SONICWALL

SONICSENTRY

MXDR

24×7 SOC Protection for Endpoint, Cloud, & Network

How Our Expert-Led SOC Detects, Defends, and Stops Threats – Wherever They Appear

1 What is MXDR?

Managed Extended Detection & Response (MXDR) pulls together threat data from your **endpoints, cloud apps, and network perimeter**, giving our 24×7 Security Operations Center (SOC) a complete view of your environment. That way, we can act fast when threats appear.

Endpoint:
Managed Detection & Response (MDR) using EDR tools and next-gen antivirus.

Cloud:
Cloud Email Security to block phishing and Cloud Threat Analytics to detect suspicious logins, admin changes, and more in many common business SaaS apps.

Network:
Monitoring of firewalls, servers, switches, domain controllers, and other edge devices to spot threats early and add important context.

2 SOC in Action: How We Handle Threats

Our SOC team watches over your environment around the clock. When alerts come in, they investigate, prioritize, and respond.

Minor Alerts (Possible Anomalies)

- Low risk, often false positives (like a file quarantined in a strange folder).
- The SOC will email you if needs a second look.

Major Alerts (Likely Threats)

- Confidence of malicious activity you should be aware of that was stopped by security tools.
- The SOC emails you for your awareness and suggests actions, like password resets or end-user training.

Critical Alerts (Active Breach)

- High confidence of a real compromise in progress.
- The SOC jumps in immediately: isolating devices, blocking malicious traffic, and updating firewalls.
- Emergency Calls begin right away: every 15 minutes in the first hour, then hourly until contact. The defense starts even if no one answers.

3 What Happens After a Threat Is Stopped

Once the danger is contained, our SOC team:

- **Delivers an Incident Report** explaining what happened and how far it spread.
- **Gives You Next Steps** like restoring devices, resetting accounts, or applying patches.
- **Supports a Full Cleanup** to return your systems to a safe, stable state.

4 One SOC. Full-Surface Protection.

With MXDR, we connect data from **endpoints, cloud services, and the network**. This gives our SOC full visibility to detect and respond faster and smarter

24/7 all year long.

To learn more about **SonicSentry MXDR** and how you can get started, contact us today.

Contact Us
210-465-1604

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