Endpoint Data Defense

Project Manager: Amber Buening
Project Sponsors: Helen Patton (Chief Information Security Officer)

OVERVIEW
Protecting workstations, laptops, and other devices requires a variety of tools because of the variety of threats. Simple anti-virus solutions are not sufficient. By deploying Symantec Endpoint Protection (SEP), university devices will be protected from multiple threats, with a management structure that allows participating units flexibility and cost efficiencies.

RATIONALE
The university required an improved endpoint solution, to provide immediate capabilities such as anti-malware, anti-spyware, personal firewalls, host-based intrusion prevention.

Future capabilities will also allow for port/device control, application white listing and other controls to manage emerging threats from removable media usage. It will streamline costs by protecting endpoints; reducing hardware costs to the University and improving IT staff response time.

RESULTS
• Deployment of 70% of the University total FTE count. Participating units include:
  - CFAES (ATI & DARD)
  - Marion
  - Mansfield
  - OCIO
  - OSU/NMC
  - College of Medicine
  - Additional OCIO-managed unit
• Provides Symantec training to participating units’ responsible resources
• Creation of a unit-led endpoint protection steering committee for ongoing service quality

End results:
A university-wide service which facilitates compliance with the Information Security Standard, and contributes to strategies to reduce risk of device compromise and data loss and provides enterprise reporting capabilities.

Milestones
Each project deliverable will complete according to the FY15 agreed activities. Completion of the entire project will be April 30, 2015

RESOURCES
People and their roles
Executive Leader: Helen Patton
Tech Lead: Patrick Mayer
Resource Manager: Ryan Treptow
Steering Committee: To Be Determined

Enterprise Security
• Accountable for ensuring the design and completion of this project.
• Partnership with the following groups is also required:
  - Participating Units – for local unit deployment and communications
  - OCIO Communications – for unit engagement
  - OCIO Service Management – for creation of Service in the OCID catalog
  - OCIO Infrastructure – for servers/database build/deploy

Other resources
Virtual Operating systems, storage and licensing support will be required ongoing.
Dependent on OCIO Active Directory program for rollout to OCIO supported units

Project Milestone Gantt

END RESULTS
There will be an implementation review process with each unit deployment, as well as an overall project review

Review:
Project wrap-up and review: (DATE TBD)

RISKS
• Resource conflicts due to operational/project priorities
  • Mitigation: Bi-weekly resource alignment touch points
• Engineering single point expertise
  • Mitigation: Work with Security team to cross-train and/or identify alternative support resources

RUN
Documentation: https://infosec.osu.edu

Reporting Plan/Roadmap:
• Monthly status report to Executive Leader (to be shared with Project Sponsors)
• Reporting to the Steering Committee (frequency to be determined)

Rollout Plan:
Beginning with OCIO, will rollout solution functionality, training and communication support to participating units. Units will determine deployment timelines based on individual scheduling concerns.

FY16 unit deployments will be explored outside the scope of the project

THE O HIO STATE UNIVERSITY