Endpoint Protection Proposal

November 2013

# Purpose

The Security team is seeking approval and funding to replace the University’s current VENDOR endpoint protection suite. The following proposal will outline investment options for an endpoint protection replacement, and highlight the security teams recommended solution.

# Background

The University’s current VENDOR endpoint protection suite is operating on legacy systems that require a significant redesign to improve performance and reliability. The redesign will require re-installation of all client agents on managed endpoints; therefore OU IT has the opportunity to investigate alternate endpoint protection suites while reducing licensing costs.

# Requirements

The proposed endpoint protection solution should offer the following:

* Provide robust protection for University owned endpoint assets
* Support multiple operating systems
  + Microsoft Windows
  + Mac OSX
  + Linux
* Provide multi-tenancy policy management for departments through a centrally management console
* Reduce licensing costs

# Value to the University

*Reduce Cost*

This project reduces annual spending for by approximately **$ 40,592** or  **$ 200,856** over three (3) years

Cost reductions could potentially extend further than endpoint protection maintenance to include annual maintenance spending for the following:

* Web content filtering (Websense $5,370/yr)
* Full disk encryption (VENDOR4 - ~$5,000/yr)
* Mobile Device Management (? - $3,000/yr)

*Reduce Risk*

Quality antivirus capabilities reduce risk to University information technology resources by proactively preventing, or reducing the probability of, University system infection by malware that can result in negative impacts to the University resources. Antivirus software also works as a detective control to alert incident response and intelligence teams of increasing threats to the campus environment, and as a corrective control to remove malware threats that have affected unprotected systems.

# Recommendation

**Option 1 – VENDOR2**

This option offers the best value, meets all established requirements, and provides many added features not offered by the other options. Even though the University’s Microsoft contract allows for the use of the Forefront client, the system is very complex, difficult to manage, and the protection offered are well below industry averages. Therefore, the security team does not recommend this solution.

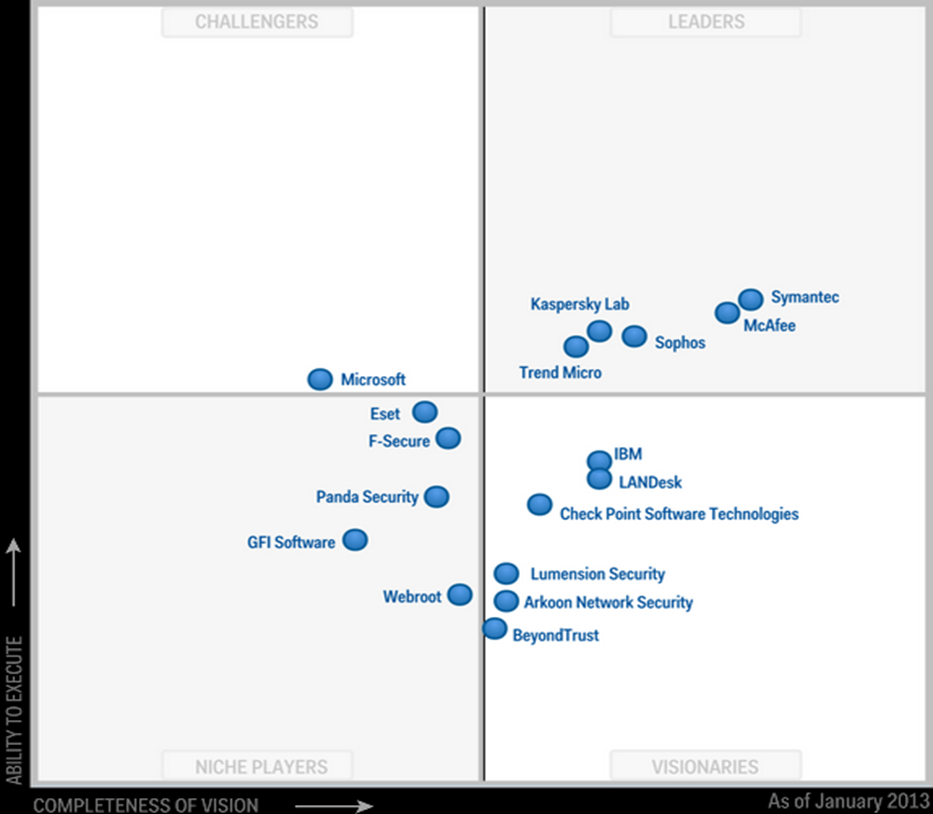
**Roadmap:**

* Purchase VENDOR2 (approximately 6-week lead time for professional services)
* VENDOR Endpoint Protection Expires (10 December 2013)
  + Renew VENDOR Endpoint Protection at reduced count (from 15,000 to 6,000 )
* VENDOR2 on site Professional service days ( 5 Days )
* VENDOR2 Soft Rollout – December 2013 🡪 January 2014
* VENDOR2 Campus Rollout – February 2014
* Complete VENDOR replacement – Summer 2014
  + Decommission VENDOR infrastructure (Ensure logs are retained for compliance)

# Investment Options

## Gartner Magic quadrant for Endpoint protection

**Gartner definition:** The endpoint protection platform provides a collection of security utilities to protect PCs and tablets. Vendors in this market compete on the quality of their protection capabilities, the depth and breadth of features, and the ease of administration.

**Published:** 2 January 2013 (Revised: 27 March 2013)

## Option 1 – VENDOR2

The VENDOR2 provides a good set of endpoint protection tools. It utilizes a single anti-malware agent that detects, blocks or removes malware, adware, suspicious files and web-borne threats and prevents users from accessing malicious websites.

Features included in this suite:

* Enterprise console
* Device control
* Web filtering
* Application control
* Data control
* Client firewall
* Encryption
* Anti-virus
* Patch assessment
* Host intrusion prevention system (HIPS)

***Pros:***

* Mac OSX Support
* Complete endpoint protection solution
* Lighter client, therefore more resources are available to the user and operating system
* Granular access controls
* Free client available to faculty and staff for home use

***Cons:***

* Last year they released an update that caused an outage
* Fat client, this will require additional windows license costs for the target architecture

## Option 2 – VENDOR Endpoint Protection

The VENDOR endpoint protection suite is the university’s current solution. VENDOR Endpoint Protection is a solution that protects laptops, desktops, Mac computers and servers in a network against malware. It combines virus protection with advanced threat protection to proactively secure computers against known and unknown threats. The tool combines traditional scanning, behavioral analysis, intrusion prevention and community intelligence into its security system.

***Pros:***

* Familiarity, current solution.
* Reporting tools are fairly robust

***Cons:***

* Requires professional services to assist with redesign. These fees will most likely not be included in our annual renewal fees
* Poor Max OSX adoption due to performance issues
* Additional feature or solutions are not included in current license

## Option 3 – VENDOR3 Endpoint Protection

The endpoint protection manager deploys and configures endpoint protection, manages firewall settings, configures antimalware policies, updates antivirus definitions, manages email alerts and creates reports. It manages security protocols such as blocking incoming connections, suspicious downloads and rootkit exploits, monitors spyware and manages network profiles.

***Pros:***

* Included in the licensing agreement with VENDOR3
* Granular access controls

***Cons:***

* Only product evaluated that is not certified by 3rd party due to lack of protection
* Limited reporting
* Limited Mac OSX support, only supported if PKI infrastructure is in place
* Significant infrastructure needed to deploy and manage this solution
* Complex group and user management

# Appendix A - Feature Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **VENDOR2** | **VENDOR** | **VENDOR3** | **VENDOR4** |
| Antivirus | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |
| Web Protection | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |
| Firewall | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |
| Cross Platform | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |
| App Control | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png |
| Device Control | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |
| Data Protection | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png |
| Network Control | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png |
| Encryption | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png |
| Virtual Machine | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png |
| Email | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |
| Hips | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |
| TCO Per User  TCO Per Endpoint | $ 22.26 per User  $ 7.42 per Device | $ 42.35 Per User  $ 42.35 per Device | $ 9.07 per User  $ 9.07 per Device | $ 27.56 per User  $ 27.56 per Device |

# Appendix B - Total Cost of Ownership Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **VENDOR2** | **VENDOR** | **VENDOR3** | **VENDOR4** |
| Year 1 |  |  |  |  |
| S2 VM  Software  Labor  Sub-Total | $ 8,100.00\*  $ 49,987.90  $ 21,320.00†  **$ 79,407.90** | $ 5,040.00\*  $ 120,000.00  $ 21,320.00†  **$ 146,360.00** | $ 3,120.00*₸*  **[TBD]***₸*  $ 34,060.00‡  **$ 37,180.00** | $ 8,892.00\*  $ 69,433.33  $ 21,320.00†  **$ 99,645.33** |
| Year 2 |  |  |  |  |
| S2 VM  Software  Labor  Sub-Total | $ 8,100.00\*  $ 49,987.90  $ 13,520.00†  **$ 71,607.90** | $ 5,040.00\*  $ 120,000.00  $ 13,520.00†  **$ 138,560.00** | $ 3,120.00*₸*  **[TBD]***₸*  $ 23,660.00*‡*  **$ 26,780.00** | $ 5,040.00\*  $ 69,433.33  $ 13,520.00†  **$ 87,993.33** |
| Year 3 |  |  |  |  |
| S2 VM  Software  Labor  Sub-Total | $ 8,100.00\*  $ 49,987.90  $ 13,520.00†  **$ 71,607.90** | $ 5,040.00\*  $ 120,000.00  $ 13,520.00†  **$ 138,560.00** | $ 3,120.00*₸*  **[TBD]***₸*  $ 23,660.00*‡*  **$ 26,780.00** | $ 5,040.00\*  $ 69,433.33  $ 13,520.00†  **$ 87,993.33** |
| Total | **$ 222,623.70** | **$ 423,480.00** | **$ 90,740.00** | **$ 275,631.99** |

*\* Prices do not include SQL cluster, service is not yet available in Shared Service*

*† Labor costs are based on $65 an hour, 2 FTE, 2 hours a week each; Year one has an additional 60 hours for setup and configuration*

# Appendix C - AV-Test Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **VENDOR2** | **VENDOR** | **VENDOR3** | **VENDOR4** |
| Protection |  |  |  |  |
| 0-Day Malware  *Industry Average 90 (Measured in %)*  Well Known Malware  *Industry Average 98 (Measured in %)* | 94  100 | 100  100 | 68  92 | 94  100 |
| Performance |  |  |  |  |
| Visiting websites, downloading software, installing and running programs and copying data  *Industry Average 4 (Measured in Seconds)* | 4 | 2 | 2 | 4 |
| Usability |  |  |  |  |
| False warnings or blockages when visiting websites  *Industry Average 0 (Measured in #)*  False detections of legitimate software as malware during a system scan  *Industry Average 3 (Measured in #)*  False warnings concerning certain actions carried out whilst installing and using legitimate software  *Industry Average 0 (Measured in #)*  False blockages of certain actions carried out whilst installing and using legitimate software  *Industry Average 0 (Measured in #)* | 0  1  0  0 | 0  1  0  0 | 0  0  0  0 | 0  1  0  0 |
| Certified |  |  |  |  |
| AV-Test Certified | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\1G11X2T4\MC900439584[1].png | C:\Users\enge7888\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTL3XN64\MC900441310[1].png |