

Royal Holloway
University of London

Desktop AV Project

Huw Michael – Infrastructure Technical Architect

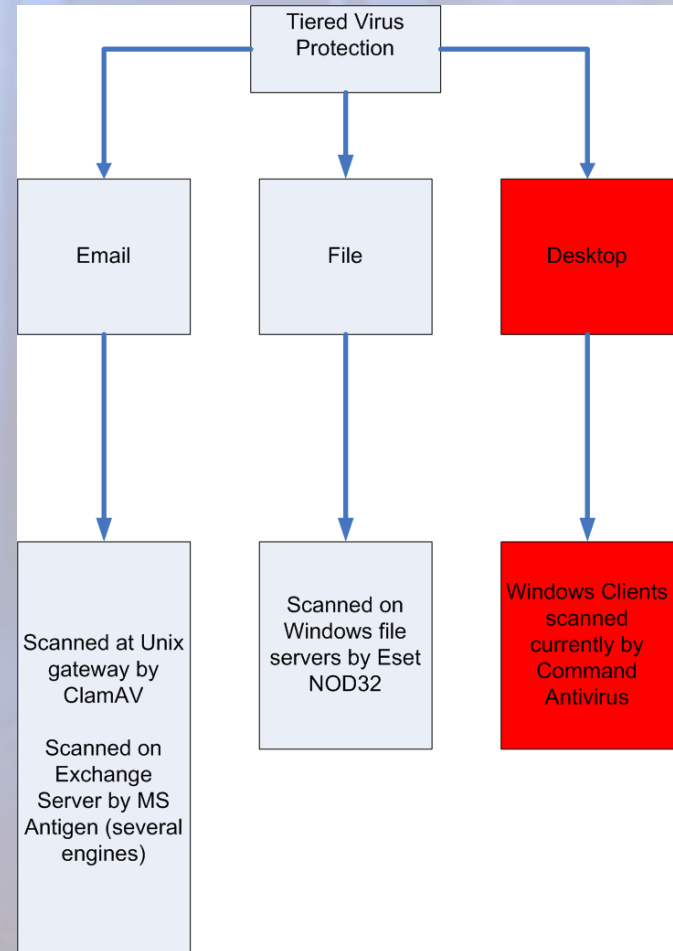


Environment

- 7000 Students
- Over 2000 Staff
- 3000 Desktop Clients – predominantly Windows
- 80% of clients in Active Directory forest
- No formal desktop management solution
- RHUL dissatisfied with existing Desktop Antivirus solution
- Server solution replaced with ESET NOD32 in 2006 - NOD is great but management doesn't scale

Tiered Protection

- Windows Server: NOD32
- UNIX & Linux Servers: ClamAV
- Exchange 2003: Antigen
- Workstations: Solution Required
- Mac: ClamAV / New solution
- Linux: ClamAV / New solution



Project

- Server AV replacement – sysadmin task after product selection
- Campus desktop AV replacement is a project
- Formal methodology very useful in selection process
- Beware of “projects” with no formal resources
- Scope of project to replace AV solution but opportunity taken to deploy full anti-X suite

Approach

See supporting documentation

RFP

- 4 vendors chosen for RFP process
- 2 large vendors eliminated as “no response”
- Sophos and Kaspersky responses both positive
- RFP scores very close but Kaspersky selected on cost & desire to work with RHUL
- CHEST deal used for optimal pricing

Pilot

- Kaspersky Admin Kit and KAV workstation security
- Kaspersky provided engineer for initial configuration
- Kaspersky support used for configuration queries
- Typical use cases and desktop configurations tested
- AD integration bit clunky to set up but once configured very competent
- Home user product tested as part of pilot

Technical Solution

- Kaspersky Admin Kit: policy / task / report
- Kaspersky Network Agent: secure comms with admin kit
- Kaspersky workstation 6: policy from Admin kit via agent
- Network agent installs without reboot, runs as windows svc
- Reports on various competitors but not Command AV
- Logon scripts used for audit of domain desktops
- Zero touch deployment including removal of Command AV using AD Organisational Units as targets for deployment

Zero touch deployment

- Logon script assigned to OU: download KAV package to C:\
- Startup script – install KAV network agent from C:\
- Network agent comms with KAV admin kit
- Group in KAV admin kit linked to OU
- KAV Task assigned to group: network agent run silent Command removal script then install KAV
- Reboot requested – KAV install complete
- All KAV chatter suppressed by policy for initial deployment

Post Deployment Tasks

- Administrator & support staff training
- Tune solution & “unsuppress” user notifications
- Handover of general admin to desktop support team
- MSI deployment for new AD clients
- SP3: fix some network driver issues
- Commence testing of other anti-x features
- Agree support model & distribution method: home licenses

Issues / Lessons Learned

- Stale comp accounts in Active Directory
- KAV policy doesn't reach all settings – require avp.com & login script to fix one issue – disappointing
- Some network driver incompatibilities – docked laptops & network monitoring tools – sp3 fixes most
- Sp3 upgrade is remove and reinstall, not challenging using network agent but not ideal
- Kaspersky released 2 bad updates in last 3 months but no issues and support has been proactive

Questions?

