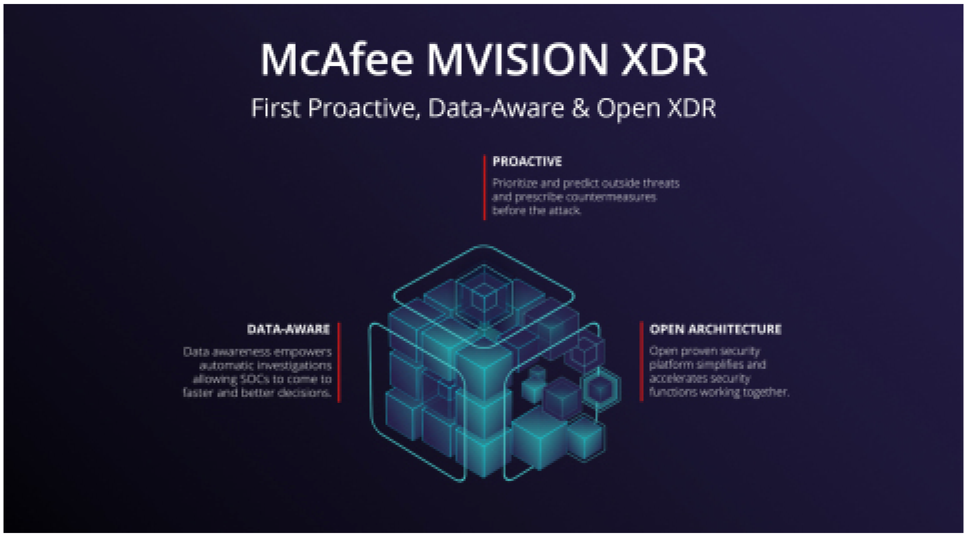
McAfee Breaks Through XDR Market With SASE-Enriched Threat Protection to Proactively Stop Targeted Attacks

May 18, 2021

MVISION XDR automates security investigation and response processes with actionable threat insights harnessed from deeply integrated cloud data sources

SAN JOSE, Calif.--(BUSINESS WIRE)--May 18, 2021-- **RSA CONFERENCE 2021.,** McAfee Corp. (Nasdaq: MCFE), the device to cloud cybersecurity company, today announced significant expansion of its MVISION Extended Detection and Response (XDR) solution by correlating the extensive telemetry of McAfee's endpoint security solution, Secure Access Service Edge (SASE) solution, and threat intelligence solution powered by MVISION Insights. These integrations protect organizations against the most advanced threats while simplifying security operations with unified control and visibility from device to cloud.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20210517005883/en/


McAfee MVISION XDR
First Proactive, Data-Aware & Open XDR
PROACTIVE
Prioritize and predict outside threats and prescribe countermeasures before the attack.
DATA-AWARE
Data awareness empowers automatic investigations allowing SOCs to come to faster and better decisions.
OPEN ARCHITECTURE
Open proven security platform simplifies and accelerates security functions working together.

McAfee MIVISION XDR: First Proactive, Data-Area & Open XDR (Graphic: Business Wire)

This timing is pivotal, as security operation centers (SOC) are dealing with increasingly sophisticated threat actors targeting remote employees and cloud services using more evasive techniques across expanding digital attack surfaces - making adversaries harder to spot with traditional security controls. A recent survey of IT security professionals by The Enterprise Strategy Group found that the cloud poses the biggest gap for most organizations' threat detection and response capabilities. Unsurprisingly, according to Ernst & Young, about six in 10 companies have faced a material or significant incident in the past twelve months, however, only 26 percent of companies say their SOC identified their most significant breach.

McAfee MVISION XDR is the first proactive, data-aware, and open XDR platform designed to help organizations stop these sophisticated, multi-vector attacks with unified threat detection and response that connects and fuses disparate endpoint, network, and cloud data sources. Starting today, XDR incidents are enriched with actionable threat insights from McAfee's SASE solution, which detects cloud threats that occur within web and SaaS environments. It improves situational awareness, drives better and faster decisions, and elevates the SOC to a new level of efficiency and effectiveness.

"SOC processes involve siloed monitoring and detection tools that generate an overwhelming volume of security alerts that often require manual effort to sort through and force analysts to take a reactive posture," said Shishir Singh, chief product officer of McAfee's enterprise business. "AI Guided Investigations serves as the catalyst allowing analysts to more effortlessly orchestrate smart and efficient workflows. MVISION XDR delivers end-to-end threat visibility across all attack surfaces, greater context, and situational awareness using automation to streamline operations so organizations can preempt an attack rather than scramble to contain a breach."

MVISION XDR capabilities include:

- **Advanced threat detection**: Automatically correlates attack telemetry from multiple data sources including endpoint detection and response (EDR), cloud access security broker (CASB), data loss prevention (DLP) and secure web gateway (SWG), and fuses with active threat campaigns to reveal the full picture of an adversary's work across the entire attack lifecycle.
- **Automated threat management tasks**: By combining the latest machine learning techniques with human analysis, MVISION XDR simplifies analyst workflows across complex threat campaigns with AI-guided investigations and MITRE ATT&CK™ mapping to accelerate investigation and move more rapidly to resolution.
- **Proactive threat hunting and optimized response**: The integration of MVISION Insights with MVISION Cloud Security Advisor delivers actionable intelligence to security teams through correlated security posture scoring across all vectors - from endpoints to the cloud – that helps them strengthen security hygiene and advance investigations and analysis with critical context on threat groups.

"MVISION XDR is designed with the SOC experience in mind," said Ariel, Banco Delta (Panama). "It can grant analysts greater control, along with a more comprehensive view of threat context beyond the endpoint – saving time and allowing us to act more deliberately with a better understanding of threats – before they occur or incur damage.”

“Threat detection doesn’t happen in a vacuum. Without weaving together forensic data from endpoint and non-endpoint sources to paint the bigger picture kill chain, it’s incredibly difficult to see attackers traversing your environment and answer the investigative questions that matter to SOC teams,” said Chris Kissel, research director, IDC. “XDR is the next logical step from EDR. McAfee’s XDR has significant potential to achieve what security analytics tools have largely been unable to offer by natively integrating more types of telemetry with threat intel into a single user experience for detection and response.”

The new capabilities in MVISION XDR are available today. Attendees of RSA Conference can register here for McAfee's virtual booth.

Resources:

- McAfee MVISION XDR
- McAfee blog
- What Is Extended Detection and Response (XDR)?

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates consumer and business solutions that make the world a safer place. www.mcafee.com.

McAfee technologies’ features and benefits depend on system configuration and may require enabled hardware, software, or service activation. No computer system can be absolutely secure. McAfee® and the McAfee logo are trademarks of McAfee, LLC or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others.

View source version on businesswire.com: https://www.businesswire.com/news/home/20210517005883/en/

Tracy Holden
media@mcafee.com

Source: McAfee Corp.