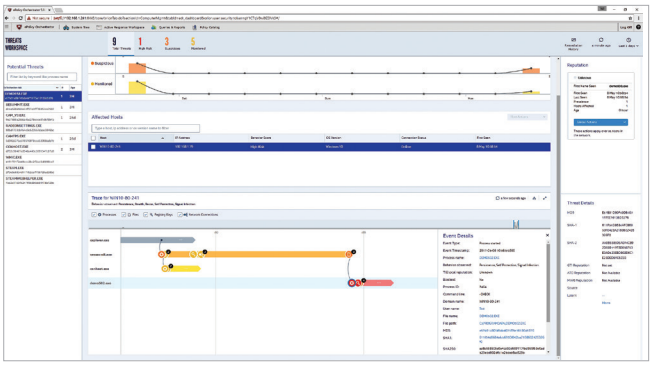

McAfee
Endpoint Security

McAfee delivered a fully configured virtual test environment installed on an Intel Next Unit of Computing (NUC) system.

After connecting the NUC device to a keyboard, mouse and monitor, we were ready to complete the installation of the virtual files needed to establish five endpoint machines and two virtual (host) servers, as well as access to the internet.

Our test package included McAfee Endpoint Security (ENS), Data Loss Prevention (DLP), McAfee Active Response (MAR) Server, Threat Intelligence Exchange (TIE) Server, and Data Exchange Layer (DXL). While these components can be purchased separately, we found that this product package offers layered endpoint security and ease of real-time monitoring and management across the enterprise using McAfee ePolicy Orchestrator (ePO).

McAfee ePO is where the action is for managing endpoint security. The user interface is clean, well-organized and easy to understand. Its menu provides a comprehensive, though not complicated, layout which serves as an excellent roadmap to all of the functional product areas, such as policy management, user management, systems, software, configuration, automation, common catalog, data protection and reporting.

We walked around the system for a few minutes exploring some of the product documentation and then launched into our evaluation with several data exfiltration and malware attacks on targeted endpoints. To determine the impact of these attacks we opted to view the "Active Response Workspace," found in McAfee ePO, which displays a visual timeline for total, high risk, suspicious, and monitored threats, including information related to affected hosts and trace details.

The exfiltration attacks used a cut/paste approach to remove folders and files from one machine to another. Although not blocked (based on our policy), these attacks were detected in real time, and displayed in the monitored threats category, described as "Data Stolen" events. We also found detailed trace information for each of the targeted endpoints, conveying where the exfiltration process started, the file command line data, reputation and IOC (Indicator of Comprise) data, as well as file creation events.

The help portal is another valuable resource to quickly reference additional details about McAfee products in the package – what they do, how they work, etc. – including examples and connectivity diagrams. We visited this area a few times and quickly found exactly what we were looking for by using the index and search options.

– Judy Traub, program project manager, SC Lab

DETAILS

Vendor McAfee

Price Dynamic Endpoint: $68 (perpetual license with one-year support); Dynamic Endpoint: $41 (subscription license with one-year support).

Contact mcafee.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Solid performance, straightforward operation and tight integration.

Weaknesses None that we found.

Verdict Overall, an excellent product, but you'll get the most out of it as part of the entire McAfee suite managed by ePolicy Orchestrator. For its comprehensive feature set and excellent performance and support, we make this our Best Buy.

McAfee LLC
2821 Mission College Boulevard,
Santa Clara, CA 95054,
1.888.847.8766
www.mcafee.com