Anti-Virus Power Consumption Trial

Executive Summary

Open Market Place (OMP)

ISSUE 1.0

ISSUE STATUS

Issue Number	Date of Issue
0.1	11th April 2014
1.0	12th April 2014

RECORD OF AMENDMENTS

Revision	Date	Reason for Change	Amended by
0.1	11th April 2014	First draft	Chris Howden
1.0	12th April	Minor Changes, Approved for Public Release	Chris Howden

QUALITY ASSURANCE

ORIGINATION

This issue was prepared for release by:

Chris Howden

Systems Integrator

NCITE UK

APPROVAL FOR RELEASE

Executive:

John Plumb

NCITE UK Manager

Signature

Date: 12th April 2014

DISTRIBUTION

This document has been approved for public release.

1 Executive Summary

1.1 Key Points

- Up to 50% of the operating costs of a data centre are from electricity, this particular demand is rising 12% year on year and could top 3% of total global energy consumption in 2014.
- A typical enterprise server can use more than £200 of electricity per annum and IT departments rarely assume responsibility for these often excessive energy costs; the bill typically picked up by facilities.
- Progress has been made to address energy efficiency at a hardware level on the servers that operate within these data centres, with virtualisation techniques having particularly quelled demand.
- Opportunities exist to examine and optimize energy efficiency within the software that runs on these machines; Lockheed Martin NCITE UK funded research has been conducted within this domain.
- Anti-virus (AV) products were the particular focus for a detailed research article, with comparison drawn against a new and comparable type of cyber security solution: a Host Integrity Technology (HIT); Abatis Hard Disk Firewall (HDF). This application has been shown to be more effective in an industry test than 8 household name AVs and has been successfully validated by Lockheed Martin NCITE UK in a previous trial.
- Using a standardised environment and experiment, three of the major AV products were compared against HDF and average energy and power values obtained for all four applications.
- Abatis Hard Disk Firewall is shown to block unnecessary background processes and applications from executing, saving 0.55W of electricity when compared to the standardised environment and 14.78W from the worst performing antivirus product.
- The financial implication is significant, by using Abatis HDF savings could be in excess of £12 per server per annum. In a data centre environment with 10,000 servers this scales to more than £125,000 per annum.
- A recent report has identified that if 1 watt of electricity is saved at the processor level, 2.84 Watts are saved by the facility. This £125,000 saving becomes more than £350,000 due to this cascade effect; the magnification incorporating reduced cooling, power conversion and distribution.

- These savings when coupled with the additional layer to any cyber security approach the technology could offer have to make adoption and deployment, particularly in critical infrastructure a viable and sensible enterprise approach.
- Research method is and should be transferred to other operating systems and devices, including the evaluation of mobile devices, where energy resources are often finite.

1.2 Background

Modern data centres and cloud computing platforms are a part of a highly connected and developed digital world, which continue to support and revolutionise both the enterprise and personal computing experience. As the technology becomes more refined and proficient, both operating costs and heat output have steadily risen; increasing overhead costs and environmental impact. Up to 50% of data centre operating costs in the future will be for electricity [1], global demand increases by 12% year on year and is expected to exceed 3% of total global energy consumption in 2014 [2]. The incessant demand by consumers and the aspiration of providers to ensure continuous high availability and instant connectivity through redundancy are the most significant factors driving excessive power data centre use.

Within these computing devices the central processing unit (CPU) is the single largest consumer of electricity. The effect of performing progressively more intensive CPU tasks is increased electricity use and heat output which must be dissipated, also impacting on the required cooling systems. Active servers even when idle use 60% of their peak power [3] and techniques have been developed to counteract this power usage; not least virtualisation, effective resource scheduling and load balancing. It has been recently documented that if 1 watt of electricity is used at the CPU level, 2.84 Watts are used by the facility [4]; therefore if a typical modern server is assumed to use an average of 200W of power, then this becomes 568W at facility level. To run one server per annum it could cost nearly £500.00, in a data centre with 10,000 servers this figure is close to £5m. Fewer than 20% of IT departments pay the data centre power bill within the enterprise, this ongoing cost typically being allocated to the facilities budget; hence absolving responsibility for and lacking consideration towards these ongoing and significant costs [5].

Computer systems must be protected to preserve confidentiality, integrity and availability. Firewalls and intrusion detection systems form part of this defence, the previous failing to address denial of service or insider threats [6]. The latter has become increasingly problematic due to the proliferation of virtualisation; as these solutions cannot typically interpret encrypted traffic to a host and may not identify an attack due until after the event, due to high traffic volumes [7]. If compromise occurs at the hypervisor level, data may never even leave the device, effectively rendering any external security solution worthless [8].

Antivirus traditionally form part of this layered approach to security; however their presence typically requires a path to the internet to maintain validity, making them an attractive proposition for compromise. These products consume CPU cycles to perform file auditing and process threat information. An identified alternative to this is Host Integrity Technology (HIT); which is emerging to resolve these issues, by blocking the execution of unwanted and malicious processes before they can inflict any damage.

1.1 Aims and Objectives

1.1.1 Research Aim

Host Integrity Technologies have the potential to reduce the energy overhead on a system when compared to a system that uses antivirus software. The latter has to compare virus and malware signature files against an extensive database for matches and subsequently report any events. The decrease in power consumption which could be experienced when removing these actions will become magnified in data centre environments, due to the sheer number of devices. The aim of the research undertaken was to either confirm or deny this hypothesis.

1.1.2 Research Objectives

- Conduct an investigation into and then devise a series of verifiable, repeatable and bespoke experiments; mimicking the experience found in a data centre environment.
- Document the results, which will demonstrate the application efficiency of three of the most common antivirus products [9].
- Compare these products against an alternative Host Integrity Technology (HIT): Abatis Hard Disk Firewall.
- Demonstrate energy efficiency in tangible, concrete, real world values that are readily understandable.

1.2 Results & Key Findings

- Sensor data can be collected from a typical enterprise level server including temperature, fan speed and current voltages.
- Relationships between energy and power, relative and specific heat, CPU utilization, power and heat can be established and exploited to calculate unknowns.
- The total power of a computing system is the combination of two values, one static and one dynamic; the latter being dependent on the amount of work being performed.
- A general rule has been established that allows these static and dynamic values to be obtained; allowing power values for a hypervisor, operating system and a running application to be derived.

- Total server power can also be expressed as a polynomial function with four top level elements; the latter three the components of the described, work dependent, dynamic value:
  1. A static value required to maintain the system.
  2. A linear relationship between CPU utilization and power.
  3. Power requirements of other minor components.
  4. System inefficiencies.
- Using these findings and leveraging a virtualised environment to permit repeatability, experiments could and were undertaken to plot CPU utilization against power and the calculation of average energy consumption values for three of the most commonly used anti-virus products.
- A Host Integrity Technology: Abatis Hard Disk Firewall, was also tested using the same standardised environment and shown to block applications and background processes from executing; saving energy from a baseline configuration.

Table 1- Demonstrating Energy Costs Per Day and Annum per Day and Per Annum (at Average £0.10 per KwH)

Product	Energy Cost to Run 1 Server for 24 hours (KwH)	Energy Cost to Run 1 Server for 24 hours (£, 1KwH @ £0.10)	Energy Cost to Run 1 Server for 365 days (£, 1KwH @ £0.10)	Energy Cost to Run 1 Data Centre with 10,000 Servers for 365 days (£, 1KwH @ £0.10)	Energy Cost to Run 1 Application for 365 Days on 1 Server (£, 1KwH @ £0.10)	Energy Cost to Run 1 Application for 365 Days on 10,000 Servers (£, 1KwH @ £0.10)
No AV Product installed	4.43	£0.44	£161.66	£1,616,565		
AV Product 1 Installed	4.53	£0.45	£165.36	£1,653,615	£3.71	£37,050.18
AV Product 2 Installed	4.75	£0.47	£173.24	£1,732,417	£11.59	£115,851.58
Abatis HDF Installed	4.39	£0.44	£160.29	£1,602,925	-£1.36	-£13,639.90
AV Product 3 Installed	4.53	£0.45	£165.22	£1,652,201	£3.56	£35,636.23

- These energy costs can be converted into monetary values, and scaled up to demonstrate costs per day and per year for both a single server and a data centre instance with 10,000 servers. These calculations have been performed and are demonstrated in Table 1.
- Between best case, HDF and worst case, AV Product 2 there is a potential annual cost saving in excess of £12 at server level, this scaling up to £125,000 in a data centre with 10,000 servers.
- These results can be demonstrated graphically, identifying in Figure 1 total power consumption for each application and in Figure 2 costs for the described data centre scenario.

- When multiplied up to facility level to allow for cooling, power conversion and distribution energy savings this figure will rise to more than £350,000.

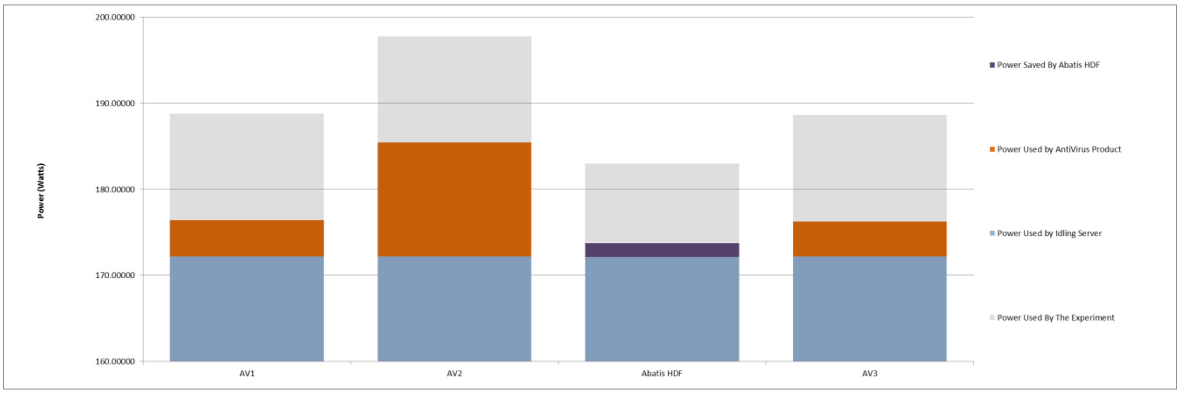

Figure 1 – Demonstrating Average AV & Host Integrity Technology Power Consumption for a Single Server

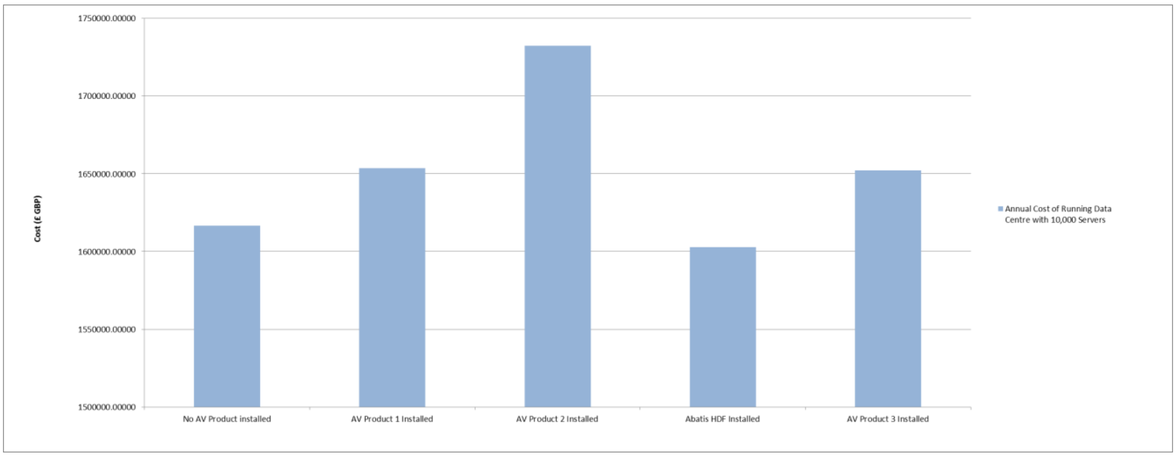

Figure 2 - Demonstrating Potential Cost Savings at Server Level for 10,000 Devices; Excluding Cooling and Power Distribution

1.3 Implications

The results clearly demonstrate that application choice impacts onto the ongoing cost of data centre management and can contribute to a more intelligent, efficient way of managing the enterprise; permitting this concept to become a key differentiator in resource supply and provision.

The factors of confidentiality, integrity and assurance must still be considered, but the power efficiency of an AV product can and should now be considered an important part of application choice. These solutions can and do now have real world values placed against them.

These power figures when taken for a single OS install are multiplied up to data centre proportions are highly significant. The costs savings must surely provoke thought not only how current configurations can be affected, but how future design can be manipulated.

1.4 Recommendations

There is an opportunity to conduct further research with the goal of understanding the energy efficiency interaction between two or more applications; particularly pertinent as one scenario could involve the use of both an AV product and HDF together to provide additional reassurance to the consumer. Experimentation can be extended to multiple virtual machines on the same host, clarifying whether the developed method works in all scenarios. It would also permit the development of an understanding of the most efficient use of a given set of resources. Achieving this through a formal equation is a suggested and desirable end point. This will develop and deliver a better understanding as to the most effective way of managing server provisioning and demand and is the recommended next step.

Capturing historic data and using analytics to predict how, where and when resources should be spun up would return not only the ability to analyse a given scenario and offer the most appropriate solution based on application efficiency; but to provide increased intelligence to resource provision. Integrating this solution with the cooling system, spinning it up only when required will certainly bring further power savings. These are longer term goals.

Finally, there is no reason why the approach taken in this work cannot be adopted, tested and applied to any application efficiency scenario; given a suitable level of research, development, testing and verification. Mobile devices typically have finite resources and often limited access to recharging. It is not uncommon for a mobile phone or tablet with wireless access, global positioning and background processes and notifications constantly running to have to be recharged on a daily basis. Their proliferation and mass adoption make them an easily identifiable target to apply these techniques against. Even greater savings can be made, driving the cost of both enterprise and personal energy use down even further. These recommendations must be considered now and actioned in the near term; demonstrating an innovative and deep commitment to energy efficiency and providing a clear differentiator when delivering enterprise IT solutions.

References

[1] Gartner, 2009. [Online]. Available: gartner.com.

[2] Greenpeace, “How Dirty is Your Data?,” 21 April 2011. [Online]. Available: http://www.greenpeace.org/international/en/news/features/New-Greenpeace-report-digs-up-the-dirt-on-Internet-data-centres/. [Accessed 31 March 2014].

[3] G. Chen, W. He, J. Liu, S. Nath, L. Rigas, L. Xiao and F. Zhao, “Energy-Aware Server Provisioning and Load Dispatching for Connection-Intensive Internet Services.,” *NDSI,* vol. 8, pp. 337-350, 2008.

[4] Emerson Network Power, “Energy Logic 2.0: New Strategies for Cutting Data Center Energy Costs and Boosting Capacity,” 2014. [Online]. Available: http://www.emersonnetworkpower.com/documentation/en-us/latest-thinking/edc/documents/white%20paper/is03947_2012_energylogic_fin.pdf. [Accessed 12th April 2014].

[5] Uptime Insititute , “2013 Data Center Industry Survey,” 2013. [Online]. Available: http://c.ymcdn.com/sites/www.data-central.org/resource/collection/BC649AE0-4223-4EDE-92C7-29A659EF0900/uptime-institute-2013-data-center-survey.pdf. [Accessed 1 April 2014].

[6] C. Modil, D. Patell, A. Patel and R. Muttukrishnan, “Bayesian Classifier and Snort based Network Intrusion Detection in Cloud Computing,” in *Third International Conference on Computing Communication & Networking Technologies (ICCCNT)*, Coimbatore, 2012.

[7] J. Hu, X. Yu, D. Qiu and H. H. Chen, “A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection,” *Network,* vol. 23, no. 1, pp. 42-47, 2009.

[8] K. Benzidane, S. Khoudail and A. Sekkaki, “Autonomous Agent-based Inspection for inter-VM Traffic in a Cloud Environment,” in *International Conference For Internet Technology And Secured Transactions*, London, 2012.

[9] Intervictus, “Information Security Solution,” 2013. [Online]. Available: http://intervictusltd.com/index.php/information-security/solution. [Accessed 11 April 2014].