

# Andrew McDonnell

Andrew solves tricky problems for a living as Vice President of Security Solutions with AsTech Consulting, and has been a Mac user since before the first time Apple was “doomed”.





# Managing Security With the Growing Threat of Malware





# Wrong





# Susceptibility



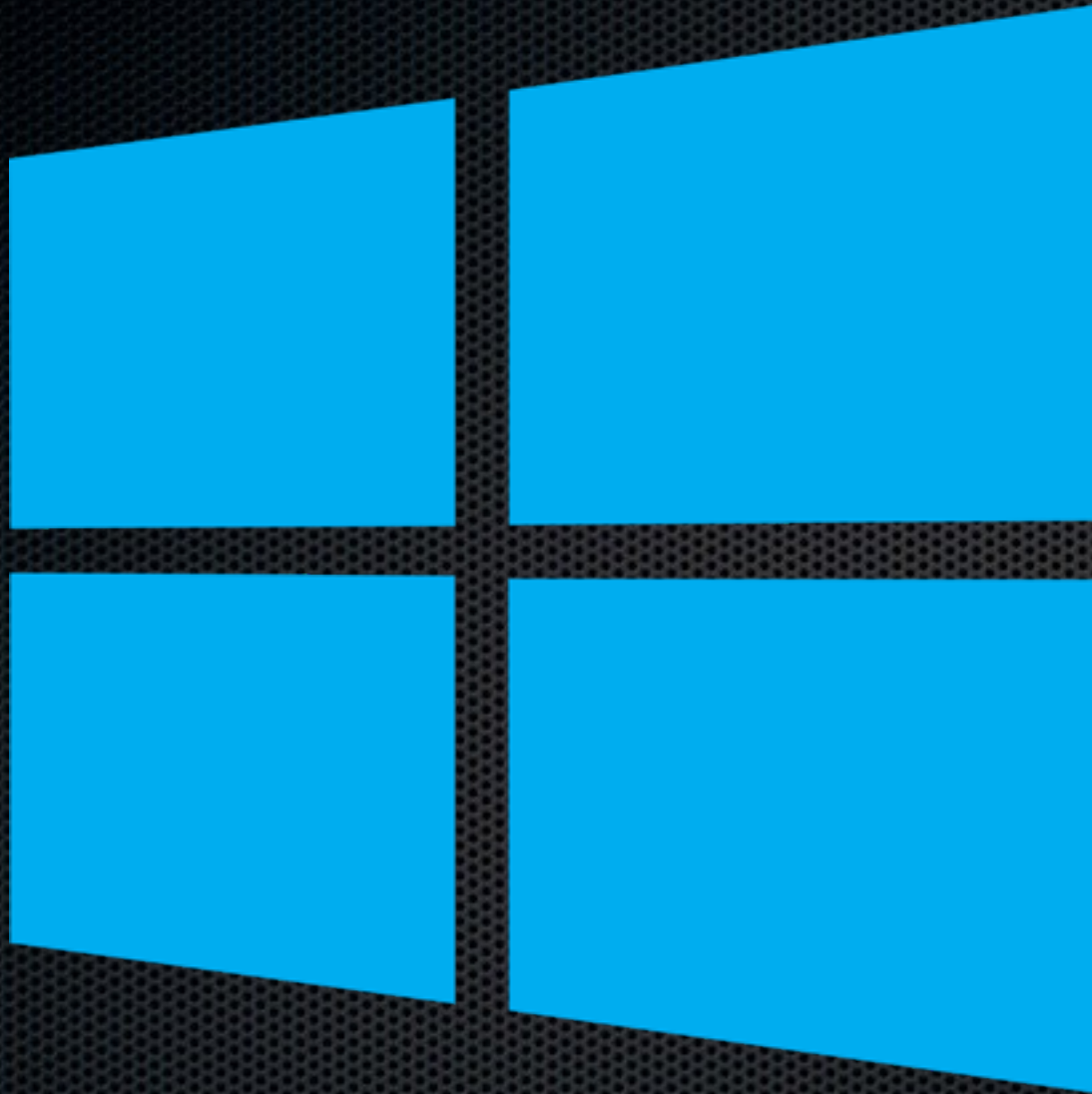


# What's the difference?

- Virus
- Adware
- Trojan
- Ransomware
- Windows Viruses

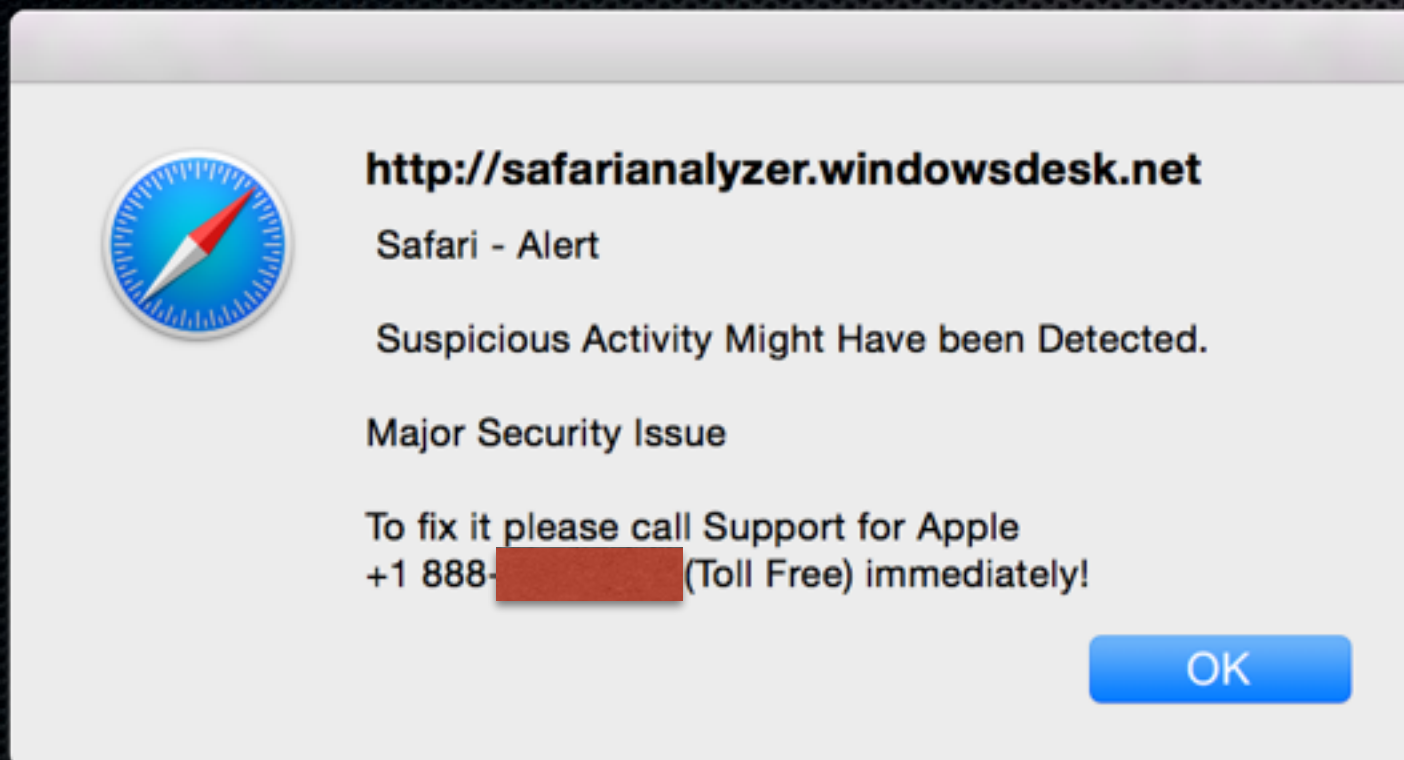


# Not Immune





# Also Not Immune



## Read Immediately!!!!

Everyone running 2.90 on OS X should immediately upgrade to and run 2.92, as they may have downloaded a malware-infected file. This new version will make sure that the "OSX.KeRanger.A" ransomware (more information available here) is correctly removed from your computer.

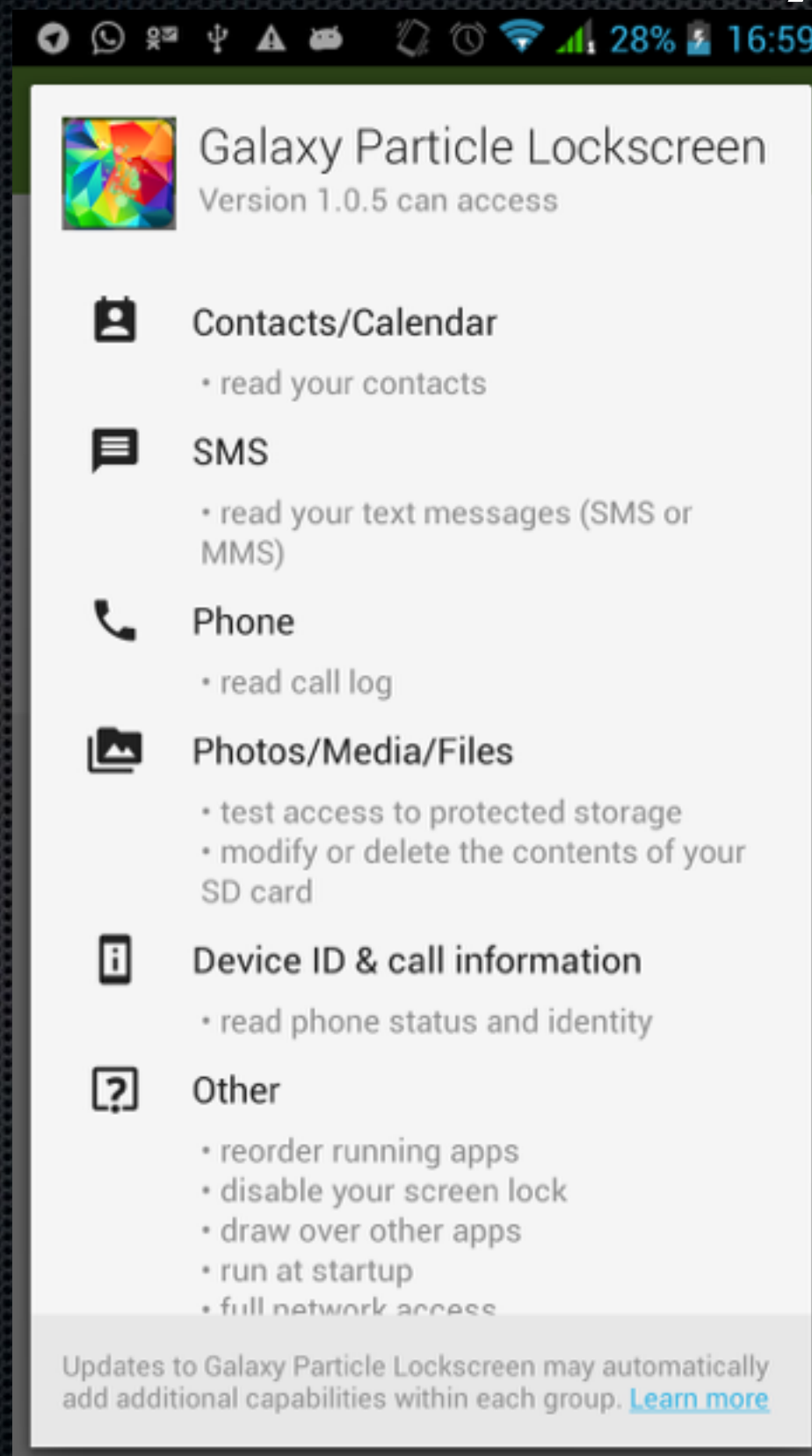
Users of 2.91 should also immediately upgrade to and run 2.92. Even though 2.91 was never infected, it did not automatically remove the malware-infected file.

## Transmission 2.92

[Download Now](#)  
[Release Notes](#)  
[Previous Releases](#)



# 2.3% Immunity





# Trouble Brewing



开天地 化混沌 立乾坤

**PANGU JAILBREAK**  
for iOS9.0-9.1



Download

Version:1.3.0 Size:76.8MB



Download

Version:1.1.0 Size:74.3M



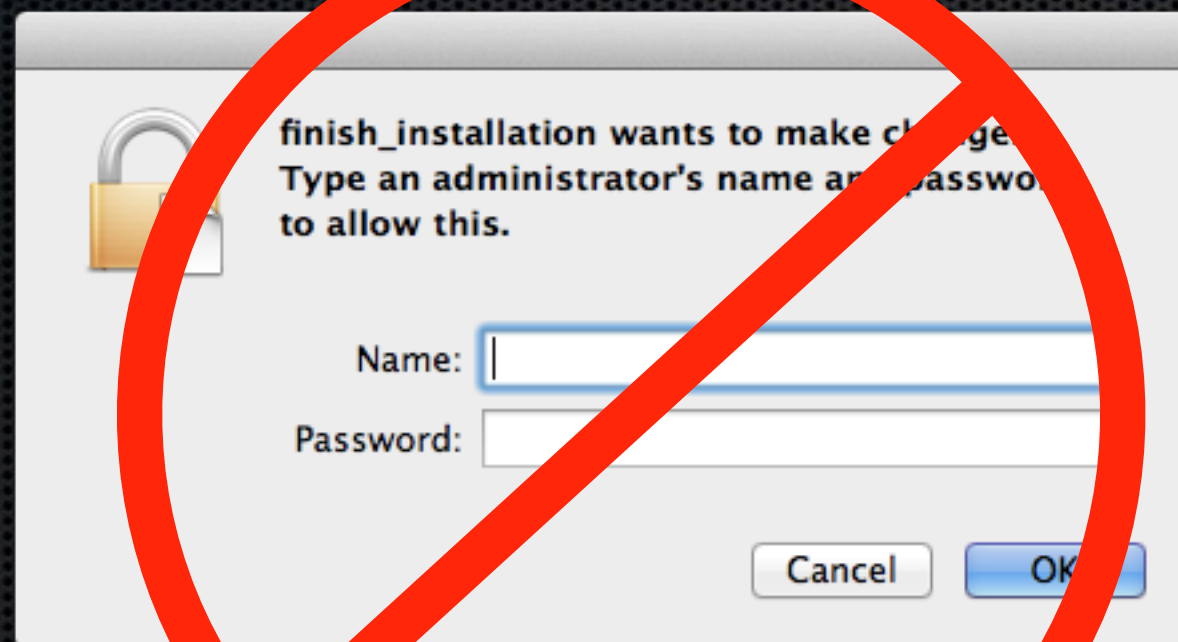




# What Can I Do?

- User Education – Security Mindset
- Update Everything
- Protection
- Response
- Backups – Redundant & Offline





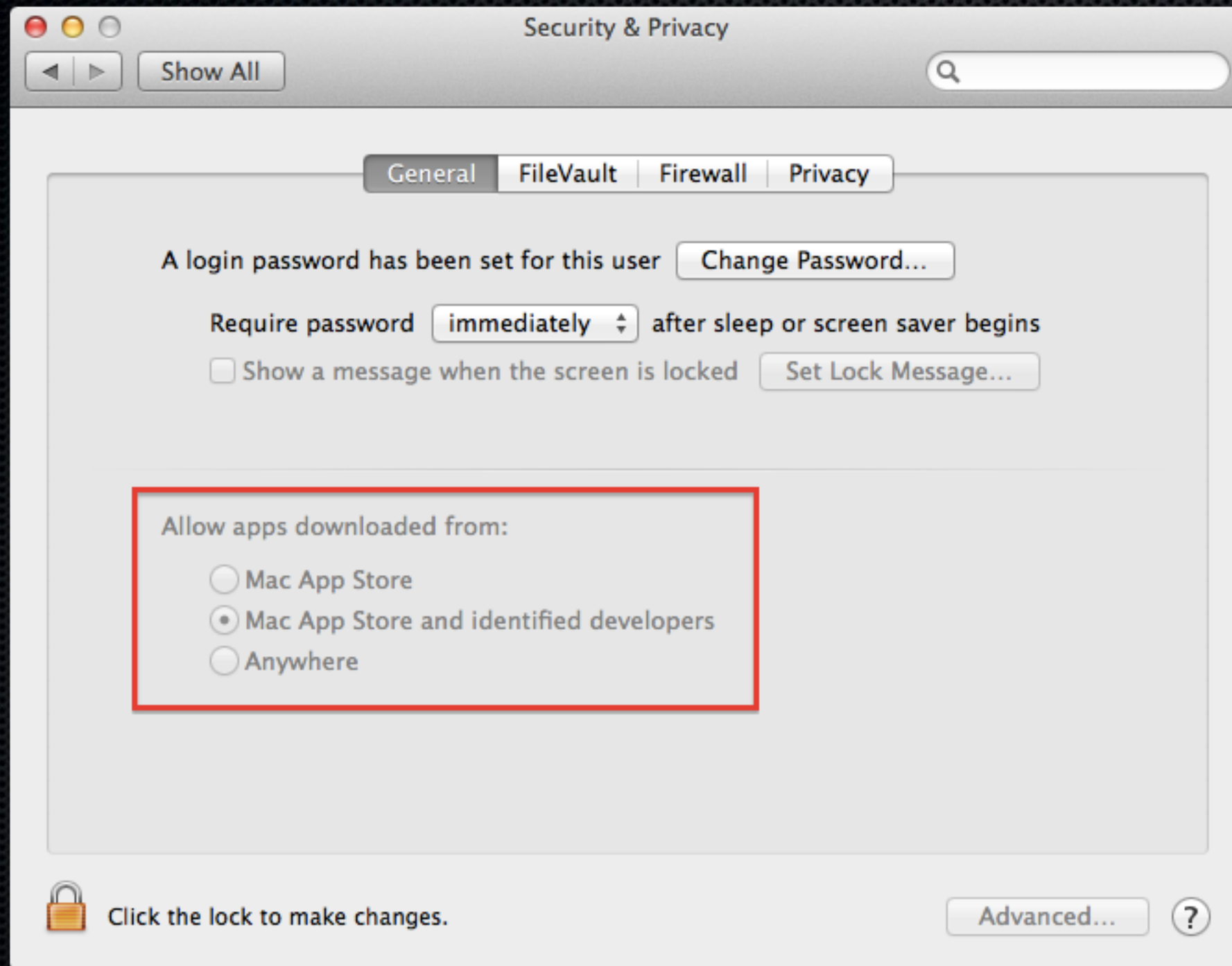


# Basic OS X Hardening





# Basic OS X Hardening



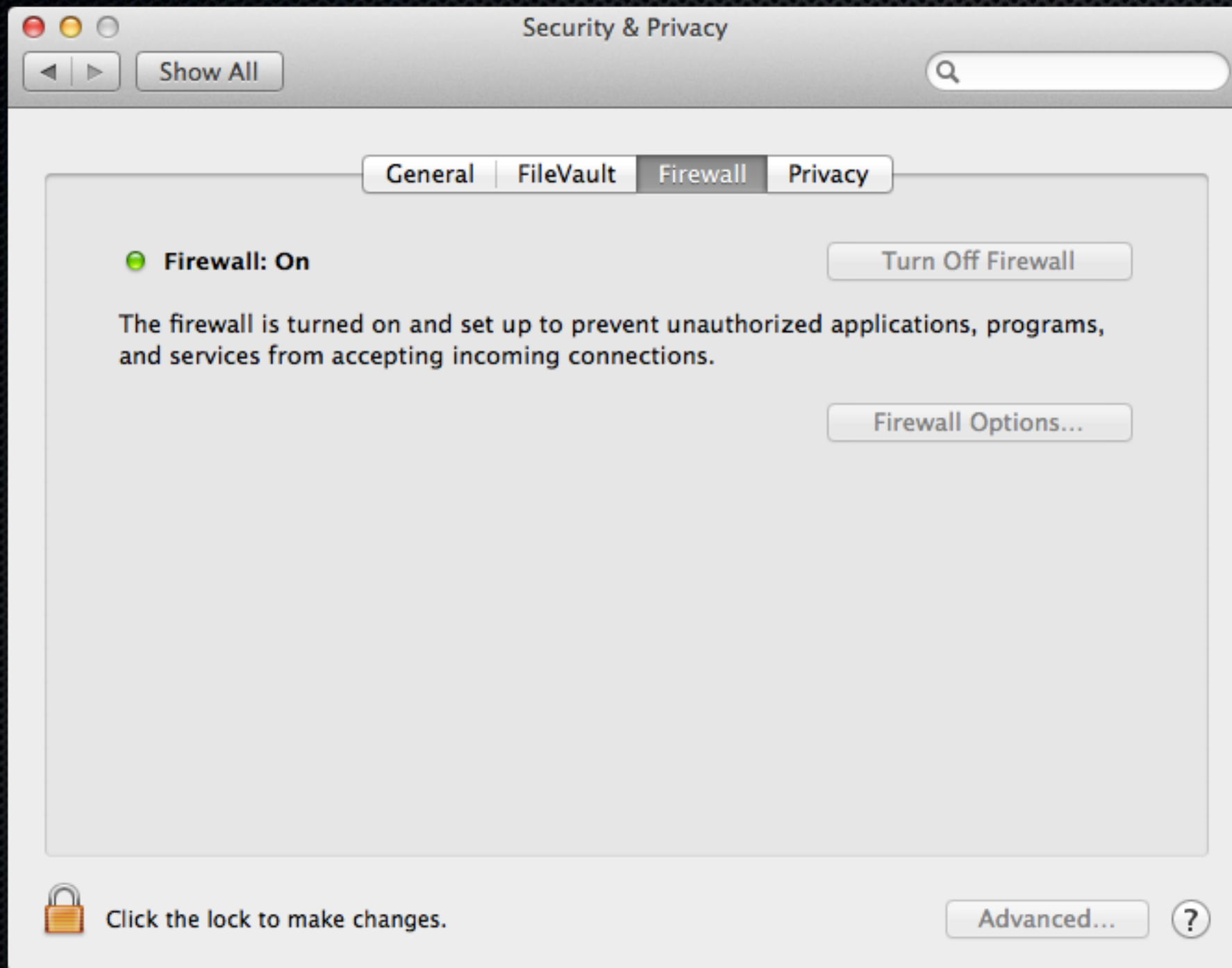


# Basic OS X Hardening



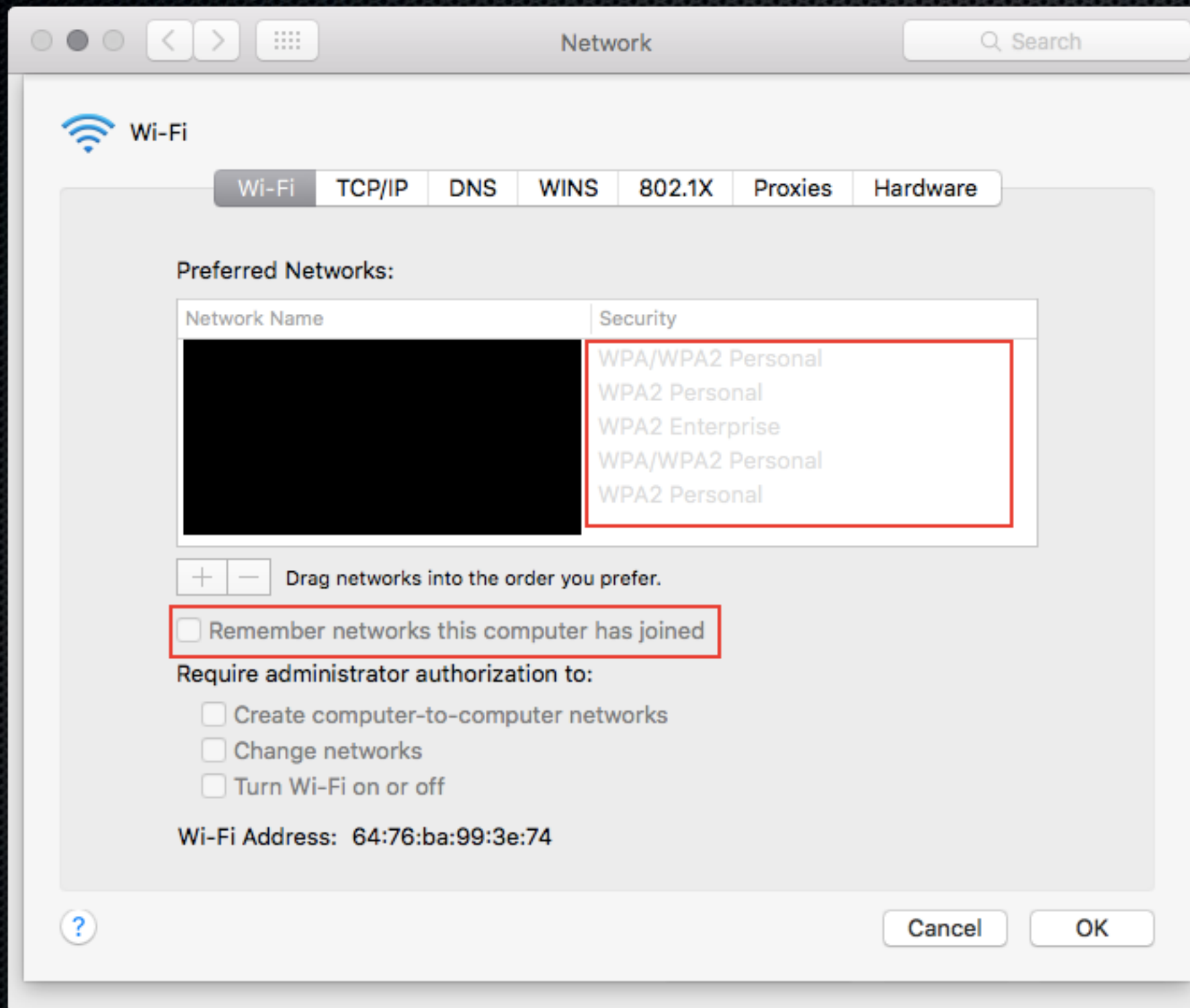


# Basic OS X Hardening



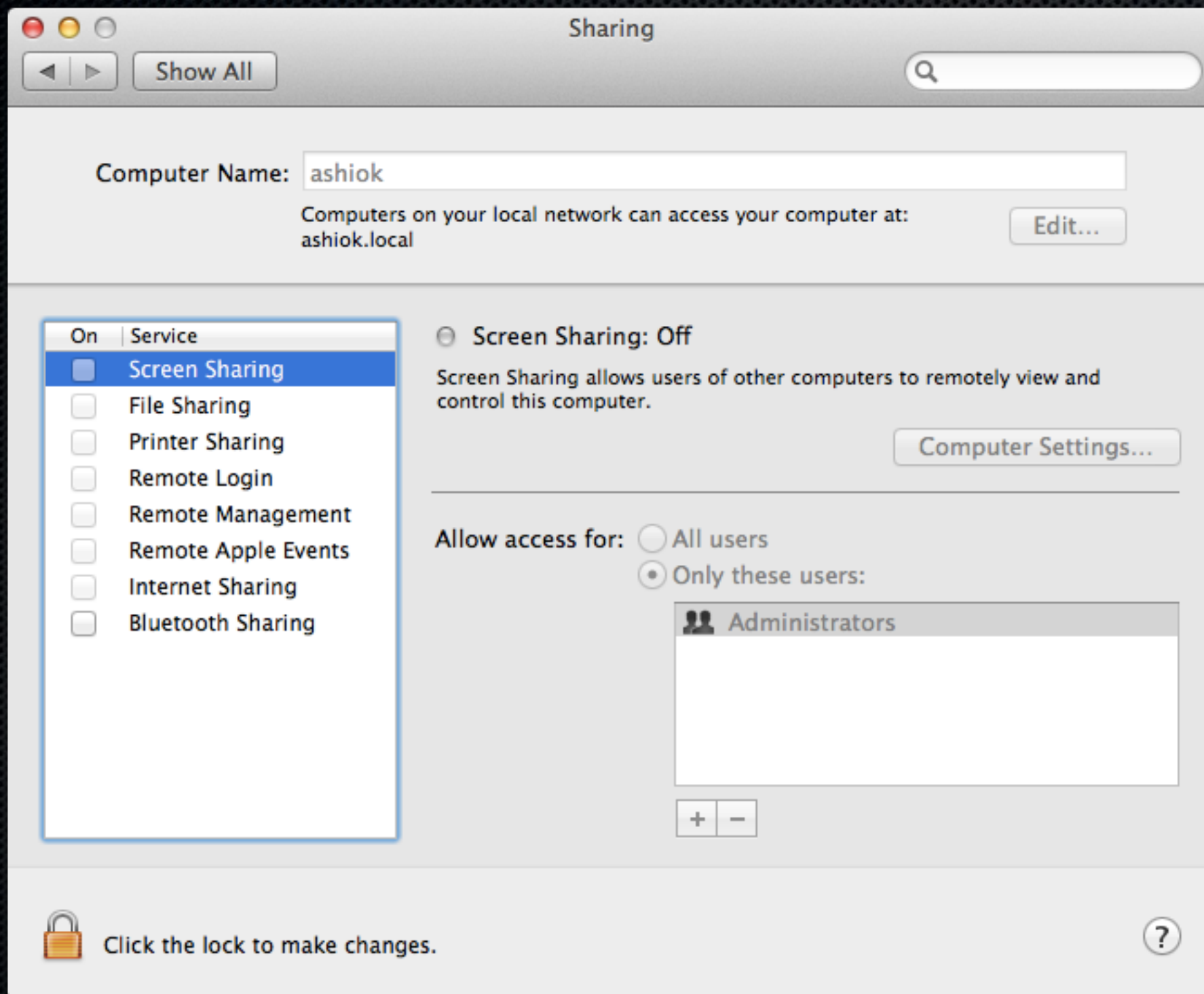


# Basic OS X Hardening



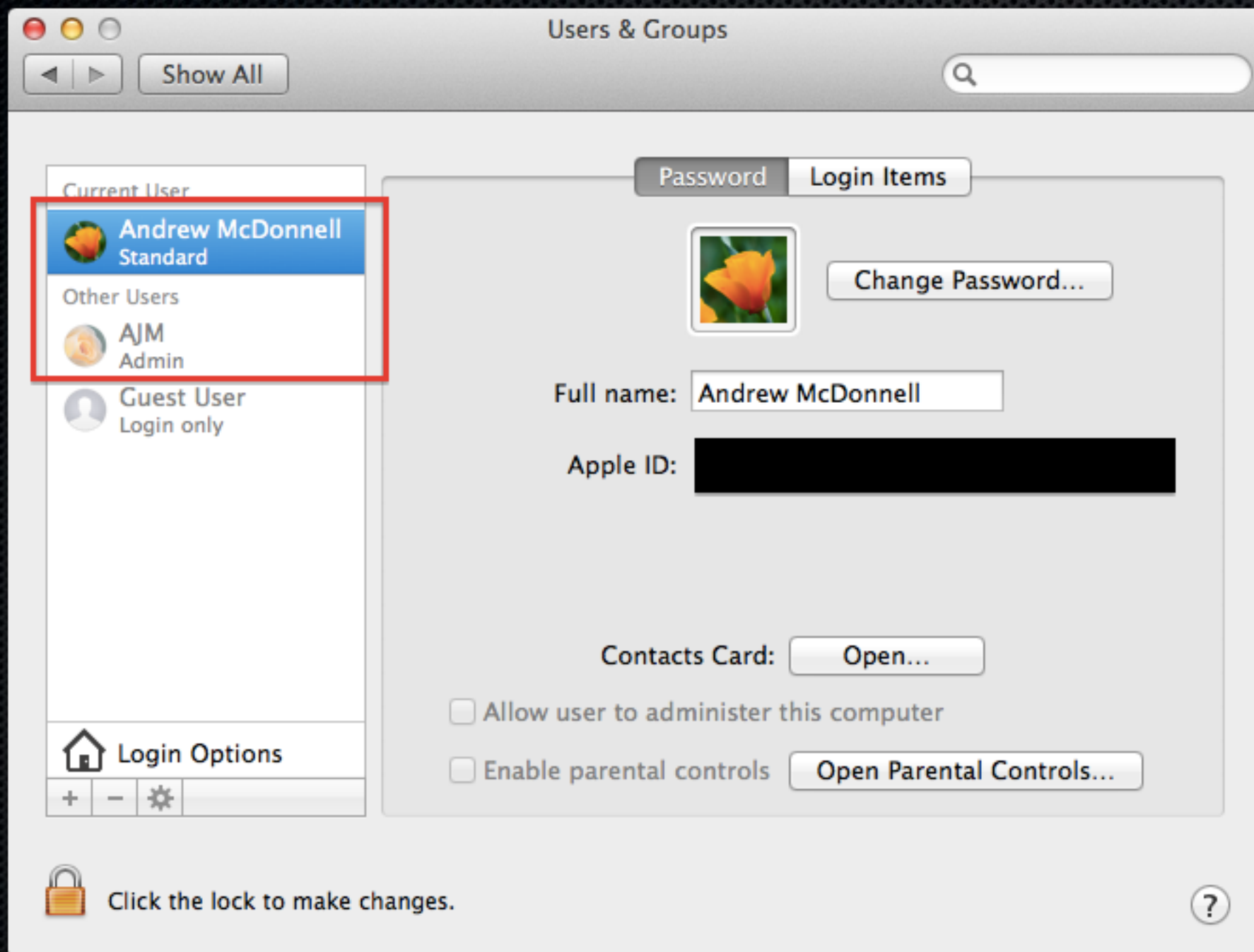


# Basic OS X Hardening



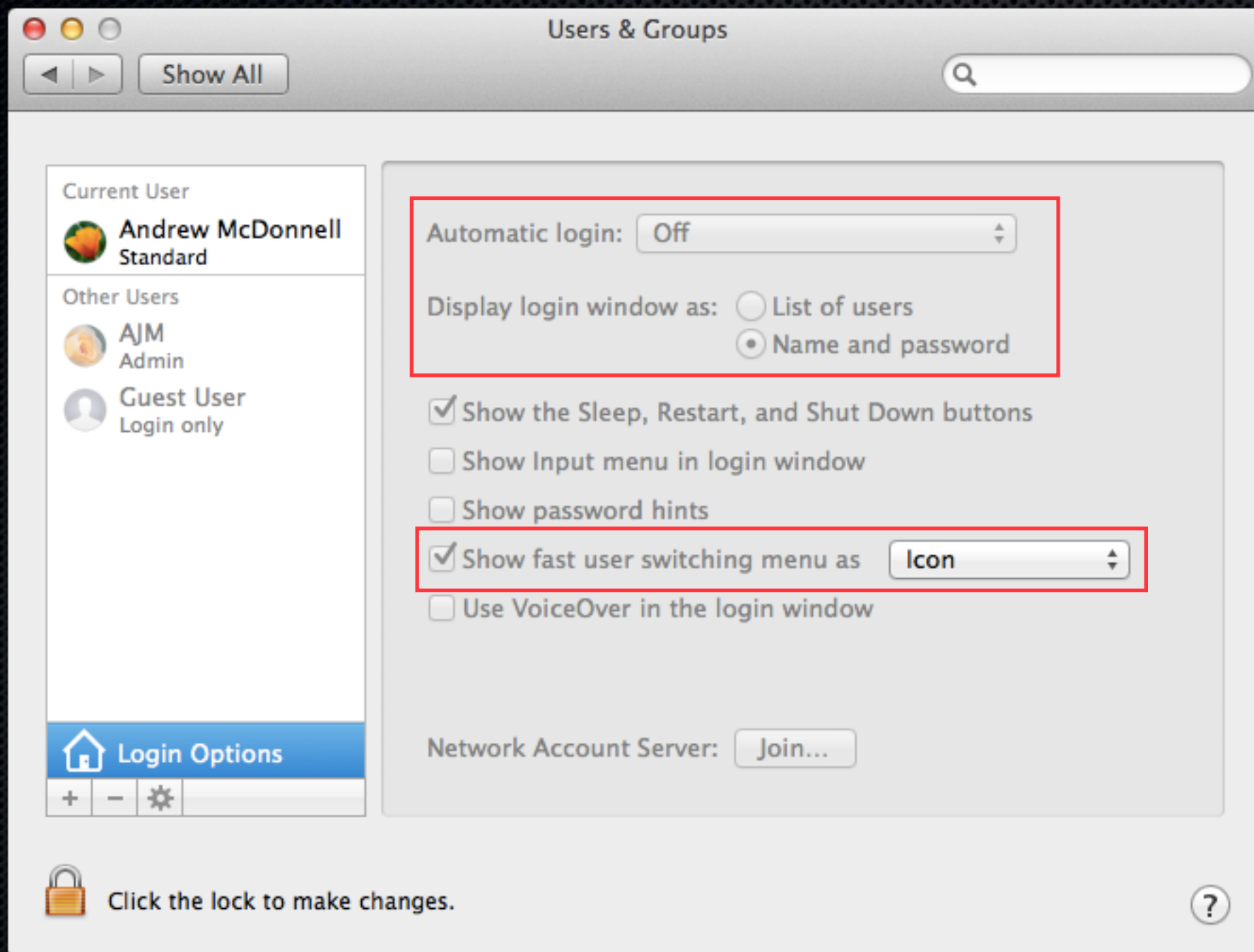


# Basic OS X Hardening



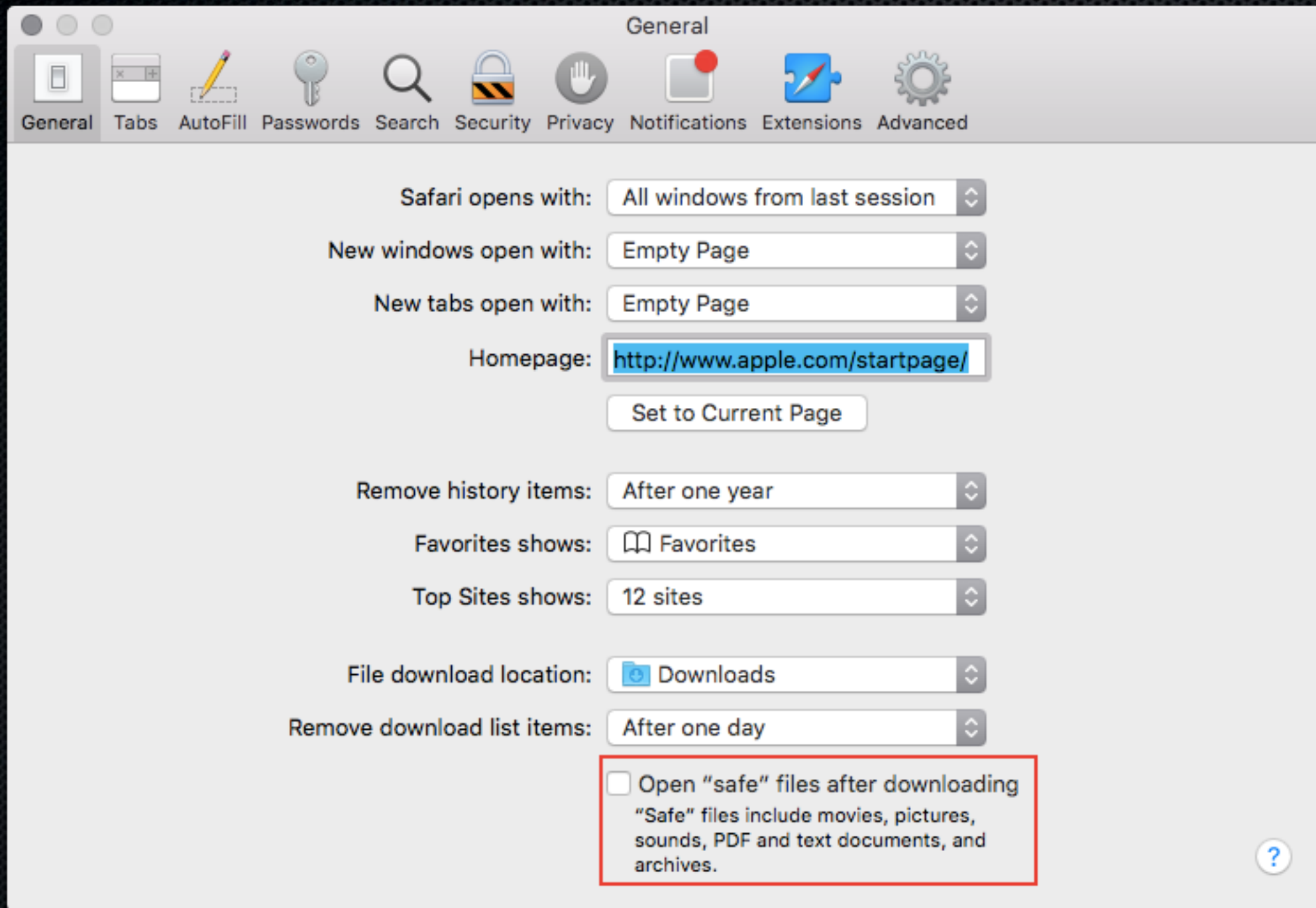


# Basic OS X Hardening





# Basic OS X Hardening





# Get Rid of These





# Managing Endpoints

- Control Spectrum – Users  $\longleftrightarrow$  Administrators
  - Hands-off
  - Shared
  - Locked Down
- Endpoint Protection
  - Policies
  - NAC
  - Definitions
  - Central Management



# Endpoint Protection Tools

- Active vs. Passive – Performance
- Apple
- Kaspersky
- Sophos
- McAfee
- Ghostery
- MalwareBytes



# Impostors

- Genieo / InstallMac
- MacProtector
- MacKeeper
- Avoid good software from bad sources



# More Resources

- [thesafemac.com](http://thesafemac.com)
- [www.us-cert.gov](http://www.us-cert.gov)
- [cve.mitre.org](http://cve.mitre.org)
- [schneier.com](http://schneier.com)
- [arstechnica.com/apple](http://arstechnica.com/apple)
- [krebsonsecurity.com](http://krebsonsecurity.com)
- [astechconsulting.com](http://astechconsulting.com)



# Questions?



Andrew McDonnell  
[andrew@astechconsulting.com](mailto:andrew@astechconsulting.com)