SOLUTION BRIEF

Check Point and McAfee

Prevent zero-day and command-and-control attacks though intelligence sharing

Organizations often deploy a wide variety of point solutions to protect their critical assets from cyberthreats. While more solutions may seem more secure, independently deployed solutions behaving in silos can increase complexity, add unnecessary costs, and overload IT. This lack of communication among solutions leaves companies susceptible to a variety of zero-day and command-and-control (C&C) attacks. Together, Check Point and McAfee are closing this security gap with simple, bi-directional integration to protect critical assets and users.

McAfee Compatible Solution

Check Point
- NGTX (including SandBlast)
- NGTP (including Anti-Bot)

McAfee
- McAfee ePolicy Orchestrator
- Data Exchange Layer
- McAfee Active Response
- McAfee Enterprise Security Manager

Solution

By unifying endpoint and network security intelligence, the McAfee and Check Point joint solution delivers a simple and automated way to share, detect, and block cyberattacks. Customers can utilize Data Exchange Layer (DXL) as a communication fabric to share high-value information with Check Point's suite of products. Specifically, Check Point Anti-Bot software blade blocks C&C traffic and alerts McAfee® ePolicy Orchestrator® (McAfee ePO™) software, as well as other integrated third-party security solutions over common DXL topics. With this intelligence, McAfee automatically initiates relevant remediation workflow for endpoint devices.

Check Point and McAfee can also detect and prevent zero-day attacks and convert them into known attacks, regardless of whether the attacks are coming from the network or the endpoint. By exchanging mission-critical intelligence in real time, the integration enables our respective products to detect, block, and remediate threats in an automated fashion.

Block C&C Threats

As hackers try to establish a command-and-control channel of communication to export sensitive information to the outside, the Check Point Anti-Bot software blade identifies and blocks this C&C traffic. Check Point instantaneously sends this C&C event to McAfee ePO software, as well as publishes a C&C DXL topic that other McAfee ecosystem partners and customers can leverage. Utilizing this event, McAfee ePO software can initiate a remediation workflow, including quarantine and remediation of infected endpoints via McAfee Active Response, thereby preventing lateral infections within the company's network.

Block Zero-Day Attacks

Cybercriminals are constantly evolving their techniques and using zero-day attacks to bypass traditional security measures. Check Point SandBlast Zero-Day Protection combines CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, zero-day threats, and targeted attacks. Check Point and McAfee can identify and block these unknown attacks coming from the network and endpoints and share these indicators of compromise (IOCa) to better protect and remediate endpoint devices. Check Point SandBlast Threat Emulation events can be published over common DXL topics that can instantly enhance the security posture of all McAfee and third-party solutions connected to the DXL framework.

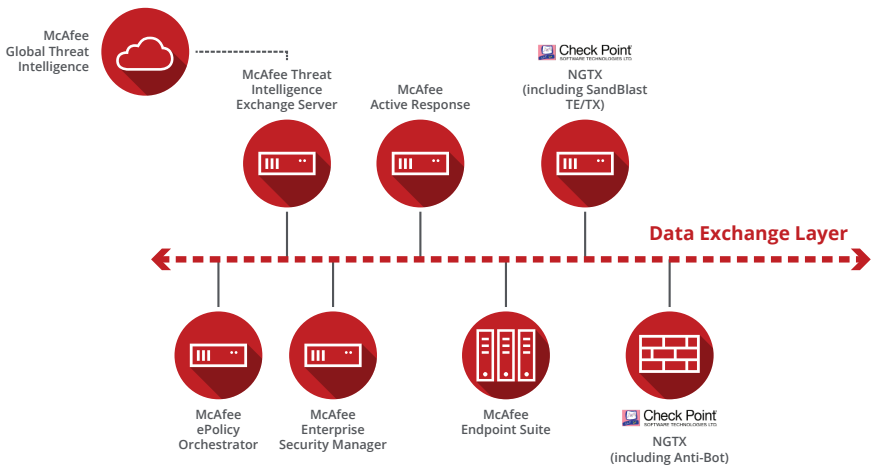

Figure 1. Bi-directional integration of McAfee and Check Point solutions, made possible by DXL.

Key Benefits

- Bi-directional and real-time intelligence sharing.
- Comprehensive visibility.
- Automatic or manual blocking.
- Automated remediation workflow.

Summary

As the complexity and volume of cyberattacks increase and the cost to mitigate downtime and brand damage skyrocket, a common communication framework to share threat intelligence is essential in decreasing time to detect, block, and remediate attacks. This continuous communication between network and endpoint management systems connects security silos and utilizes high-value information to trigger prevention across all products in real time. By providing best-of-breed security solutions, McAfee and Check Point provide an end-to-end threat defense lifecycle solution to strengthen the security posture of any corporation. This ultimately leads to improved performance and efficacy for your business, saving time and money.

About Check Point

Check Point Software Technologies Ltd. is the largest network cybersecurity vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises—from networks to mobile devices—in addition to the most comprehensive and intuitive security management. Check Point protects more than 100,000 organizations of all sizes. **www.checkpoint.com**

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all. **www.mcafee.com**

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com