Nomination: 20247

SonicWall - RTDMI

Page: General Information
Name of Organization / Company
SonicWall
Logo
Download File (https://asiastevieawards.secure-platform.com/file/31158/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJtZWRpYUlkIjozMTE1OCwiYWxsb3dOb3RaWduZWRVcmwiOiJGYWxzZSIsImlnbb Sonicwall_Logo_RGB_Black_Orange.jpg)
Web Site Address
https://www.sonicwall.com/ (https://www.sonicwall.com/)
Page: Entry Information
Entry Title
SonicWall - RTDMI
Category
N01 - N07 - Award for Innovation in Technology > N04. Award for Innovation in Artificial Intelligence (AI) and Machine Learning (ML) > Computer Industries
Submission Format
An Essay of up to 625 Words

Essay

Address Hard-to-Catch Data Breaches with Innovative AI-Enabled Cybersecurity Solution
Expanding network perimeters creating entryways for cybercriminals

Imagine your organization adapting to the new-age work culture, relying on various online tools to stay connected and productive. Now, picture discovering that the sensitive data entrusted to these systems has been stolen. It is like finding out your company's most confidential information has been exposed to the world without your consent. This is the harsh reality of data breaches.

With remote and hybrid work becoming the norm, IT environments have grown more scattered and flexible. As companies adopt more apps, devices, and cloud services to support their workforce, they inadvertently create entry points for cybercriminals and expand system vulnerabilities. The once well-defined network perimeters dissolve, increasing organizations' exposure to evolving threats.

Over the past few years, the attack surface has significantly expanded. These statistics highlight the severity of the problem –

• Cryptojacking increased by 659% from 2022 to 1.06 billion attacks in 2023

• IoT malware attacks reached 77.9 million, a 37% year-to-date increase, surpassing any other six-month period on record

• Between 2022 and 2023, 2.6 billion personal records were leaked in data breaches

Considering the growing scale and variety of cyberattacks, organizations have no choice but to turn to AI-powered cybersecurity systems and remain vigilant to mitigate zero-day attacks, new vulnerabilities, and unknown threats. As cybersecurity software floods the market, third-party certifications serve as crucial benchmarks to guide organizations in selecting the most effective solutions.

Thwarting encrypted malware with innovative ML-powered memory inspection
SonicWall applied artificial intelligence (AI) and machine learning (ML) principles to enhance its cybersecurity solutions deploying Capture Advanced Threat Protection (ATP) with Real-Time Deep Memory Inspection™ (RTDMI™). After rigorous testing over several quarters, this innovative product delivered 100% threat detection scores, earning it standardized certifications seven times.

During Advanced Threat Defense assessments by ICSA Labs, SonicWall firewalls with SonicWall Capture ATP and patented RTDMI™ technology were tested over seven quarters. The tests, which spanned 223 days and 9,071 individual runs, showed SonicWall Capture ATP detecting all 4,251 malicious samples, most of which were under four hours old, with only one false positive out of 4,820 benign applications.

Additionally, Capture ATP and RTDMI™ earned NetSecOPEN Certification - Network Security Product Performance Testing for blocking 100% of cyberattacks. NetSecOpen's accredited lab reported that SonicWall's firewall effectively blocked 5,388 vulnerabilities, including public, and private vulnerabilities, malware and evasion techniques.

Capture ATP's multilayer sandbox and RTDMI™'s proprietary technology identify new vulnerabilities and prevent zero-day attacks often missed by traditional sandboxes. Using memory inspection, CPU instruction tracking, and ML, they detect evasion tactics in real time, stopping over 1,600 new malware variants daily. This proactive approach enables businesses to better safeguard data and minimize breach risks.

Success story
Challenge: The client was a renowned hospitality business that operates hotels across multiple locations. As part of their amenities, they wanted to provide their guests with secure wireless connectivity for business and leisure purposes. Concern over unknown malware attacks from user devices triggered their need for a proactive cybersecurity solution.
Solution: The company opted for Capture ATP with RTDMI™ along with SonicWall's next-gen firewalls in high-availability mode to protect their networks from malware attacks.

Outcomes: The new installation transformed the company's network performance into a juggernaut. They could now provide high-speed connectivity to VPN users and users on campus alike. Guests could connect with their own devices and use the wireless connection with confidence. Large file downloading now takes just a minute or even less. Additionally, despite high usage, the company found that Capture ATP and RTDMI™ prevented unknown malicious attacks, resulting in zero data breaches and malware intrusion attempts through encrypted SSL packets.

For this category please provide

An essay of up to 625 words describing the nominee's innovative achievements in technology since July 1 2022, **OR** a video of up to five (5) minutes in length illustrating the same.

Optional (but highly recommended), a collection of supporting files and web addresses that you may upload to our server to support your entry and provide more background information to the judges.

Do You Have Supporting Files You Would Like to Upload?

Yes

Audio (Mp3), Documents (PDFs, Word, PowerPoints), Images (PNG, JPG, TIF), and Video (Mp4)

200 MB Max per File

File 1

████████████████████
███
██

█████

████████████████████
███
██

File 3

███████████████████████████

███

██████████████████████████████

███████

███████████████████████████

███

███████████████████████

██████

███████████████████████████

███

██

File 6

███████████████████████████

███

██

File 7

No File Uploaded

File 8

No File Uploaded

File 9

No File Uploaded

File 10

No File Uploaded

Do You Have Website URLs you would like to link to

Yes

URL 1

██

███████

███

██████████████████████████

URL 3

URL 4

URL 5

URL 6

URL 7

URL 8

URL 9

URL 10

By your submission of this entry to The Stevie Awards you verify that you have read and agree to abide by the regulations, terms and conditions of the competition (http://asia.stevieawards.com/rules-and-terms-conditions-competition).

Terms and Conditions

I Agree