

Advanced Threat Identification-ATI

Preemptive Defense

Enable preemptive defense on McAfee ePO-managed assets

Allen Corporation's Advanced Threat Identification (ATI) efficiently enforces unauthorized use policies and protects against security threats.

By leveraging the investment organizations have made in McAfee Total Protection for Endpoint, extending the one security agent and centralized management view provided by McAfee's ePolicy Orchestrator (ePO), and utilizing the enforcement features of McAfee Host Intrusion Prevention (HIPS), ATI helps companies protect their critical assets and save time and money.



Business Problem

Reports by the US Secret Service and Carnegie Mellon's CERT estimate that over 70% of successful cyber attacks originate from employees and contractors inside an organization. The applications used by these malicious insiders in their attempts to access business critical systems and information, and the methods used to leak that information often go undetected by the desktop and server protection commonly deployed in the enterprise. And while Data Loss Prevention solutions (DLP) can often detect the existence of sensitive information on a desktop or server, and the transmission of sensitive information out of the enterprise, savvy criminals can use covert channels to both hide the existence of that information at rest and in motion through the use of steganographic techniques.

McAfee + Allen Corporation Solution and Benefits

Allen Corporation and McAfee are partnering to bring ATI and preemptive defense capabilities to McAfee customers. Allen Corporation has been a leader in advanced malware discovery research and technology for over ten years. ATI leverages that research which has resulted in the most comprehensive collection of malware signatures in the industry. These signatures, which target programs and tools used by cyber criminals, represent a robust and complementary extension to the database of threat signatures offered by McAfee. Allen Corporation's malware signature database has been an essential component in its industry-leading forensic malware investigation tool, WetStone Gargoyle Forensic Pro.



Gargoyle, which is used by digital investigators and forensic examiners worldwide, was recognized by SC Magazine as the Best Computer Forensic Product of 2008, and in December 2009 as one of the top twenty security products in the last twenty years.

The integrated McAfee/Allen Corporation ATI solution:

- Preempts dangerous software from running on end points,
- Identifies end-points that are attempting to run unauthorized applications, and
- Classifies unauthorized behavior by threat, category and location.

Advanced Threat Identification provides; an additional layer to the defense in depth strategy, early indication of authorized use violations and potentially harmful actions, allowing security personnel to correct harmful actions quickly and to educate users, provides end-point coverage far beyond typical anti-virus protection, and provides at-a-glance visualization by threat across the enterprise. Advanced Threat Identification is an integrated solution that allows ePO administrators to:

- Generate custom security policies that identify and specify actions to be taken when programs in the following malware categories attempt to execute on ePO managed nodes:

Steganography
Virus and Worm Development Toolkits
Keyloggers
Encryption
Password Crackers
Wireless Tools
Anti-Forensics
Denial of Service
Exploit Scanners
Botnets
Credit Card Fraud
Peer to Peer Network
Remote Access
Root Kits
Scareware

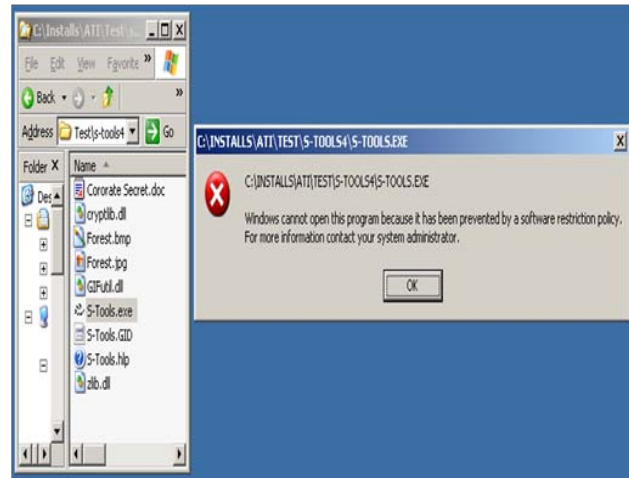
- Utilize the application blocking feature of McAfee Host Intrusion Prevention to monitor application creation and application “hooking” on a managed node, and block execution of applications that violate the organization's acceptable use policy.
- Notify the IT and Physical Security Groups of violations of policy using the communication mode (email, PDA, voice) suited to the severity of the incident and duty schedules. Broadcast and escalation features guarantee 24/7 notification, persistently sending alerts and escalating messages until an appropriate response is received to ensure problem resolution.

How Advanced Threat Identification Works

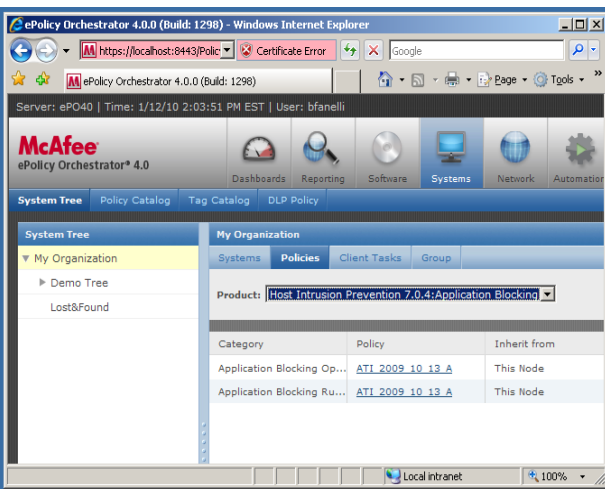
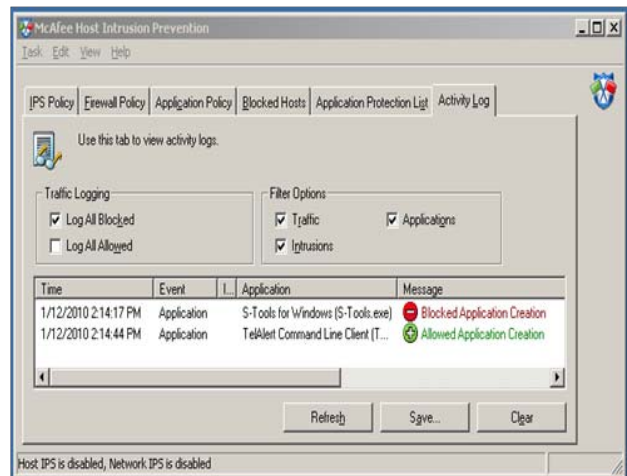
Advanced Threat Identification uses ePO to define security policies, manage modifications to these policies when the ATI malware datasets are updated, organize managed systems into units for the assignment of these policies, and enforce blocking actions when execution of potentially dangerous software is attempted on an end-point. The ePO administrator can create policies by selecting entire ATI malware categories and/or by choosing individual components within a category. ePO enables ATI policy enforcement on end-points to be highly scalable, with each ePO server able to manage up to 250,000 systems

STEP 1: Administrator uses ePO ATI to generate a policy which detects and blocks malicious programs.

STEP 3: HIPS application blocking monitors the node for application creation and blocks S-Tools when execution is attempted.



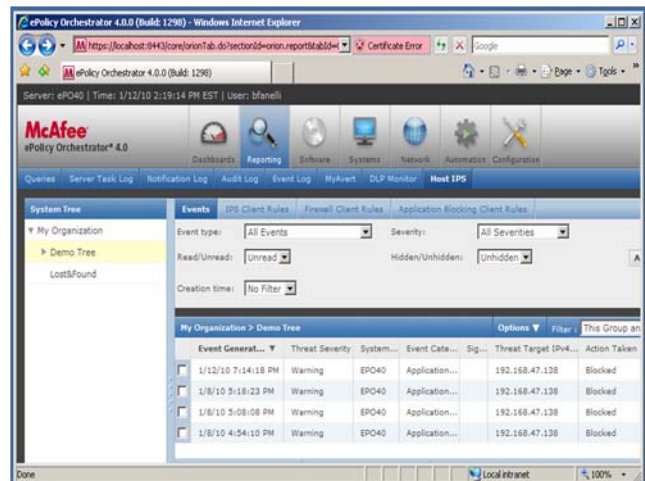
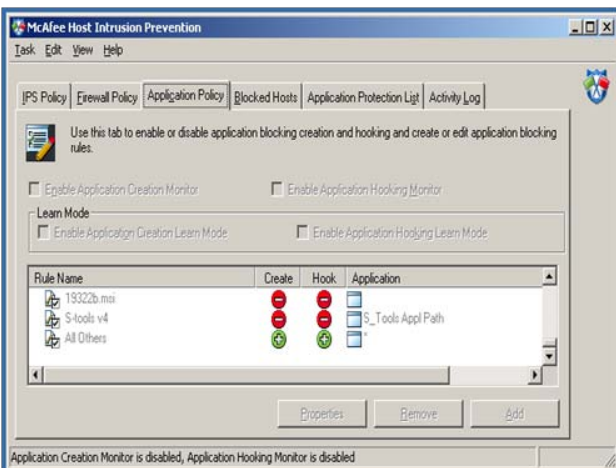
At which point the application block is logged locally by the ePO agent.



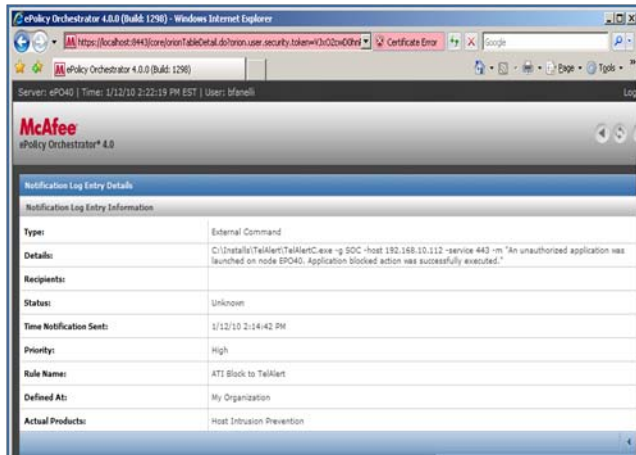
The following is a representative policy showing a rule that blocks S-Tools, a widely-used steganography application. S-Tools can covertly leak confidential information by embedding a secret file (payload) in an image (carrier) file.

STEP 2: ePO pushes the policy to the managed endpoint(s), and it is applied by the client-resident ePO agent.

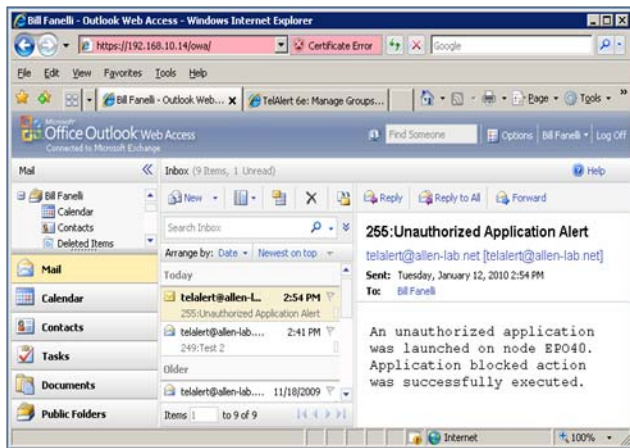
STEP 4: The application blocking event is forwarded to the ePO console and database, where it is available for ATI queries and reports.



STEP 5 (ATI Option): ePO sends an alert based on a defined notification strategy – event severity, schedule, escalation policy, communication mode. And the appropriate recipients are alerted in compliance with the notification strategy.



System requirements



Management Console

McAfee ePO version 4.0 or 4.5

Endpoints

McAfee ePO Master Agent version 4.5



The McAfee Security Innovation Alliance is the foundation of a technology ecosystem designed to assemble the world's leading security innovations. Working together, McAfee and its partners deliver solutions more comprehensive than those available from any single vendor. You'll find the McAfee Compatible logo on products that have passed McAfee's integration testing. For more information, visit www.mcafee.com/sia.

About Allen Corporation of America

Headquartered in Fairfax, VA, Allen Corporation of America is a dynamic, rapidly growing company that provides expertise in several major technology areas, including: Cyber Security; Logistics and Logistics Support; Systems Integration; Training and Distributed Learning; Voice over IP Communications; and Enterprise Management. Allen subsidiary, WetStone Technologies, is an industry leader in Cyber Security solutions for the digital investigator, including award-winning training and WetStone-branded products for malware and steganography investigation, live forensics, intrusion detection and secure time. Allen and WetStone are also leaders in cyber security research, and were awarded the Small Business Research Innovation Program's Tibbetts award for innovative research in the area of biometric liveness.

Contact Us:

10400 Eaton Place, Suit 450
Fairfax, VA 22030

1-877-HQALLEN ext5
csdsales@allencorporation.com

www.allencorporation.com/csd

McAfee, ePolicy Orchestrator, ePO, and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products.