NAND RESEARCH

RESEARCH NOTE

NETAPP AUTONOMOUS RANSOMWARE PROTECTION

STEVE MCDOWELL, CHIEF ANALYST
MARCH 12, 2024

CONTEXT

NetApp recently announced enhanced cyber-resiliency capabilities to help customers better protect against and recover from ransomware attacks. Integrating AI and ML into its enterprise primary storage solutions, NetApp offers real-time ransomware protection for both primary and secondary data, irrespective of whether it's stored on-premises or in the cloud.

ONTAP AUTONOMOUS RANSOMWARE PROTECTION

NetApp's ONTAP Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) aims for over 99% precision in detecting sophisticated cyber threats by analyzing file-level signals in real-time.

Here are some of the key features and benefits that ONTAP ARP/AI. provides:

1. **Real-time Detection and Mitigation**
    - **AI/ML Integration**: By leveraging adaptive AI and ML models within the enterprise primary storage, ONTAP ARP/AI scrutinizes file-level activities in real time. This allows for the immediate detection of unusual patterns or signals that may indicate a ransomware attack.
    - **High Precision and Recall**: The system is designed to achieve a detection precision and recall rate of over 99%. This high level of accuracy ensures that legitimate operations are not hindered by false positives, while effectively identifying and mitigating genuine threats.
2. **Advanced Ransomware Protection**
    - **Autonomous Response**: Unlike traditional systems that may require human intervention, ONTAP ARP/AI autonomously responds to detected

threats, significantly reducing the window of opportunity for ransomware to cause damage.

- **Continuous Evolution**: The AI/ML models used in ONTAP ARP/AI are continuously learning and evolving, improving their ability to detect new and sophisticated ransomware variants over time.

3. **Seamless Integration and Ease of Use**

- **Integration with Existing Infrastructure**: The new capability is designed to integrate seamlessly with NetApp's existing storage solutions, offering customers an easy upgrade path to enhanced security without requiring significant changes to their IT infrastructure.

- **Simplified Management**: ONTAP ARP/AI simplifies the complexity associated with managing ransomware protection strategies. It offers an intuitive interface and automated processes, reducing the operational burden on IT and security teams.

4. **Proactive Protection**

- **Future-Ready Defense**: By focusing on the detection of ransomware attacks in real-time and directly at the storage level, NetApp positions organizations to proactively defend against emerging threats, rather than reacting to them after the fact.

5. **Technology Preview and Availability**

- NetApp announced that it would be offering the first technology preview of ONTAP ARP/AI within the next quarter, signaling its commitment to rapidly bringing advanced ransomware protection capabilities to the market.

ANALYSIS

Storage systems are engineered to move data efficiently and consistently, all while performing a range of computationally expensive real-time operations like compression and encryption. Introducing sophisticated inspection of in-flight data without disrupting the system's performance is a complex engineering challenge.

NetApp's announcement was preempted by IBM just a week earlier, with NetApp's competitor announcing real-time malware detection with goals similar to NetApp's new solution. IBM solved the challenge of real-time malware detection by moving much of the compute into its custom flash drives, essentially offloading the problem from the system's controllers. NetApp's architecture doesn't allow that flexibility, so it had to get clever.

NetApp's ARP solution implements the detection using its existing controllers with minimal disruption to the system’s overall performance. NetApp has been shy in

sharing the underlying technical details, so we don't know exactly how it's implemented. However, we know that layering in-line real-time malware detection into the data path while not adding additional compute capacity to the controllers is a notable engineering feat.

Embedding malware detection into the data path allows organizations to intercept threats before manifesting into full-blown attacks. This is an approach that makes sense. It's also a complex problem to solve, which will doubtless vex NetApp's competitors as customers increasingly ask for this level of data protection. Its Autonoous Ransomware Detection is a significant differentiator for NetApp.

NetApp's new ransomware protection is more than just a product update; it's a strategic pivot that acknowledges the shifting battleground of cybersecurity. The new capability extends NetApp’s reach into the forefront of a new wave of integrated, intelligent cyber defense technologies. This is a challenging role for any storage vendor, but it is one NetApp is comfortable taking on.