

Cloud DNS Threat Intelligence & Protection

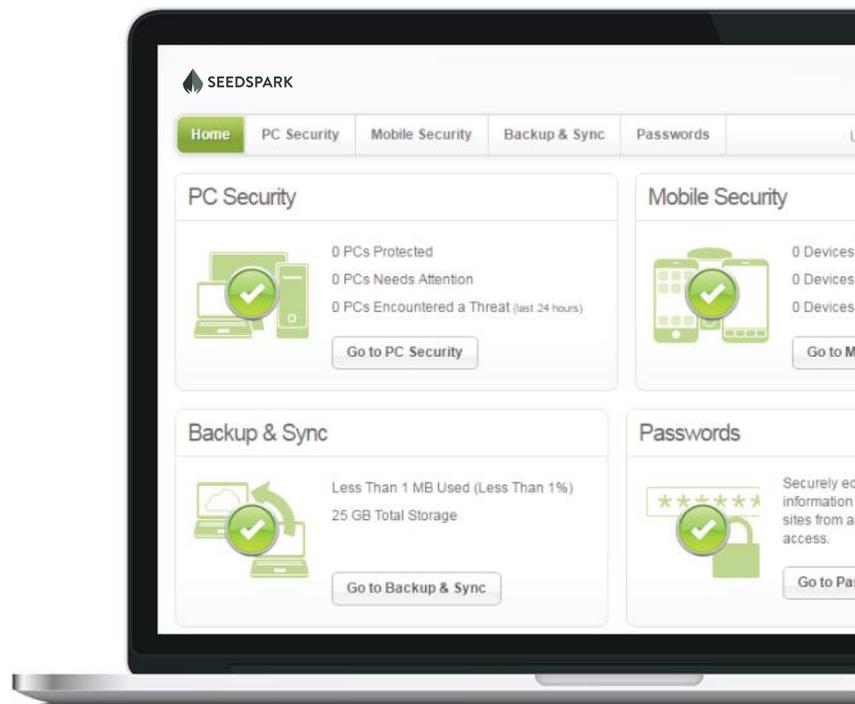
These days, using the internet is a high risk activity for every business, regardless of size. From users browsing inadvertently to websites that deliver malvertising, to drive-by downloads that immediately drop ransomware and other malware from a command and control server, uncontrolled web usage on the corporate network is fraught with risk.

Protection Straight from Our DNS Cloud

Our Cloud DNS Threat Intelligence & Protection is the same threat intelligence relied upon by industry-leading networking and security firms. It leverages an advanced, cloud-based security platform with fifth-generation machine learning and a contextual analysis engine used to determine relationships with known malicious objects in order to gain deep insight into today's threat landscape. This self-learning platform continuously scans the internet and incorporates inputs from millions of real-world endpoints, along with active scanning and passive sensor networks to quickly and accurately identify zero-day and previously unknown threats at an unprecedented scale.

With more than 80 URL categories, Cloud DNS Threat Intelligence & Protection provides an additional layer of web filtering protection from sites that host malware or spyware, and also provides far more granular control over the types of domains accessed at client sites. The service enhances our partners' network security solutions by increasing real-time protection against known malicious threats, unauthorized network access, and distributed denial of service (DDoS) attacks, while drastically improving their visibility and control over internet access.

With Cloud DNS Threat Intelligence & Protection, there's a straightforward and highly effective way to control internet usage and prevent it from becoming a risk to your business. The intuitive web-based console enables admins to finely tune web access policies by IP address or IP range, by group, or even down to a specific device. It offers more than 80 discrete URL categories, ranging from Abused Drugs to Violence and Weapons, allowing you full control over usage policies for your organization.



Benefits



No Hardware or Software to Install

The simple setup of this internet threat prevention layer allows you to begin protecting your network and controlling internet usage across all devices using your WiFi connection in a matter of minutes.



Block Malware and Other Threats at the Network Perimeter

Phishing, Botnet, and Malware across all ports and protocols are automatically filtered under basic protection and policy controls. Granular controls in URL categorization provide added flexibility in designing internet usage policies that comply with HR rules and industry regulations, including blocking questionable site categories automatically.



Control Internet Usage

Utilize pre-configured policies or customize your own for full control over internet usage within your organization quickly, easily and effectively. Our innovative agent enables you to protect and manage devices even when they're roaming or off-site.



On-Demand Drill-Down Reporting

Generate threat reports as well as productivity reports highlighting the most common domain categories visited and export them to be utilized by other reporting systems.



Better Network Speeds

By blocking undesirable traffic such as media streaming and other unwanted or malicious content at the domain layer, you can drastically improve network bandwidth.



Productivity & Visibility

Cloud DNS Threat Intelligence & Protection provides immediate visibility into overall web usage and threats that have been prevented. This reduction in infection rates and online distractions due to usage policies results in a significant improvement in user productivity.

Free Trial

Call us today for a free 30 day trial of unlimited Cloud DNS Threat Intelligence & Protection!



Additional Support

704 246 5052, *option 1*
support@seedspark.com