

SOLUTION BRIEF

Prioritized Risk Insights from Code to Cloud



Modern cloud-native applications rely heavily on open source code—but securing those components across distributed environments is a complex challenge. Traditional SCA tools often surface massive lists of vulnerabilities without context, leaving teams overwhelmed and unsure where to focus. At the same time, cloud security tools can lack visibility into the exploitability of application-layer issues.

Mend.io and Microsoft Defender for Cloud (MDC) deliver a connected solution that bridges the gap between application security and cloud runtime defense—giving security teams the context they need to act fast and fix what matters most.

Smarter, Context-Aware Security

Together, Mend.io and Microsoft Defender for Cloud streamline the identification, prioritization, and remediation of vulnerabilities—linking code-level risk with runtime context in a single view.



Mend.io's Application Security Platform brings deep visibility and risk prioritization across your application attack surface with industry-leading software composition analysis (SCA) and container reachability analysis.



Microsoft Defender for Cloud provides unified cloud-native application protection (CNAPP) across infrastructure, workloads, and runtime environments with advanced threat detection and attack path analysis.

Pinpoint What Matters Most



Exploitability-Driven Prioritization. Use Mend.io's reachability analysis to identify which open source vulnerabilities are actually exploitable—right inside the Defender for Cloud console. Eliminate the noise and focus on the vulnerabilities that pose real threats.



Attack Path Visualization with Context. The integration extends MDC's attack path graph to include reachable open source dependencies and container vulnerabilities, helping teams visualize how vulnerabilities flow from code to container to runtime. This makes it easier to understand impact, verify exploitability, and act faster.



Actionable Insights Across the SDLC and Cloud. Gain end-to-end visibility—from vulnerable packages in your CI pipeline to exposed workloads in Kubernetes pods. Whether you're securing code, infrastructure, or runtime, this integration helps you close the loop faster.



Built for Speed. Get a filtered, focused view of exploitable risks—so you can act on what matters, not everything that might matter.

How It Works

01

The Mend.io integration surfaces a comprehensive list of SCA and container findings directly within the MDC cloud security explorer.

02

The Mend.io integration adds metadata to findings, specifically tagging those that are reachable, to enhance prioritization within MDC.

03

The Mend.io integration extends the MDC attack path graph by displaying reachable findings, providing critical context for threat assessment.

Together, Mend.io and Microsoft Defender for Cloud bring intelligent, contextual security to modern development teams—helping you protect what matters most, from code to cloud.

Visit us online!

→ Mend.io

→ Microsoft Defender

