SonicWall Capture Advanced Threat Protection (ATP)

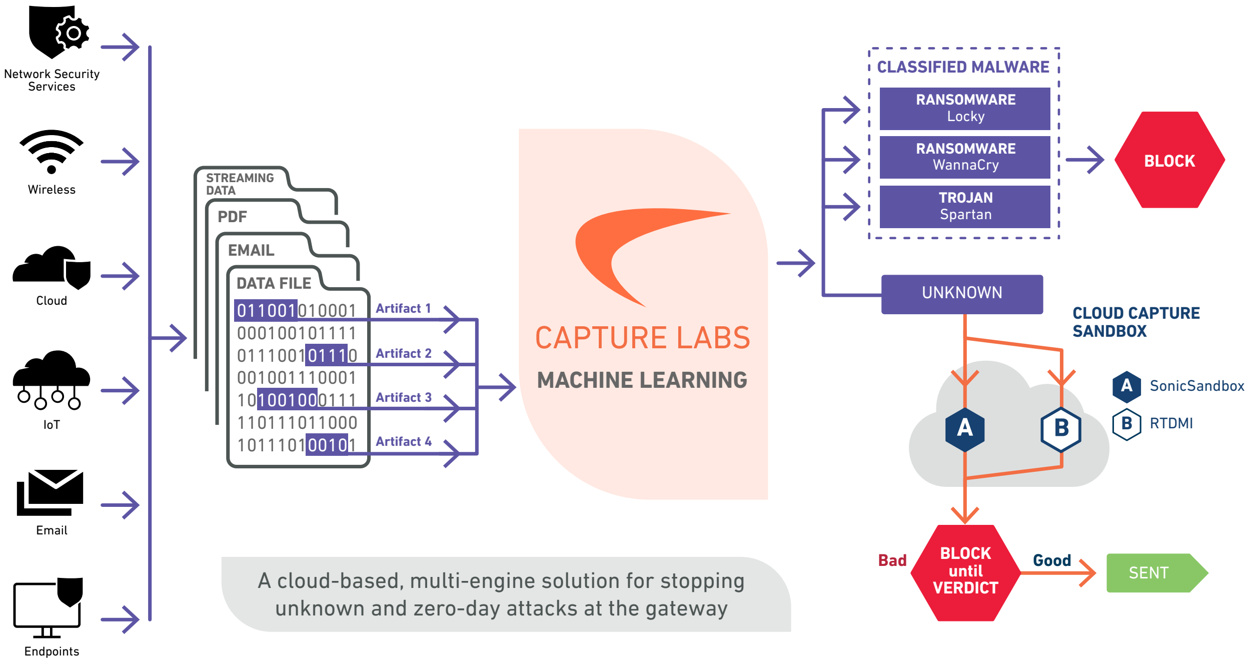
Effective on-prem and cloud based advanced threat protection with multi-solution flexibility.

To effectively protect against sophisticated threats, organizations require advanced solutions that incorporate robust malware analysis technologies capable of detecting evasive and emerging threats. SonicWall's Capture Advanced Threat Protection ™ (ATP) was the industry's first multi-engine sandbox to offer block-until-verdict capabilities. This innovative technology rapidly delivers accurate verdicts on suspicious files and seamlessly integrates across the entire SonicWall product ecosystem for comprehensive protection both in the cloud and on premises.

HIGHLIGHTS

Benefits

- **Advanced Threat Protection:** Detects unknown malware before it enters the network
- **Real-Time Deep Memory Inspection (RTDMI™):** Identifies hidden or dormant malware with memory-based analysis
- **Multi-Engine Sandboxing:** Detects evasive threats with multiple analysis engines
- **Broad File Type Coverage:** Inspects various file types
- **Automated Threat Blocking:** Blocks files at the gateway until verdict based on your policies
- **Seamless Integration:** Integrates with SonicWall solutions across your security architecture



A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway

DATASHEET

Features

Capture ATP is a flexible and effective advanced threat protection with numerous deployment options to protect organizations of all sizes. By scanning and analyzing a wide range of file types and sizes, its global threat intelligence quickly deploys remediation signatures, ensuring fast response times, and high security effectiveness.

MULTI-ENGINE ADVANCED THREAT ANALYSIS

Capture ATP Service inspects traffic, and it detects and blocks intrusions and known malware. Suspicious files are sent to the SonicWall Capture ATP Cloud for analysis. The multi-engine sandbox platform, which includes RTDMI and full system emulation technology, executes suspicious code and analyzes behavior, and provides comprehensive visibility to malicious activity while resisting evasion tactics and maximizing zero-day threat detection.

REAL-TIME DEEP MEMORY INSPECTION (RTDMI)

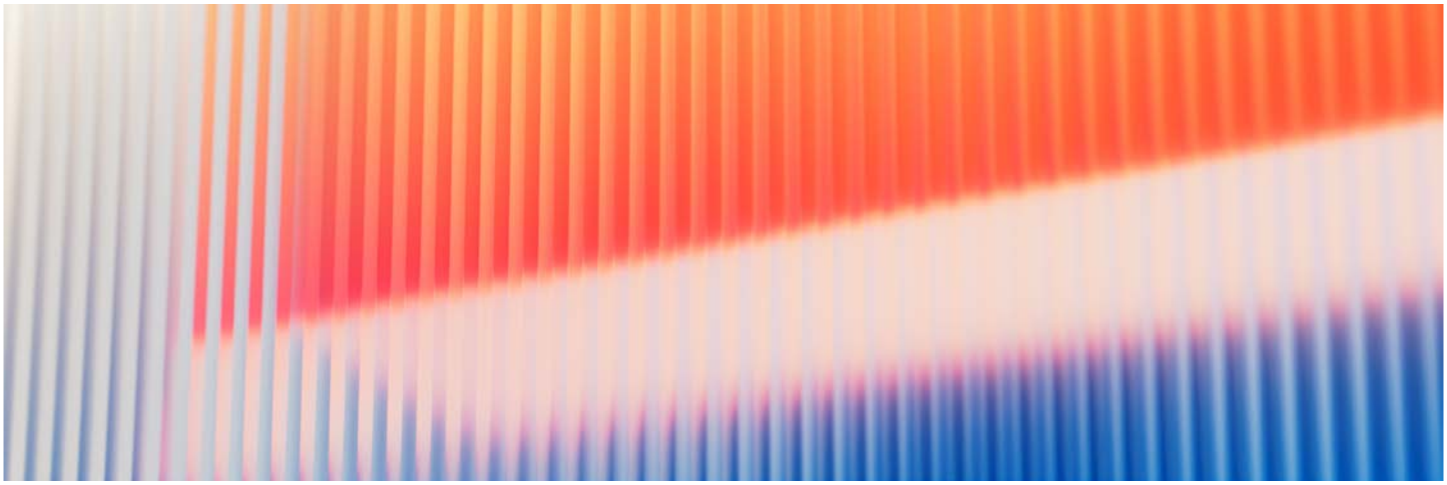
The RTDMI engine enhances Capture ATP through proactively detecting and blocking mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks.

BROAD FILE TYPE ANALYSIS

Capture ATP analyzes a wide range of file types and sizes, including executables (PE), DLLs, PDFs, MS Office documents, archives, JARs, and APKs, across Windows and Android platforms. Administrators can customize protection by specifying which files to analyze based on file type, size, sender, recipient, or protocol. They can also manually submit files for analysis. Malicious files are retained in the database for one month, while benign files are automatically deleted within 24 hours.

BLOCKS UNTIL VERDICT

To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined .



RAPID DEPLOYMENT OF REMEDIATION SIGNATURES

When a file is identified as malicious, a signature is immediately generated for SonicWall Capture ATP products to block future attacks. The malware is also submitted to SonicWall Capture Labs for further analysis and added to the Gateway Anti-Virus and IPS databases, as well as URL, IP, and domain reputation databases within 48 hours.

REPORTING AND ALERTS

The SonicWall Capture ATP provides an at-a-glance threat analysis dashboard and reports, which detail the analysis results for files sent to the service, including source, destination and a summary plus details of malware action once detonated.

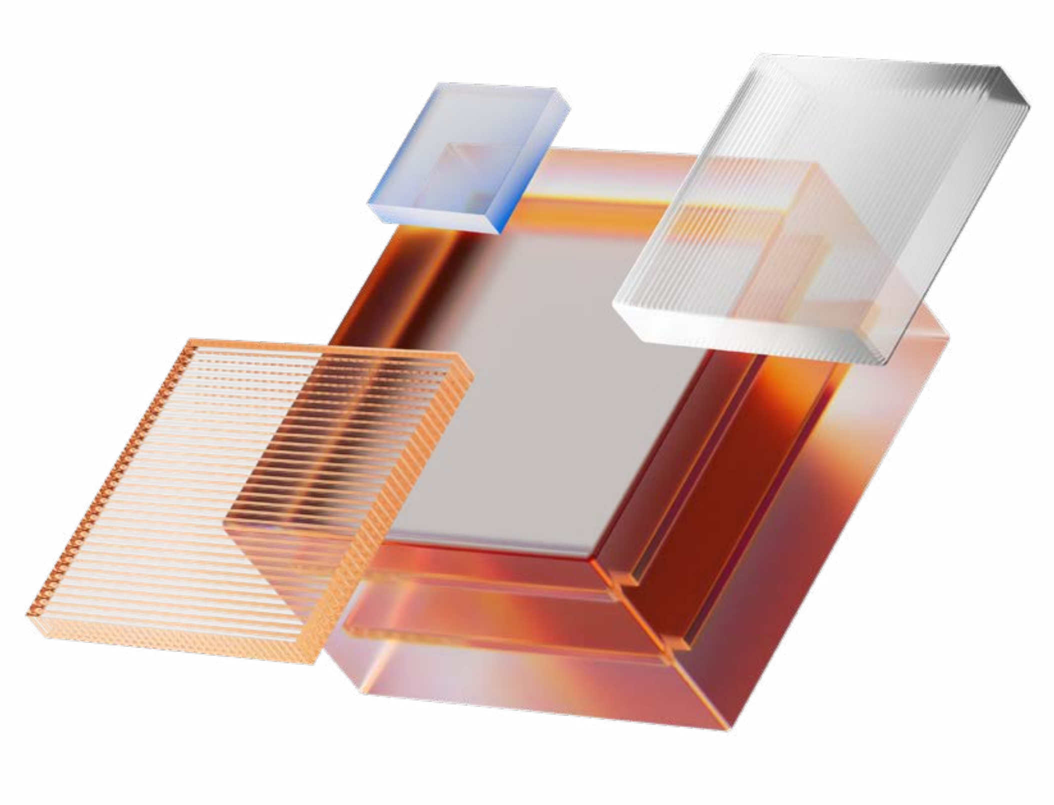
File Types Supported	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzip2 .7z .xz .gz .zip

CSA

CAPTURE SECURITY APPLIANCE (CSa)

Capture Security Appliance (CS*a*) brings the technology of Capture ATP and RTDMI to on-premises deployment scenarios. CS*a* offers customers a hardware platform that allows them to retain all their data inside their organization, while taking advantage of Capture ATP's sophisticated threat detection capabilities.

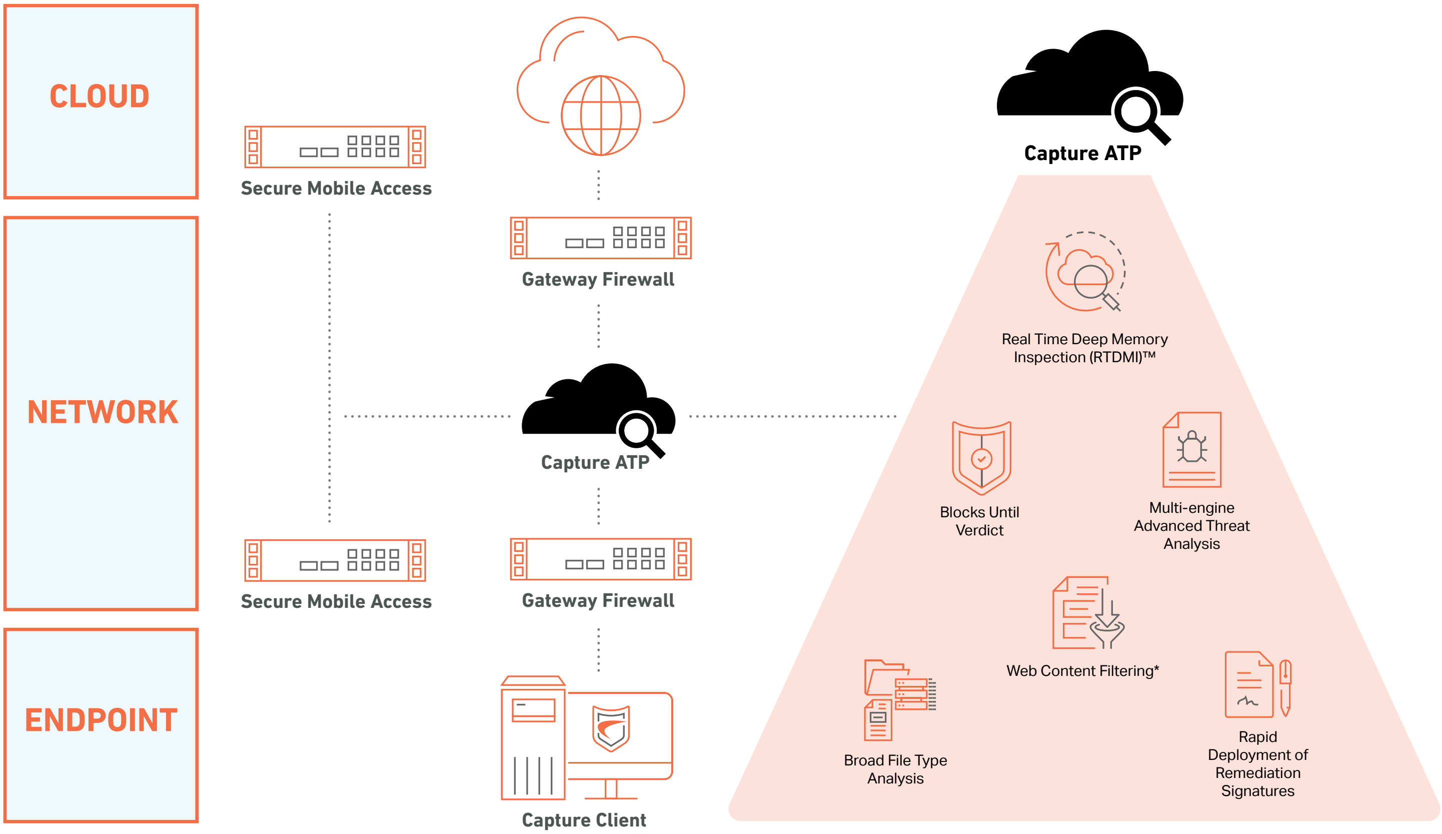
Learn more about Capture Security Appliance (CS*a*) here.



Threat Mitigation at Every Layer

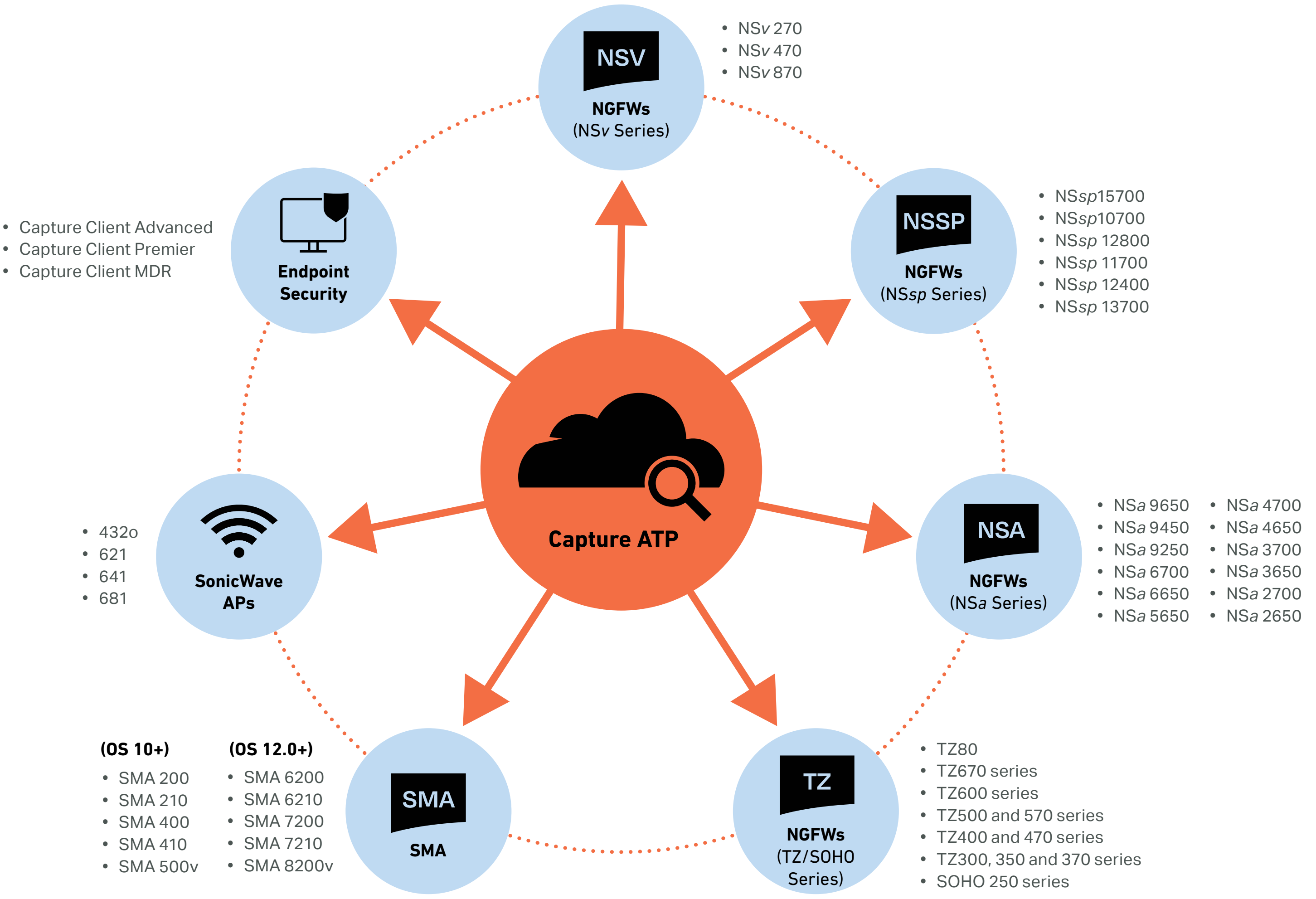
Capture ATP strengthens threat mitigation by blocking advanced threats across cloud, network, and endpoint environments. Its real-time detection, multi-layer sandboxing, and integration with global threat intelligence ensure comprehensive protection against today's evolving cyber threats.

1. **Cloud**
   Capture ATP integrates with cloud-based applications and services, inspecting incoming files and data for malicious content. It blocks threats before they infiltrate cloud environments.
2. **Network**
   Capture ATP scans all traffic entering the network, detecting and blocking malware at the network perimeter before it reaches endpoints and/or critical systems. Administrators can configure network traffic rules to filter files by type, size, or protocol, allowing granular control over which files are analyzed and which are allowed into the network.
3. **Endpoint**
   By blocking threats at the endpoint, Capture ATP helps prevent malware from spreading laterally through the endpoint. If a malicious file is detected, Capture ATP generates a signature in real-time, ensuring all connected endpoints are protected from follow-on attacks.



*Web Content Filtering is available with Capture Client and Firewall Security Services

Supported Products



NSV
NGFWs
(NS*v* Series)

- NS*v* 270
- NS*v* 470
- NS*v* 870

NSSP
NGFWs
(NS*sp* Series)

- NS*sp*15700
- NS*sp*10700
- NS*sp* 12800
- NS*sp* 11700
- NS*sp* 12400
- NS*sp* 13700

NSA
NGFWs
(NS*a* Series)

- NS*a* 9650
- NS*a* 9450
- NS*a* 9250
- NS*a* 6700
- NS*a* 6650
- NS*a* 5650
- NS*a* 4700
- NS*a* 4650
- NS*a* 3700
- NS*a* 3650
- NS*a* 2700
- NS*a* 2650

TZ
NGFWs
(TZ/SOHO Series)

- TZ80
- TZ670 series
- TZ600 series
- TZ500 and 570 series
- TZ400 and 470 series
- TZ300, 350 and 370 series
- SOHO 250 series

SMA
SMA

(OS 10+)

- SMA 200
- SMA 210
- SMA 400
- SMA 410
- SMA 500v

(OS 12.0+)

- SMA 6200
- SMA 6210
- SMA 7200
- SMA 7210
- SMA 8200v

SonicWave APs

- 432o
- 621
- 641
- 681

Endpoint Security

- Capture Client Advanced
- Capture Client Premier
- Capture Client MDR

Note: SonicWall Capture ATP is supported on firewalls running SonicOS 7.0 and higher

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

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