Solution Brief

The Evolving Landscape of Desktop Security

The desktop security landscape has been evolving due to multiple factors, including targeted malware, end-user convenience concerns, and IT support and operations costs. Traditionally, implementing desktop security is akin to buying an insurance policy against possible risks with no significant consideration of any other factors. In the corporate common operating environment (COE) setting, desktop security has resulted in a challenge for IT teams as they have had to balance end user flexibility and security needs.

Desktop Environments

As suggested by various studies there are two different sets of desktop environments:

- *Standard users*—Restricted COE type images, otherwise known as fixed-function, or common image desktops. In these environments, the end user does not have privileges to install or uninstall software.
  Example of COE images: workstations in retail, financial, and hospital scenarios
- *Power users*—Users have ability to install their own software
  Example of power users: engineering and graphic design environments

For the purposes of this discussion, we are going to focus on the COE security model.

Current Desktop Security Challenges

Over the last 20 years, as we have moved towards a knowledge-based economy, the security challenges of maintaining the fidelity of the IT infrastructure have grown dramatically. There has been a massive increase in the number of malware samples enountered by security researchers around the world, from thousands of malware samples in a year to thousands of malware samples per day. On an operational level, endpoint security (desktop/laptops) has grown more complex, and IT security managers frequently report a mix of threat-based and operational security challenges.

Malware explosion

The phenomenal increase of malware in circulation is the topmost concern for security managers. There is a visible increase in complexity and in the number of malware providing multiple vectors of attack on IT infrastructure.

Performance

Secondly, the performance of traditional solutions remains a concern, partially due to the significant increase in the number of malware signatures.

Operational security

Thirdly, a major concern is on the operational aspect of security. When malware traverses through an IT environment, it debilitates the security infrastructure. In addition, traditional signature-based security solutions may not be able to mitigate exposure to zero-day attacks and advanced persistent threats (APTs).

Proliferation of unauthorized applications

Finally, of particular concern is the containment of unauthorized applications that proliferate on end-user desktops. In emerging markets, this also includes preventing pirated and unlicensed software from proliferating in the corporate environment.

Behavioral challenges of security management

On the behavioral side, there is a persistent struggle in COE environments between the administrator's need to enforce security and the end user's need for a flexible and secure environment. Both of these objectives must be met without compromising security or productivity within the organization. A solution needs to address both the administrator's and the user's security requirements without compromising the overarching principle of sustained productivity.

Is Help Available?

With its whitelisting capabilities, McAfee® Application Control coupled with traditional antivirus technology offers a viable solution to many of these problems. McAfee Application Control is a marked improvement over traditional desktop security, offering malware resistance combined with better outbreak management capabilities.

Application whitelisting

The whitelisting approach is fundamentally based on the identification of "known good" files for an IT environment, allowing only "known good" files on the system. Its implementation has many variations: on the one hand, there are stand-alone deployments, and, on the other hand, a whitelisting solution can exist with traditional blacklisting solution such as antivirus. Here we are focusing on an IT environment with antivirus that can be enhanced by incorporating whitelisting technology.

Observation mode

McAfee Application Control offers an operational capability called "observation mode." This mode essentially is non-enforcing, monitoring only versions of McAfee Application Control. Once McAfee Application Control has been installed and has completed an inventory scan, observation mode can be activated. As part of the initial rollout in an organization, this mode can help build policies that aid in the discovery of noncompliance to security standards and identifies valid operational exceptions.

When deployed along with a traditional antivirus tool, observation mode enables antivirus to remain the primary security tool. This helps a security administrator keep monitoring the IT assets while allowing antivirus to take care of the actual security at user endpoints. On the whole, this translates into a productive desktop user with enhanced security insights for IT administrators.

File reputation-enabled with McAfee Global Threat Intelligence™ (McAfee GTI™)

McAfee Application Control also includes McAfee GTI-enabled file reputation capabilities; it can pull the entire file inventory of endpoints to McAfee® ePolicy Orchestrator® (McAfee ePO™) software. This inventory is then verified against file reputation scores received from the McAfee GTI server. This provides an offline and offloaded ability to verify files in the enterprise as malware or otherwise troublesome. If a file is identified as malware, the McAfee ePO interface offers a single pane of glass to quickly find the location of all instances of such malware across the IT environment.

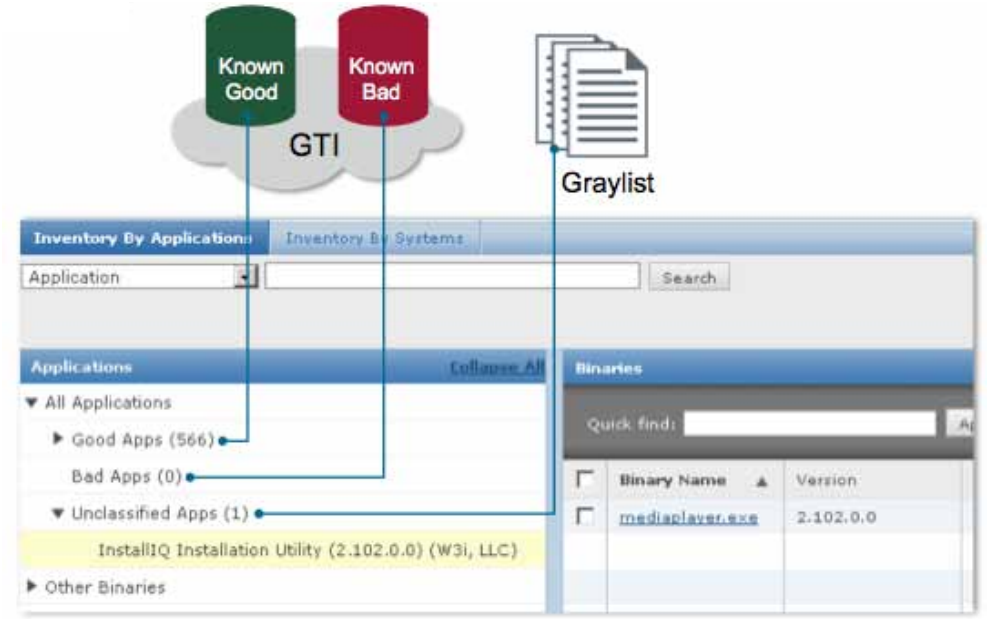

Figure 1. McAfee GTI file reputation categorizes every application in the enterprise.

Malware outbreak resistance

McAfee Application Control's ability to exist in observation mode, with antivirus as the primary security software, provides an unprecedented advantage in resisting malware outbreaks and further allows the administrator to move from observation mode to enforced mode and vice versa as circumstances require. The moment a malware outbreak is suspected, moving McAfee Application Control to enforce mode effectively freezes the system state across the IT infrastructure, preventing malware from traveling deeper into the organization. This, coupled with the ability to manage inventory-based malware detection in McAfee ePO software, enables simplified and timely remediation of infected machines.

User interactivity with dynamic whitelisting

Finally, if McAfee Application Control is deployed in enforced mode and consequently is at a higher level of security, the end user must submit requests to IT to allow changes to his/her machines. This is essentially the dynamic part of the whitelisting, brokered through a well-defined interaction between the user and the administrator. With this functionality, McAfee Application Control is able to offer higher security while managing the user experience at the same level as with a traditional antivirus tool.

Figure 2. Desktop notifications and approval request for non-whitelisted applications.

Managing unauthorized applications

In emerging markets, the security context is also defined with the ability to track down unauthorized, unsecured software in an IT environment. As the inventory is available at the McAfee ePO software level, it is possible to export this inventory and reconcile with a corporate-approved and secured software list. The delta between the corporate-approved software list and the inventory list exported by McAfee ePO software can be used to identify the violation of general security policies and licensing requirements, as the case may be.

Conclusion

Application whitelisting is evolving into a viable primary layer of defense for a certain class of desktop systems. When used in conjunction with existing antivirus solutions, it not only provides a strong defense against emerging threats like APT and targeted malware, it also contributes to reduced operational costs by controlling the sprawl of unauthorized applications. With the extended benefits of application whitelisting and recent technology enhancements that make it easier to implement whitelisting, administrators can look forward to a simpler desktop security model.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

McAfee
An Intel Company

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

41101brf_desktop-security_0112_fnl_ETMG