FAMILY DATA SHEET

McAfee Endpoint Threat Defense and Response Family

Detect zero-day malware, secure patient-zero, and combat advanced attacks

The escalating sophistication of cyberthreats requires a new generation of protection for endpoints. Advancing threats and the increasing risk of unknown vulnerabilities are causing organizations to piece together overlapping, disconnected security solutions that provide limited visibility and increased complexity. McAfee solves this problem with McAfee® Endpoint Threat Defense and McAfee Endpoint Threat Defense and Response. Both solutions leverage static and behavioral analysis and synthesized intelligence to protect, detect, correct, and adapt to combat emerging threats. Unified security components act as one through an open, integrated approach with shared visibility and threat intelligence and simplified workflows. Connected security and actionable threat forensics provide a secure infrastructure to quickly and confidently convict threats and stay ahead of potential attackers.

Defeat Zero-Day Malware, Greyware, and Ransomware

Stay ahead of emerging threats with static and dynamic threat analysis leveraging enhanced reputation and behavioral analytics to detect potential exploits. Apply synthesized intelligence with McAfee Threat Intelligence Exchange to immediately block and contain threats and instantly update threat reputation to prevent future attacks.

McAfee Endpoint Threat Defense and McAfee Endpoint Threat Defense and Response defeat zero-day malware by identifying similarities between exhibited malicious behaviors and the extensive Real Protect threat models using a cloud lookup (data centers hosted in the United States). This behavioral classification technique is used to root out live threats that may have evaded other security software defenses. It provides actionable threat intelligence through McAfee ePolicy Orchestrator

Key Advantages

- Detect, protect, and correct while proactively adapting your defenses against zero-day malware, greyware, and ransomware.
- Protect more effectively using dynamic reputations, behavioral analysis, and machine-learning.
- Minimize impact to users and trusted enterprise applications with enhanced protection.
- Respond and remediate more threats, faster with threat intelligence shared across your security ecosystem.
- Streamline incident investigation and remediation with unified workflows and a single console for management through McAfee® ePolicy Orchestrator® (McAfee ePO™) software.

software to enable zero-day discovery and real-time remediation. Behavioral classification is automatically evolved through dynamic machine-learning, providing maximum protection and efficiency while limiting security exposure.

Reduce the Number of Events and Resolve Threats Faster

Focus on what's most important by reducing the number of security events, automatically convicting more threats, sharing intelligence, and utilizing proactive alerts to define automatic responses. Ease the effort required to investigate and resolve threats with simplified workflows that resolve events faster and expand security capacity while increasing protection across your entire organization.

Connected components automatically share valuable security information through McAfee Data Exchange Layer. McAfee Threat Intelligence allows you to synthesize comprehensive threat intelligence across your entire ecosystem, including McAfee Global Threat Intelligence and other third-party sources, and immediately share threat information to automatically adapt your protection.

Secure Patient-Zero

Detect and stop zero-day malware from making malicious changes to endpoint systems. Dynamic Application Containment watches the behavior of greyware and prevents malicious changes to effectively stop exploits before they begin. Secure endpoints on and off networks and contain malicious behavior with protection that is invisible to users.

Operationalize Security Processes to Scale and Adapt

Policy enforcement, incident investigation, and remediation are streamlined through McAfee ePO software, a single-pane-of-glass management console that provides visibility across all systems so you can readily assess the security posture of endpoints and enable protection in real time. Reduce monitoring, search, and response efforts with unified workflows and single-click remediation across a single endpoint or the entire infrastructure. With McAfee Endpoint Threat Defense and McAfee Endpoint Threat Defense and Response, leverage automated machine-learning to update behavior classification models and instantly share threat intelligence across all security components so they can act as a single, unified system against emerging threats. Prevent future attacks and leverage pre-configured reactions to contain potential threats, so you can free up your staff and allow them to focus on other security management priorities.

Uncover, Prioritize, and Remediate Advanced Attacks

McAfee Endpoint Threat Defense and Response helps you determine the origin, scope, and impact of an attack. It uses McAfee Active Response technology to provide both live and historical visibility across endpoints in your infrastructure. Indicators of attack are identified and prioritized with robust context to enable faster response.

Proactively hunt with precision, speed, and agility to defeat threats that are actively propagating, lying in wait, or have erased their tracks to evade detection. Knowledge-driven visibility and control can pinpoint where threats are attempting to establish a foothold and allow your responders to immediately contain and remediate, reducing exposure from months to minutes or even milliseconds.

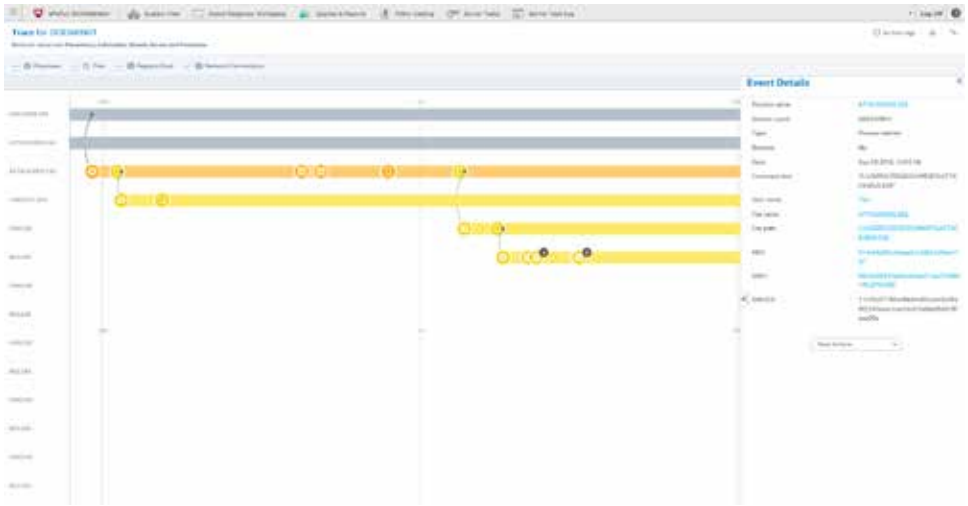

Figure 1. The threat workspace traces the origin and behavior of suspicious incidents to speed incident response.

McAfee Endpoint Threat Defense and Response Family Capabilities

Component	Advantage	Customer Benefits	Differentiation	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Dynamic Application Containment[1]	Secures patient zero by preventing greyware from making malicious changes to endpoints both on or off the network.	▪ Enable potential threat analysis without sacrificing patient zero. ▪ Enhance protection without impacting users or trusted applications ▪ Reduce the time from encounter to contain with minimal manual intervention. ▪ Secure patient zero while maintaining endpoint productivity and isolating the network from infection.	▪ Integrated part of the McAfee infrastructure for optimal protection and efficiency. ▪ Works with or without an internet connection and requires no external input or analysis. ▪ Transparent to the user. ▪ Observe mode provides instant threat visibility to potential exploit behaviors within the environment.	√	√

Component	Advantage	Customer Benefits	Differentiation	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Real Protect	Applies machine-learning behavior classification to block zero-day malware before it executes and stops live threats that evaded previous detection.	▪ Easily defeat more zero-day malware, including difficult-to detect objects, such as ransomware. ▪ Automatically unmask, analyze, and remediate threats without requiring manual intervention. ▪ Adapt defenses using automated classification and a connected security infrastructure.	▪ Static and dynamic behavioral analysis provide better protection than single-stage approaches. ▪ Detects malware that can only be found through dynamic behavioral analysis. ▪ Deep integration shares real-time reputation updates and enhances security efficacy for all security components.	√	√
McAfee Threat Intelligence Exchange	Connects security components to share contextual insights and provide organization-wide visibility and control for adaptive threat protection.	▪ Enable patient-zero threat identification and instant sharing across the security system to prevent the next infection. ▪ Reduce total cost of ownership and efficiently operationalize endpoint security. ▪ Connect security components to create closed-loop protection by transforming independent security technologies into a single coordinated system.	▪ Synthesize McAfee Global Threat Intelligence feeds, third-party, and local intelligence. ▪ Define what is trusted and not trusted with local or third-party intelligence. ▪ Instantly connect threat reputation information across endpoint, web, network, and cloud products. ▪ Extract detailed actionable threat intelligence reports to adapt defenses.	√	√
McAfee Data Exchange Layer	Connects security to integrate and streamline communication with both McAfee and other third-party products.	▪ Reduce risk and response time. ▪ Lower overhead and operational staff costs. ▪ Optimize processes and practical recommendations.	▪ Share threat information across all security products. ▪ Instantly share patient-zero threat insight with all other endpoints to prevent infections and update protection.	√	√
McAfee ePO Management Platform	A single pane of glass for highly scalable, flexible, and automated management of security policies to identify and respond to security issues.	▪ Unify and simplify security workflows for proven efficiencies. ▪ Single-pane visibility across all systems to readily assess security posture and protection in real time. ▪ Quickly deploy and manage McAfee protection with customized policy enforcements. ▪ Reduce the time from insight to response with dynamic automated queries, dashboards, and responses.	▪ Granular control, lower costs, and faster operational security management through a single console. ▪ Drag-and-drop dashboards provide increased real-time visibility across the entire ecosystem. ▪ Open platform software development kits (SDKs) facilitate rapid adoption of future security innovations.	√	√
McAfee Active Response	Proactive threat visibility, timelines, live and historical hunting, and detection, with the ability to take immediate actions and adapt protection.	▪ Quickly search live and historical threat data to determine the full scope of an attack, accelerate investigations, and reduce the time to respond. ▪ Automate threat responses and provide live security protection without manual intervention. ▪ Prioritize high-priority threats. ▪ Use continuous monitoring and customizable collectors to search deeply for indicators of attack that are not only running or lying dormant, but that may have even been deleted.	▪ Instant visibility of unknown exploit attempts and risky behaviors executing in the environment that were not detected by protection technologies. ▪ Investigate timeline of events on each endpoint with integrated live search across all endpoints to hunt for threats. ▪ Single-click action to protect, correct, and adapt, reducing multiple tools and steps into a single operation.		√

Specifications

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Supported Platforms:	**Supported Platforms:**
▪ Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary	▪ Microsoft Windows: 7, 8, 8.1, 10, 10 Anniversary
▪ Mac OSX version 10.5 or Later	▪ RedHat 6.5
▪ Linux: RHEL, SUSE, CentOS,	▪ CentOS 6.5
▪ OEL, Amazon Linux, and Ubuntu latest versions	▪ Windows Server 2008, 2012, 2016
Servers:	
▪ Windows Server (2003 SP2 or greater, 2008 SP2 or greater, 2012), Server 2016	
▪ Windows Embedded (Standard 2009, Point of Service 1.1 SP3 or greater)	
▪ Citrix Xen Guest	
▪ Citrix XenApp 5.0 or greater	

1. McAfee Endpoint Threat Defense and Response includes hosted data centers located in the United States used to validate customer authentication, check file reputations and store data relevant to suspicious file detection and hunting. Although not required, Dynamic Application Containment will perform optimally with a cloud connection. Full McAfee Active Response, Dynamic Application Containment and Real Protect product capabilities require cloud access, active support and are subject to Cloud Service Terms and Conditions.

Learn More

Learn more about the benefits of McAfee Endpoint Threat Defense at **www.mcafee.com/endpointdefense**.

Learn more about the benefits of McAfee Endpoint Threat Defense and Response at **www.mcafee.com/ETDR**.

McAfee
Together is power.

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