SONICWALL®

Zero Trust in the Age of AI-Powered Cyberattacks – Why Businesses Must Act Now

Zero Trust is no longer just a buzzword; it is a necessary response to a radically evolving threat landscape. According to the **SonicWall Cyber Threat Report 2025**, the situation has intensified dramatically: on average, organizations were targeted by critical attacks for **68 consecutive days. IoT attacks surged by 124%**, while **encrypted threats rose by 93%. Small and medium-sized businesses (SMBs)** were especially affected – often lacking the resources for advanced cybersecurity defenses.

Zero Trust means: **"Never trust, always verify."** Every access request – internal or external – is strictly validated. Core components of this model include **microsegmentation, multi-factor authentication (MFA)**, and **role-based access controls**. But Zero Trust only works effectively when it's approached holistically.

That's why SonicWall is transforming from a traditional product vendor into a **comprehensive platform solutions provider**. The **Capture Security Center** (CSE) serves as a centralized management and analytics hub that unifies all security solutions – from firewalls and endpoint protection to cloud security – into a single, intuitive interface. Threats can be identified, correlated, and mitigated in real time.

For organizations seeking external expertise, SonicWall also offers robust **Managed Security Services (MSS)**. These services are particularly valuable for SMBs, allowing them to access enterprise-grade security without the need for in-house security teams.

The Zero Trust approach – combined with SonicWall's **platform strategy** – is the key to building cyber resilience against today's and tomorrow's threats. Businesses that act now will lay a secure foundation for their digital future.