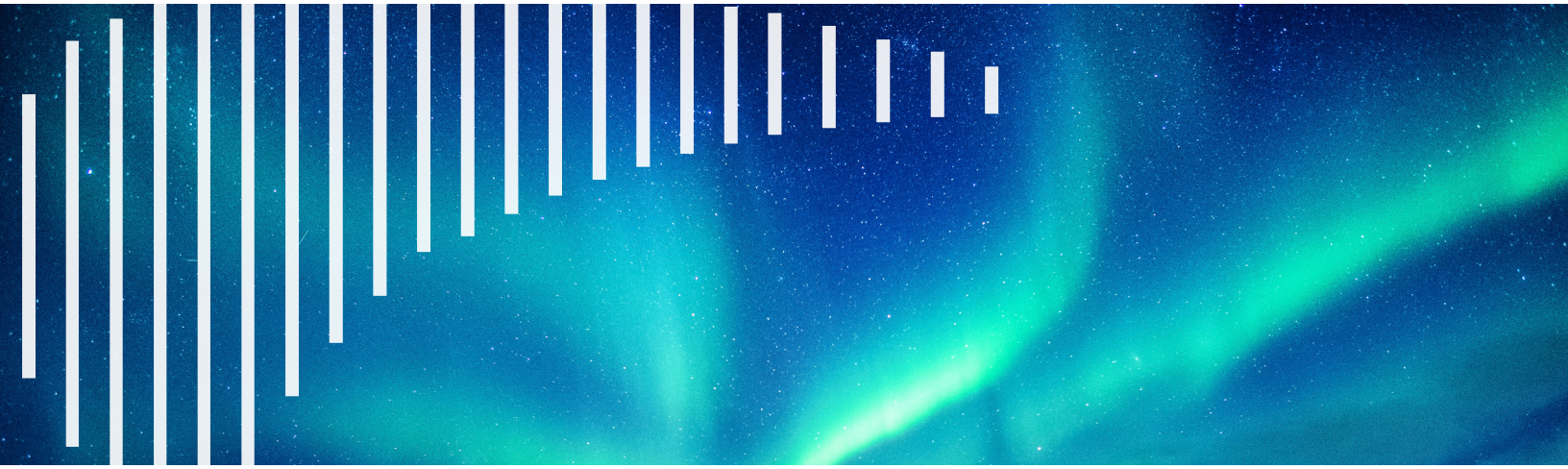


Perfecting Security Efficacy: SonicWall Sets New Standard for Threat Protection

How AI and machine learning helped propel Capture ATP with RTDMI to the head of the pack — and earned it multiple third-party certifications along the way.

The past two years have seen a more profound shift in the IT environment than any other time in history. With remote and hybrid work arrangements becoming the way forward, perimeters are more dynamic than ever before. The attack surface, however, only continues to grow, as new apps, devices and clouds are adopted — bringing with them ever-increasing risk.

This sort of chaos is ripe for exploitation. In 2021, attacks rose across the board, with ransomware up 105%, cryptojacking up 19% and IoT malware attacks up 6%. These trends pushed losses from cybercrime up from $4.2 billion in 2020 to $6.9 billion in 2021 — a 64% increase in just one year. And by midyear 2022, we've already seen cryptojacking rise 30% and IoT malware spike 77% over the same time last year.

But while organizations are becoming increasingly aware that they can't afford to fall behind in the cybersecurity arms race, that doesn't mean they can afford to keep up. The cost of materials and labor are rising faster than they have in decades, putting downward pressure on IT budgets just when they're needed most.

Capture ATP Leads the Pack in ICSA Certifications

With the stakes higher than ever, how can cybersecurity professionals know they're getting the best protection for the best price? With a dizzying number of solutions on the market, the reassurance that comes with third-party certifications is more important than ever. That's why SonicWall is proud to have earned an amazing six consecutive 100% threat detection scores in independent ICSA testing.

As part of its Advanced Threat Defense evaluations, third-party testing firm ICSA Labs has spent the past six quarters testing a SonicWall NS*a* 3600 NGFW equipped with SonicWall Advanced Threat Protection (ATP) and patented Real-Time Deep Memory Inspection™ (RTDMI) technology. And the testing results are unmatched by any other security vendor currently participating in ICSA testing:

For 195 days of continuous testing, consisting of 7,779 total test runs, SonicWall Capture ATP found all 3,579 malicious samples — the majority of which were four hours old or less. And it did so while misidentifying only one of the 4,200 innocuous apps scattered out.

"In today's fast-moving and unpredictable threat landscape, it is really hard to earn consistent third-party validation," said SonicWall Vice President of Software Engineering & Threat Research Alex Dubrovsky. "Our consecutive perfect scores are a confirmation of our vision and a significant milestone to the SonicWall team's dedication to providing organizations with the very best threat intelligence technology."

SOLUTION BRIEF

How RTDMI™ Gets Smarter, Faster, Better

While third-party testing firms were busy evaluating SonicWall Capture ATP with RTDMI™, its performance was also being monitored by SonicWall Capture Labs. Based on its performance over the course of 2021 and into 2022, threat researchers determined that not only was Capture ATP with RTDMI besting its competitors — it was also besting all previous versions of itself.

In 2021, the technology identified a total of 442,151 never-before-seen malware variants, a 65% increase over 2020's count. In October 2021, the monthly total of never-before-seen malware variants identified by RTDMI™ surpassed 50,000 for the first time, only to climb even higher the following month.

This stellar performance continued into 2022. In the first half of the year, RTDMI found 270,228 never-before-seen malware variants, a 45% increase year-to-date. Since the introduction of RTDMI in early 2018, the number of new variants discovered has skyrocketed 2,079%.

While full-year 2022 numbers have not yet been tallied, in 14 of the last 18 quarters through the middle of 2022, the number of new malware variants identified has exceeded that found in the previous quarter. With a total of 147,851 never-before-seen malware attacks, Q1 2022 had by far the highest number of malware detections on record.

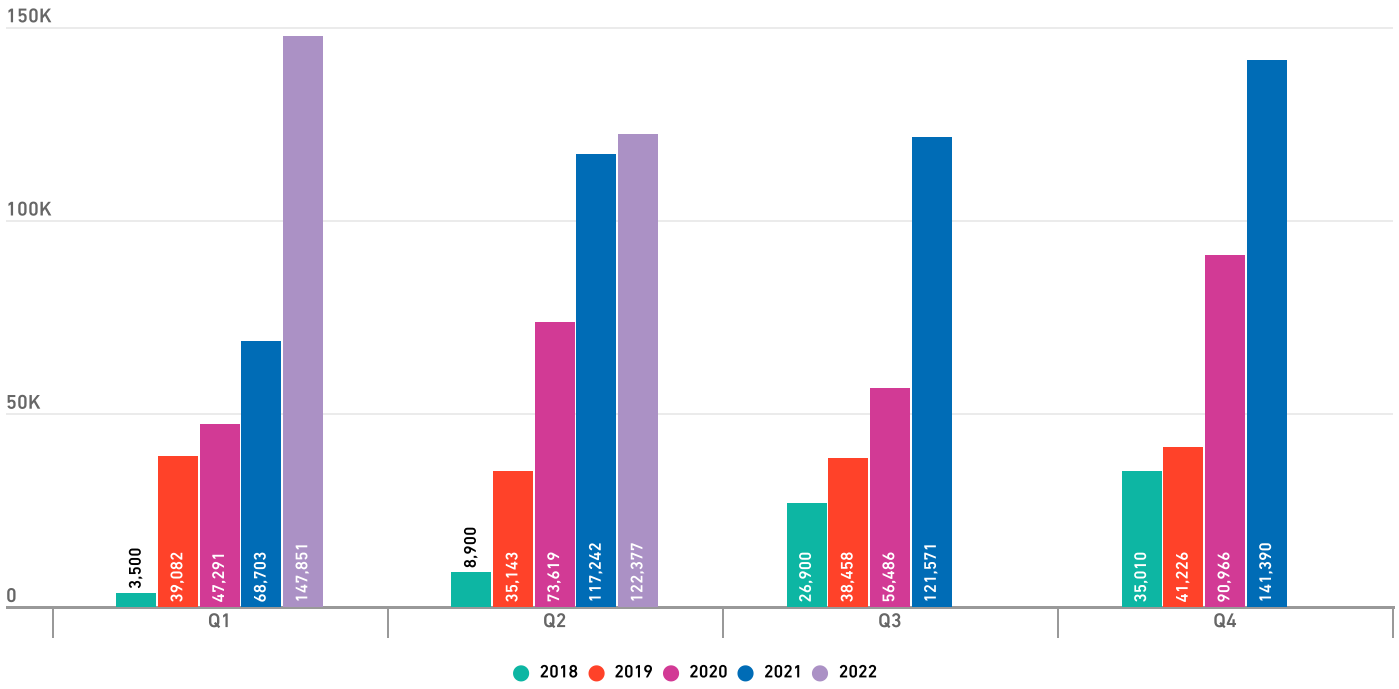
"Armed with more than a decade of machine-learning experience, RTDMI plays an essential role in quickly identifying destructive malware strands not detected by traditional sandboxing technology," said SonicWall SVP and Chief Technology Officer John Gmuender. "As cyberattacks continue to strengthen and escalate, so must technology and the creative thinking of researchers who work around the clock to ensure that organizations in all industries can advance their reliance on the digital and connected world."

SonicWall NGFWs Are ICSA-Certified, Too

Capture ATP isn't the only SonicWall solution to earn ICSA Labs certification. Based on comprehensive and robust performance testing, SonicWall next-generation firewalls — including SonicWall TZ Series, NS*a* Series, NS*sp* Series and NS*v* Series — have earned ICSA Labs Enterprise Firewall Certification, the highest level of firewall certification to date.

The TZ, NS*a*, NS*sp* and NS*v* firewalls have also earned the ICSA Labs Anti-Malware Certification, based on monthly malware testing cycles that ensure certified products are continuously ahead of the latest malware trends.

'Never-Before-Seen' Malware Variants Found by RTDMI™



SONICWALL

Testing Results

Q1 2021

From Jan. 20, 2021, through Feb. 23, 2021, SonicWall Capture ATP was subjected to 35 days of continuous testing by ICSA Labs. To measure the technology's threat detection capabilities, a mix of 1,471 test runs were conducted — 580 of which consisted of new and little-known threats, such as recently harvested threats not detected by traditional security products. The test cycles also included 891 innocuous apps and activities, designed to rate Capture ATP's ability to detect threats without raising false positives.

According to the final Q1 2021 ICSA Labs report, "SonicWall Capture ATP did remarkably well during this test cycle, detecting 100% of previously unknown threats while having zero false positives."

Q1 2021 ICSA Labs Testing Results			
Test Length	35 Days	Test Runs	1,471
Malicious Samples	580	% Detected	100%
Innocuous Apps	891	% False Positives	0%

Read the full report here.

Q2 2021

Beginning on April 13, 2021, and culminating on May 15, 2021, the testing round for Q2 2021 brought SonicWall another 100% score. After 33 days of continuous testing and 1,144 total test runs, SonicWall Capture ATP once again performed perfectly, identifying all 544 malicious samples (including 216 threats that were 4 hours old or less) without flagging a single one of the 600 innocuous apps.

These results represented a unique achievement among current ICSA participants: SonicWall is the only vendor to earn two back-to-back perfect scores.

"It is a milestone moment to see our technology reach this level and to receive such a wonderful score when tested against some of the most unknown and rigorous threats today," said SonicWall President and CEO Bill Conner. "These third-party, real-world tests play a vital role in ensuring that we continue to strive for and deliver excellent products and services to organizations that often feel bombarded and overwhelmed during the buying process."

Q2 2021 ICSA Labs Testing Results			
Test Length	33 Days	Test Runs	1,144
Malicious Samples	544	% Detected	100%
Innocuous Apps	600	% False Positives	0%

Read the full report here.

Q3 2021

SonicWall Capture ATP continued to perform perfectly throughout the Q3 2021 test cycle, when 28 days of continuous testing yielded yet another 100% score — still with no false positives. From July 14 through Aug. 10, 2021, SonicWall Capture ATP was subjected to 1,348 test runs. During these evaluations, the technology flagged all 653 malicious samples without misidentifying any of the 695 innocuous apps.

Q3 also brought SonicWall another distinction. Once final results were tallied, SonicWall became the active vendor with the highest total number of perfect scores, doing in nine months what no other active vendor had been able to achieve since testing began in 2015.

"Technology is constantly changing as is the complexity of environments," said SonicWall Executive Director of Product Marketing Kayvon Sadeghi. "Unbiased testing is crucial during the selection process, and we want our participation to help simplify a task that can be daunting with so many options in the marketplace."

Q3 2021 ICSA Labs Testing			
Test Length	28 Days	Test Runs	1,348
Malicious Samples	653	% Detected	100%
Innocuous Apps	695	% False Positives	0%

Read the full report here.

Q4 2021

During the final quarter of 2021, SonicWall again participated in ICSA Advanced Threat Defense testing. The result? Yet another perfect score. Between Oct. 13, 2021, and Nov. 13, 2021, SonicWall Capture ATP with RTDMI™ faced 1,625 total test runs, detecting all 801 malicious samples without incorrectly identifying any of the 824 innocuous apps.

"On 32 of 32 days during the Q4 2021 test cycle, SonicWall Capture ATP was 100% effective," the ICSA Labs Q4 report stated.

Q4 2021 ICSA Labs Testing Results			
Test Length	32 Days	Test Runs	1,625
Malicious Samples	801	% Detected	100%
Innocuous Apps	824	% False Positives	0%

Read the full report here.

Q1 2022

January brought both a new year and continued success for SonicWall Capture ATP. From Jan. 19 through Feb. 19, 2022, SonicWall Capture ATP and RTDMI™ was once again put through its paces. And once again, it correctly identified all 553 malicious samples without flagging any of the 578 innocuous apps.

"As one would expect from an advanced threat defense solution that was 100% effective during the Q1 2022 test cycle, the SonicWall Capture ATP solution was very effective at detecting malware across malware types and across malware families," the ICSA report on SonicWall's performance read.

"SonicWall has now received an amazing five consecutive perfect scores when tested against some of the most unknown and rigorous threats — an unprecedented achievement among tested vendors," said SonicWall President and CEO Bill Conner. "These third-party, real-world tests validate SonicWall as a clear leader in the cybersecurity space and play a significant role in our efforts to deliver quality-driven security products."

Q1 2022 ICSA Labs Testing Results			
Test Length	32 Days	Test Runs	1,131
Malicious Samples	553	% Detected	100%
Innocuous Apps	578	% False Positives	0%

Read the full report here.

Q2 2022

During the second quarter of 2022, SonicWall Capture ATP with RTDMI™ did it once again. Over 35 days, from June 1 to July 5, the solution correctly identified all 448 malicious samples (including the 203 threats that were three hours old or less), earning a 100% threat detection score. This marks the sixth consecutive quarter that SonicWall has earned a 100% score for identifying malicious samples.

Out of the 612 innocuous samples mixed in, SonicWall properly identified 611, issuing just one false positive. This was the lowest false-positive rate among those who got a 100% score. Since Q1 2021, SonicWall's false positive rate stands at .02%.

"SonicWall Capture ATP was 100% effective during the Q2 2022 test cycle, detecting all of the new and little-known malicious threats in the test set," the ICSA Labs Q2 2022 report stated.

Q2 2022 ICSA Labs Testing Results			
Test Length	35 days	Test Runs	1,060
Malicious Samples	448	% Detected	100%
Innocuous Apps	611/612	% False Positives	.16%

Read the full report here.

Capture ATP and RTDMI: SonicWall's Threat-Detection Dream Team

SonicWall Capture Advanced Threat Protection (ATP) multi-layer sandbox service is designed to mitigate new forms of malware that use sophisticated evasion tactics to circumvent traditional network defenses. This cloud-based service, available for SonicWall firewalls and other solutions, was built to give malicious code different environments in which to detonate harmlessly, sparing the network itself.

Included as part of Capture ATP, SonicWall's patented Real-Time Deep Memory Inspection (RTDMI™) leverages proprietary memory inspection, CPU instruction tracking and machine learning capabilities to become increasingly efficient at recognizing and mitigating cyberattacks never before seen by anyone in the cybersecurity industry — including threats that don't exhibit any malicious behavior and hide their weaponry via encryption. These are attacks that traditional sandboxes will most likely miss.

RTDMI is capable of finding malware that relies on various evasion techniques — frequently variants of existing malware that have been obfuscated, repacked or recompiled to evade all existing industry detection.

And since RTDMI can detect malicious code or data in memory and in real time during execution, no malicious system behavior is necessary for detection. In other words, the presence of malicious code can be identified prior to any malicious behavior taking place, allowing for a quicker verdict.

Best of all, because it incorporates AI and machine learning technologies, RTDMI™ is continuously becoming more efficient and effective.

What Is ICSA Labs Testing and How Does It Work?

For more than two decades, SonicWall has been committed to independent third-party testing performed by ICSA Labs, an independent division of Verizon. The goal of ICSA Labs is to significantly increase trust in information security products and solutions by providing credible, independent third-party security product testing and certification.

Standard ICSA Labs Advanced Threat Defense (ATD) testing is designed with vendor solutions in mind, and helps determine new threats traditional security products do not detect. Eligible security vendors are tested quarterly for a minimum of three weeks.

During that time, ICSA Labs subjects the vendors' advanced threat defense solutions to hundreds of test runs consisting of a mixture of innocuous applications, new threats and little-known threats. These threats are delivered via the primary threat vectors that lead to enterprise breaches, according to Verizon's Data Breach Investigations Report. The focus is on how effectively vendor ATD solutions detect these threats while minimizing false positives.

Learn more about how SonicWall Capture ATP with patented RTDMI™ technology can protect your organization from sophisticated, never-before-seen threats.

www.sonicwall.com/products/capture-advanced-threat-protection

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

SolutionBrief-ICSA-JK-7011