McAfee Complete Endpoint Threat Protection

Advanced threat protection for sophisticated attacks

The kinds of threats your organization faces require high visibility and tools that allow you to act and take ownership of the complete threat defense lifecycle. This means arming your security specialists with capabilities that act with greater precision and that offer stronger insights into advanced threats. McAfee® Complete Endpoint Threat Protection provides advanced defenses that investigate, contain, and take action against zero-day threats and sophisticated attacks. Core endpoint protection works with integrated machine learning and dynamic containment to detect zero-day threats in near real time, classifying and halting them before they can infect your systems. Actionable forensic data and reports keep you informed and help you make the move from responding to outbreaks to investigating and hardening your defenses. And, because it is built using an extensible framework, you can add other advanced threat defenses with ease, both today and in the future, as your needs and the threat landscape evolve.

Key Advantages

- Help you stay ahead of zero-day threats, ransomware, and greyware with machine learning and DAC
- Speeds remediation and protect your productivity with automated actions and analysis
- Simplifies your environment, deployment, and ongoing management with centralized management

Automated, Advanced Threat Defenses

You need to stop advanced threats before they start. That's why McAfee Complete Endpoint Threat Protection includes Dynamic Application Containment (DAC) and Real Protect1 technologies. DAC automatically contains greyware and suspicious zero-day threats when malicious behaviors are detected, preventing them from infecting your systems or impacting your users. Using machine learning, Real Protect is able to investigate and classify threats, saving the insights it gains for future actions that can be taken automatically.

Built to Reduce Complexity

Complexity is the enemy of efficiency. Now you don't have to spend time trying to manage multiple point solutions with different interfaces and management consoles. McAfee Complete Endpoint Threat Protection is managed using a single console: McAfee® ePolicy Orchestrator® (McAfee ePO™) software. With this single pane of glass, you're able to more quickly ramp up, speed deployment times, and reduce ongoing management burdens. Customers with multiple operating systems in their environment will be able

to increase their productivity using cross-platform policies for Microsoft Windows, Apple Macintosh, and Linux systems.

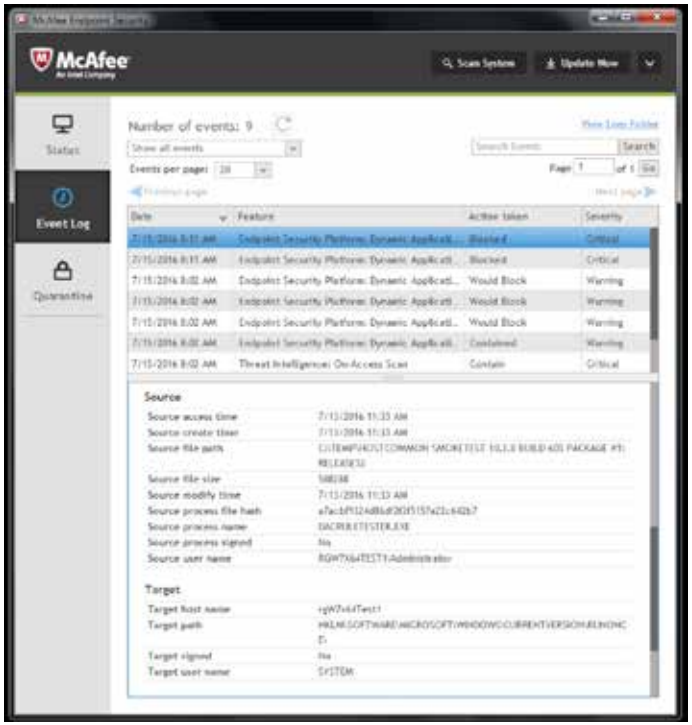

Figure 1. DAC blocks and contains threats according to severity.

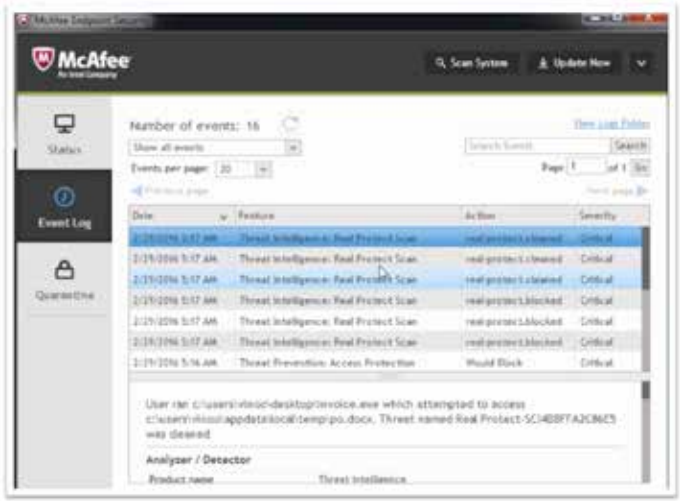

Figure 2. Real Protect uses machine learning to detect in near real time zero-day malware that signature-based scans often miss.

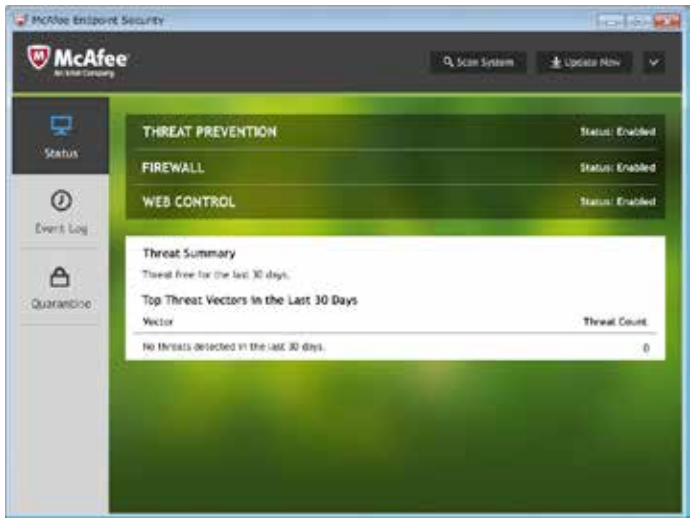

Figure 3. The intuitive user interface keeps things simple for administrators and users.

A Flexible Framework Built for Today and Tomorrow

McAfee Complete Endpoint Threat Protection provides you with a connected, collaborative framework and near real-time protection across multiple protection technologies. This not only allows stronger analysis of threats, it also allows the threat forensic data that is gathered to be shared with other defenses to make them more intelligent. Using a common communication layer, core endpoint protection defenses can inform and consult with advanced threat defenses for stronger insights and convictions from the moment they are first encountered.

Deployment is also more flexible, thanks to this approach, so you can install everything that comes with your purchase today. You can decide on the capabilities that will be configured and active now and then easily activate those you decide to use later with a policy change.

Lastly, our framework lets you expand your protection as your needs change, thanks to an architecture designed to include additional technologies.

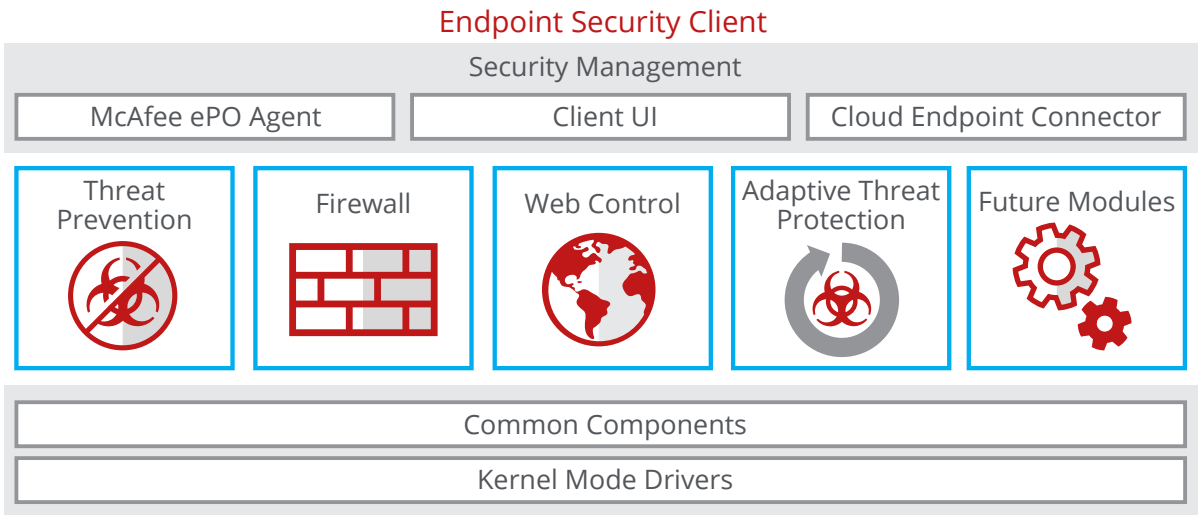

Figure 4. The McAfee endpoint security client framework.

Supported Platforms

- Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OSX version 10.5 or later
- Linux 32 and 64 bit platforms: RHEL, SUSE, CentOS, OEL, Amazon Linux, and Ubuntu latest versions

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

Component	Advantage	Customer Benefits	Differentiation
Dynamic Application Containment	Secures patient zero by preventing greyware from making malicious changes to endpoints	▪ Enhances protection without impacting end users or trusted applications ▪ Reduces the time from encounter to containment with minimal manual intervention ▪ Secures patient zero and isolate the network from infection	▪ Works with or without an internet connection and requires no external input or analysis ▪ Transparent to the user ▪ Observe mode providing instant threat visibility to potential exploit behaviors within the environment
Real Protect	Applies machine-learning behavior classification to block zero-day threats before they execute and stop live execution of threats that evaded previous detection.	▪ Easily defeats more zero-day malware, including difficult-to-detect objects such as ransomware ▪ Automatically unmasks, analyzes, and remediates threats without requiring manual intervention ▪ Adapts defenses using automated classification and a connected security infrastructure	▪ 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.
Threat Prevention	Comprehensive protection that finds, freezes, and fixes malware fast with multiple layers of protection	▪ Stops known and unknown malware using heuristics and behavioral and on-access scanning techniques ▪ Simplifies policies and deployments with protection for desktops and servers across Windows, Macs, and Linux machines ▪ Boosts performance by avoiding scans on trusted processes and prioritizing those appearing suspicious	Multilayered anti-malware that collaborates with web and firewall defenses for stronger analysis and threat prevention.
Integrated Firewall	Protects endpoints from botnets, distributed denial-of-service (DDoS) attacks, untrusted executables, advanced persistent threats, and risky web connections	▪ Protects users and productivity by enforcing your policies ▪ Guards bandwidth by blocking unwanted inbound connections and controlling outbound requests ▪ Equips users by informing them of trusted networks and executables and risky files or connections	Application and location policies that safeguard laptops and desktops, especially when they are not on the corporate network

Component	Advantage	Customer Benefits	Differentiation
Web Control	Ensures safe web browsing with web protection and filtering for endpoints	▪ Reduces risk and guards compliance by warning users before they visit malicious sites ▪ Prevents threats and protects productivity by authorizing or blocking website access ▪ Stops dangerous downloads safely by blocking them before they can be downloaded	Protection across Windows, Mac, and multiple browsers
McAfee Data Exchange Layer	Connects security to integrate and streamline communication with both McAfee and other third-party products	▪ Reduced risk and response time through integration ▪ Lower overhead and operational staff costs ▪ Optimized processes and practical recommendations	Shares the most important threat information between security defenses
McAfee ePO Management	A single pane of glass for highly scalable, flexible, and automated management of security policies to identify and respond to security issues	▪ Unifies and simplifies security workflows for proven efficiencies ▪ Greater visibility and flexibility to take action with confidence ▪ Quickly to deploy and manage a single agent with customizable policy enforcement ▪ Shortens the time from insight to response with intuitive dashboards and report	▪ Greater control, lower costs, and quicker operational security management with a single console ▪ A proven interface that has been widely recognized throughout the industry as superior ▪ Drag-and-drop dashboards across a vast security ecosystem ▪ Open platform that facilitates rapid adoption for security innovations

Learn More

For more information about the benefits of McAfee Complete Endpoint Threat Protection, visit: **www.mcafee.com/CETP**.

1. The solution includes hosted data centers located in the United States used to check file reputations and store data relevant to suspicious file detection. Although not required, DAC will perform optimally with a cloud connection. Full DAC and Real Protect product capabilities require cloud access, active support and are subject to Cloud Service Terms and Conditions.

McAfee™
Together is power.

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