Enhanced Protective DNS Add-On

In today's rapidly digitalizing environment, where remote work has become commonplace, the risk landscape has significantly evolved. Cyber attackers are persistently exploring new avenues of vulnerability, with techniques such as DNS tunneling rising in prominence. This strategy aids in exfiltrating valuable data by manipulating the DNS system, a foundational component of the modern network infrastructure. Recognizing this challenge and the gaps in traditional security measures, the iboss Enhanced Protective DNS Add-On emerges as a groundbreaking solution.

This advanced add-on relentlessly monitors every DNS query originating from any endpoint, ensuring each is scrupulously passed through multifaceted security checks. Leveraging real-time threat feeds, the system possesses an innate capability to identify and block malicious threats emanating from phishing attempts, ransomware infections, and covert Command & Control Callback communications. For remote employees, iboss Cloud Connector agents are strategically installed on their devices. These agents act as the first line of defense, intercepting DNS queries right at the source. Once captured, these queries are encrypted, ensuring a layer of privacy and security before they are forwarded through the iboss platform for further analysis. This design eliminates the vulnerability that arises from local network DNS resolvers, especially in untrusted remote environments.

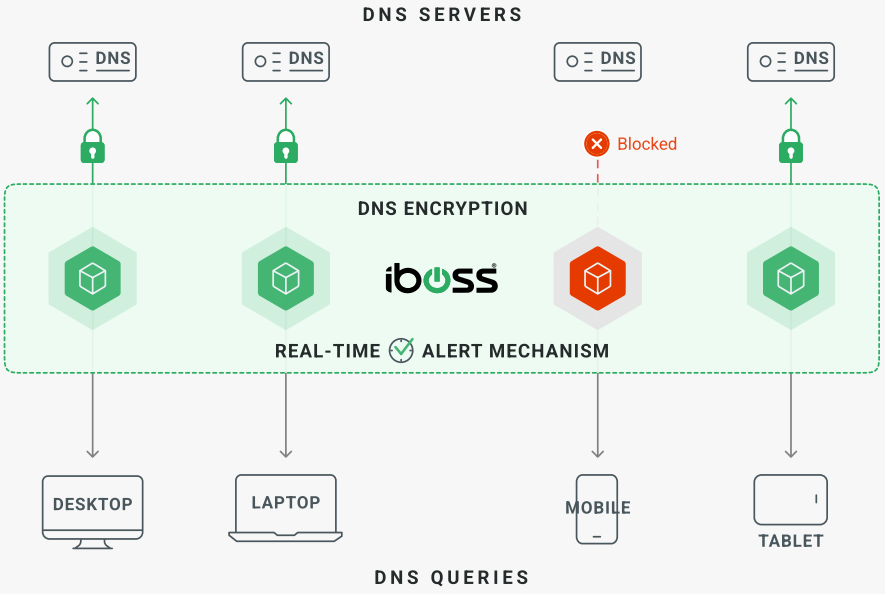
What sets the iboss Enhanced Protective DNS Add-On apart is its meticulous alignment with the recommendations laid down by esteemed bodies like the NSA and CISA as well as the UK government. And with features like DNS Rate Limiting and thorough content filtering, we ensure every DNS query is not just secure, but also adheres to organizational content standards.

BENEFITS

- Enhanced Security: Detect and block DNS tunneling, phishing, ransomware, and Command & Control threats.
- Remote Workforce Protection: Ensure safe DNS resolution for both on-site and remote users.
- Protect OT, IoT and network infrastructure that do not support agents by forwarding all DNS for protection.
- Advanced Threat Detection: Benefit from DNS Rate Limiting, and extensive threat feeds.
- Seamless Integration: Forward log events to any SIEM real-time and enjoy a cloud-based admin console.
- Customized Policies: Tailor security policies based on user groups or locations.

Enhanced Protective DNS Add-On

Protect your network with iboss' Enhanced Protective DNS Add-On. Detect and block DNS tunneling and other threats with state-of-the-art monitoring and analytics. Ensure secure DNS resolution for on-site and remote users while meeting stringent government requirements.



Ordering Information

SKU: Enhanced Protective DNS Add-On

Required Package: All Packages Advanced or Higher

HOW IT WORKS

- **DNS Monitoring:** Constantly monitor and log all DNS queries from endpoints, checking against threat feeds, phishing and malicious destinations.
- **Remote User Protection:** Utilize iboss Cloud Connector agents to intercept, encrypt, and send DNS requests from remote users through the iboss platform.
- **OT and IoT Protection:** Secure all infrastructure and IoT that do not support agents by forwarding all DNS queries for protection.
- **Protect from DNS Tunneling:** DNS rate limiting and security controls ensure DNS is not utilized for data hijacking via DNS tunneling.
- **Integration with SIEMs:** Natively forward DNS log events to any SIEM in real-time, centralizing and streamlining your security reporting.