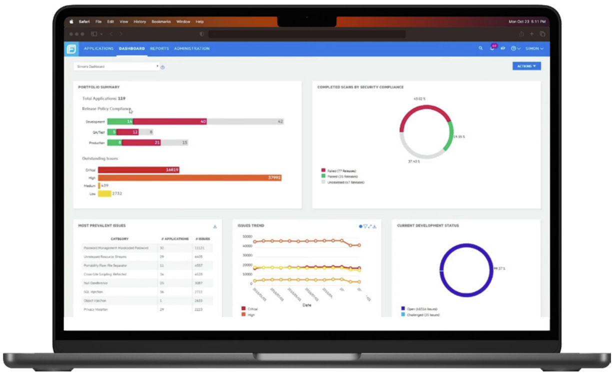
Top reasons MSPs sell OpenText Core DNS Protection

Improve client security with user-friendly and scalable OpenText Core DNS Protection



Cyber threats represent a real danger for MSPs and SMBs. With DNS (Domain Name System) Protection, MSPs can add an extra layer of protection to safeguard SMB customers against internetbased attacks before they reach the endpoint or network. Take control of the internet and grow your MSP business with solutions that are easy to install, manage, and scale.

Reasons you'll profit from selling our solution:

1 **Leverage leading-edge DNS Protection**
Domain filtering is only as good as the threat intelligence it employs. With OpenText's proprietary OpenText™ Threat Intelligence Platform, we deliver top protection with machine learning and AI capabilities.

2 **User-friendly security for SMBs**
OpenText™ Core DNS Protection is designed with ease-of-use in mind, for both small business owners and MSPs. The OpenText solution is cost effective and cloud-based with no additional hardware, so it takes only minutes to set up and use.

3 **Give customers peace of mind**
Shared responsibility gives your SMB customers peace of mind, especially knowing OpenText Core DNS Protection reduces the number of security incidents their businesses will face. In turn, this reduces the costs associated with threats – saving time, money, and productivity.

4 **Address compliance and HR concerns**
For customers that have compliance requirements (PCI, HIPAA, GDPR, etc.), OpenText Core DNS Protection makes it easy to manage internet use across your devices and networks, helping to ensure compliance and Zero Trust access for all employees on any device.

5 **Simplify management to save time**
Our customizable console provides a single pane of glass to simplify cybersecurity management, including time-saving tools that scale to thousands of users with no latency. Manage clients separately, in bulk, or individually with ease.

88% of network infections can be reduced through DNS filtering.

OpenText Core DNS Protection

6

Integrate with other solutions
OpenText Core DNS Protection is highly flexible and will seamlessly integrate with your customers' current infrastructure, network topology, tools, and management system stack. It also supports a wide range of firewalls, devices, and widely used VPNs.

7

Improve your bottom line
There is proven value to including additional layers of cybersecurity through domain filtering. When bundled with OpenText Core Endpoint Protection and OpenText™ Core Security Awareness Training, the value for your customers is beyond compare.

8

Sell better with support and tools
Over and above our award-winning OpenText Threat Intelligence, we offer sales and marketing tools, training, and resources, ensuring you have everything you need to sell OpenText solutions effectively and to scale your business.

Top questions SMBs ask about DNS Protection

What is OpenText Core DNS Protection?

DNS is the address book of the internet. It translates domains to the addresses your system needs to access any resource on the internet. OpenText Core DNS Protection applies intelligence and control to this address book, helping to ensure that the resources provided are safe and appropriate.

Why does my business need DNS filtering?

DNS filtering can have a significant effect on security and productivity. Systems running DNS filtering with quality intelligence are exposed to 33% less threats, which translates to reduced risk for the business and fewer interruptions for the user. Additionally, since DNS filtering can control available content, it can help remove distractions and further improve productivity.

Who is OpenText Core DNS Protection designed for?

OpenText Core DNS Protection is known for its focus on the MSP and DNS Protection follows this ethos. It is designed to be easy to deploy and manage, while also including the necessary features to make it amazingly effective at protecting your clients. Deploying the agent to an entire client, both network and agent, takes only minutes, while reporting and billing are simple and yet tailored to your needs.

How does DNS filtering work?

The average system makes 2000 DNS requests each day. DNS filtering applies intelligence to these requests by selectively providing the DNS resolution. If the malicious or inappropriate resource is not provided, the system and user are not exposed to the threat.

Why is OpenText Core DNS Protection unique?

OpenText Core DNS Protection leverages BrightCloud® threat intelligence to filter DNS requests. This allows you to use the industry's leading intelligence to quickly identify and block phishing and malware sites. Additionally, OpenText Core DNS Protection is innovating and leading the market by leveraging DoH (DNS over HTTPS) and providing cutting edge features and functionality.

Ready to see OpenText Core DNS Protection in action?
Start a trial.