Why are NGFWs Needed in the Public Cloud?

Risk	How Does NGFW Address This Risk?
Outbound Connections When HTTP(s) connections are allowed, customers are at risk of misuse with acts such as crypto-mining, command-and-control and data exfiltration	NGFW applies inline deep learning to stop advanced web-based attacks, while securing your apps as they connect to legitimate web-based services
Unknown and Unpatched Vulnerabilities Unknown and unpatched vulnerabilities (such as log4j) are regularly exploited by attackers before security patches are applied	NGFW blocks exploit attempts, evasive techniques and unknown command-and-control, thwarting attackers while you work on patching
Lateral Movement Threats already inside your cloud environment may stay hidden and then move laterally to get access to sensitive data and applications	NGFW blocks known and unknown threats, whether they are attempting to break in or attempting to move laterally

paloalto®
NETWORKS