SECURITY
Keeping them out!

Ben Greiner
Forget Computers

ben@forgetcomputers.com

Security Spectrum

Security Spectrum

None | Average | Ultimate

- **High Risk**
- **Low Cost**
- **Low Maturity**

Low Risk •
High Cost •
High Maturity •

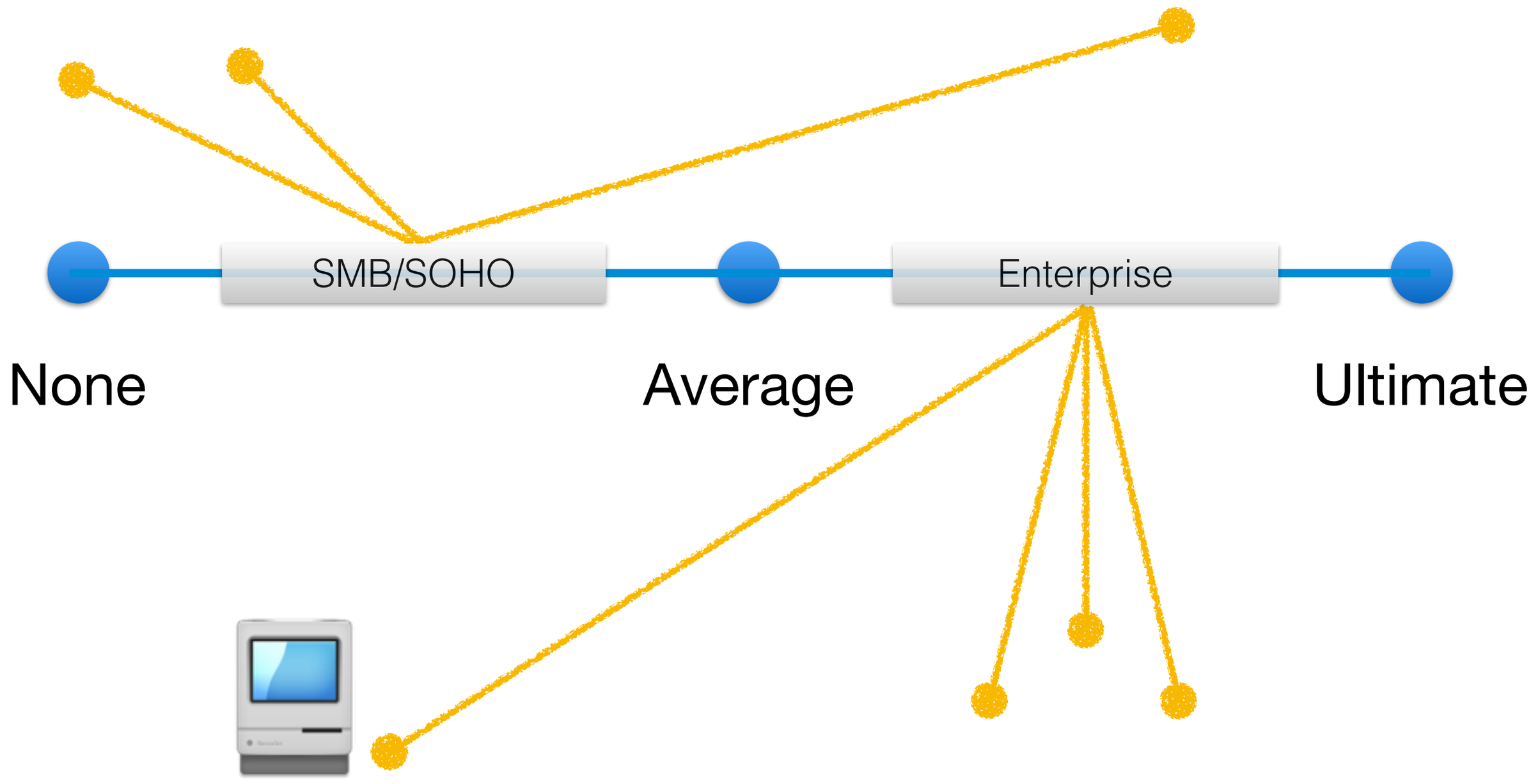
Security Spectrum

None | Average | Ultimate

- **High Risk**
- **Low Cost**
- **Low Maturity**

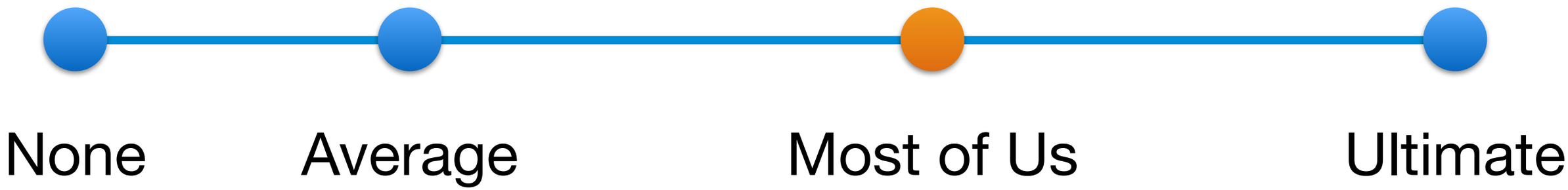
Low Risk •
High Cost •
High Maturity •

Security Spectrum



Security Spectrum

Security Spectrum



Security Spectrum

Security Spectrum

Security Audit

Serious About Security?

Hire a Security Expert
(3rd party auditor)

Security Audit Summary

1. Discovery
2. Document
3. Execute & Enforce

} REPEAT

Discovery

External Penetration Testing

Collect, verify and dive deeper into the security practices of an organization.

Discovery

1. **CANVAS** - With packaged vulnerability scanner with modules for scripting and a powerful framework for developing original security checks, Immunity CANVAS provides a way to have a concrete picture of their security posture, without guesswork or estimation.
2. **Nmap** – A freeware port scanner and traffic generator tool, which can conduct scans using unconventional methods not commonly caught by either an Intrusion Detection System (IDS) or a firewall. Nmap can be used to launch various attacks, including denial of service.
3. **Foundstone** – A commercial security scanning tool for identifying vulnerabilities which can be launched as a service from the Internet or internal to a client via an appliance.
4. **Nessus** – A security scanning tool for identifying vulnerabilities.
5. **Webscanner –** An open-source Perl script used to scan web sites for common configuration errors and software vulnerabilities.
6. **Achilles** – A local web proxy used to test web applications which allows manipulation of input values and cookies sent to the web server.
7. **Burp Proxy –** A Java based web proxy used to capture or alter inbound and outbound http/https traffic which runs on Windows, Linux and Solaris.
8. **Dig – Domain Information Groper -** Included in current Linux distributions, DIG performs various types of Domain Name Service lookups.
9. **Ike-scan –** An open source VPN server scanning tool. Ike-scan attempts to establish an ike (VPN) connection with target hosts and reports successful connections.
10. **BRUTUS -** A password cracking utility with the capability of connecting on well-known ports to accomplish its attacks.
11. **Unix/Linux Utilities (Nslookup, Ping, Traceroute …) -** Several built-in Unix/Linux utilities.
12. **Ethereal –**A Unix and Windows network packet sniffer also capable of displaying packets captured by a number of other tools.

Document

Security Policies

[Written]

Written documents that describe how an organization can best protect itself from various threats, including a list of steps to be taken should certain security-related events take place.

Document

CO-PO-001 Corporate Governance Policy.docx
CO-ST-001 Corporate Policy, Standard & Procedure Format Standard.docx
IT-PO-001 Information Security Policy.docx
IT-PO-002 Password Policy.docx
IT-PO-003 Change Management Policy.docx
IT-PO-004 Patch Management Policy.docx
IT-PO-005 HR Policy.docx
IT-PR-001 Change Management Standard and Procedure.docx
IT-ST-001 Acceptable Use of Electronic Mail Standard.docx
IT-ST-003 Acceptable Use of the Internet Standard.docx
IT-ST-004 Acceptable Use of Telephones Standard.docx
IT-ST-005 Physical Security Standard.docx
IT-ST-006 System Planning and Acceptance Standard.docx
IT-ST-007 Problem and Incident Reporting Standard.docx
IT-ST-008 System Logging and Monitoring Standard.docx
IT-ST-009 Information Backup Standard.docx
IT-ST-010 Configuration Management Standard.docx
IT-ST-011 Network Management Standard.docx
IT-ST-012 Network Access Management Standard.docx
IT-ST-013 Malware Management Standard.docx
IT-ST-014 Application Management Standard.docx
IT-ST-016 Access Management Standard.docx
IT-ST-017 Asset Inventory Standard.docx
IT-ST-018 Risk Management Standard.docx
IT-ST-019 Service Level Management Standard.docx
IT-ST-020 Third Party Services Management Standard.docx
Visio-Change Management workflow.docx
Visio-Incident Management Process Flow.docx

Execute & Enforce

Security Policies

[Automations]

Policies that are enforced on all devices to best protect the company information from various threats.


STOP
KQED 9

Find Balance

“Balance between the needs to protect the organization and run the business.”

Use Automation!

- OS and App Patching
- AntiVirus/Malware (ClamXav)
- Disable Automatic Login
- Require Login Passcode
- Require Screen Saver Passcode
- FileVault Encryption (w/stored keys!)
- Rootkit Hunter (on servers)
- Restrict software from launching
- Restrict Gatekeeper settings
- Set Lock Message on iPhones and Macs.

One Problem

Awareness
[SMB and SOHO]

Security takes time and money!

Many small businesses don't value and are not willing to pay for security.

Build Awareness

Client Education

Get them thinking about security —
at home and at work.

What can I do today?

What are we protecting?

Keep them out of …

Network

Safe.
In-house.

Cloud

Scary.
Out there!

Devices

Data,
Everywhere!?

The Network

Traditionally, a firewall device.

BASIC
Change default passwords on devices!
(Routers, wireless access points, VoIP phones, everything!)

ADVANCED
RADIUS (Remote Authentication Dial In User Service),
or certificate based authentication.

The Cloud

BASIC
Enforce *strong* passwords.

ADVANCED
Hosted Identity Management,
with support for Two-factor and Certificates.

Hosted ID Management

- SAML (Secure Assertion Markup Language)
- SSO (Single Sign-On)
- Multi-Factor (Two-Factor) Authentication
- Directory Integration (in-house AD)
- Certificates

Hosted ID Management

SAML / 2-Factor / Certificates

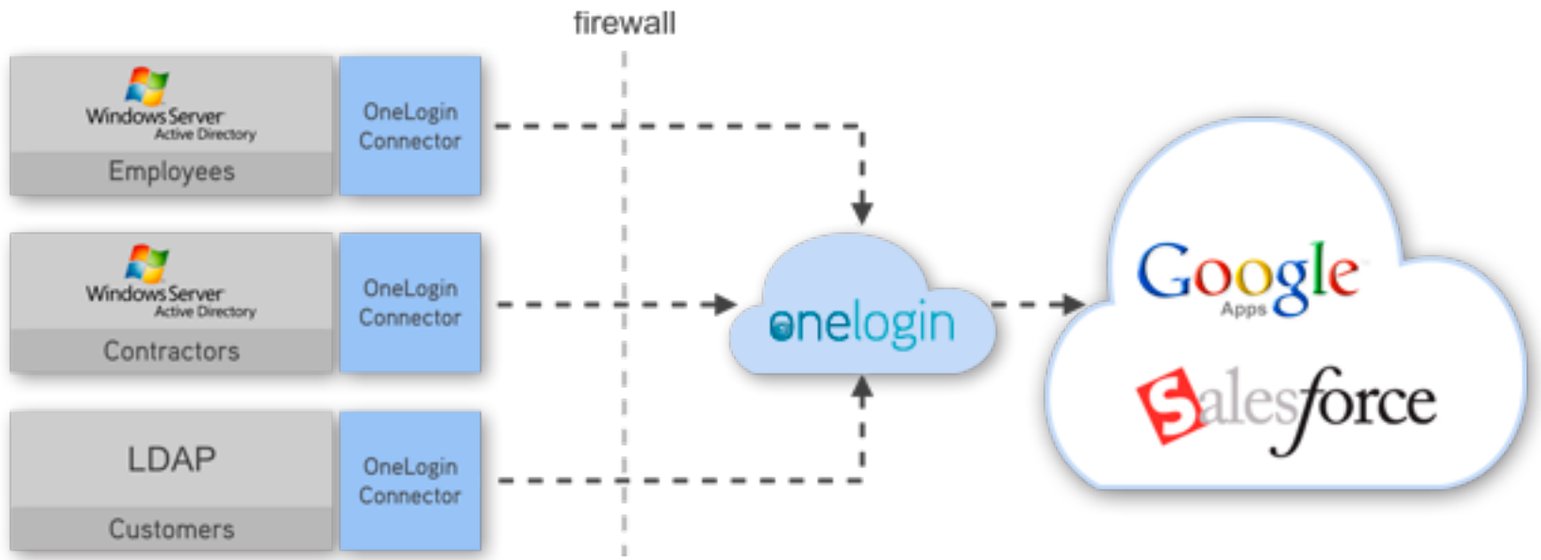
BALANCE

Beware, it’s not always practical.

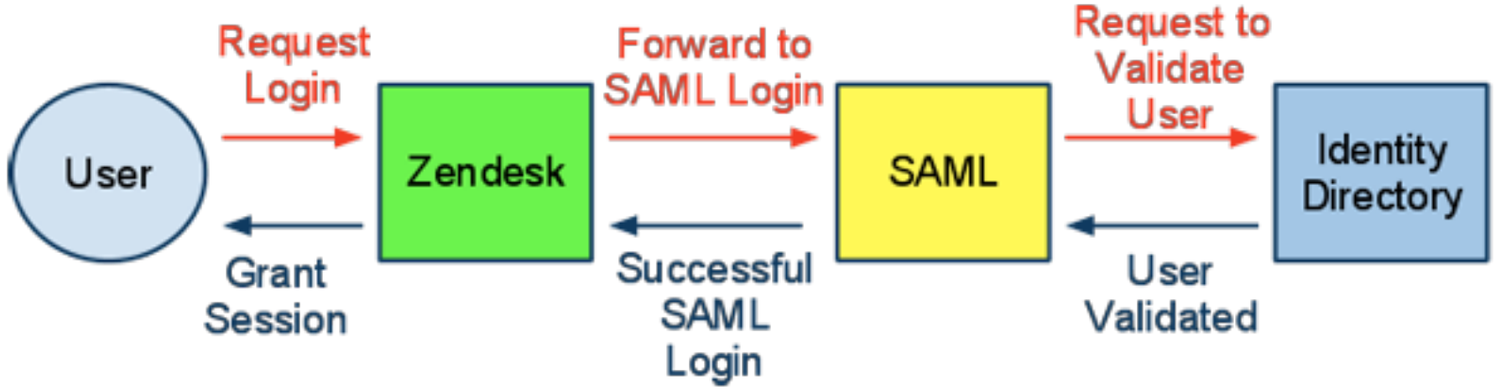
Can’t yet force100% across all devices.

(web vs apps)

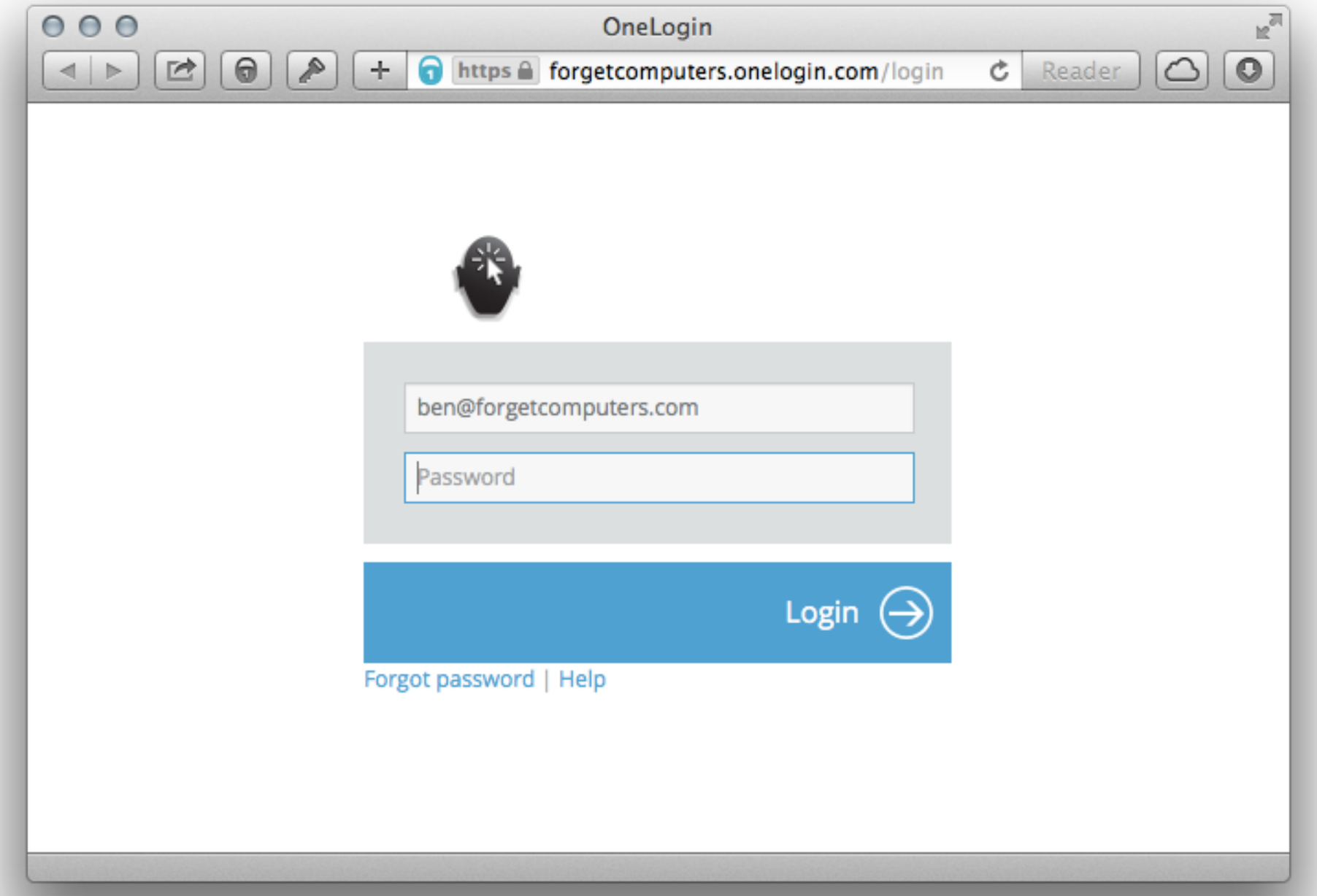
Hosted ID Management



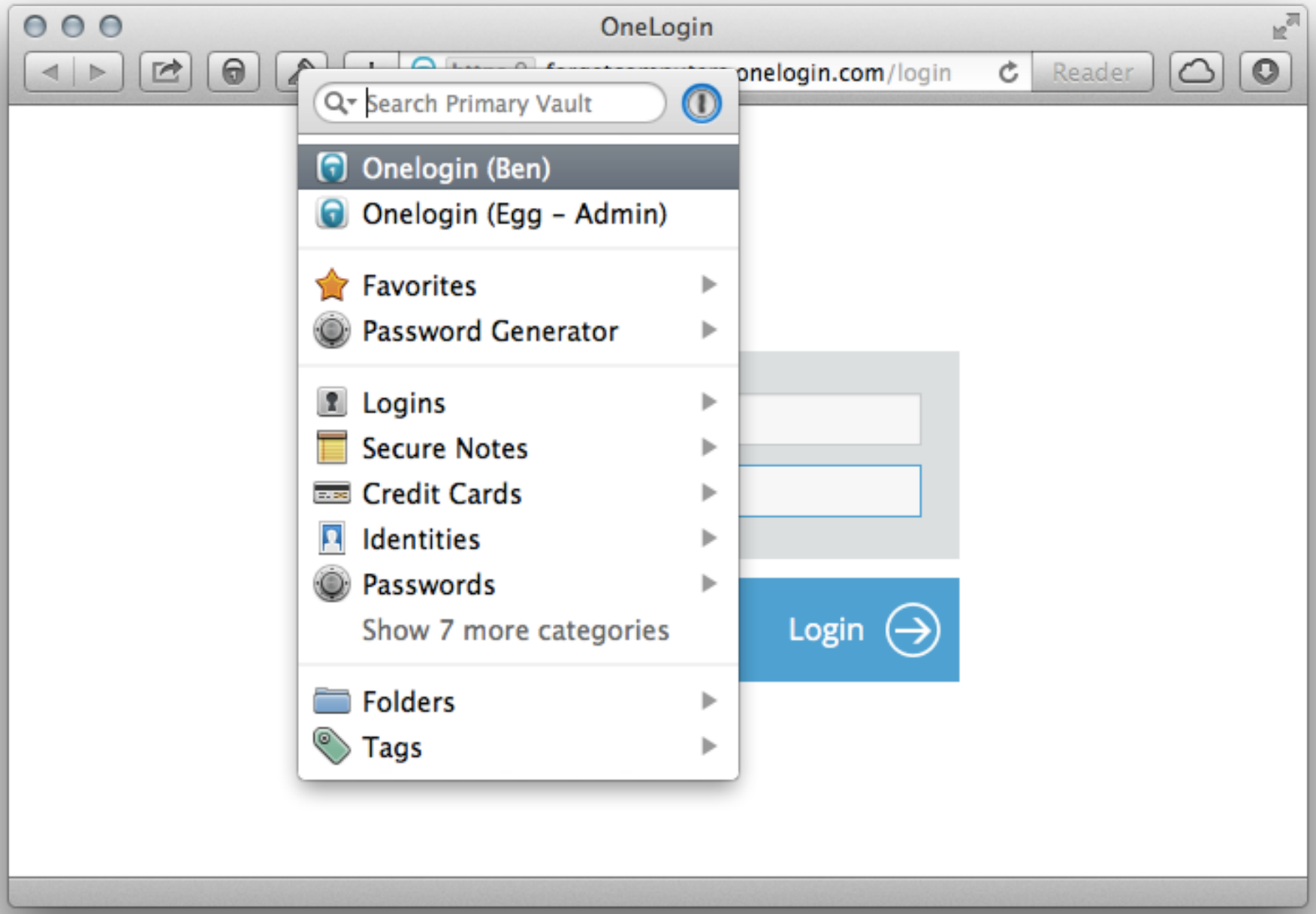
Hosted ID Management



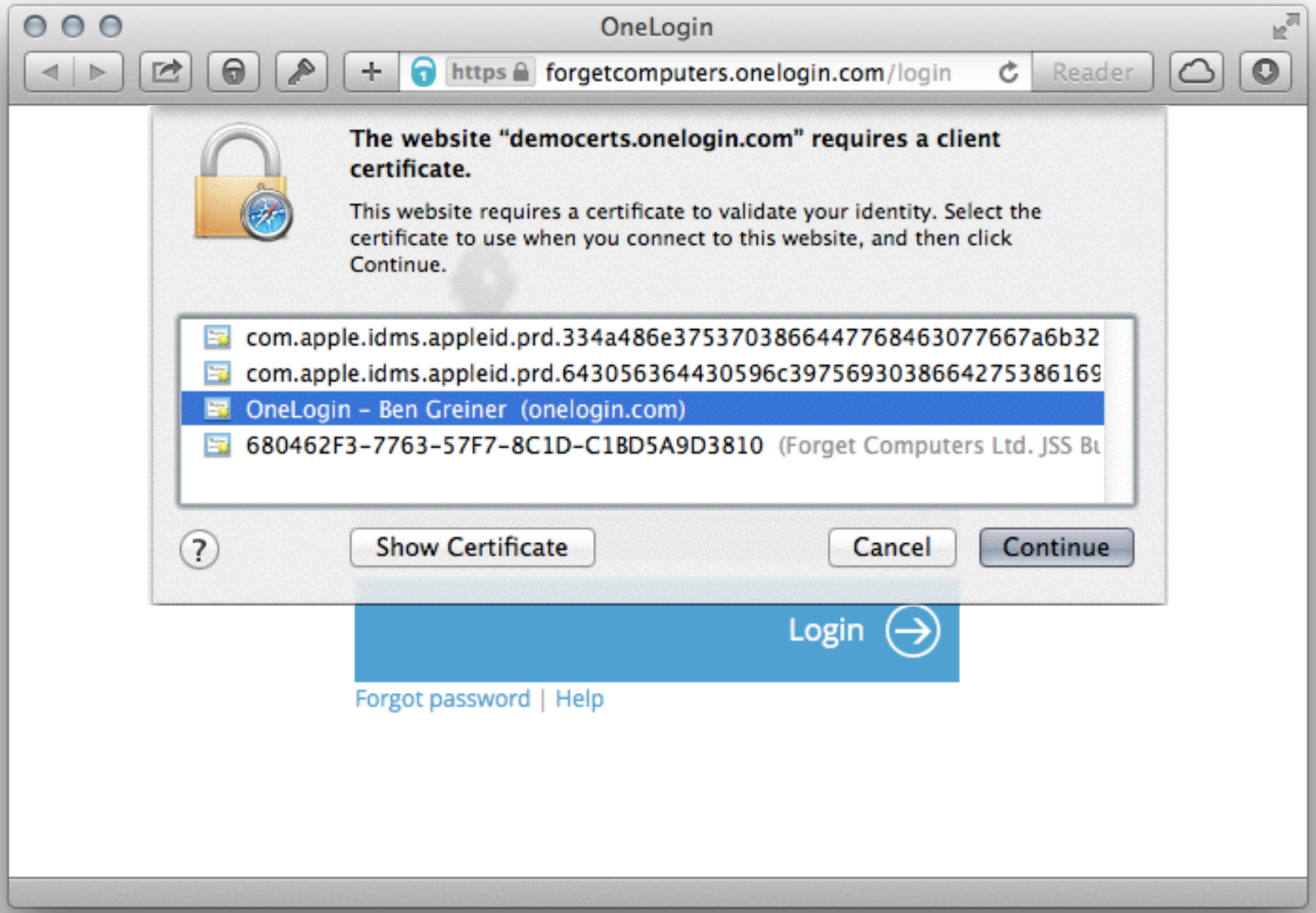
Example


OneLogin
https
forgetcomputers.onelogin.com/login
Reader
ben@forgetcomputers.com
Password
Login
Forgot password | Help

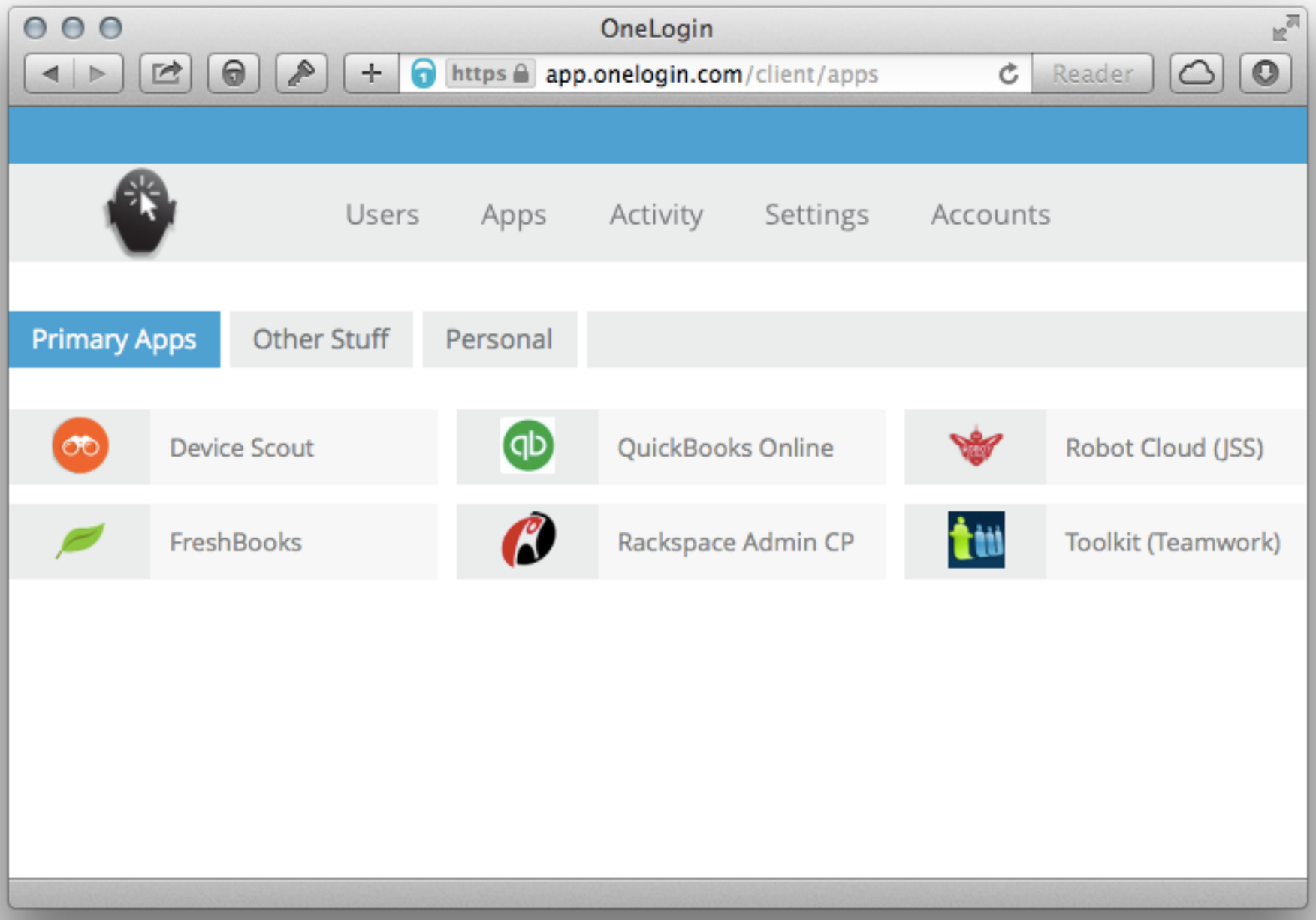
Example


OneLogin
onelogin.com/login
Reader
Search Primary Vault
Onelogin (Ben)
Onelogin (Egg – Admin)
Favorites
Password Generator
Logins
Secure Notes
Credit Cards
Identities
Passwords
Show 7 more categories
Folders
Tags
Login

Example


OneLogin
https
forgetcomputers.onelogin.com/login
Reader
The website "democerts.onelogin.com" requires a client certificate.
This website requires a certificate to validate your identity. Select the certificate to use when you connect to this website, and then click Continue.
com.apple.idms.appleid.prd.334a486e375370386644776846307766 7a6b32
com.apple.idms.appleid.prd.643056364430596c3975693038664275386169
OneLogin - Ben Greiner (onelogin.com)
680462F3-7763-57F7-8C1D-C1BD5A9D3810 (Forget Computers Ltd. JSS Bu
Show Certificate
Cancel
Continue
Login
Forgot password | Help

Example


OneLogin
https
app.onelogin.com/client/apps
Reader
Users
Apps
Activity
Settings
Accounts
Primary Apps
Other Stuff
Personal
Device Scout
QuickBooks Online
Robot Cloud (JSS)
FreshBooks
Rackspace Admin CP
Toolkit (Teamwork)

Devices

BASIC
Enforce strong passwords.

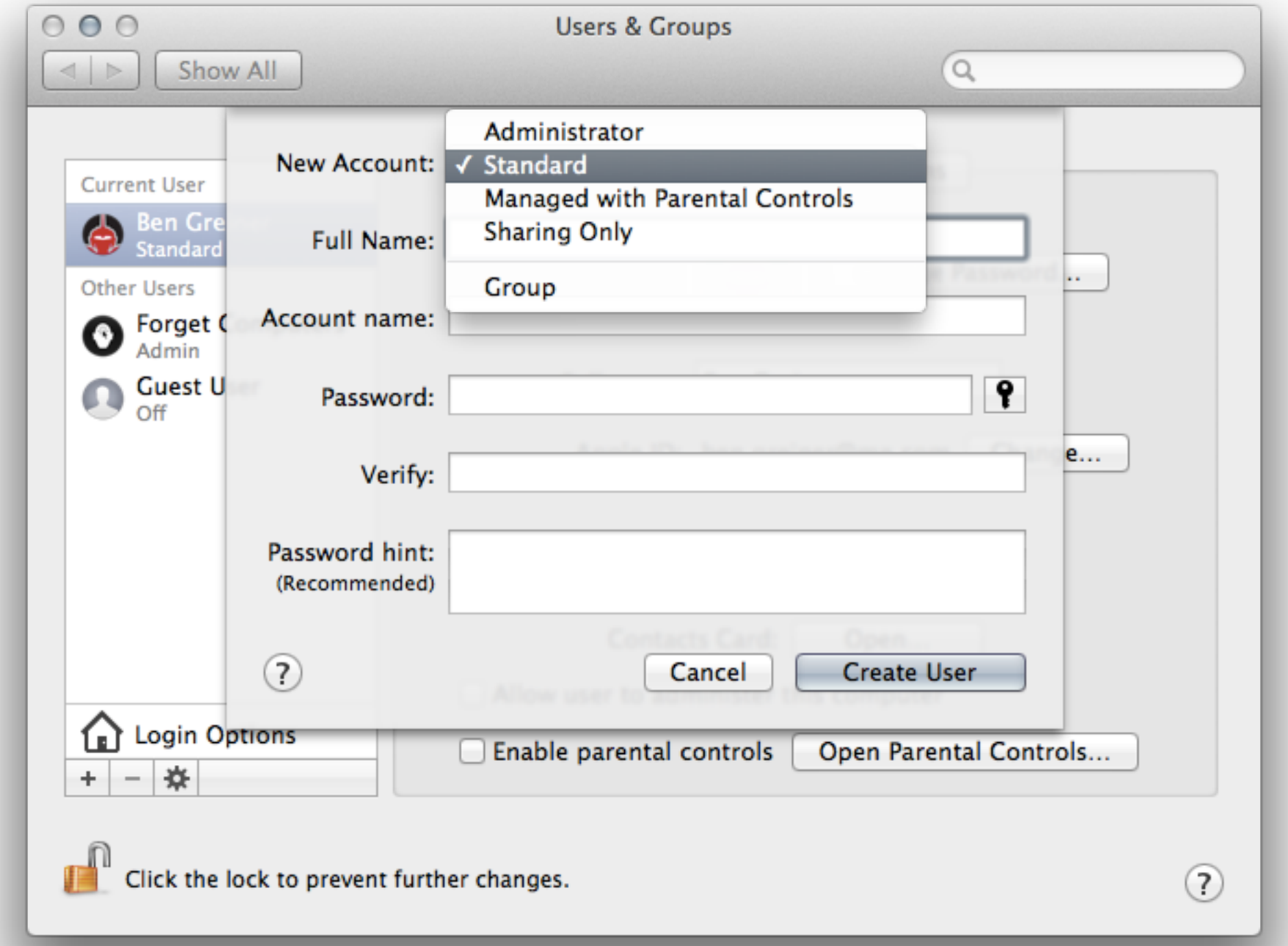
BASIC+
Find My Mac and Find My iPhone.
Activation Lock!

ADVANCED
Leverage ActiveSync (still pretty basic),
or a full management solution with security policies.

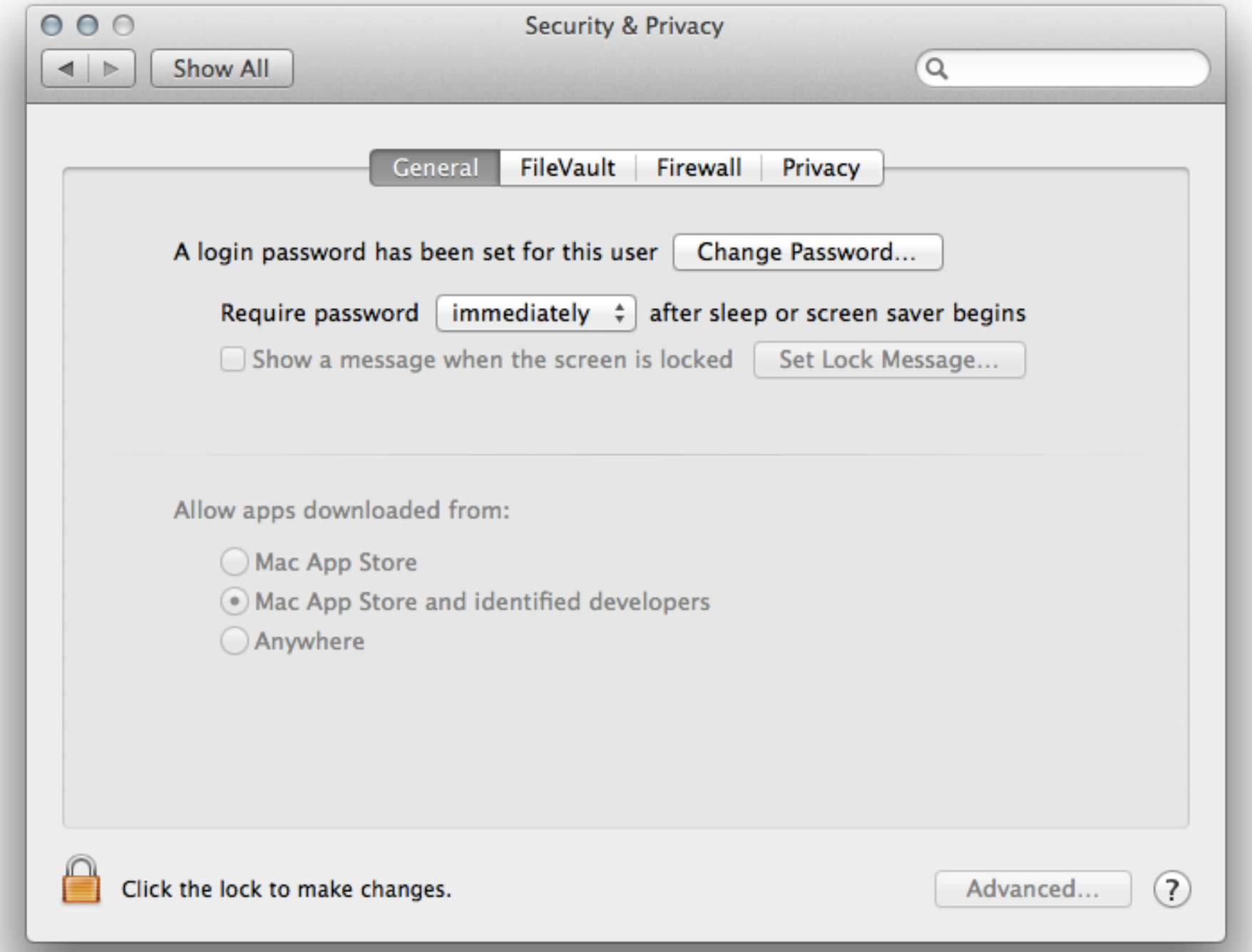
Devices


Old Location
Ben's MacBook Air Gen 2
Yesterday at 6:58 PM
Notify me when found
Play Sound
Lock
Erase Mac

Basic Mac Security

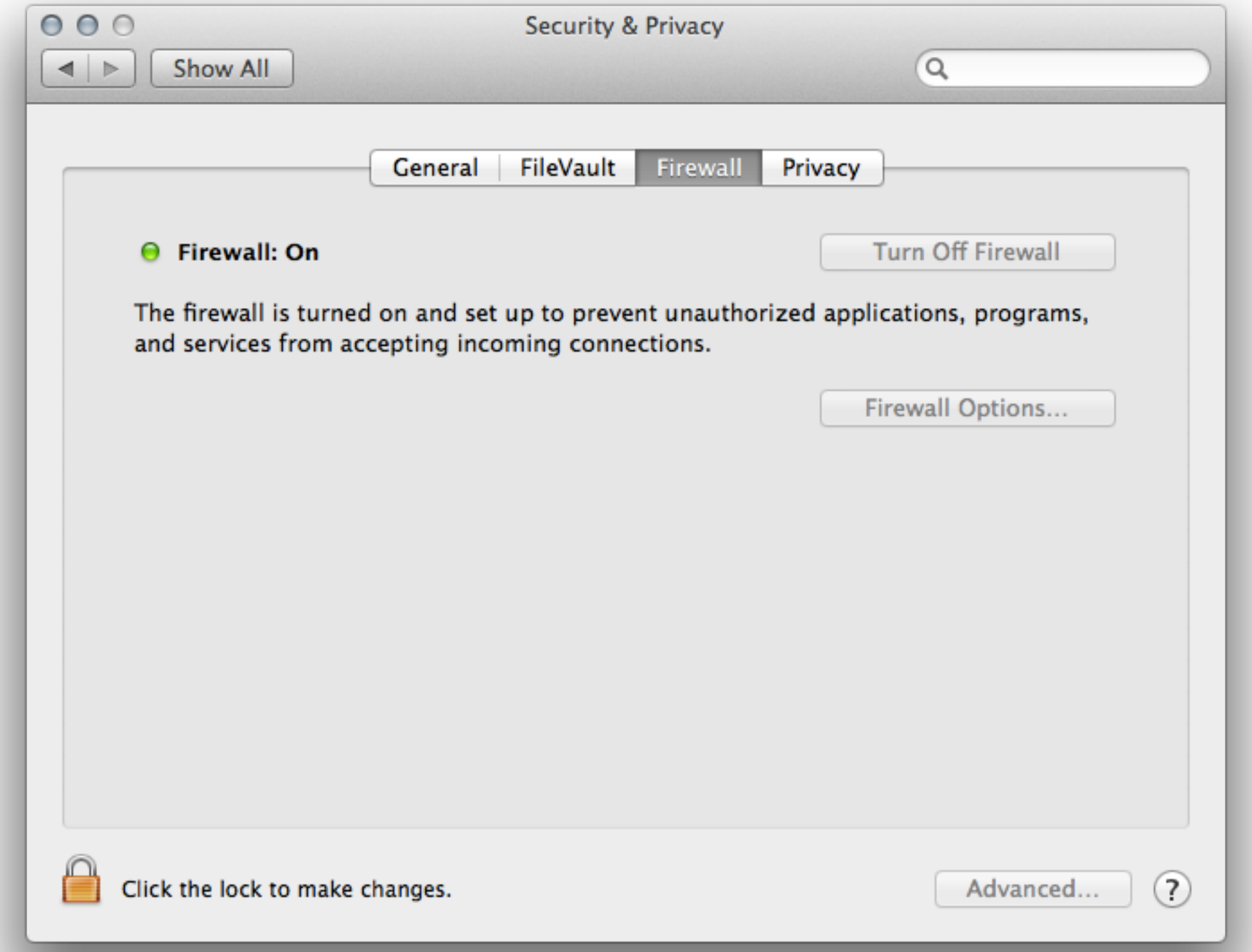


Basic Mac Security

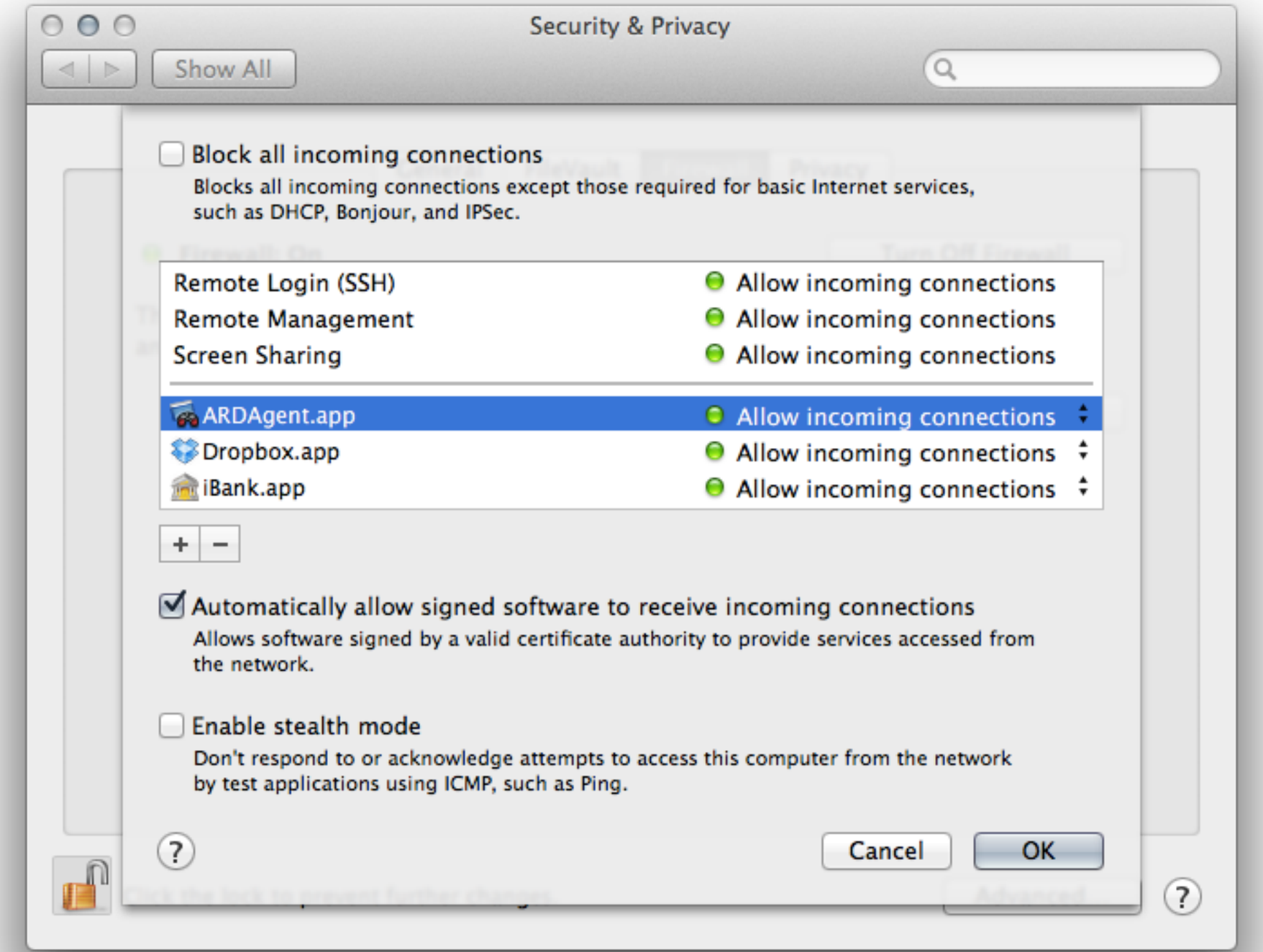


Basic Mac Security

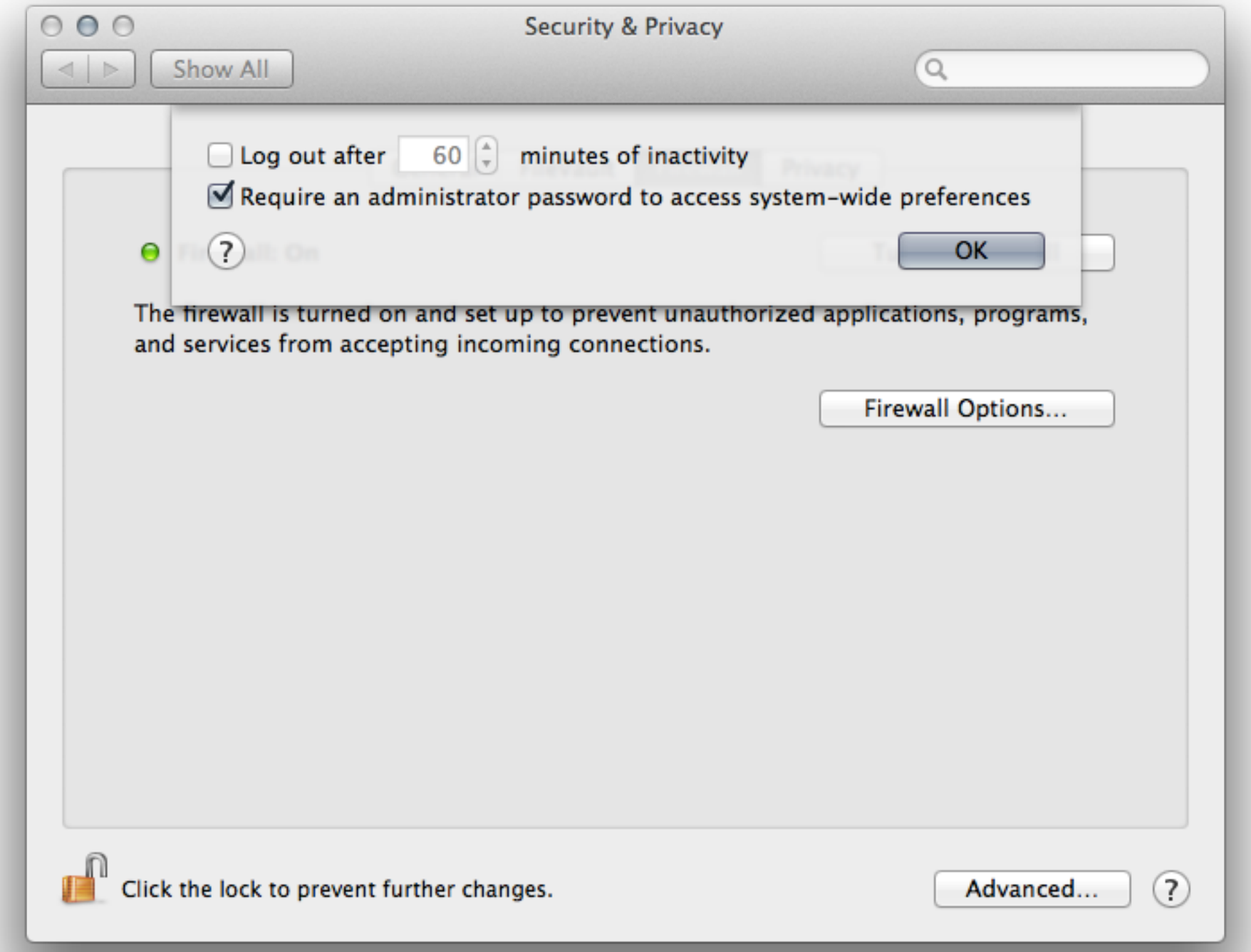
Basic Mac Security



Basic Mac Security



Basic Mac Security



Password Management

iCloud Keychain

Your passwords. Stored, encrypted,
and automatically entered.

Multiple and Shared Vaults

Securely share with family or team members

Email Encryption

Challenging!

Encrypt At Rest

iOS 8 will have *per-message*
signing and encryption.

Let’s Review

[And get really basic]

The Basics

[FIRE-E]

1. **Forget**: Your passcodes (all but a few).
2. **Inventory**: Know what you're protecting.
3. **Run**: As a Standard User.
4. **Encrypt**: FileVault (passcodes required).
5. **Enable**: Find my Mac/iPhone.

Forget

frgt.co/1PW-MacTech

25% discount through the end of July.

Inventory

Mac

iPhone

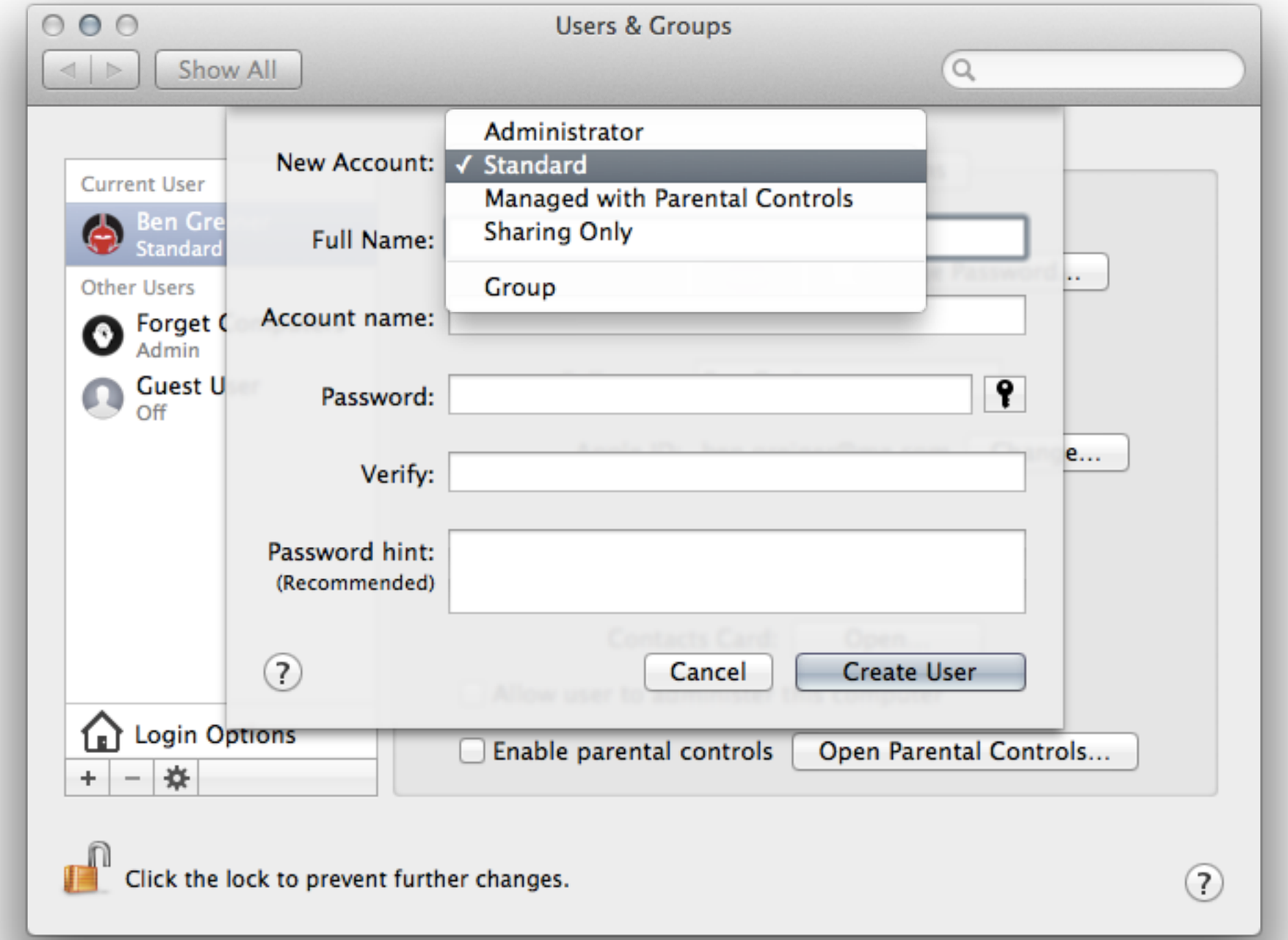
iPad

Apple TV

iCloud

Apple ID

Run

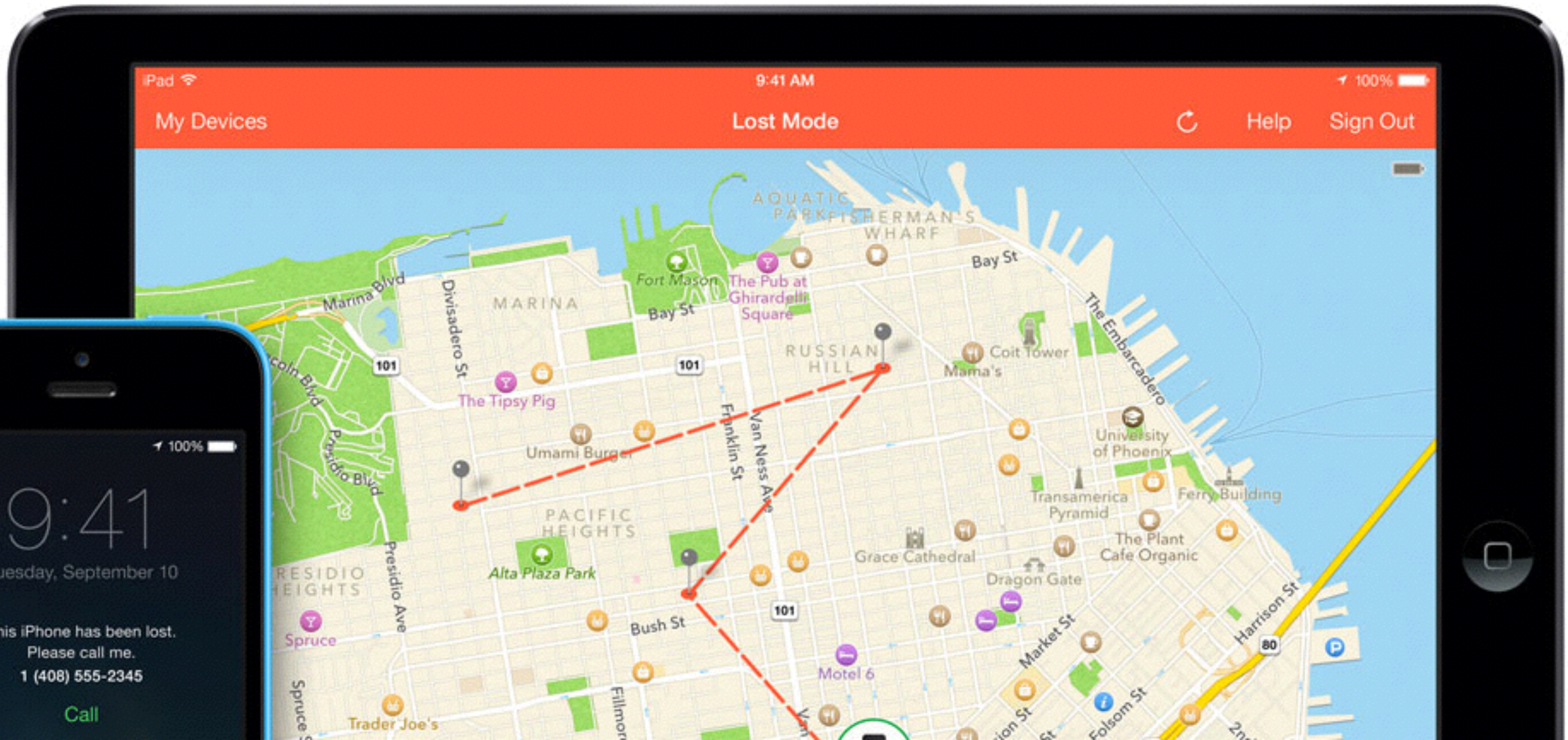

Users & Groups
Show All
Current User
Ben Gre
Standard
Other Users
Forget C
Admin
Guest U
Off
Login Options
New Account:
Administrator
Standard
Managed with Parental Controls
Sharing Only
Group
Full Name:
Account name:
Password:
Verify:
Password hint:
(Recommended)
Cancel
Create User
Enable parental controls
Open Parental Controls...
Click the lock to prevent further changes.

Encrypt

(FileVault or other disk encryption)

Enable

(Find my Mac/iPhone)



Do The Basics

[FIRE-EE]

1. **Forget**: Your passcodes (all but a few).
2. **Inventory**: Know what you're protecting.
3. **Run**: As a Standard User.
4. **Encrypt**: FileVault (passcodes required).
5. **Enable**: Find my Mac/iPhone.
6. **Enforce**: Can't trust the users.

Enforce

MDM/Supervision/Profiles

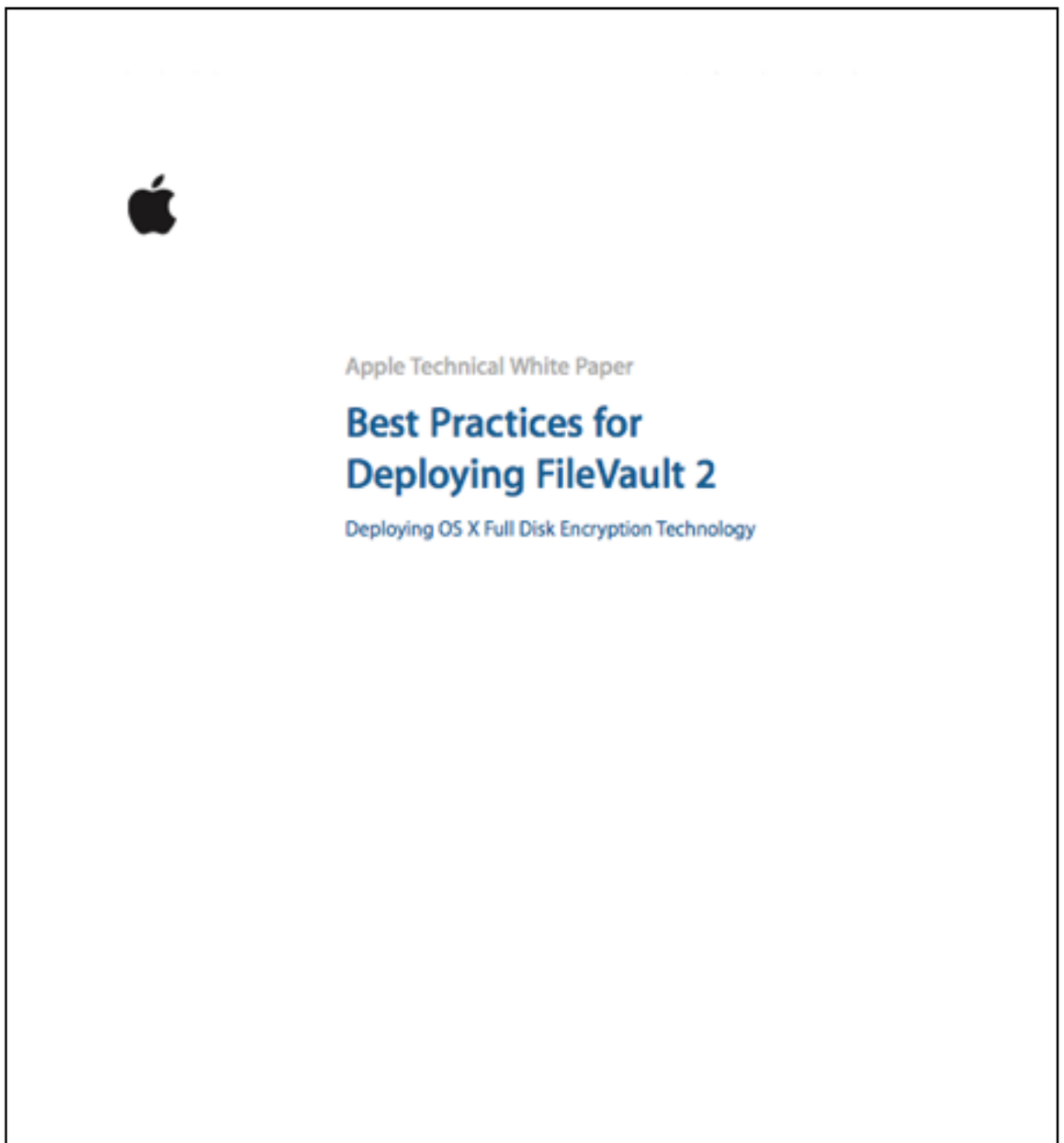
- Passcodes
- Restrictions
  - AirDrop
  - iMessage (SMS)
- Managed Apps
- Single App Mode (Kiosk)
- AirPlay
- Web Content Filter

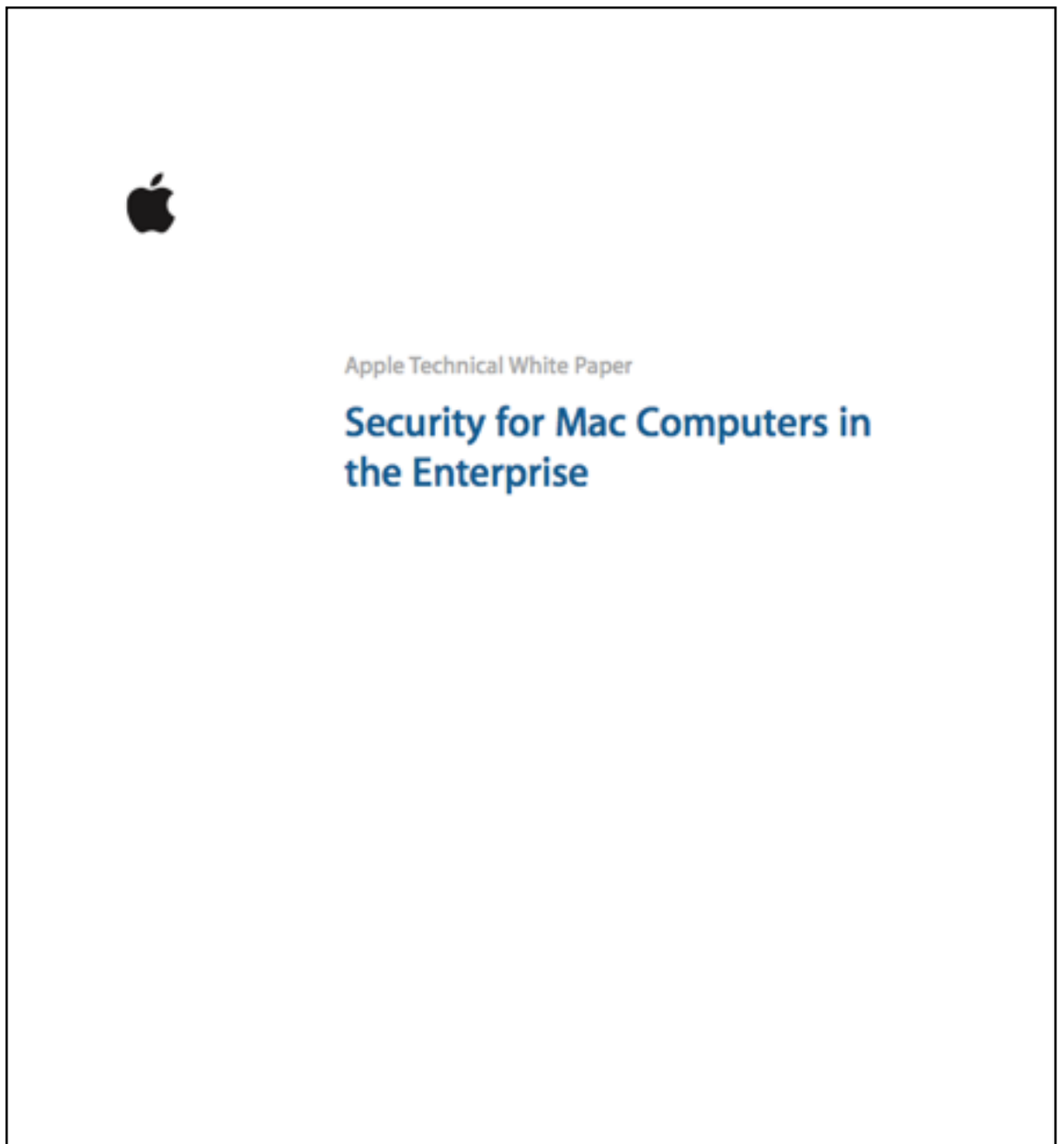
Summer Reading

Summer Reading

- https://gotofail.com
- http://www.knocktounlock.com
- https://agilebits.com
- Six Steps to Better Mac & iOS Security http://frgt.co/1tvn1s9
- GPGTools - It's worth protecting what you love http://frgt.co/WxBp8q
- PGP for iOS - iPGMail http://frgt.co/1lr2rnl
- Email encryption: Using PGP and S/MIME - TechRepublic http://frgt.co/1pB3B2v
- The best PGP tutorial for Mac OS X, ever | Jerzy's Notes http://frgt.co/WxC9KC
- S/MIME mail encryption in iOS 8 … Eight reasons why iOS 8 is going to be a big hit with BYOD | ZDNet http://frgt.co/1uc0NQ0
- The Rootkit Hunter project http://frgt.co/1ryGudE
- How to track a lost computer with Find My Mac | Macworld http://frgt.co/1rt7zNy
- Why I Phished My Own Company - Tom Cochran - Harvard Business Review http://frgt.co/WxKw93
- OneLogin Channel Program | OneLogin http://frgt.co/1nxZtmK
- http://twofactorauth.org
- https://securityinabox.org/en
- The Most Overlooked Part of Your Data Security - Kyle Marks - Harvard Business Review http://frgt.co/1sMT7Sv
- How to Get Funding for Your Security Program http://frgt.co/1rsWVGC
- Creating your physical security policy | Security In A Box http://frgt.co/1ueYICT
- Harvard Business Review: 3 Key Cyber Security Questions | http://frgt.co/1tzYlia
- Harvard Business Review Posts Terrible Advice for CEOs on Information Security http://frgt.co/1z23KSa
- Target Hackers Broke in Via HVAC Company — Krebs on Security http://frgt.co/1nUqiMa

Apple White Papers





Q&A

Ben Greiner
Forget Computers

ben@forgetcomputers.com

Thank you!

Ben Greiner
Forget Computers

ben@forgetcomputers.com