Office 365 Security Brief for Businesses

The biggest cyber security risks for businesses, small to large, is related to email, web browsing and remote workers.

Considering that most people now have some kind of hybrid working environment, the risks are higher than ever. When your staff or contractors work from non-business-owned devices, the risk increases further. This is because the business has no control over the devices or how they are used. Nor are the business security systems in place on those devices. Meaning that all the hard work and money you have put into your cyber security becomes far less effective.

Traditionally, all applications and data used to live on the business network, safely behind a firewall. The firewall would scan the gateway (between the internet and the internal network) for viruses and malware, all end-user web traffic, and then protect the network from unauthorised access from the outside world (IPS – Intrusion Prevention Service). Web filtering, more often than not, takes place there too.

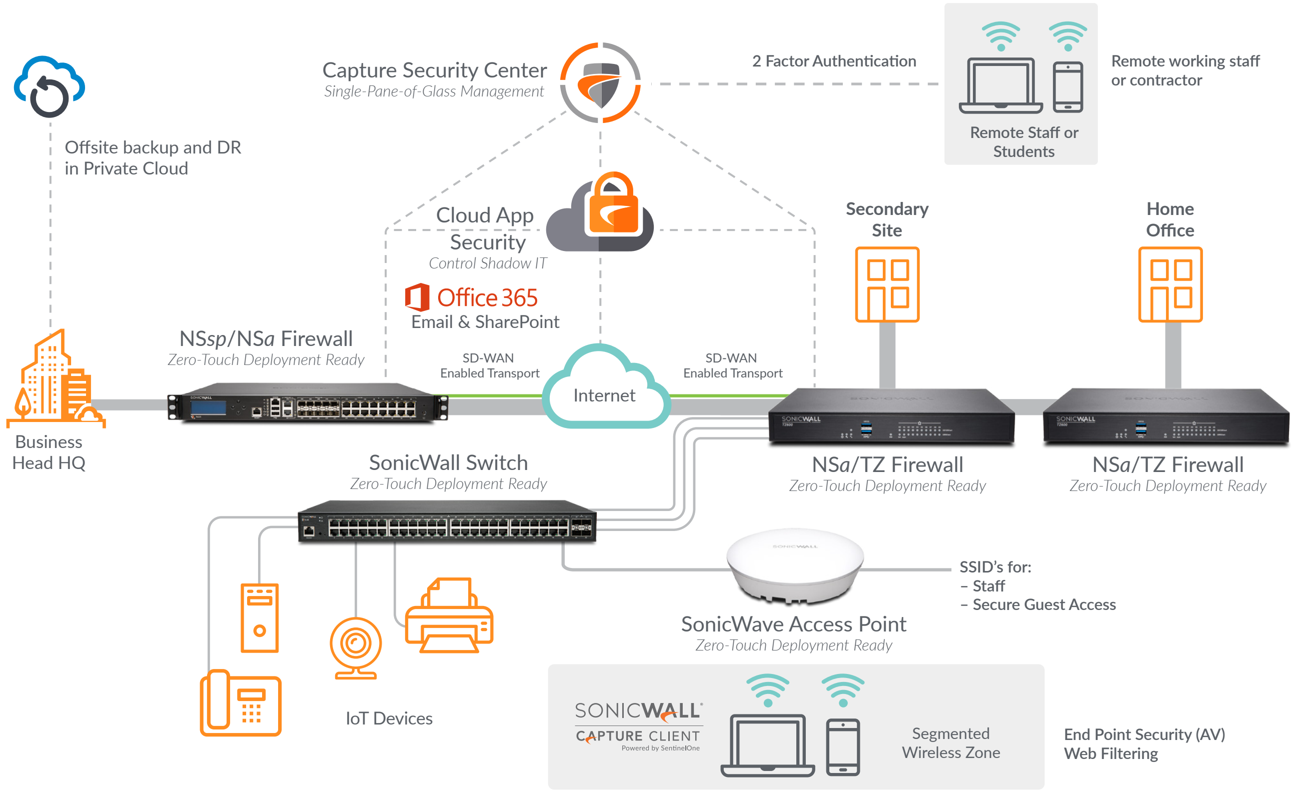
In the event that malware, as an example, managed to get through the system scanning, we had the device's anti-virus (now referred to as End Point Security) in place as the last line of defence, which would then hopefully remove the malware and avoid scenarios such as a keylogger being installed that records your banking details or Windows login credentials.

It makes much more sense to remove malware at the gateway rather than hope that the anti-virus (End Point Security) will clean it and prevent everything from being damaged, encrypted, personal details stolen, etc.

The same applies to email. Emails were scanned by an email security solution or anti-spam product that looks for viruses, malware, phishing, spam, bad URLs, embedded images, etc. A clean email is then delivered to the mail server. A similar principle as the above, in the sense that it removes the unwanted emails before they land on your system.

In the event that something was not picked up by the email security solution, such as ProofPoint, then the server anti-virus (End Point Protection), such as Sophos, would be the next layer of defence.

The distributed network security model:



The COVID lockdown has definitely changed the way we work and has also accelerated the adoption of cloud services. This has had a significant impact on the above cyber security model as our end users, applications, and data no longer reside behind the safety of our firewalls. Nor do we host the data and applications on our servers, where our End Point Protection can remove any malware as the last line of defence.

Microsoft Office 365 with Exchange Online Email, MS Teams, SharePoint, and OneDrive (not mentioning all the other apps) is a no-brainer. However, we need to consider how we use the system and if we have all the same security measures in place as we did when we hosted our own applications and data. You wouldn't have an Exchange or File Server without End Point protection.

As we learn and become more educated on the use of these systems, most people realise that Office 365 natively, is not secure enough.

Most businesses we see now have the following systems in place:

- Two-factor or multi-factor authentication is used to secure our user names and passwords.
- Backup of all email and data
- Email Security and Anti-Spam Scanning

The 'security gap' lies in what happens to the data once it lands on the Office 365 servers, where you would normally have your endpoint security. As Sophos would protect your server.

Most security vendors have now started releasing a security application that plugs into Office 365 and scans the files and folders in SharePoint and the emails that are received. Very similar to the scenario we used to have with server anti-virus or endpoint security. The same principle applies, apart from the "server," which is now just hosted elsewhere and not in your server room.

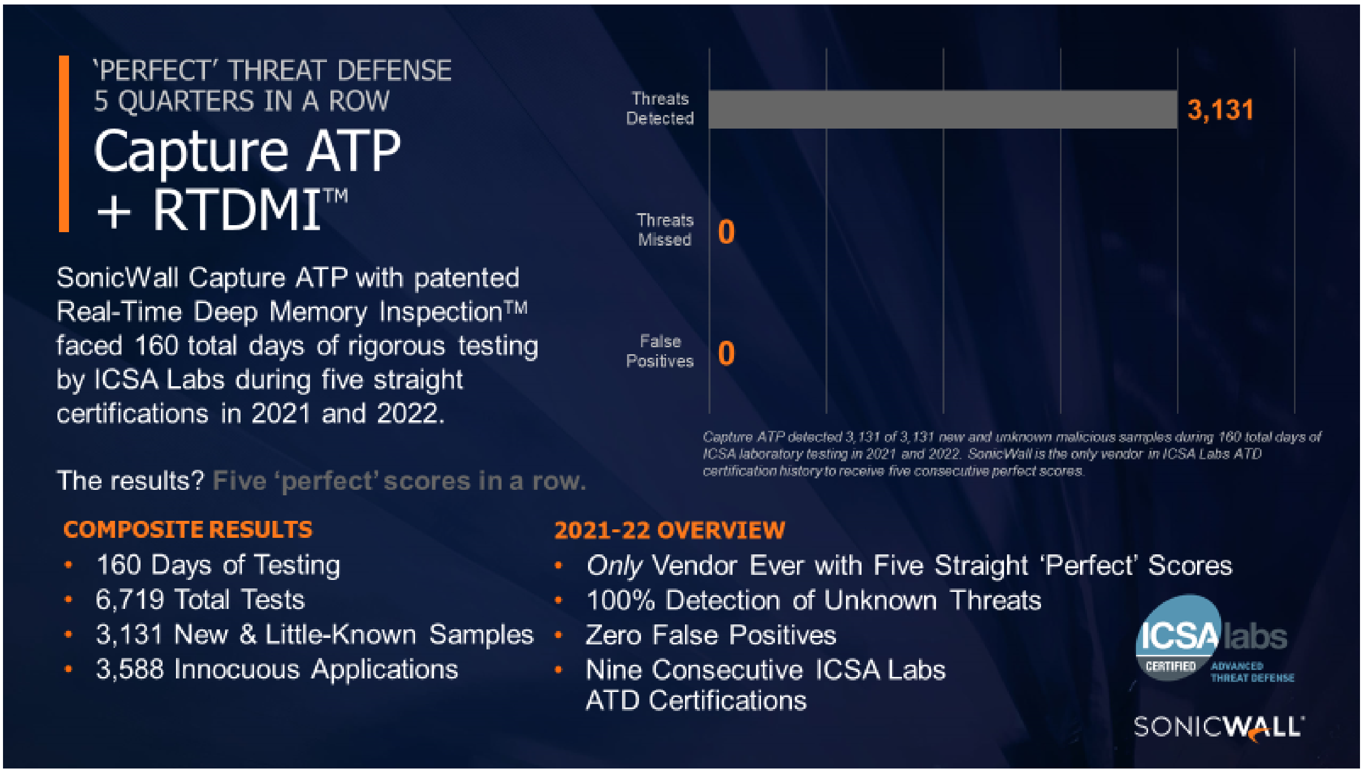
If you have a SonicWall firewall, then SonicWall has an application called CAS (Cloud Application Security).

It provides the same levels of Anti-Malware and Anti-Virus as the firewalls and can be managed from a central cloud interface. Meaning it removes the gap with data in Office 365 not being scanned.

Sonicwall has the industry's best detection rates for Malware and false positives, as can be seen below. Note that this has been independently tested and certified by ICSA Labs.

From that perspective, it makes complete sense to have the same level of protection and the same security technology protecting both the business's internal network and cloud resources.

From a management perspective, it can be centrally managed with the firewalls on a cloud-based management interface.



'PERFECT' THREAT DEFENSE
5 QUARTERS IN A ROW

Capture ATP + RTDMI™

SonicWall Capture ATP with patented Real-Time Deep Memory Inspection™ faced 160 total days of rigorous testing by ICSA Labs during five straight certifications in 2021 and 2022.

The results? **Five 'perfect' scores in a row.**

Capture ATP detected 3,131 of 3,131 new and unknown malicious samples during 160 total days of ICSA laboratory testing in 2021 and 2022. SonicWall is the only vendor in ICSA Labs ATD certification history to receive five consecutive perfect scores.

COMPOSITE RESULTS

- 160 Days of Testing
- 6,719 Total Tests
- 3,131 New & Little-Known Samples
- 3,588 Innocuous Applications

2021-22 OVERVIEW

- *Only* Vendor Ever with Five Straight 'Perfect' Scores
- 100% Detection of Unknown Threats
- Zero False Positives
- Nine Consecutive ICSA Labs ATD Certifications

Author: Craig Van Aswegen, MD & Snr IT Management Consultant, Breathe Technology