Your PDNS CMMC Checklist
For the Manufacturing Industry

Protective DNS (PDNS) is now required as a part of CMMC compliance, an audit you need to prepare for if you plan on becoming a contractor for the Department of Defense (DoD)—contracts that manufacturing companies often seek. Many DoD contractors also require all manufacturing subcontractors to be CMMC compliant to ensure their entire supply chain is protected. The purpose of the CMMC is to protect Controlled Unclassified Information (CUI).

From the NSA and CISA’s guidance around Selecting a Protective DNS Service: “Due to the centrality of DNS for cybersecurity, the Department of Defense (DoD) included DNS filtering as a requirement in its Cybersecurity Maturity Model Certification (CMMC) standard (SC.3.192).”

The following checklist will ensure that your DNS provider is truly a PDNS provider, giving you ample threat protection from cyber threats. A recent study indicates that up to 33% of cyber security breaches could be prevented using DNS protection software.
So before you move forward with a DNS threat solution, confirm it allows you to:

- Block malware domains
- Block phishing domains
- Protect your organization from Domain Generation Algorithms (DGA) used in malware
- Leverage Machine Learning or Artificial Intelligence to augment threat static feeds
- Checks domains against millions of daily queries to determine risk level
- Offer the option to proactively identify and block brand new domains
- Filter content
- Access an API for developers to integrate DNS data with other platforms
- Validate DNSSEC
- Perform DNS encryption via either DoT or DoH
- Create policies by group, device, or network
- Deploy flexibly within cloud, hybrid, and on-prem architectures
- Allow for IT reporting of domain and application access at a user and device level
- Use a web-based dashboard
To learn more about how Protective DNS can help secure your manufacturing company, and position you to win more DoD contracts, contact us today for a demo of our secure, fast, and easy-to-use software.

About DNSFilter

DNSFilter is a venture-backed startup that provides edge-layer security via DNS for modern companies that are no longer tied to a central office. They protect over 15,000 organizations from ransomware, phishing, botnet, and other cybersecurity threats—all while running on the fastest network within the DNS security industry. DNSFilter identifies threats up to 154 hours faster than competitors, and uniquely categorizes more than 76% of domain-based threats, including zero-day threats.