

Gateway Anti-Malware

powered by Bitdefender

Smoothwall's SWG and UTM solutions include market leading anti-malware protection powered by Bitdefender, ensuring your organisation is secure against malware and ransomware threats.

About Bitdefender

Bitdefender is the creator of one of the world's fastest and most effective lines of internationally certified Internet Security software.

The company is an industry pioneer, introducing and developing award winning protection since 2001. Today, Bitdefender has the world's largest security delivery infrastructure, securing the digital experience of 500 million users worldwide and performing 11 billion security queries each day.

Key Features

-  Finds and blocks malware based on powerful heuristics that detect behaviour - not only reliant on libraries of malware 'signatures'
-  Works on complex behavioural analysis to detect previously unknown types of ransomware
-  Detects and blocks the execution of every known ransomware family
-  Independently shown to protect against 99% of previously unseen threats, outperforming the industry average of 75%
-  Detects and blocks against known and unknown ransomware

How Bitdefender works

Conventional anti-malware protection relies on signatures. Anti-malware signatures are code snippets extracted from malware samples and used by anti-malware programs to perform pattern-matching. However this isn't done instantly - anti-malware vendors need to obtain a sample of the malware, develop a signature and then push that signature to users, creating a 'window' of vulnerability.



To strengthen detection, Bitdefender also uses heuristics, a form of proactive detection that closes the 'window' during which computers are vulnerable. Rather than relying on signatures or code fingerprints, heuristic detection uses complex algorithms that specify actual patterns and behaviours, which may indicate that an application is malicious. Examples of suspicious behaviour would include attempting to drop files or disguise processes, or injecting or executing code in another process's memory space. This works because malicious programs inevitably attempt to perform actions in a context that legitimate applications do not.

Because heuristic detection looks for behavioural characteristics rather than relying on simple pattern-matching, Bitdefender is able to detect and block new and emerging threats for which a signature or fingerprint has yet to be released.

Highest performance score against unknown threats

Bitdefender outperformed all other solutions in 2017, blocking 99% of samples while the market average continues to drop according to the AVComparatives Proactive Protection Test. The report tests leading anti-virus and anti-malware products against new or zero-day malware and ranks performance based on the ability to block malware samples.

How Bitdefender protects against Ransomware

Ransomware is polymorphic meaning that each sample is unique and customised for each victim. Bitdefender uses signature-based detection as the first line of defense against ransomware attacks. To maximise detection Bitdefender also signs the 'dropper', a small piece of software that acts as a downloader for the actual ransomware piece. Droppers can be used on multiple devices by the same threat, therefore each new victim targeted by a specific dropper will be fully protected.

Uncovers never-before-seen ransomware

Bitdefender also uses heuristic technology to detect and block new and emerging ransomware threats, which conventional protection wouldn't highlight until a signature or fingerprint has been released.

Bitdefender can detect a total of 2.8 million unique ransomware samples from the last 2 years alone.

More information on Smoothwall's SWG and UTM solutions can be found on the individual datasheets.

0870 1999 500 

Smoothwall 

@Smoothwall 

enquiries@smoothwall.com 

www.smoothwall.com 