Q3 2021

Advanced Threat Defense

Certification Testing Report

SonicWall Inc.
SonicWall Capture Advanced Threat Protection (ATP)

Tested against this standard

ICSA Labs Advanced Threat Defense Criteria v.1.0

October 12, 2021

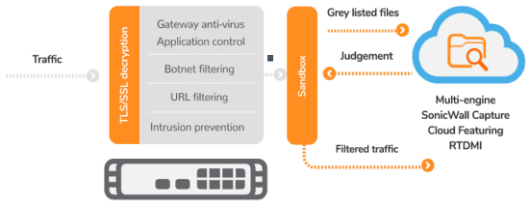
Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

ICSA Labs Advanced Threat Defense – Report-at-a-Glance

SonicWall Inc.

SONICWALL™

SonicWall Capture ATP



www.sonicwall.com

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

ICSA Labs
Advanced Threat Defense

Certified

Test Period: Q3 2021
Certified Since: 04 / 2020

Executive Summary

During 28 days of testing during the third quarter of 2021, ICSA Labs tested the detection capabilities of SonicWall's advanced threat defense solution, SonicWall Capture Advanced Threat Protection (ATP), with a mix of 1,348 test runs. The mix was primarily composed of new and little-known malicious threats – i.e., recently harvested threats not detected by traditional security products.

Periodically, ICSA Labs launched innocuous applications and activities to additionally test SonicWall Capture ATP in terms of false positives. Throughout testing, ICSA Labs observed product logs to ensure not only that SonicWall Capture ATP indicated the existence of a malicious threat but also that logged threats were distinguishable from other logged traffic and events.

SonicWall Capture ATP passed, having met all criteria requirements. As seen in Figure 1 below, SonicWall Capture ATP did remarkably well during this test cycle - detecting 100% of previously unknown threats while having zero false positives. Figures 2 and 3 below further highlight the solution's detection effectiveness and false positives (FPs).

Test Length	28 days	**Malicious Samples**	653	**Innocuous Apps**	695
Test Runs	1,348	**% Detected**	**100%**	**% False Positives**	**0%**

Fig. 1 – High Detection Effectiveness & Few False Positives

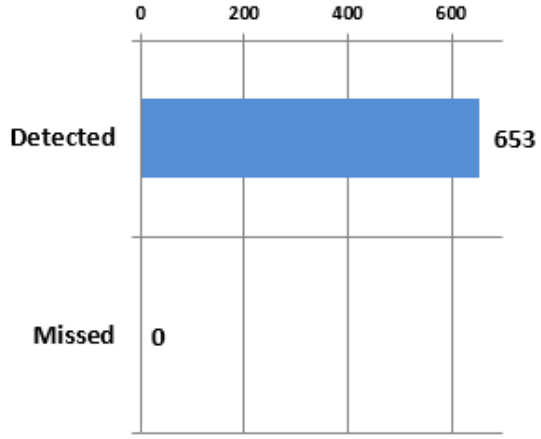


Fig. 2 – Detected 653 of 653 *New & Little-Known* Malicious Samples

Fig. 3 – Zero Alerts on 695 Innocuous Applications

Introduction

This is SonicWall's seventh ICSA Labs Advanced Threat Defense Certification testing report for SonicWall Capture Advanced Threat Protection (ATP).

Standard ICSA Labs Advanced Threat Defense (ATD) testing is aimed at vendor solutions designed to detect new threats that other traditional security products miss. Thus, the focus is on how effectively vendor ATD solutions detect these unknown and little-known threats while minimizing false positives.

The remainder of the report presents a more detailed look at how the SonicWall advanced threat defense solution performed during this cycle of standard ICSA Labs ATD Certification testing. To better understand how to interpret the results, this report documents not just the testing results themselves but the threat vectors, sample sources, and kinds of samples that ICSA Labs employed for this cycle of ATD testing against SonicWall Capture ATP.

Test Cycle Information

This report reflects the results of one test cycle at ICSA Labs. Standard ATD and ATD-Email test cycles are performed by ICSA Labs each calendar quarter and typically range from three to five weeks in duration. To be eligible for certification, security vendor solutions must be tested for at least 3 weeks. Because testing is performed quarterly, ICSA Labs tests ATD solutions four times during a calendar year.

During each test cycle ICSA Labs subjects advanced threat defense solutions to hundreds of test runs. The test set is comprised of a mix of new threats, little-known threats and innocuous applications and activities – delivered and launched one after another continuously for the length of testing. Below in Figure 4 is information about the test cycle from which this findings report is based.

Start Date	July 14, 2021	**Days of Continuous Testing**	28
End Date	August 10, 2021	**Test Runs**	1,348

Fig. 4 – This Test Cycle

ATD Solution Tested

During this testing cycle, ICSA Labs tested:

- SonicWall – NSA3600 – SonicOS Enhanced 6.2.8.0-24n
- SonicWall Capture Advanced Threat Protection (ATP)

  According to SonicWall, the SonicWall Capture Advanced Threat Protection service, featuring the RTDMI engine, is a cloud-based multi-engine sandbox designed to discover and stop unknown, zero-day attacks such as ransomware at the gateway with automated remediation. This cloud-based service extends firewall threat protection and analyzes suspicious files to help discover and block newly developed malware from entering your network.

  For more information about SonicWall Capture ATP please visit:

  https://www.sonicwall.com/products/firewalls/security-services/capture-advanced-threat-protection/

Detection Effectiveness

To meet the criteria requirements and attain (or retain) certification through ICSA Labs testing, advanced threat defense solutions must be at least 75% effective at detecting new malicious threats. As shown in Figure 5 the SonicWall Capture ATP detected 100% of the threats it encountered during testing, considerably better than the percentage required for certification.

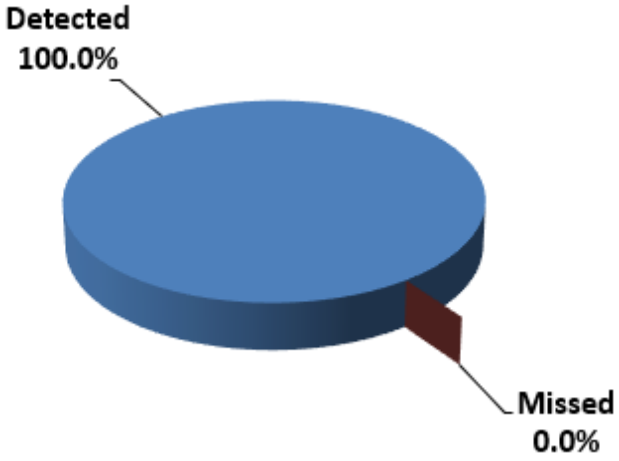


Fig. 5 – Detection Effectiveness of SonicWall Capture ATP

A second plot depicting the detection effectiveness of SonicWall Capture ATP appears in Figure 6. For the SonicWall advanced threat defense solution, the chart sheds light on whether or not SonicWall Capture ATP did better or worse – the newer the malicious sample. Of threats one hour old or less, (and like all malicious threats this test cycle) SonicWall Capture ATP detected 100% of new threats during the Q3 2021 test cycle.

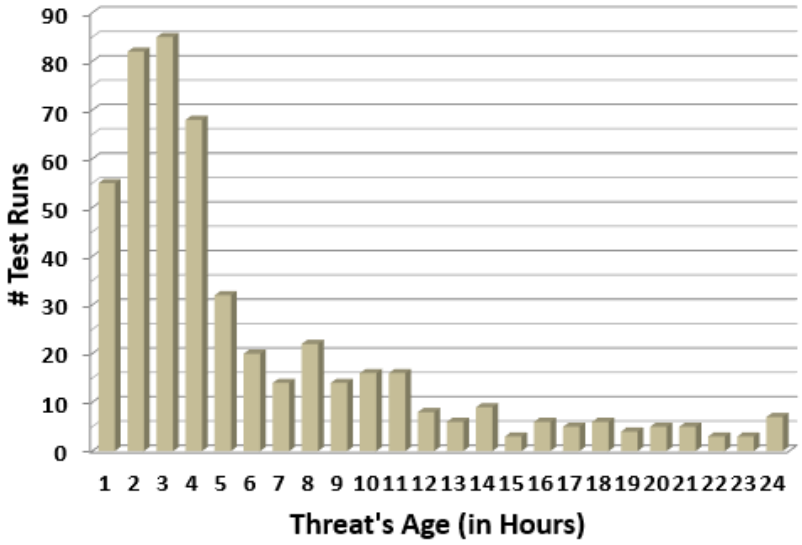


Fig. 6 – Detection Effectiveness by Age of Threat (Threats < 24 Hours Old)

A final effectiveness-related plot to consider for the SonicWall Capture ATP solution during this test cycle is Figure 7 below. Plotted below is each of the 28 days during the test cycle along with how effective SonicWall Capture ATP was on each of those days. On all 28 days of the test cycle the SonicWall Capture ATP was 100% effective at stopping the malicious threats in the test set.

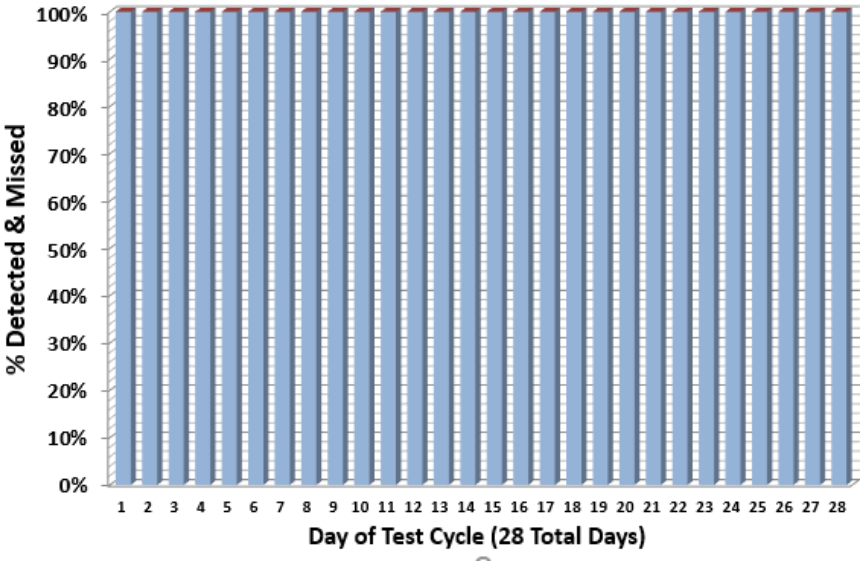


Fig. 7 – Detected & Missed Threats by Day of Test Cycle

Threat Vectors

In testing, ICSA Labs delivers new and little-known malicious threats to security vendor solutions using many of the top threat vectors that have led to enterprise cybersecurity incidents and breaches as reported in the latest Verizon Data Breach Investigation Report (DBIR).

DBIR data indicates that malware has been a key factor in thousands of security events where an information asset had its integrity, confidentiality, and/or availability compromised. Figure 9 on the following page depicts the threat vectors involved in these malware-related security incidents throughout the over fifteen-year history of Verizon's DBIR. Figure 8 below illustrates the most common malware-related threat vectors that lead to enterprise breaches during 2020 according to data from the 2021 DBIR.

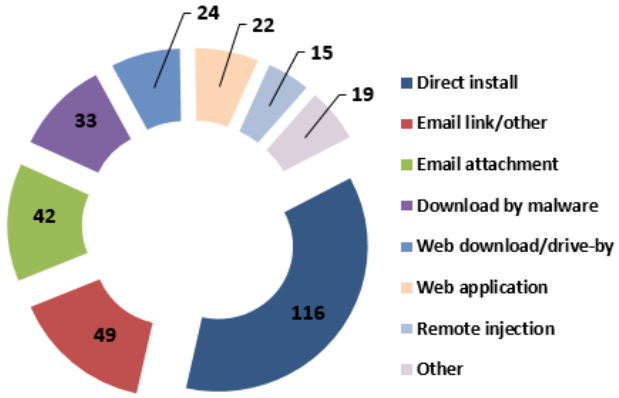


Fig. 8 – Top Threat Vectors Leading to Breaches in 2020 (per 2021 DBIR data)

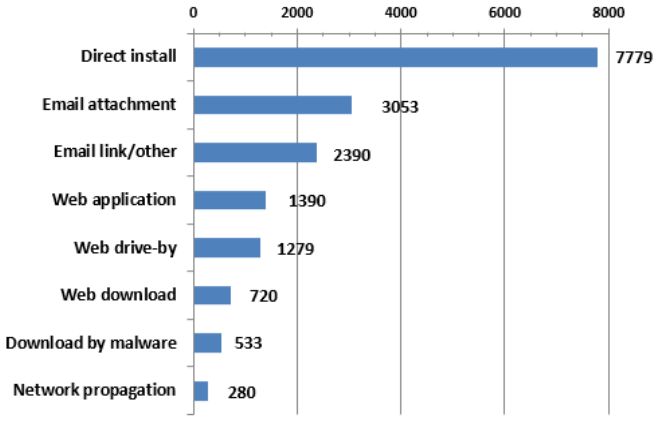


Fig. 9 – Malware-Related Threat Vectors Involved in Incidents (DBIR All-Time)

Standard ICSA Labs ATD testing includes the threat vector that is by far the most prevalent over time, "Direct Install". In addition, standard ATD testing includes the threat vectors labeled "Web download", "Web drive-by", and "Download by malware". In the separate but related, ICSA Labs ATD-Email testing, ICSA Labs delivers new and little-known malware in email attachments and emails with malicious URLs, corresponding to DBIR threat vectors "Email attachment" and "Email link/other", the latter being the second most common threat vector leading to enterprise breaches according to the 2021 DBIR (see Figure 8).

Source of Samples

A number of sample sources feed ICSA Labs' standard ATD and ATD-Email testing.

One source is the spam ICSA Labs collects. The labs' spam honeypots receive approximately 250,000-300,000 spam email messages/day. For ICSA Labs ATD testing, the team harvests attachments in that spam, making use of the ones that are malicious.

Samples may also come from malicious URLs. Some of these come from the spam mentioned above. From feeds like this ICSA Labs filters and checks the URLs to see if there is a malicious file on the other end of that URL -- either as a direct file link or a series of steps (e.g. a drive-by attack with a multi-stage download process) leading to it. If so, ICSA Labs collects the sample for potential use in testing.

ICSA Labs additionally uses other tools and techniques to create unique malicious files as an attacker or penetration tester might do. In some cases, these are trojanized versions of clean executables. In other cases, they may be original executables that are malicious.

Still another source of samples is the samples themselves. Any dropped files resulting from running another malicious sample are also evaluated and potentially used in testing.

Finally – and importantly to test for false positives – ICSA Labs also launches legitimate executables. Running innocuous applications helps ensure that vendor solutions aren't just identifying everything as malicious.

Regarding the Samples from this Test Cycle

Samples harvested for use in ATD testing are often unmodified and used as is. That is the case if ICSA Labs determines that the sample is new enough and/or not being detected by traditional security products. In many cases malicious samples require modification before they can avoid detection by traditional security products.

Of the 653 malicious samples, Figure 10 shows that there were more original samples used and fewer samples that required some kind of modification before use in testing. Of the 650 original samples, 0 were dropped, or left behind by other malware. Figure 11 reveals the source of the 650 malicious samples used in testing that were neither modified nor dropped.

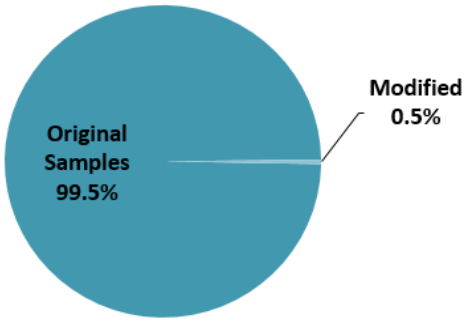


Fig. 10 –Malicious Samples – Original vs. Modified

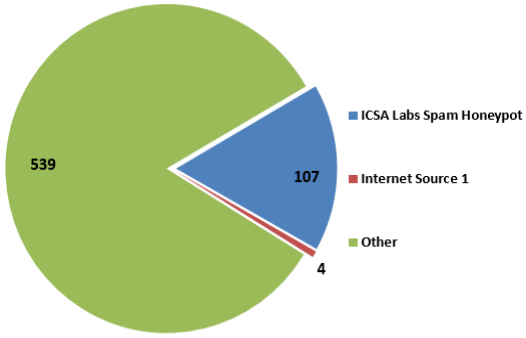


Fig. 11 – Unmodified/Non-Dropped Sample Sources

Following the test cycle, ICSA Labs analyzed the original malware samples used in testing, categorizing the malware into one of six malicious threat types: backdoor, ransomware, spyware, trojan, worm, or virus. Any malicious sample not falling into one of these six types, ICSA Labs categorized as “other”.

The six malware categories, and the number of original malicious samples used during the test cycle from each category are represented in Figure 12 below. The figure indicates how many malicious threats SonicWall Capture ATP detected and missed from each malware category during testing. In addition, the green line atop Figure 12 represents the effectiveness percentage of SonicWall Capture ATP against original malware belonging to each malware type.

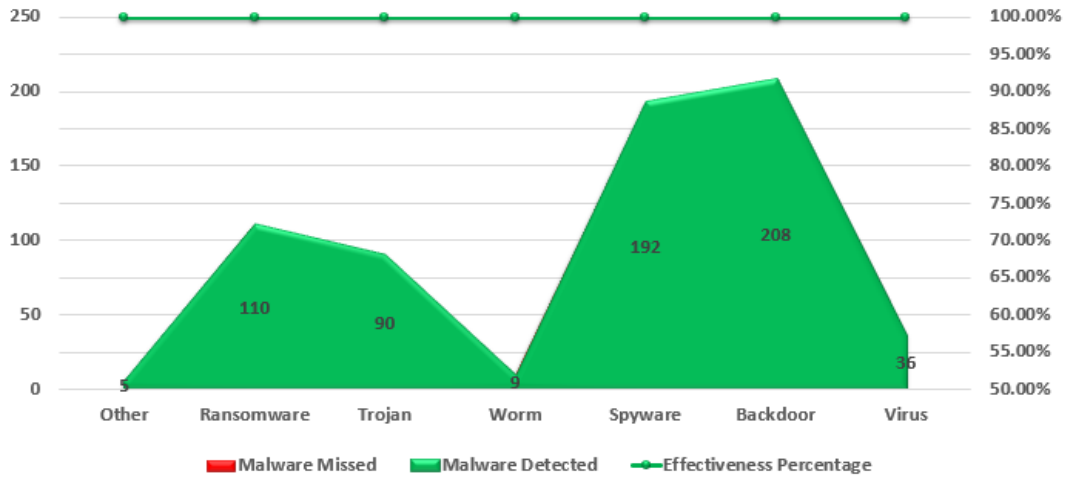


Fig. 12 – Effectiveness against original, unmodified malicious samples broken down by threat type

Figures 13 through 16 provide a deeper glimpse into four of the six malware types: ransomware, trojan, spyware, and backdoor. In its analysis of the original malicious samples used in testing, ICSA Labs further categorized malicious samples by malware family, where possible. The remaining figures, one for each of the four aforementioned malware types, are ordered by malware family. The figures show how many original malware samples SonicWall Capture ATP detected and missed across multiple malware families during the test cycle. In addition, the green line atop each figure indicates the effectiveness percentage of SonicWall Capture ATP against original malware from each malware family.

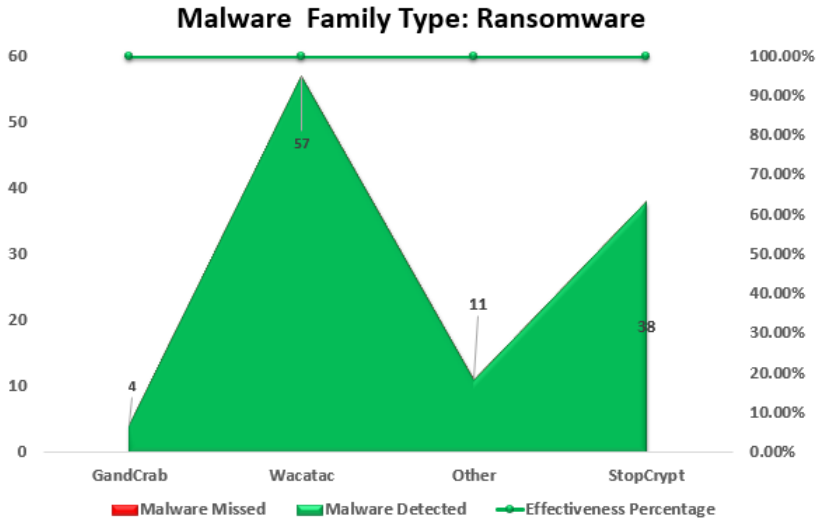


Fig. 13 – Effectiveness against Kinds of Ransomware Threats

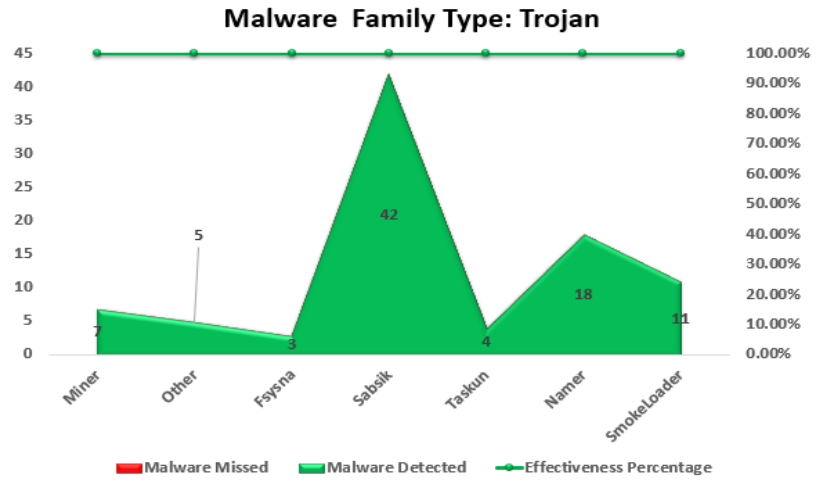


Fig. 14 – Effectiveness against Families of Trojans

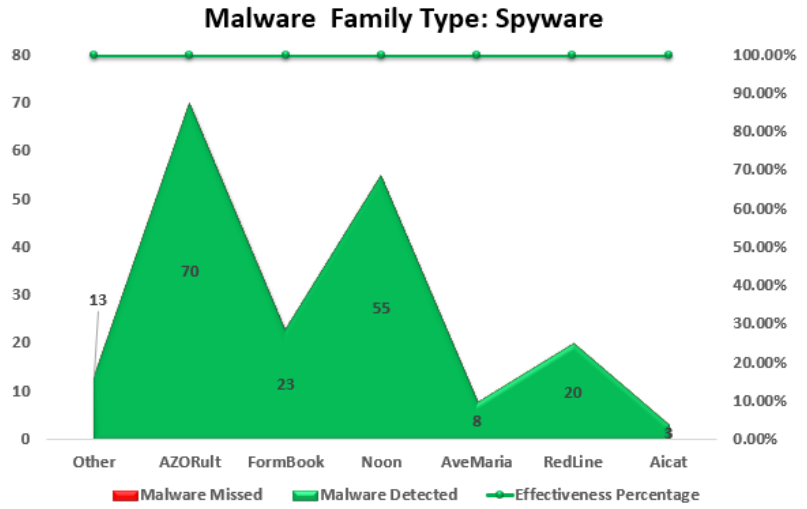


Fig. 15 – Effectiveness against Families of Spyware

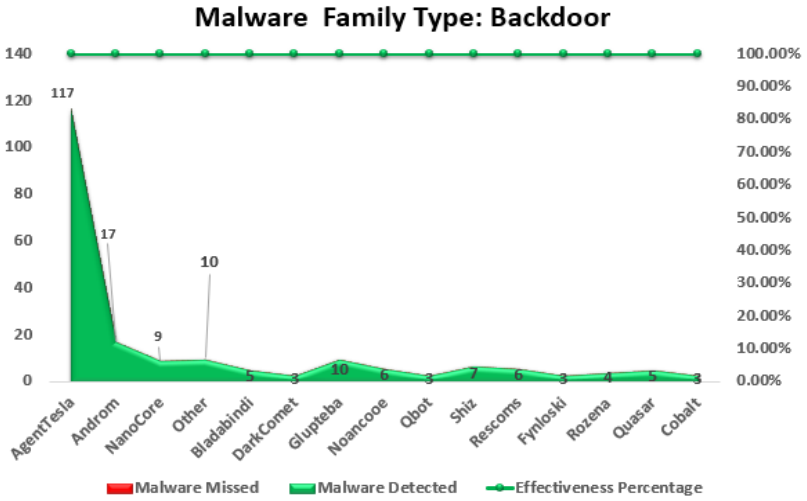


Fig. 16 – Effectiveness against Backdoors

As one would expect from the SonicWall advanced threat defense solution, given that it was 100% effective during the Q3 2021 test cycle, the SonicWall Capture ATP solution was very effective at detecting malware across malware types and across malware families.

Prior ATD Reports

With this report, SonicWall's advanced threat defense solution, SonicWall Capture ATP, passed all the test cases to retain ICSA Labs Advanced Threat Defense Certification. Successful completion of this test cycle marks SonicWall's 7th consecutive quarter having met the ICSA Labs ATD certification testing criteria.

This and all earlier SonicWall Capture ATP certification testing reports can be found on the ICSA Labs web site at:

https://www.icsalabs.com/product/sonicwall-capture-atp

Significance of the Test & Results

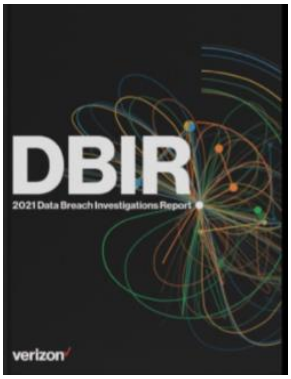
Readers of certification testing reports often wonder what the testing and results really mean. They ask, "In what way is this report significant?" The four statements below sum up what this ICSA Labs Advanced Threat Defense Certification Testing report should indicate to the reader:

1. ICSA Labs tested SonicWall's advanced threat defense solution using the primary threat vectors leading to enterprise breaches according to Verizon's Data Breach Investigations Report (DBIR).

2. ICSA Labs tests with malicious threats including new and little-known Ransomware that other security products typically miss.

3. SonicWall Capture ATP demonstrated superb threat detection effectiveness against over 650 *new and little-known* threats.

4. The SonicWall Capture ATP advanced threat defense solution had zero false positives during this test cycle, which is excellent.



Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.

Darren Hartman

Darren Hartman, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For over 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icsalabs.com

SonicWall

SonicWall has been fighting the cyber-criminal industry for over 25 years defending small, medium-size businesses and enterprises worldwide. Backed by research from SonicWall Capture Labs and coupled with the formidable resources of over 18,000 loyal channel partners around the globe, SonicWall provides award-winning real-time breach detection and prevention solutions that secure more than a million business and mobile networks as well as their emails, applications, and data. SonicWall's combination of products and partners enables an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 150 countries. These businesses can run more effectively with less concerns about being compromised.

www.sonicwall.com