SONICWALL

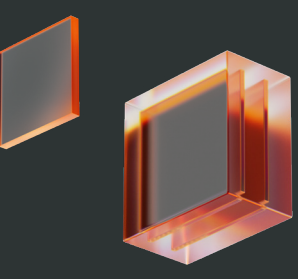
SonicSentry Managed Detection and Response (MDR)

Protecting the protectors with powerful technology and expert SOC monitoring.

SonicSentry MDR, powered by CrowdStrike, is a comprehensive service that includes 24/7 threat monitoring, threat hunting, and detection response. The service leverages advanced analytics, threat intelligence, and human expertise to deliver sophisticated and thorough incident investigation and response. Incident validation, along with remote response services such as threat containment, are also available.

- Detect advanced endpoint threats that make it past your other defenses
- Deliver proactive security services to your customers via a 24x7 expert-led SOC leveraging the latest threat intelligence
- Prevent spreading of ransomware with automatic network isolation and termination of ransomware processes
- Overcome alert fatigue and reduce false positives
- Our flagship offering leverages CrowdStrike's powerful endpoint protection tools.
- We also support SentinelOne, Capture Client, Windows Defender, and Sophos, giving you ultimate flexibility.

> "SonicWall's SOC detected strange activity on a client's server at 2 a.m. We were able to contain the breach at an early stage. I sleep better at night knowing SonicWall is watching over my networks."
>
> **—DAN BROWNE, CEO, DTM CONSULTING**



Discover what true partnership with a security provider is like: Increase visibility across your ecosystem and access rapid response from our fully manned 24x7x365 SOC.

To learn about the wide range of benefits enjoyed by SonicWall SecureFirst partners, contact us today!
partnerdevelopment@sonicwall.com

PROVEN TECHNOLOGIES. SUPERIOR PROTECTION.

Here's how SonicSentry MDR improves security while optimizing resources:

AGENT-BASED DEPLOYMENT

Lightweight agents are installed on endpoints, providing persistent and continuous access while enabling real-time monitoring and collection.

ANOMALY-BASED DETECTION

Utilizing heuristics, statistical analysis and machine learning, the agent highlights any atypical events or features of an artifact or file, aiding in detection of advanced or zero-day threats.

Anomaly-Based Detection includes:

- Real-time process and script monitoring
- Continuous live memory analysis
- Detects PowerShell and other Living Off the Land (LOTL) adversary techniques
- Prevents abuse of user accounts and legitimate administrative tools
- Stops threats from moving laterally

BEHAVIOR-BASED DETECTION

The behavioral analytics engine inspects legitimate processes and events for suspicious behaviors. These anomalies are then mapped to known attacker tactics, techniques and procedures (TTPs) as described by the MITRE ATT&CK Framework. By focusing on 20 of the most commonly observed ATT&CK techniques, SonicSentry MDR is highly effective at catching adversaries in the act.

FORENSIC STATE ANALYSIS

The agent can collect and analyze live forensic data from endpoints, including volatile and non-volatile memory. This allows proactive inspection of thousands of hosts for current and historical compromise, and helps you identify the root cause of detected attacks. Analysis can be conducted agentlessly or via the ARR agent.

Forensic State Analysis includes:

- Active processes and scripts
- Triage of live volatile memory
- Registry and autoruns (run keys, startup folders, lnk files, schtasks/cron, etc.)
- Execution artifacts (shimcache, amcache, prefetch)
- Os subversion (api hooks, disabled controls)
- Local event log triage
- Privileged accounts
- Installed applications and vulnerabilities
- Active host connections and listeners

CONTINUOUS ENDPOINT MONITORING, RESPONSE AND FORENSICS

Advanced threat hunting and monitoring adds another layer of security. This capability is focused on identifying key behaviors observed during and following an attack. Automated forensic analysis enables our experts to proactively verify the integrity of endpoints and to quickly determine a root cause once a breach is found. MDR simplifies and accelerates the identification, investigation and response to sophisticated cyberattacks.

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

SONICWALL®