Next Generation DNS

Thunder NSI

Protecting Small & Medium Enterprise

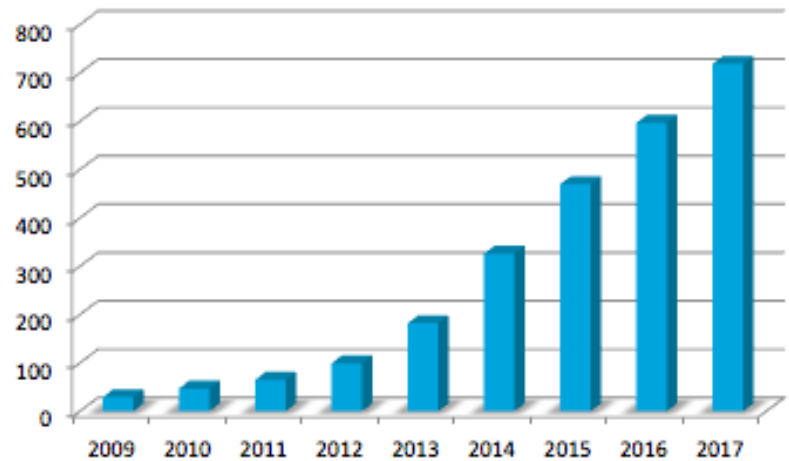
Security as a Service

Small to Medium Enterprises (SME) are looking for ways to protect themselves from cyber threats. They are increasingly using DNS Cyber Security technologies as part of the defense to protect their systems and information. This adoption is primarily driven by increased attacks on the SME market and DNS's ability to offer powerful security at a low cost.

SME market is under cyber attack

Cyber threats are increasingly targeting the SME market. Three main reasons for this are, first, many SME's deploy Internet and Cloud technologies without any experience or understanding of how those technologies work. These new deployments expose them to threats on the open Internet. Second, SME's lack the cyber security expertise to protect themselves or implement cyber security best practices. Third, SME's don't have the budget to pay for high-end security systems to protect their vulnerable systems.

Total Malware Definitions (millions)



As shown in the graph above, new cyber threats are developed every few seconds and experts predict attacks to increase in frequency and severity over the next few years.

As a result, it is near impossible to protect a business through a single security layer. Cyber defense best practice is to implement a defense in depth, multi-layered, security approach. SME's with limited budget should protect themselves by adopting efficient, low cost security technologies such as Domain Name System Security.

58%	10X	$6 Trillion
Of all Malware Attacks are on SME Business	Increase in Ransomware attacks in 2017	Worldwide cost of Cyber Attacks by 2022

Using DNS to provide Cyber Security

DNS is a fundamental building block of the Internet that translates memorable domains names into IP addresses. The advantage of using DNS for security is that DNS is used by virtually everything to navigate the Internet, including the vast majority of malware. As such, it is perfectly positioned to act as a gatekeeper and automatically block communication between infected devices and command and control servers, rendering these threats ineffective.

One of the most attractive attributes of DNS cyber security to the SME market is its efficiency and low cost. These attributes are primarily due to its focus on ensuring only safe connections are established. DNS security stays out of the data path and is not impacted by the migration to secure web traffic (i.e. https). As a result, DNS security provides better coverage and requires significantly less compute resources than traditional security solutions.

Additionally, unlike cloud based DNS security solutions, Thunder DNS partners with local service providers and integrators to host Thunder DNS security within their region. Local deployments ensure traffic is routed most efficiently and leverages our partners existing footprint further reducing the cost of service.

SME businesses will continue to be targets of cyber attacks until they implement multiple layers of security. Thunder and its partners are working to protect those business by providing world class DNS based security at an affordable cost.

Thunder develops next generation Networking, Security, and Intelligence technologies. Originally founded in Silicon Valley, our company has since grown internationally with our headquarters in Las Vegas, USA. Our team includes world class engineering talent with experience from high growth telecommunications, security, and enterprise class product companies including Microsoft, Ubiquiti, Ericsson, Verisign, E-Bay, Telstra, and Syniverse. Our business approach is to empower Service Providers and Solution Integration partners with innovative technologies.

Thunder NSI

www.thundernsi.com/dns

Las Vegas, USA