishing attacks such as link manipulation.

99.99% Uptime
Consortium DNS is hosted on Amazon AWS in multiple regions providing an uptime of 99.99%.

Wide Range of Support
In addition to standard DNS protocols, Consortium DNS supports DNS-over-TLS (DoT), TLS 1.3, and TCP Fast Open for secure, reliable, fast, and mobile compatible operation.

Attack Protection
Instantly identify and block suspicious domains protecting from many modern malware attacks.

THE CONSORTIUM DIFFERENCE
Consortium Networks is committed to providing businesses with the most relevant, up-to-date technology information, with a focus on cybersecurity. By connecting technology customers, vendors, and experts, we strive to be the go-to resource for guidance regarding all of your IT requirements. We are the first organization dedicated to providing real-world feedback and data on solutions in operation in production environments at peer organizations.

800-530-8350
contact@consortium.net
www.consortium.net