In fourth quarter 2024 Miercom conducted an independent industry wide study on Cloud NGFW products. Palo Alto Networks submitted their Cloud Next Generation Firewall for evaluation.

This report is a synopsis of Palo Alto Networks' Cloud NGFW capabilities compared to native firewall offerings from leading cloud providers. This independent assessment focused on the firewall's capabilities to detect and respond to critical, high and medium vulnerabilities (NIST CVSS).

The comprehensive published industry wide study on Cloud NGFW solutions is available at miercom.com.
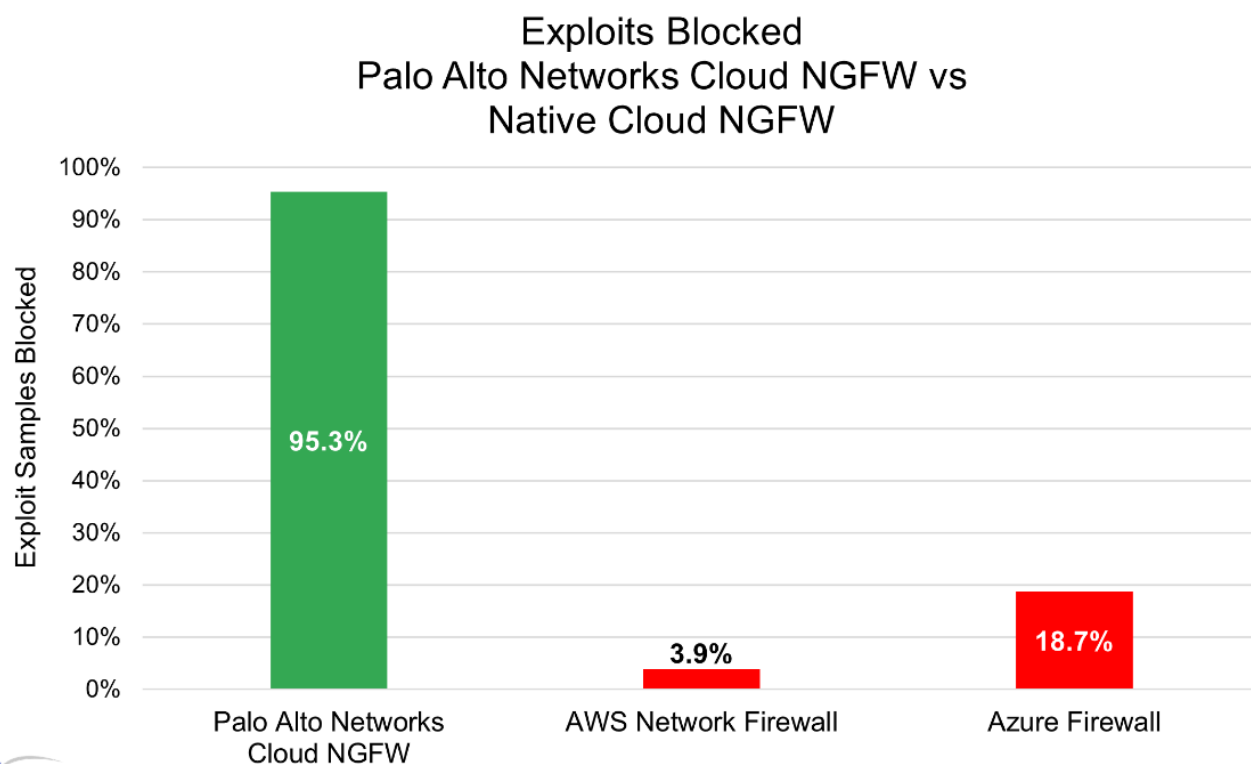
The Miercom Market Impact Analysis™ Grid shown to the right shows overall security efficacy ratings by products reviewed on the vertical (y-axis) compared to the User Experience (x-axis) for the overall effectiveness for deploying and piloting the solution.

Cloud NGFW Vendors Market Impact Analysis™

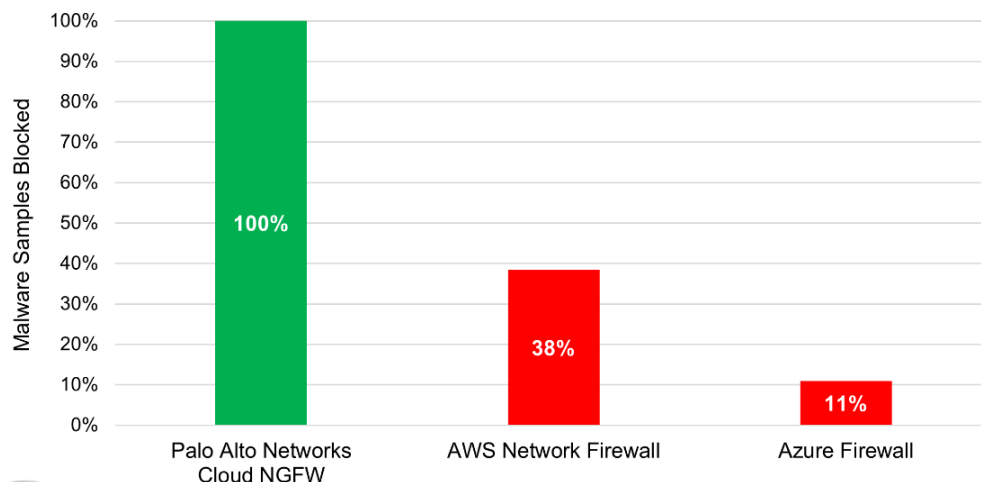Miercom Cloud NGFW Security Benchmark™ 2025
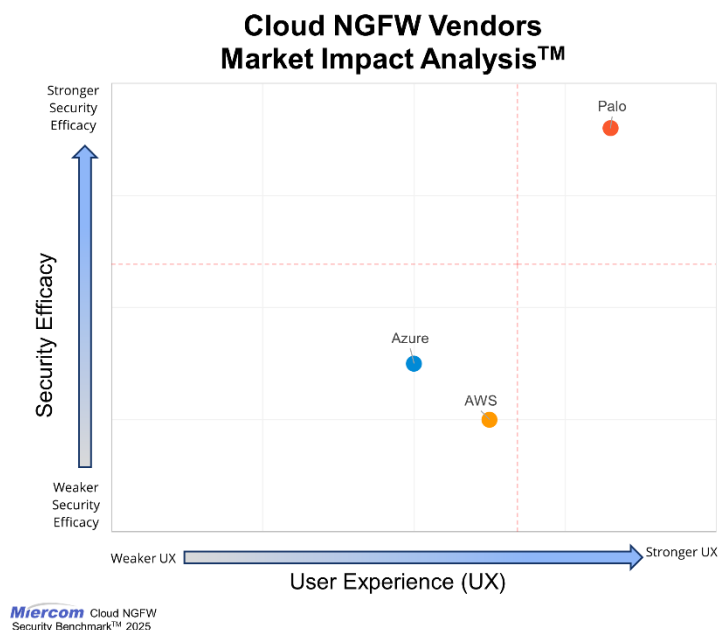
Vulnerability Assessment

The chart below shows the effectiveness of Palo Alto Networks Cloud NGFW, AWS Network Firewall, and Azure Firewall in blocking CVSS vulnerability exploits—critical, high and medium.

Palo Alto Cloud NGFW demonstrates the highest average blocking rate at 95.5%, across all categories, significantly outperforming AWS Network Firewall's 3.9% and Azure Firewall's 18.7%.

**Exploits Blocked
Palo Alto Networks Cloud NGFW vs
Native Cloud NGFW**

	Palo Alto Networks Cloud NGFW	AWS Network Firewall	Azure Firewall
Exploit Samples Blocked	95.3%	3.9%	18.7%

Miercom Cloud NGFW Security Benchmark™ 2025

Malware Protection

Malware Samples Blocked
Palo Alto Networks Cloud NGFW vs Native Cloud NGFW

Malware Samples Blocked

- Palo Alto Networks Cloud NGFW: **100%**
- AWS Network Firewall: **38%**
- Azure Firewall: **11%**

Miercom Cloud NGFW
Security Benchmark™ 2025

The chart on the left shows the effectiveness of malware blocking by Palo Alto Networks Cloud NGFW, AWS Network Firewall, and Azure Firewall across different threat levels: critical high, medium, and low.
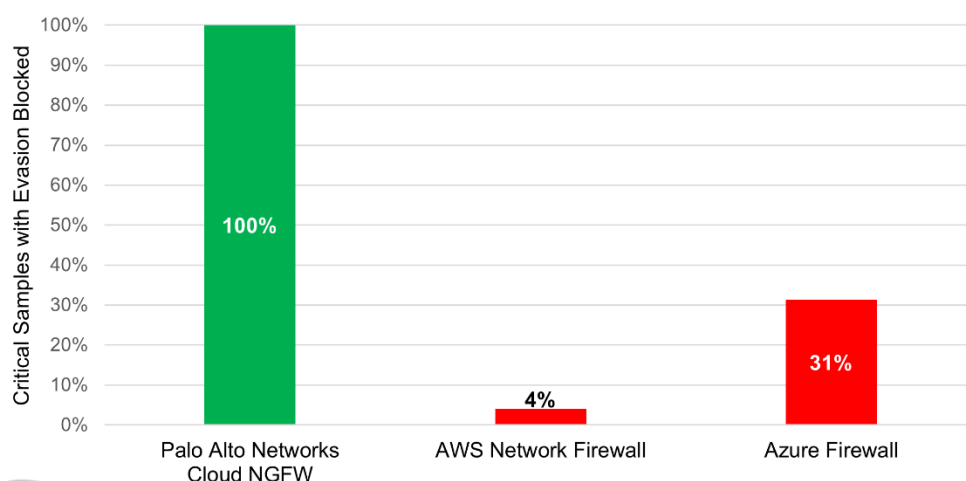
Palo Alto Networks Cloud NGFW demonstrates 100% block rate across all categories. AWS Network Firewall's 38% and Azure Firewall's 11% block rate exhibits lower performance in detecting and blocking malware.

Evasion Protection

The chart on the right show the effectiveness of blocking critical exploits with evasion techniques. These malware samples employ environment awareness, time-based methods, user interaction, domain, IP identification and Internet Connection, Stegosploit, and code obfuscation, encryption or compression.

Palo Alto Networks Cloud NGFW blocked 100% of evasive exploits while AWS Network Firewall's 4% and Azure Firewall's 31% block rate were notably lower.

Critical Exploits with Evasion
Palo Alto Networks Cloud NGFW vs Native Cloud NGFW

Critical Samples with Evasion Blocked

- Palo Alto Networks Cloud NGFW: **100%**
- AWS Network Firewall: **4%**
- Azure Firewall: **31%**

Miercom Cloud NGFW
Security Benchmark™ 2025

Based on our findings, the Palo Alto Networks Cloud NGFW was validated for its protection against critical, high and medium exploits or strikes (NIST CVSS), ability to detect and block evasive malware, and its superior User Interface Experience earning the **Miercom Certified Secure** certification.

miercom.com/paloaltonetworks