HPE Introduces Aruba NDR

MICHAEL MCDOWELL, PRINCIPAL ANALYST
9/9/24

CONTEXT

HPE Aruba has expanded its enterprise security portfolio by introducing a new Network Detection and Response (NDR) platform. The solution integrates AI-driven behavioral analytics to enhance threat detection, particularly focusing on the growing security challenges posed by IoT devices.

The new platform is embedded within HPE Aruba Networking Central, the company's flagship cloud-based network management system, and it leverages telemetry data from a comprehensive data lake to identify and respond to anomalies in network traffic and device behavior.

BACKGROUND: WHAT IS NDR?

Network Detection and Response (NDR) refers to a cybersecurity technology designed to monitor, detect, and respond to threats within a network environment.

Unlike traditional security systems that focus on perimeter defenses or endpoint protection, NDR provides continuous monitoring of internal network traffic, identifying suspicious behaviors and anomalies that may indicate security threats.

Key Characteristics of NDR:

1. **Behavioral Analytics:** NDR platforms use advanced analytics, often powered by AI and machine learning, to establish a baseline of normal network behavior. They can then detect deviations from this baseline that may signify a potential security incident, such as unauthorized access, lateral movement of malware, or unusual data exfiltration.
2. **Threat Detection Across Network Layers:** NDR solutions typically analyze traffic at various layers of the network stack, from the application layer to the transport layer, providing comprehensive visibility into the internal network.

3. **Real-Time Response:** Once a threat is detected, NDR platforms can automate responses, such as isolating affected devices, blocking malicious traffic, or alerting security teams for further investigation.

4. **Integration with Other Security Tools:** NDR solutions typically integrate with various other security technologies, such as Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) tools, and firewalls, to provide a near holistic security posture.

5. **Focus on Network Traffic:** Unlike EDR, which focuses on endpoints, NDR concentrates on data flows across the network, making it particularly useful for detecting threats that bypass endpoint protections or originate within the network.

NDR is especially effective in environments with extensive IoT devices, complex internal networks, or where traditional security measures might struggle to detect sophisticated threats like advanced persistent threats (APTs) or insider attacks.

HPE ARUBA NDR

As enterprise threats rapidly escalate, security teams seek AI-driven solutions for fast, robust, and effective security management. Maintaining its status as a world-class leader in networking, HPE Aruba's NDR solution includes all essential components of standard NDR platforms.

What sets HPE's solution apart is its seamless integration with existing infrastructure, requiring no new hardware, and an interface (Aruba Central) familiar to existing Aruba customers.

KEY FEATURES AND CAPABILITIES:

1. **AI-Driven Behavioral Analytics:**
   - The NDR platform uses AI and machine learning to analyze traffic patterns and dynamic attributes of networked devices. By detecting behavioral anomalies, the platform can identify potential security threats that traditional security measures might overlook, especially in IoT devices that are often outside the direct control of, and unfamiliar to security teams.
2. **Focus on IoT Devices:**

  - Given the increasing ubiquity and vulnerability of IoT devices in enterprise environments, HPE Aruba has prioritized IoT security within its NDR solution. The platform continuously monitors the behavior of these devices, identifying unusual activities that could indicate a compromise.

3. **Seamless Integration with Existing Infrastructure:**
   - One of the significant advantages of this NDR solution is its native integration with HPE Aruba Networking Central. This eliminates the need for additional hardware, simplifying deployment and reducing costs while enhancing security across wired, wireless, and data center environments.
4. **Zero-Trust Controls:**
   - HPE Aruba has also extended zero-trust security policies to its edge LAN environments, ensuring consistent security enforcement across both cloud and on-premises networks. This development is a step toward creating a universal Zero Trust Network Access (ZTNA) framework, which aims to provide unified access control and security from a single console across all network users, devices, and workloads.
5. **Enhanced Visibility and Policy Management:**
   - The NDR platform not only detects potential threats but also provides actionable insights for policy adjustments that are based on actual enterprise data flows. To ensure minimal disruption to production environments, the platform allows for pre-deployment modeling. This proactive approach allows organizations to mitigate risks by enforcing strict access controls and responding swiftly to identified threats.

MARKET CONTEXT AND COMPETITIVE LANDSCAPE:

The introduction of this NDR platform comes at a time when cybersecurity threats are increasingly targeting operational technology (OT) and IoT systems. Competitors like Fortinet have reported significant increases in cyberattacks on OT systems, emphasizing the growing need for advanced security solutions like HPE Aruba's NDR.

The platform's ability to integrate AI-driven analytics without requiring new appliances positions it as a compelling option for enterprises looking to bolster their security posture without incurring substantial additional costs.

ANALYSIS

As organizations increasingly contend with sophisticated cyber threats, particularly those targeting IoT and operational technology (OT) environments, the need for advanced detection and response mechanisms has never been more critical. HPE Aruba's NDR solution addresses these challenges head-on by leveraging AI-driven behavioral analytics to detect and respond to anomalous network activity.

Advanced detection techniques are essential to a true zero-trust security model. HPE Aruba’s NDR solution is quick to deploy, offering a strong foundation for enterprise customers starting their zero-trust implementation.

HPE Aruba strategically positions its NDR platform to address a critical gap in enterprise security: detecting threats within the network itself, rather than just at the perimeter or endpoint. The focus on internal network traffic is essential, as many cyberattacks, particularly advanced persistent threats (APTs), often evade traditional security measures. IoT is a significant vulnerability for conventional security models, which HPE Aruba’s NDR platform effectively mitigates with minimal involvement from network engineers.

By embedding AI and machine learning directly into its cloud-based Networking Central platform, HPE Aruba enables organizations to monitor and secure enterprise networks without the need to deploy specialized hardware. Utilizing existing infrastructure can significantly reduce the time and cost required to deploy HPE’s NDR capabilities. This integration is especially beneficial for enterprises aiming to streamline their security infrastructure and minimize operational complexity.

The new capabilities strengthen HPE Aruba's security offerings while also aligning with broader industry trends toward AI-powered threat detection and response, making it a key player in the competitive cybersecurity landscape.

Aruba's focus on AI-driven analytics and zero-trust principles positions it well against competitors like Fortinet, which has also highlighted the growing threat landscape in OT and IoT environments. With cyberattacks on OT systems rising sharply, as evidenced by Fortinet's own reports, Aruba's timely introduction of its new NDR solution should capture significant interest from organizations looking to enhance their defenses against such threats.

HPE Aruba's new NDR platform is a strong addition to its enterprise security portfolio, offering advanced threat detection capabilities tailored to the challenges posed by IoT devices. Its seamless integration with existing network management systems, combined with AI-driven insights and zero-trust controls, makes it a valuable tool for organizations to enhance their cybersecurity defenses in an increasingly complex threat landscape.

.

The information contained within this document was believed by NAND Research to be reliable and is provided for informational purposes only. The content may contain technical inaccuracies, omissions, or typographical errors. This document reflects the opinions of NAND Research, which is subject to change. NAND Research does not warranty or otherwise guarantee the accuracy of the information contained within.

NAND Research is a technology-focused industry analyst firm providing research, customer content, market and competitive intelligence, and custom deliverables to technology vendors, investors, and end-customer IT organizations.

Contact NAND Research via email at info@nand-research.com or visit our website at nand-research.com.