Protective Monitoring Capability

Abatis Central Management Console (CMC)

Making Security Management Simple and Cost-Effective

Abatis HDF Central Management Console (CMC) is specifically designed to monitor all HDF protected computers for real-time HDF logging, status of HDF clients, security trends, security alarm, and to interrogate the HDF operating parameters as well as system and hardware information. Through CMC, the HDF administrator can control HDF clients, to turn-on/off protect mode, set the allowed processes and so on.

Benefits of Abatis Host Integrity Technology (HDF) and Central Management Console:

- Reduces operational costs by eliminating incidence of malware infection and associated fix/clean-up costs
- Provides confidence in proactive defences rather than reactive clean-up after infection
- Improves management oversight and control of the estate (including enforcing the security policy)
- Over time can be used in conjunction with traditional AV to clean-up infected or compromised estate (targeted removal of APTs)
- Low cost, virtually fit-and-forget solution
- Works in SCADA and Virtualised environments with your existing security controls and products
- Protects new and legacy equipment as old as Windows NT4.

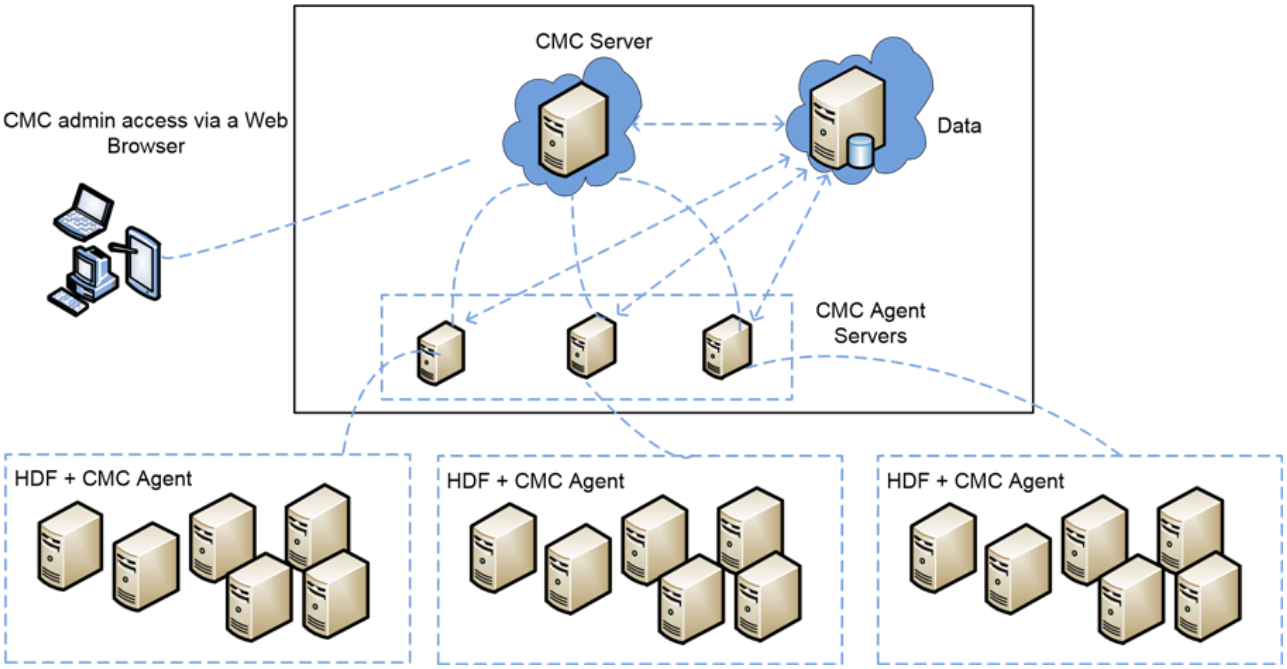
What is the Central Management Console?

HDF Central Management Console (CMC) is a monitoring and management tool for HDF-protected computers within the company/organization. It is a web-based application with a combination of functionality such as log collection, log analysis, log query (report), real-time monitoring and management. With the CMC, authorised IT administrators can easily view real-time HDF log information showing the status of HDF clients, security trends, security alarms, and can interrogate the HDF operating parameters as well as system and hardware information.

Central Management Console (CMC) provides facilities to:

- Retrieve and analyse HDF logs
- Define policy updates to HDF individually, in groups or globally depending on architectural requirement
- Web based application
- SIEM-like dashboard
- Simple, clean and easy to use
- SQL database back end allows sophisticated query, analysis and abstraction into higher level tools like Arcsight
- CMC can be used to search for identified 'rogue' files such as blocked APT updates
- Experience shows 'clean-up' of an infection can be reduced from 3 days to 2 hours (90% improvement)

Central Management Console (CMC) Network Architecture



CMC Server and CMC Agent Server System Requirements

Processor	CPU Type: Intel Xeon E5606 2.13GHz 2 cores
Operating System	Windows Server 2008 SP2 32-bit and 64-bit Windows Server 2012 R2 and Windows Server 2012 64-bit
Memory (RAM)	Minimum: 4GB Recommended: 8GB or higher
Available Hard Disk Space	Minimum: 28GB (200 clients Maximum:100GB (2500 clients)
Network	100MB

Scalability

Each CMC can accept up to 2500 HDF clients depending on target environment. CMCs can be placed in a hierarchy as required to mimic the tree-like structure of the organisation. This means that there is effectively no upper limit to the number of HDFs that can be monitored and controlled, thereby providing a dynamically extendable protective monitoring solution.

About Abatis (UK) Ltd.

Abatis is a UK based company established at Royal Holloway University of London. Abatis designs and develops security solutions to defend against the most sophisticated malware and advanced attacks by cyber criminals. For the past five years Abatis has supplied governments, financial and major corporations around the world with security solutions that have withstood the test of time against all forms of attack.

***Contact**: Kerry Davies*
***Email**: kerry@abatis-hdf.com*
***Mobile**: +44 7767 240799*
***Website**: www.abatis-hdf.com*
Royal Holloway University of London, Egham, Surrey, TW20 0EX

