Spot security

- **Continuously assesses cloud security posture:** It analyzes your public cloud environments (AWS, Azure, GCP) to find misconfigurations, exposed services, overly permissive policies, and other risks.netapp+2
- **Monitors and detects threats:** It provides continuous monitoring and threat detection to identify anomalous behavior, risky changes, and compliance issues, then prioritizes actions to reduce your attack surface.netapp+2
- **Improves compliance and governance:** Spot Security aligns with frameworks like NIST CSF and helps SecOps/CloudOps teams validate that configurations meet security and compliance requirements.netapp+1

—----------

In short, Spot Security is NetApp's **agentless, SaaS-based cloud security and posture management tool**, complementing storage-level protections like SnapLock and ARP by focusing on the configuration and security of your cloud resources.netapp+2

ONTAP One

- A comprehensive license bundle that turns on multiple ONTAP features, including **Autonomous Ransomware Protection (ARP/ARP-AI)** and other cyber-resilience capabilities.netapp+2
- ARP/ARP-AI provides **on-box, AI-driven, real-time ransomware detection and automatic snapshot creation**, and it explicitly requires ONTAP One.netapp+2

SnapLock

- Licensed ONTAP feature that provides **WORM/immutable snapshots and volumes**, forming tamper-proof recovery points against ransomware.netapp+1
- Often called out together with ARP in NetApp's ransomware guidance as a core data-security building block.netapp+2

Spot Security

- A **Spot by NetApp SaaS** that delivers **cloud security posture management and threat detection** for public cloud accounts (CSPM/CNAPP-style).netapp+2
- It absolutely helps **reduce ransomware risk in cloud workloads** by finding misconfigurations, exposed services, and suspicious behavior, but it operates at the **cloud account / workload level**, not directly on ONTAP arrays.