HDF ADVANCED MALWARE PROTECTION

Why is HDF needed?

Any business with a computer is under constant threat from cybercriminals using ever changing and more sophisticated malware to steal intellectual property, extort money, steal a customer's personal information or deface websites.
Major downtime involving corporate internet services will cripple businesses, and today's headlines report a steady stream of data breaches and ransomware attacks resulting in damaged reputations along with millions in lost revenue, legal fees, fines and cost of recovery. If viruses and malware introduced inadvertently or otherwise are not rigorously prevented from executing their malicious code, they can easily spread to infect the entire IT infrastructure. The era of antivirus as king has long been gone, and is estimated to be able to defend against 5% of new malware. Complex anti-malware tools now promising protection require an ever increasing amount of bandwidth and CPU power, therefore degrading overall network performance. Unlike HDF the systems described above will continue to be vulnerable to Zero-Day attacks.

What is HDF?

HDF is an innovative patent-protected advanced anti-malware software solution using Host Integrity Technology integrating fully into operating systems to prevent executable files from writing to computer hard drives. It serves to enforce corporate security policies and provides detailed analysis and audit information.

HDF is a proactive security software that is 99.999 % effective against Zero-Day Malware, viruses, worms, spyware, trojans, botnet and rootkit attacks/infections. This includes evolving Ransomware attacks and Advanced Persistent Threats (APT's), an exploitation of Alternate Data Streams (ADS).

HDF prevents laptop and mobile users inadvertently introducing viruses into company networks. IT also stops other unauthorized software downloads that affect computer stability.

How does it work?

Deployed as software on servers and end-user workstations and laptops, HDF is implemented as a kernel driver into Microsoft (or Linux) 32bit or 64bit operating systems and takes just one minute to install.

HDF intercepts and mediates file write access to computer hard drives, network shared storage or removable storage devices such as USB sticks and other external drives.

Host Integrity Technology is used by HDF to secure the operating system kernel by understanding what source code is required by legitimate applications (logging all executable attempts) and flags, without executing, any and all irrelevant, unnecessary, unwanted and illegal binary code. HDF continues to monitor operating process binaries, detecting additional modifications and stopping malicious code that enters applications at later dates even if dormant malware is already on the system before the HDF is installed. Malicious code (a Trojan for example) will therefore still be blocked once it attempts to execute.

HDF allows updates to Windows and other applications, but blocks the portions of those updates that include unnecessary items. A significant boost in Windows performance can be achieved.

An attacker cannot use a backdoor or rootkit approach and cannot bypass HDF control even with the highest level of computer system privilege.

There are three modes of operation:

Protect mode blocks all unwanted executables from being written to the hard drive and is the operational mode.

Learn mode records all unwanted executables that would have been blocked if HDF had been in normal protect mode and allows the user to authorise desired applications.

Audit mode records all write I/O activity and can be used to monitor all internal use of the system.

There is no additional demand on RAM and almost no CPU overhead because the HDF software is less than 100 Kbytes in size, and implemented at the file system level or zero ring (Kernel Level).

Benefits of HDF

- HDF enforces system and file integrity without complex management overheads, and is transparent to applications and users without user interaction.
- HDF does not use signatures so there is no need for constant updates to add newly discovered attacks and no threat of being the Zero-Day victim. No Blacklisting or Whitelisting hash databases are maintained and HDF is not reputation or heuristics-based. HDF is not using a "File Integrity Monitoring" model that simply notifies of a breach and it does not rely on Threat Intelligence feeds requiring additional subscription fees. All of these traditional methods will be defeated by Zero-Day attacks. HDF will not.
- HDF using Host Integrity Technology exercises robust control over the writing of files to a computer, providing true Zero-Day Attack protection.
- HDF provides additional protection against vulnerabilities caused by delayed operating system patching.
- HDF provides protection to unsupported legacy Windows operating systems such as NT4, XP and Server 2003.
- As a Defence-in-Depth layer of security, HDF serves to prevent the effects of malware missed by anti-virus solutions.
- HDF has a tiny footprint of less than 100k and once installed provides significant system speed and performance improvement Furthermore HDF is proven in independent tests by Lockheed Martin to reduce electrical energy consumption by 7% while providing effective security.
- With such a small footprint HDF is also ideal for SCADA, Process control and CCTV environments.
- HDF Central Management Console (CMC) is required by most corporate deployments. While HDF blocks unwanted executable files by default, information gathered from HDF in learn-mode is used by the CMC to create templates of all acceptable binaries and pushed globally to Windows servers and PC workstations, to one user, a group of users or all users.
- Any endpoint that is unprotected by HDF can be blocked by the CMC using APIs as part of a Firewall or Access Control rule set.
- Detailed log reporting structured for easy filtering will clearly identify what HDF has allowed and what has been blocked. Admin permissions can be defined to individuals or groups.
- When HDF is used with the CMC it provides a "Hunter Killer" capacity against APTs and identifies areas that require clean up.
- HDF demands little operational or back office management.

Apply for a demo of HDF Advanced Malware Protection at http://info.prodec.co.uk/HDF-advanced-malware-protection or call a Prodec Networks security specialist on 01189 241207

PRODEC NETWORKS LTD
Registered in England and Wales. Company No 3645275 Prodec House, Chancery Gate Business Centre, Ruscombe Park, Twyford, Berkshire, RG10 9LT
info@prodec.co.uk www.prodec.co.uk