SONICWALL®

WatchGuard®

SMB Firewall Battlecard

WatchGuard Profile

WatchGuard Profile
1996 Seattle, WA
$ Private Equity ~ Annual Revenue $252.1M
~ 0.81% network security market share, ~11,857 companies using WatchGuard

Product Mapping	WatchGuard Description	SonicWall Equivalent
Firebox NV5	Small form factor, SD-WAN ready, for remote VPN support only, no security features	SonicWall TZ270 support only
Firebox T25 & T45	Small form factor, SD-WAN ready, Wi-Fi options available	SonicWall TZ270 & TZ370
Firebox T85	Best for sites up to 50 users, built-in PoE+ ports, SD-WAN ready	SonicWall TZ470
Firebox M290 & M390	Enterprise-grade protection for SMB	SonicWall TZ570 & TZ670

WatchGuard Strengths	WatchGuard Weaknesses
Acquisitions for Innovation → Panda (March 2020) provides WG with network AV, intelligence, secure Wi-Fi, and MFA. WG also acquired **Percipient Networks** (Jan 2018) for a cloud-based automated network security platform to protect against phishing and malware. Enough time has elapsed for these technologies to be integrated into the WG ecosystem and leveraged for things like gateway AV and DNS filtering	**WG APT Blocker cannot block unknown threats** → WG APT Blocker cannot block traffic while waiting for a verdict. If a user clicks on an unknown threat while browsing, the firewall will let the unknown threat through while waiting for a verdict from APT Blocker. SonicWall uses **Block Until Verdict** technology that will block/hold an unknown file and wait for a verdict from SonicWall's ATP solution before allowing suspect files through
Endpoint Integration → WatchGuard's Firebox firewall is managed in conjunction with its endpoint security products. The vendor has a process called ***ThreatSync*** that collects event data from WatchGuard firewalls, endpoint sensors and threat intelligence feeds, analyzes the collected data, and assigns threat scores accordingly	**Limited Product portfolio** → WG lacks Switch, a remote access, and API security for Cloud mail and file sharing platforms like Microsoft 365 / Google Workspace. WG does not, for example, have additional solutions that can be integrated for cloud application security across SaaS and Web to protect productivity apps like *Microsoft 365* and *Google Workspace*
Pricing Strategy → Under the ***FlexPay*** licensing model, WatchGuard offers the choice to purchase its firewalls using upfront payments, WatchGuard Points, or WatchGuard pay-as-you-go, which is unique in the traditional capital-expenditure-based firewall appliance market. Flexible pricing is tantamount to flexible licensing, take care to understand where the buyers budget is coming from (CapEx vs OpEx) and price accordingly	**No Microsoft 365 Security** → Cloud solutions like Microsoft 365 and Google Workspace are very popular for customers and unfortunately, for hackers too. WG does not offer any security solutions to protect MS 365 email, OneDrive, and SharePoint. Email remains a very popular vector for cyber-attacks and must be considered when servicing cybersecurity solutions.

WHY SONICWALL®

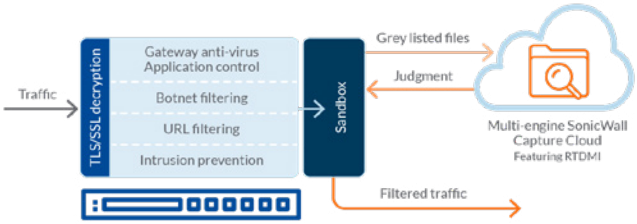
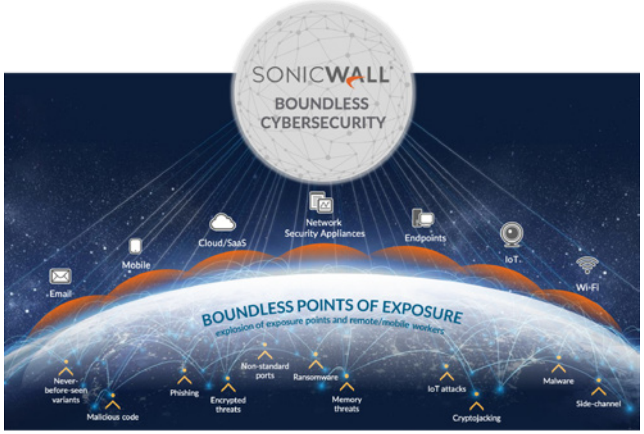
Trust and Reliability: Your clients depend on you to manage their day-to-day business operations. As a partnered vendor, SonicWall is 100% dedicated to your success for over 30 years

World-Class Support: When things go a little wrong, and they often do, remain confident with a dedicated and prompt support team. SonicWall call wait times are consistently below 3 minutes with agent satisfaction scores at 93%

Simplified Management and Visibility: Intuitive management interfaces and centralized management platforms streamlines the administration and monitoring of your network security. Save time, reduce complexity, and proactively respond to security incidents

WatchGuard®

SMB Firewall Battlecard

SonicWall Strengths	What it Means	How to Win
The multi-engine sandboxing solution is faster and more effective at finding and preventing threats  Traffic TLS/SSL decryption Gateway anti-virus Application control Botnet filtering URL filtering Intrusion prevention Sandbox Grey listed files Judgment Multi-engine SonicWall Capture Cloud Featuring RTDMI Filtered traffic	SonicWall next-gen firewalls have Capture ATP, an innovative patented sandbox with ***"Block until verdict"*** capability: ✓ Malicious files are prevented from entering the network until they have been analyzed in the cloud and a verdict returned ✓ GAV includes a large cloud DB of AV signatures for greater zero-day protection ✓ Unknown/unseen files are sent to multiple engines, rendering verdicts quickly	**Ask:** ? Does ATP Blocker limit file size for both GAV as well as sandboxing? (yes, limit = 10MB for both GAV and sandboxing – we limit for sandboxing but NOT for AV) ? Does ATP Blocker use multiple scanning engines? (Don't confuse this with WG IntelligentAV which has 2 scan engines) ? For proxies other than SMTP or IMAP, is the connection allowed? (yes, WG will retroactively alarm) ? Are you aware that you must purchase the top-tier security service from WG to enable sandboxing? (must have "Total Security" – SonicWall only requires Essential for this feature)
A full portfolio of Cybersecurity Solutions - leverage global threat intelligence, seamless real-time protection, and industry-leading TCO to offer scalable security for any business size  SONICWALL BOUNDLESS CYBERSECURITY Email Mobile Cloud/SaaS Network Security Appliances Endpoints IoT Wi-Fi BOUNDLESS POINTS OF EXPOSURE explosion of exposure points and remote/mobile workers Never-before-seen variants Malicious code Phishing Encrypted threats Non-standard ports Ransomware Memory threats IoT attacks Cryptojacking Malware Side-channel	In addition to SonicWall physical and virtual NGFWs, is an extensive portfolio of cybersecurity solutions that when combined, provide a robust multi-layered cybersecurity posture: ✓ Reduce TCO by taking advantage of more secure and cost-effective connectivity between primary locations and distributed branches with a combination of SD-LAN and SD-WAN solutions ✓ Trim costs and protect inboxes with hosted email security designed to find and block phishing attempts, malware, ransomware, malicious URLs, and more ✓ Quickly scale VPN security (physical or virtual) for secure remote access to corporate resources hosted on-premises, in the cloud, and in hybrid datacenters ✓ Control and protect network access to both managed and unmanaged devices based on identity, location, and device parameters with Zero-Trust security	**Ask:** ? Does WatchGuard feature a single-pane-of-glass cloud management system for analytics and real-time threat intelligence for your entire portfolio of network, email, endpoint, mobile, and cloud security resources? (we do – it's called Capture Security Center) ? How user-friendly is the management interface, and what level of control does it provide? ? When is this solution coming to End of Life? (EOL) ? What are your plans for mitigating phishing attacks in your email client? ? How does WG handle emerging threats and zero-day attacks? ? Please clearly articulate the scope of protection provided by WG – do they align with your organization's specific security needs and compliance requirements? ? What Zero-Trust cloud-native 100% SaaS based solutions are available? (none from WG – we have Cloud Edge)