NAND RESEARCH

RESEARCH NOTE

CROWDSTRIKE FALCON ASPM & CDR UPDATES

STEVE MCDOWELL, CHIEF ANALYST
MAY 7, 2024

CONTEXT

At the 2024 RSA conference, CrowdStrike announced enhancements to its Falcon platform, introducing its new Falcon Application Security Posture Management (ASPM) along with an expansion of its Cloud Detection and Response (CDR) capabilities.

Let's take a deeper look at what was announced.

BACKGROUND: WHAT IS CROWDSTRIKE FALCON?

CrowdStrike Falcon is a cloud-native endpoint protection platform that delivers a range of cybersecurity capabilities to help organizations safeguard their systems, data, and applications from cyber threats.

Here's a closer look at its key components and functionalities:

1. **Endpoint Protection**: Falcon provides advanced endpoint protection using signature-less AI & ML technologies, allowing it to detect and respond to threats in real-time.

2. **Threat Intelligence**: Falcon integrates threat intelligence to deliver proactive defenses against emerging threats. This continuously updates intelligence and provides insights into adversary tactics, techniques, and procedures (TTPs).

3. **Managed Threat Hunting**: Known as Falcon OverWatch, Crowdstrike's service involves 24/7 managed threat hunting, with expert security analysts monitoring networks for signs of threats and intrusions.

4. **Incident Response**: CrowdStrike offers rapid response services to help organizations react to security incidents effectively. This includes forensic

analysis to understand the depth and impact of a breach and assistance in mitigating and recovering from attacks.

5. **IT Hygiene**: The Falcon platform includes tools for basic IT hygiene, such as inventorying applications and managing patches.
6. **Zero Trust Security**: Falcon supports Zero Trust frameworks by continuously verifying the security status of endpoints and the authenticity of users based on real-time assessments to minimize risks and limit access to network resources.
7. **Visibility and Analytics**: The platform offers deep visibility into endpoint and workload activities, enabling security teams to monitor operations across environments and detect anomalies that could indicate security risks.

NEW IN FALCON

CrowdStrike introduced several significant updates to its Falcon SIEM to enhance cloud security. Here's an overview of what's new:

1. **Falcon ASPM**: This new component is integrated into Falcon Cloud Security. ASPM provides deep visibility and incident response capabilities that help secure cloud infrastructure and applications more effectively. This integration brings together essential CNAPP capabilities into a single, cloud-native platform.
2. **Expansion of CDR Capabilities**: CrowdStrike expanded CDR capabilities to include more comprehensive threat hunting and monitoring. The expansion includes:
    - **Protection for Cloud Control Planes**: Beginning with Microsoft Azure, this feature increases visibility into cloud control plane activity, complementing the existing threat-hunting capabilities.
    - **Stopping Cloud Identity Threats**: Its unified platform approach enables enhanced monitoring and prevention of compromised users and credentials in cloud attacks.
    - **Preventing Lateral Movement**: This feature helps track and prevent lateral movement from cloud to endpoint, facilitating rapid response and actionable insights for remediation.
3. **Deep Runtime Visibility**: This feature provides extensive monitoring across runtime environments, allowing quick identification of vulnerabilities across cloud infrastructure, workloads, applications, APIs, GenAI, and data.
4. **Runtime Protection**: Using industry-leading threat intelligence, Falcon Cloud Security now detects and prevents cloud-based threats in real-time.

5. **Industry-Leading MDR and CDR**: CrowdStrike unifies its managed threat hunting with deep visibility across cloud, identity, and endpoints to accelerate detection and response at every stage of a cloud attack.

ANALYSIS

Falcon ASPM and the expansion of its CDR capabilities are significant advancements to its cloud-native cybersecurity portfolio. By consolidating multiple CNAPP capabilities into a single platform, CrowdStrike addresses a critical market need for streamlined security solutions that offer deep visibility while integrating seamlessly with DevOps workflows.

CrowdStrike's expansion of CDR capabilities—encompassing enhanced threat hunting, increased visibility into cloud control plane activities, and advanced measures to prevent lateral movement and cloud identity threats—is a compelling response to the growing complexity and frequency of cloud-based attacks. Its approach improves the ability to detect and respond to threats in real-time and supports the need for a more holistic view across the cloud, identity, and endpoint security landscapes.

These announcements clearly indicate CrowdStrike's strategic intent to lead and reshape the cloud security market. By simplifying and strengthening cloud security frameworks, CrowdStrike is responding to current market demands and anticipating future security challenges, ensuring that businesses can leverage cloud technologies safely and effectively.

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.