Written by Marco Attard
10 February 2017

SonicWall extends the security capabilities of the Capture Advanced Threat Protection (ATP) service with Email Security 9.0-- a cloud-based multi-engine sandbox for the inspection of email traffic.



According to the company, Email Security 9.0 not only suspects email traffic for suspicious code, but also blocks ransomware, zero-day and other malicious files from entering the network until administrator review. It integrates with the Capture ATP service and uses cloud-based sandboxing technology to detect threats before analysis in a multi-engine sandbox.

It features anti-spam, anti-virus and anti-spoofing technologies, improved support for Office 365 and an encryption services that automatically encrypts emails identified as containing protected data. Admins can also filter messages and their contents through policy and compliance management.

"Our 2017 SonicWall Annual Threat Report found that email remains a highly successful attack vector for cyber criminals because it's all too easy for employees to fall victim to ransomware, phishing and unknown threats," the company says. "SonicWall is enabling customers to stay one step ahead of cyber criminals by bolstering our platform with innovations that inspect and render a verdict on all email coming into and going out of their organisations, while keeping performance and usability high."

Email Security 9.0 will be available from end February 2017.

Go Announcing New and Enhanced SonicWall Email Security 9.0