SonicWall Urges Customers to Replace Gen 6 Firewalls, Which Will Not Receive Security Patches



SonicWall has told customers still running Generation 6 firewalls to retire and replace them now and to stop exposing them at the internet edge, citing faster AI-assisted attacks on unsupported devices.

- SonicWall urges all customers still using Gen 6 firewalls to retire and replace them immediately.
- The devices should no longer be exposed on the internet edge.
- Per the headline, Gen 6 firewalls will not receive security patches, even for critical flaws.
- SonicWall says attackers use automation and AI to find and exploit unsupported edge devices faster than before.
- The source text is partial and gives no CVE numbers or dates.

SonicWall has advised every customer still running Generation 6 firewalls to retire and replace them immediately, and to stop exposing these devices on the internet edge. According to the source headline, the devices will not receive security patches, even for critical vulnerabilities.

The vendor's reasoning

SonicWall states that attackers now rely on automation and AI to locate and exploit unsupported edge devices faster than before. The company expects internet-facing Gen 6 firewalls to be targeted. The available source text is truncated, so further details, such as specific flaws or timelines, are not confirmed here.

What this means for regulated institutions

A perimeter firewall that cannot be patched is a standing exposure. Any institution still running Gen 6 units should treat replacement as a risk item with an owner and a deadline, not as routine lifecycle work. Where replacement cannot happen at once, reducing internet exposure is the vendor's clear direction.

Institutions should also confirm that the decision and any interim compensating measures are documented, so they can be shown to supervisors and auditors if asked.

What to do now

1. Inventory all SonicWall firewalls and identify any Generation 6 units, including those at branches and remote sites.
2. Remove Gen 6 devices from the internet edge, or restrict their exposure, as soon as possible.
3. Plan and fund replacement with a named owner and a fixed deadline.
4. Register the unpatchable devices in the risk register with interim compensating controls such as enhanced monitoring.
5. Review logs on any Gen 6 firewall for signs of unusual access, and document decisions for audit.