

McAfee ePO

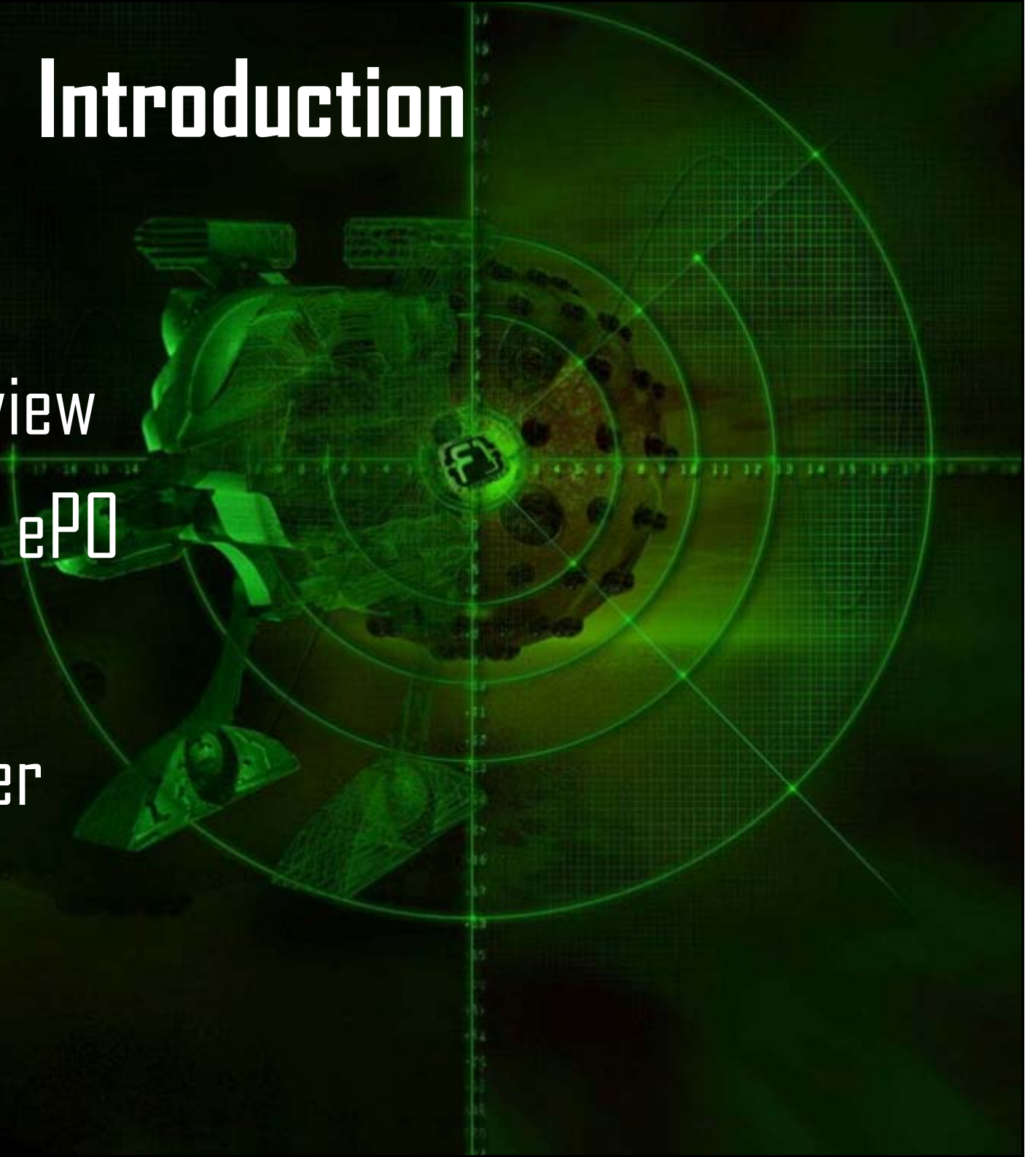
A Technical Overview

Matthew Cook

<http://escarpment.net/>

Introduction

- The past
- A project overview
- What is McAfee ePO
- Installation
- What can it offer
- Problems
- Futures



The Past

- Loughborough University has used the McAfee Anti Virus product for many years
- No formal central management
 - FTP server for DAT files
 - Is a system out of date?
 - SMS scripts on managed services

A Project Overview

- 'Virus Software Review' project
- 'Ad/Spyware' project
- Requirement of both to have a centrally managed system.
- Strong recommendation from auditors

What is McAfee ePO

- McAfee's central management console
- ePolicy Orchestrator
- Provides DAT file revisions, updates and control over the McAfee Anti Virus product
- Provides statistics on infections, early warning on outbreaks as well as client management

Installation

- Windows Server 2003
- SQL Server 2000
- ePO version 3.6
- Installed on dedicated Windows server with fault tolerance/redundancy

Installation

- Requires an agent on the desktop
- Installed by default on Staff Desktop service
- Can be push installed (PC Labs testing)
- Communications on port 8081
- Daily full communications
- Minor updates every 20 minutes

What can it offer?

- Central management of all clients
- Software repository
- DAT file repository
- Staged Software/Engine/DAT rollout
- Directory of computers which matches AD
- Standardise Desktop and Server policy settings

What can it offer?



- VSE Client details
 - Software revision
 - Patch revision
 - Engine revision
 - DAT revision
 - Last time machine updated
 - Last time machine communicated

What can it offer?

- VSE Scheduled Task Management
 - Schedule additional DAT updates
 - Schedule additional system scans
 - Schedule client updates
 - Schedule patch release

What can it offer?

- Reporting
 - DAT file revisions
 - All infections (Viruses, Files, Machines and Users)
 - Type of infection
 - Infection source
 - Infections blocked (Also includes new VSE options)

What can it offer?

- Outbreak management
- Alerts Computing Services once a threshold is reached
- Can produce reports on the computers involved in that incident
- We can then contact yourselves

What can it offer?

- Reporting on new VSE options
 - Buffer Overflow protection (142 month)
 - Unwanted Programs (492,033 month)
 - Access Protection (203 month)
 - Port Ranges (23 month)

Problems

- The ePO software is not the most stable
- Issues with Active Directory
- Very large piece of software with many components
- Rogue System Detection problems
- Users not on Computing Services managed services

Futures

- Problems reported to McAfee
- McAfee released Patch 1 (Jan 06)
- Better Active Directory integration



Questions

<http://escarpment.net/>