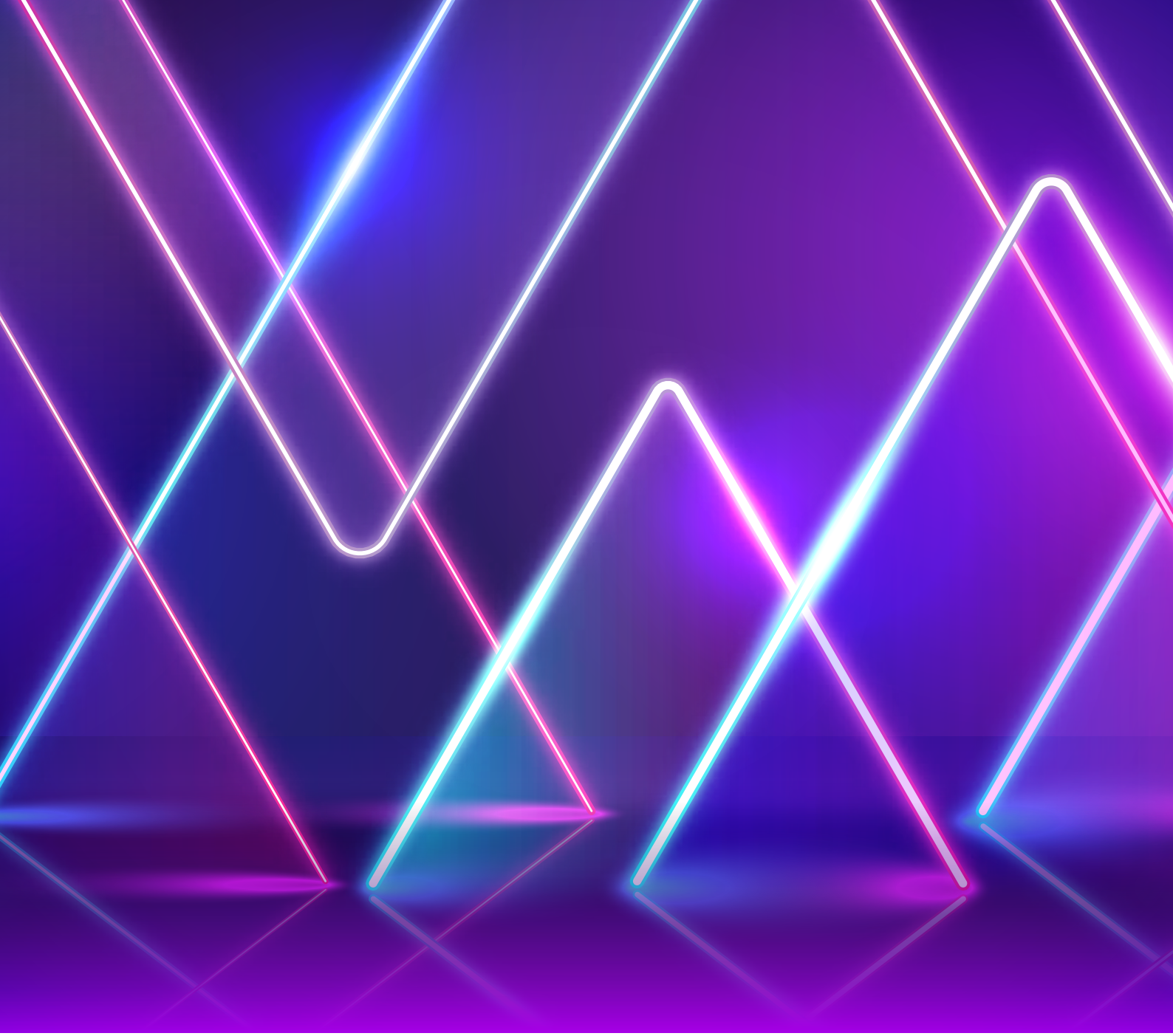


Solution Brief:

AirMDR Cloud Detection and Response (CDR)

Early and Precise Threat Detection for Multi-Cloud Environments Using Scalable, AI-Powered Detection and Response

AIRMDR

Overview

As organizations increasingly adopt multi-cloud strategies, securing cloud infrastructures becomes more complex and resource-intensive. Traditional cloud security tools often fall short in providing the real-time visibility and proactive defense that today's businesses need. This is where AirMDR steps in, delivering next-generation Managed Detection and Response (MDR) services specifically tailored for multi-cloud environments.

AirMDR empowers organizations to confidently embrace the cloud by offering AI-powered security that detects, investigates, and remediates threats across AWS, Azure, and Google Cloud platforms. Leveraging AI-driven virtual analysts, AirMDR automates over 80% of routine security tasks while providing deep insights into cloud activities. This ensures advanced protection with minimal human oversight and allows teams to focus on strategic initiatives.

Key Benefits

AI-Powered Threat Intelligence and Automation

Continuous detection and response with automated triage and virtual analysts that handle 80% of repetitive tasks, freeing human analysts for complex issues.

Comprehensive Cloud Coverage

Over 240 built-in integrations for multi-cloud environments, enabling seamless monitoring and defense across AWS, Azure, and Google Cloud.

50% Lower Costs

AirMDR services are significantly more affordable than traditional MDR solutions, with the added benefit of 24/7 coverage.

Faster Incident Response

90% of investigations are completed in under 5 minutes, ensuring swift threat containment and reduced dwell time.

Cloud-Specific Challenges & How AirMDR Solves Them

Cloud Misconfigurations

Misconfigurations, such as open storage buckets or incorrect access controls, are some of the most common and dangerous threats in cloud environments. These errors can lead to data breaches, ransomware attacks, or compliance violations.

AirMDR's Solution

AirMDR uses your tools and its AI technology to continuously scans for cloud misconfigurations and proactively identifies vulnerabilities before they can be exploited. Detailed remediation guidance is provided, helping teams bridge expertise gaps and reducing the risk of breaches due to human error.

Behavioral Anomaly Detection

With a large volume of user activity and data flow across cloud environments, detecting unusual behaviors that indicate a potential breach can be overwhelming for security teams.

AirMDR's Solution

AirMDR uses AI to detect deviations from normal activity patterns. The system correlates user and entity behaviors across cloud platforms, identifying potential threats such as compromised credentials, lateral movement, or data exfiltration. AI triage ensures that only the most relevant threats are escalated for investigation.

Cloud Workload Protection

Cloud workloads, including virtual machines, containers, and serverless functions, are increasingly targeted by attackers looking for weak points in an organization's cloud infrastructure.

AirMDR's Solution

AirMDR delivers continuous protection of cloud workloads, so that any unauthorized changes, unusual deployments, or workload compromise are detected early. This ensures that cloud-native applications remain secure from malicious interference.

Incident Response Expertise & Automation

One of the biggest challenges for cloud security teams is the lack of experienced incident response professionals. With growing threats, responding quickly and effectively to cloud-based incidents is critical.

AirMDR's Solution

AirMDR's AI-powered platform automates over 80% of routine tasks related to incident response, including initial investigation, threat correlation, and triage. This reduces the manual burden on human analysts, who can focus on high-priority incidents that require strategic intervention. The collaboration between AirMDR's AI virtual analysts and human experts ensures that while AI handles routine tasks and initial triage with speed and precision, complex decisions are managed by skilled security professionals. This combination of AI efficiency and human expertise provides organizations with a powerful incident response solution, without requiring an in-house team.

Alert Fatigue and Manual Triage

In cloud environments, security teams are often overwhelmed by a high volume of alerts, many of which lack the context needed to prioritize real threats. This alert fatigue leads to inefficiencies in manual triage, causing delays in addressing critical security incidents.

AirMDR's Solution

AirMDR's AI-driven virtual analysts alleviate alert fatigue by automatically prioritizing and triaging alerts in real-time. By analyzing data across multiple cloud platforms and reducing noise from low-priority events, AirMDR ensures that security teams can focus on addressing the most significant threats, enhancing both efficiency and response times.

Compliance Monitoring and Reporting

As regulatory demands increase, organizations must continuously monitor cloud environments for compliance with industry standards like GDPR, HIPAA, and PCI-DSS. Ensuring compliance is not just about meeting standards, but also maintaining consistent incident response and documentation practices.

AirMDR's Solution

AirMDR provides 24/7/365 compliance monitoring, ensuring continuous oversight and adherence to industry regulations. Our platform automates the detection of misconfigurations that could lead to compliance violations and ensures consistent incident response. Detailed, audit-ready reports are generated automatically, ensuring comprehensive documentation for regulatory audits, which minimizes the risk of fines and simplifies compliance efforts.

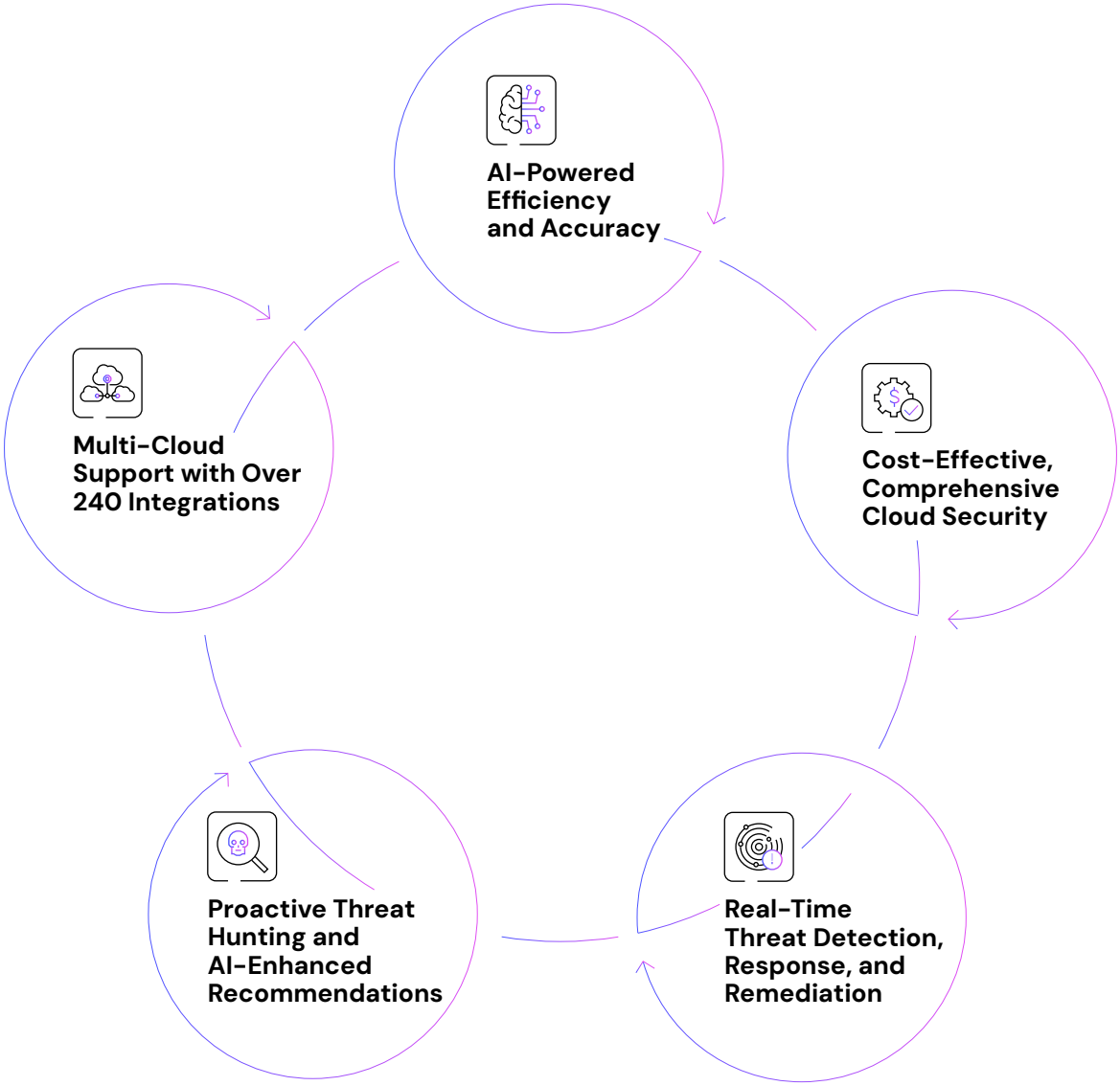
Cyber Insurance Requirements

Obtaining or renewing cyber insurance has become increasingly difficult, with insurers demanding proof of robust cloud security measures. Companies without adequate detection and response capabilities face higher premiums or reduced coverage.

AirMDR's Solution

AirMDR helps businesses meet cyber insurance requirements by providing rapid detection and response capabilities, supported by real-time analytics and reporting. This ensures organizations can demonstrate effective cloud security to insurers, reducing premiums and ensuring comprehensive coverage.

Why AirMDR for Cloud Detection and Response?



AI-Powered Efficiency and Accuracy

AirMDR's AI virtual analysts streamline the detection and response process, reducing investigation times to under 5 minutes. Our automated system provides full context for security events, ensuring accurate triage and eliminating the guesswork that often bogs down traditional security operations. This significantly reduces dwell time, minimizes the risk of attacks escalating, and improves overall accuracy in threat detection and response.

Cost-Effective, Comprehensive Cloud Security

AirMDR provides enterprise-grade security at 50% lower costs than traditional MDR services. With 24/7 continuous monitoring, automated response, and AI virtual analysts managing routine tasks, organizations can maintain a high level of security without the need for large, in-house security teams.

Real-Time Threat Detection, Response, and Remediation

AirMDR combines AI-enhanced threat detection with proactive, automated response capabilities. AI-driven playbooks execute rapid responses to security events, reducing the time it takes to contain and remediate threats. This not only improves response times but also strengthens your overall cloud security posture.

Proactive Threat Hunting and AI-Enhanced Recommendations

With advanced AI-powered playbooks, AirMDR continuously hunts for threats across your cloud environment, identifying malicious activity that may go undetected by traditional security tools. Over time, AirMDR learns from previous incidents and adapts to emerging threats, providing proactive recommendations that help optimize cloud security over time.

Multi-Cloud Support with Over 240 Integrations

From AWS to Azure to Google Cloud, AirMDR provides comprehensive coverage for your entire cloud ecosystem. With over 240 built-in integrations, AirMDR seamlessly works with your existing cloud services to provide unified visibility and defense across all platforms.

Conclusion

Confidently Secure Your Cloud Environment with AirMDR

Managing security across multi-cloud environments is a daunting challenge, but AirMDR's AI-powered approach makes it both manageable and affordable. By automating routine tasks, reducing investigation times, and providing real-time insights, AirMDR empowers your security team to stay ahead of threats. With 24/7 continuous monitoring, compliance support, and advanced threat intelligence, AirMDR is the partner you need to secure your cloud infrastructure effectively.

Contact us today to learn more about how **AirMDR** can elevate your cloud security and protect your business against the next generation of cyber threats.