Security:
Making Mavericks Work for You!

Samuel Keeley

Why Security?

- Protection
  - User Data
  - Intellectual Property
- Controlling risk
- Third-party software flaws

Topic: Enterprise Software | Investigate

Follow via:

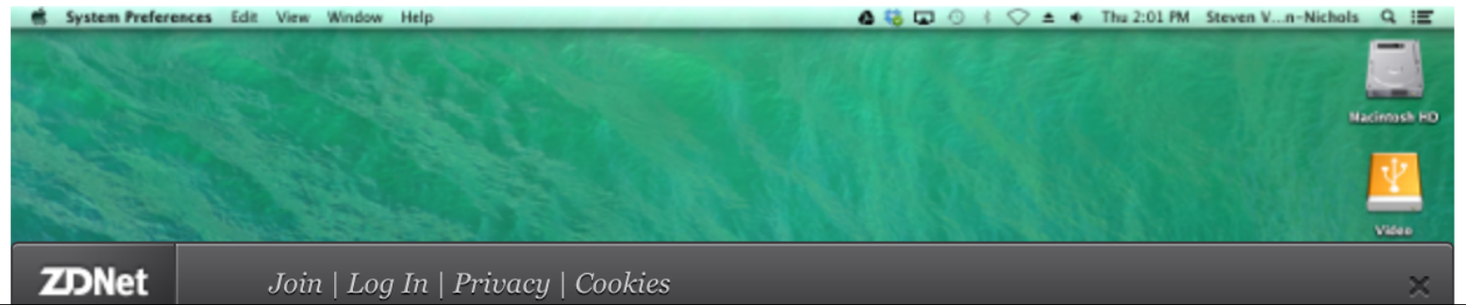
Mavericks: The end of Macs in the enterprise?

Summary: *Macs have never been that popular in business. But if Apple is indeed no longer supporting security updates for older Mac OS X versions, Macs won't have any place left in the enterprise office.*

By Steven J. Vaughan-Nichols for Between the Lines | October 24, 2013 -- 20:01 GMT (13:01 PDT)
Follow @sjvn

[UPDATE: An Apple spokesperson told ZDNet the company has not changed its update policy but said some older OS X versions go unpatched for architectural reasons. Apple declined to respond to a request for more details about their security update policy or for when the most recently disclosed vulnerabilities would be patched in Mountain Lion.]

Macs have never been that popular in the enterprise office. Sure, people love their MacBook Airs and their MacBook Pros, but CIOs usually frown at their price-tags. Still, the shiny Macs laptops have induced some big businesses, including ZDNet's own parent company CBS Interactive, to buy these high-end laptops and, thanks to the Adobe Creative Suite/Creative Cloud, publishing, graphics design, and Web design departments all still use and love their Macs. Well, they do for now. They may not tomorrow because of Apple's lack of security updates for older versions of Mac OS X.



Related Stories


5 reasons for having an enterprise app store

HP's global CISO Brett Wahlin on the future of security and risk


Microsoft's Q1: New reporting structure, same old problems

Juniper throws its hat into the open-source SDN ring

Summary: *Macs have never been that popular in business. But if Apple is indeed no longer supporting security updates for older Mac OS X versions, Macs won't have any place left in the enterprise office.*

Macs have never been more popular in business. But if Apple is indeed no longer supporting security updates for older OS X versions, outdated workflows and sysadmins supporting them won't have any place left in the enterprise office.

Managed Updates


MICROSOFT WINDOWS
Version 3.1
Copyright © Microsoft Corporation 1985-1992.
All Rights Reserved.
18.11.2010
9:37
Cheetos
Crunchy
Mtn Dew
24 cans

NetWare for Mac OS X v2.0

NetWare for Mac OS X

PROSOFT engineering, inc.

Login | Mounts

Guest

Registered User

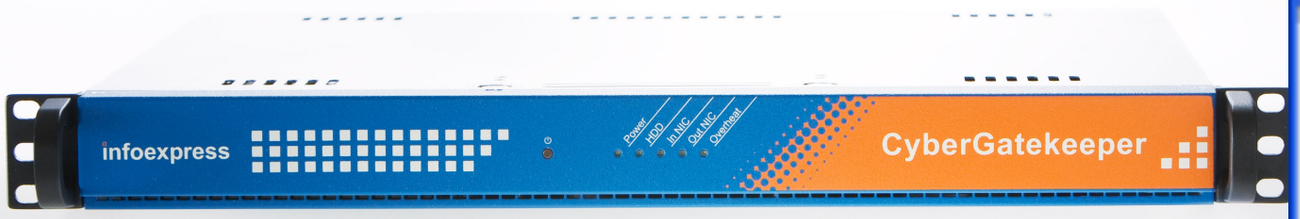
Username: user

Password:

Tree: NETWARE6

Context: TECHIES

Login



Kaspersky Security

Reports | Preferences | Support | Help

Full Scan | Quick Scan | Virus Scan

File Anti-Virus
Enabled

Web Anti-Virus
Enabled

Full Disk Encryption User Account Identification

Check Point
Endpoint Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

Enter your user account name and password to logon.

User account name

Password

SSO Active

Enable WIL

OK | Change Password | Remote Help

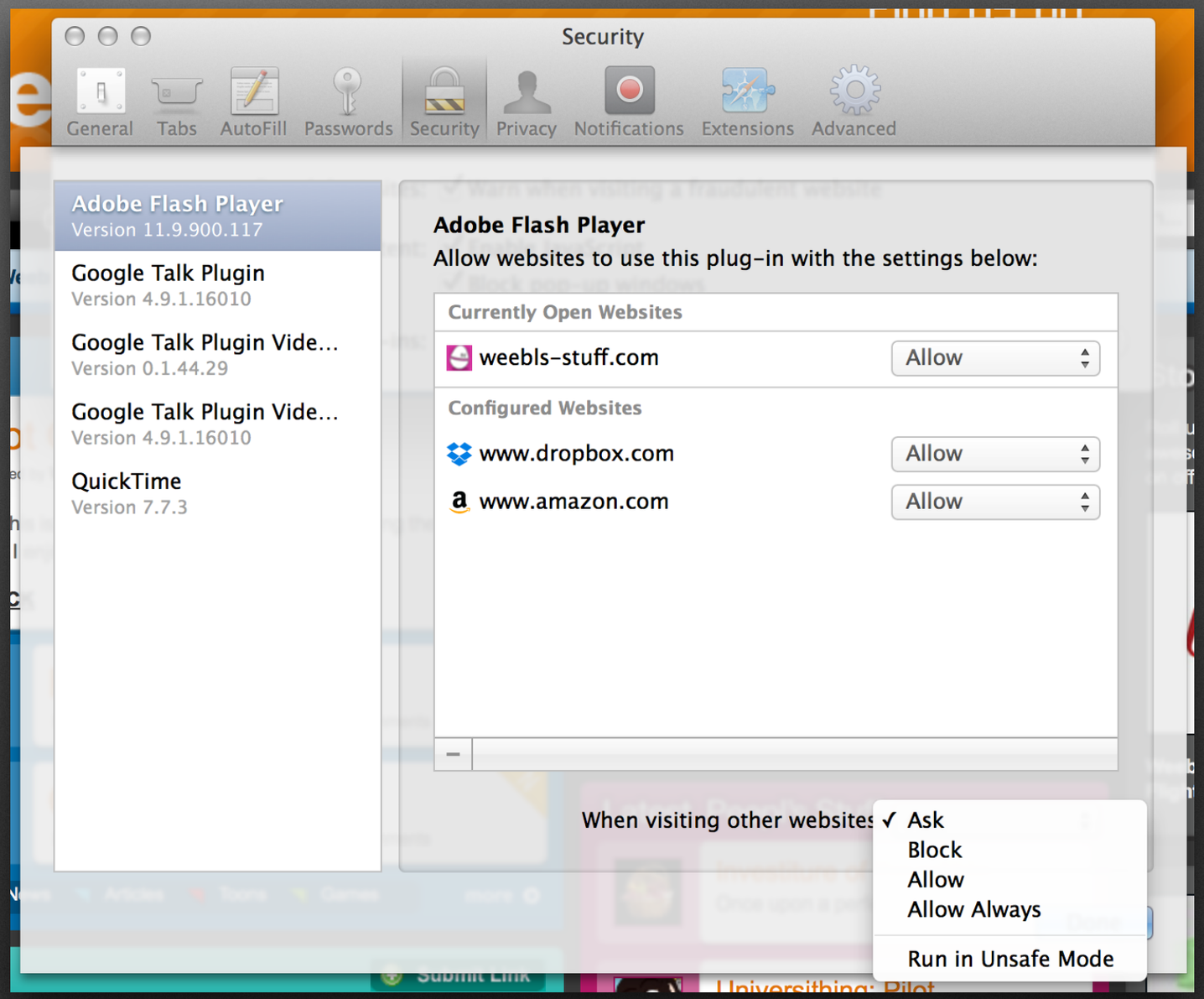
Secure Your Macs!

- Create, implement, and document a security policy.
- Ensure this policy is generally in-line with existing IT policy.
- Enforce policy to ensure security.
- Test, test, test!

Security in Mavericks

Safari Plugins

- Sandboxing
- Granularity between sites
- Insight into plugin needs



FileVault 2

- Full disk encryption
- Archivable, rotatable recovery keys
- Deferrable, allowing self-service encryption

/etc/authorization

- Deprecated in Mavericks
- On upgrade, moved to /etc/authorization.deprecated
- Replaced by /var/db/auth.db

/var/db/auth.db

id	name	type	class	group	kofn	timeout	flags	tries	version	created	modified	hash	identifier	require…	comment
39	system.preferences.accounts	1	1	admin		214748…	10	10000	0	404948…	404948…				Checked by the Admin framework w
40	com.apple.SoftwareUpdate.scan	1	2				0		0	404948…	404948…				Checked when user is updating soft.
41	system.preferences.datetime	1	1	admin		214748…	11	10000	0	404948…	404948…				Checked by the Admin framework w
42	system.identity.write.credential	1	2				0		0	404948…	404948…				Checked when changing authenticat
43	config.remove.system.	1	5				0		0	404948…	404948…				Wildcard right for deleting system ri
44	com.apple.appserver.privilege.admin	1	2				0		0	404948…	404948…				For administrative access to the App
45	system.privilege.taskport.safe	1	4				0		0	404948…	404948…				For use by Apple.
46	com.apple.DiskManagement.internal.	1	2		1		0		0	404948…	404948…				Used by diskmanagementd to allow
47	system.install.apple-config-data	1	2				0		0	404948…	404948…				
48	com.apple.AOSNotification.FindMyMac.modify	1	2		1		0		0	404948…	404948…				
49	system.print.operator	1	1	_lpoper…		214748…	11	10000	0	404948…	404948…				
50	system.restart	1	3				1	10000	0	404948…	404948…				Checked if the foreground console u
51	system.printingmanager	1	2		1		0		0	404948…	404948…				For printing to locked printers.
52	system.install.apple-software.standard-user	1	1	admin		10	40	10000	0	404948…	404948…				Checked when user is installing new
53	com.apple.DiskManagement.reserveKEK	1	1	admin		214748…	10	10000	0	404948…	404948…				Used by diskmanagementd to allow
54	com.apple.pf.rule	1	1	admin		0	8	10000	0	404948…	404948…				
55	system.disk.unlock	1	3				1	10000	0	404948…	404948…				Do not modify.
56	system.services.systemconfiguration.network	1	1	admin		214748…	330	10000	1	404948…	404948…				For making change to network confi
57	sys.openfile.	1	1	admin		300	8	10000	0	404948…	404948…				See authopen(1) for information on t
58	com.apple.lldb.LaunchUsingXPC	1	1	admin		214748…	8	10000	0	404948…	404948…				
59	com.apple.OpenScripting.additions.send	1	1	admin		214748…	10	10000	0	404948…	404948…				Used to send restricted scripting ad.
60	com.apple.library-repair	1	1	admin		214748…	8	10000	0	404948…	404948…				
61	com.apple.XType.fontmover.restore	1	2				0		0	404948…	404948…				
62	system.csfde.requestpassword	1	1	staff		0	24	10000	0	404948…	404948…				Used by CoreStorage Full Disk Encry
63	com.apple.Safari.show-passwords	1	1			10	12	10000	0	404948…	404948…				This right is used by Safari to show .
64	system.sharepoints.	1	1	admin		214748…	11	10000	0	404948…	404948…				Checked when making changes to t.
65	com.apple.dashboard.advisory.allow	1	1	admin		300	8	10000	0	404948…	404948…				
66	system.volume.external.adopt	1	2		1		0		0	404948…	404948…				system.volume.(external|internal|re.
67	config.modify.	1	2		1		0		0	404948…	404948…				Wildcard right for modifying rights.
68	system.login.screensaver	1	2				0		1	404948…	404948…				The owner or any administrator can
69	com.apple.builtin.confirm-access	1	3				1	1	0	404948…	404948…				
70	system.install.iap-software	1	1			214748…	34	10000	0	404948…	404948…				
71	system.preferences.energysaver	1	1	admin		214748…	11	10000	0	404948…	404948…				Checked by the Admin framework w
72	system.keychain.create.loginkc	1	3				0	10000	0	404948…	404948…				Used by the Security framework whe
73	system.install.apple-software	1	2				0		0	404948…	404948…				Checked when user is installing App
74	com.apple.security.assessment.update	1	2				0		0	404948…	404948…				
75	com.apple.desktopservices.scripted	1	1	admin		0	8	10000	0	404948…	404948…				For scripting-initiated privileged file
76	com.apple.docset.install	1	1	admin		214748…	8	10000	0	404948…	404948…				Used by Xcode to restrict access to a
77	com.apple.Safari.parental-controls	1	2		1		0		0	404948…	404948…				Checked when changing parental co
78	com.apple.	1	2				0		0	404948	404948				

<< < 1 to 100 of 147 > >>

/var/db/auth.db

- SQLite3 database.
- Checked through Authorization Framework for system-level changes.
- Generated from /System/Library/Security/authorization.plist

‘security’ command

- security authorizationdb write system.preferences.energysaver authenticate-everyone

- security authorizationdb read system.preferences.energysaver

‘security’ command

```
list-keychains    Display or manipulate the keychain search list.
default-keychain  Display or set the default keychain.
login-keychain    Display or set the login keychain.
create-keychain   Create keychains and add them to the search list.
delete-keychain   Delete keychains and remove them from the search list.
lock-keychain     Lock the specified keychain.
unlock-keychain   Unlock the specified keychain.
set-keychain-settings Set settings for a keychain.
set-keychain-password Set password for a keychain.
show-keychain-info Show the settings for keychain.
dump-keychain     Dump the contents of one or more keychains.
create-keypair    Create an asymmetric key pair.
add-generic-password Add a generic password item.
add-internet-password Add an internet password item.
add-certificates  Add certificates to a keychain.
find-generic-password Find a generic password item.
delete-generic-password Delete a generic password item.
find-internet-password Find an internet password item.
delete-internet-password Delete an internet password item.
find-certificate  Find a certificate item.
find-identity     Find an identity (certificate + private key).
delete-certificate Delete a certificate from a keychain.
set-identity-preference Set the preferred identity to use for a service.
get-identity-preference Get the preferred identity to use for a service.
create-db         Create a db using the DL.
export            Export items from a keychain.
import            Import items into a keychain.
cms               Encode or decode CMS messages.
install-mds       Install (or re-install) the MDS database.
add-trusted-cert  Add trusted certificate(s).
remove-trusted-cert Remove trusted certificate(s).
dump-trust-settings Display contents of trust settings.
user-trust-settings-enable Display or manipulate user-level trust settings.
trust-settings-export Export trust settings.
trust-settings-import Import trust settings.
verify-cert       Verify certificate(s).
authorize         Perform authorization operations.
authorizationdb   Make changes to the authorization policy database.

execute-with-privileges Execute tool with privileges.
leaks             Run /usr/bin/leaks on this process.
error             Display a descriptive message for the given error code(s).
create-filevaultmaster-keychain Create a keychain containing a key pair for FileVault recovery use.
```

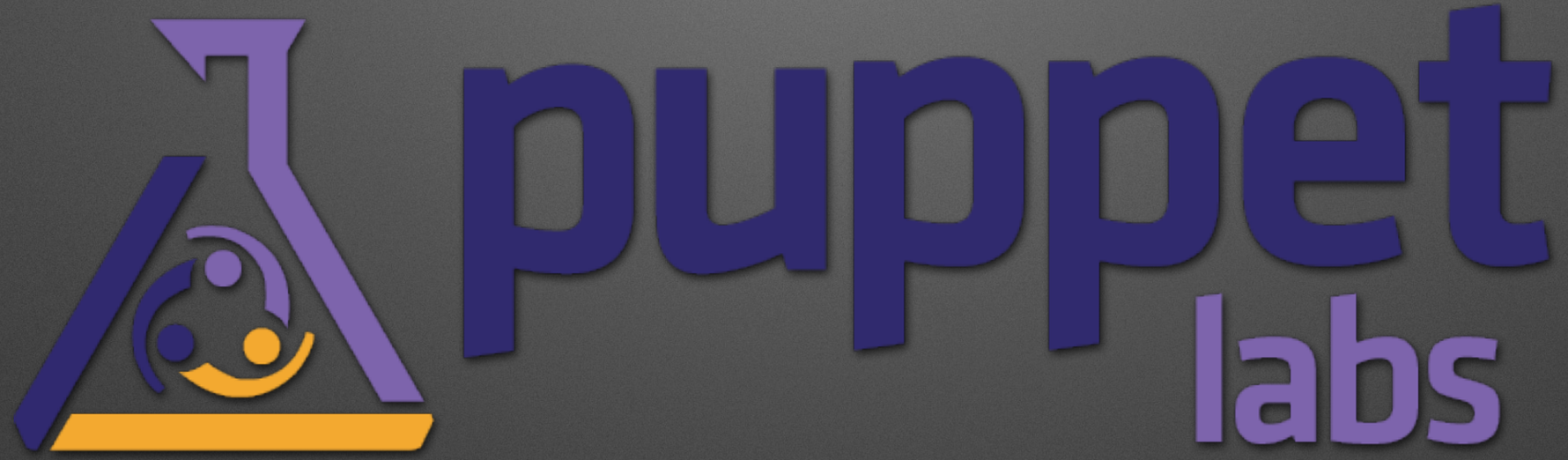
Creating a Policy

- Ask questions:
  - Should all users be local admins? Should some of them?
  - Should secure settings be enforced, or simply set once?
  - Should IT be the solution to HR issues?
  - What will give the best user experience?

What to Control

- App Store
- iCloud
- Printers
- Package installs
- Software Update
- Bluetooth
- AirDrop
- Dictation
- Time Machine
- Single User Mode
- Startup Disk
- Account creation
- Location Services
- Back to My Mac
- Sharing Services
- Date & Time
- Infrared
- Remote Management
- SSH
- Screensaver time

Managed Security?


puppet
labs

Puppet Uses

```
# Creates the localadmin account
class standard_users::localadmin {
  user { 'localadmin':
    ensure     => 'present',
    comment    => 'localadmin',
    gid        => '20',
    groups     => ['_appserveradm', '_appserverusr', '_lpadmin',
'admin'],
    home       => '/Users/localadmin',
    iterations => '50000',
    password   =>
‘sldfhjhfiuhweiouhvnb21kl3j512lk5jbl2iuyh3521klj3h5bl12kb5lk2b35lk21h
b5lk21h35pguvvu9x8ucnhw9h8e98sdf7685sg784dsg578sdfg6097sdg87dsg985sd8
9fb5s9b86x5968b5xzc87b6sb985xb5dfn‘,
    salt       =>
'j9u0v98cxzv6718623ghksgvxcquisyerbkj7824e1c9c9c2b39c29b',
    shell      => '/bin/bash',
    uid        => '499',
  }
}
```

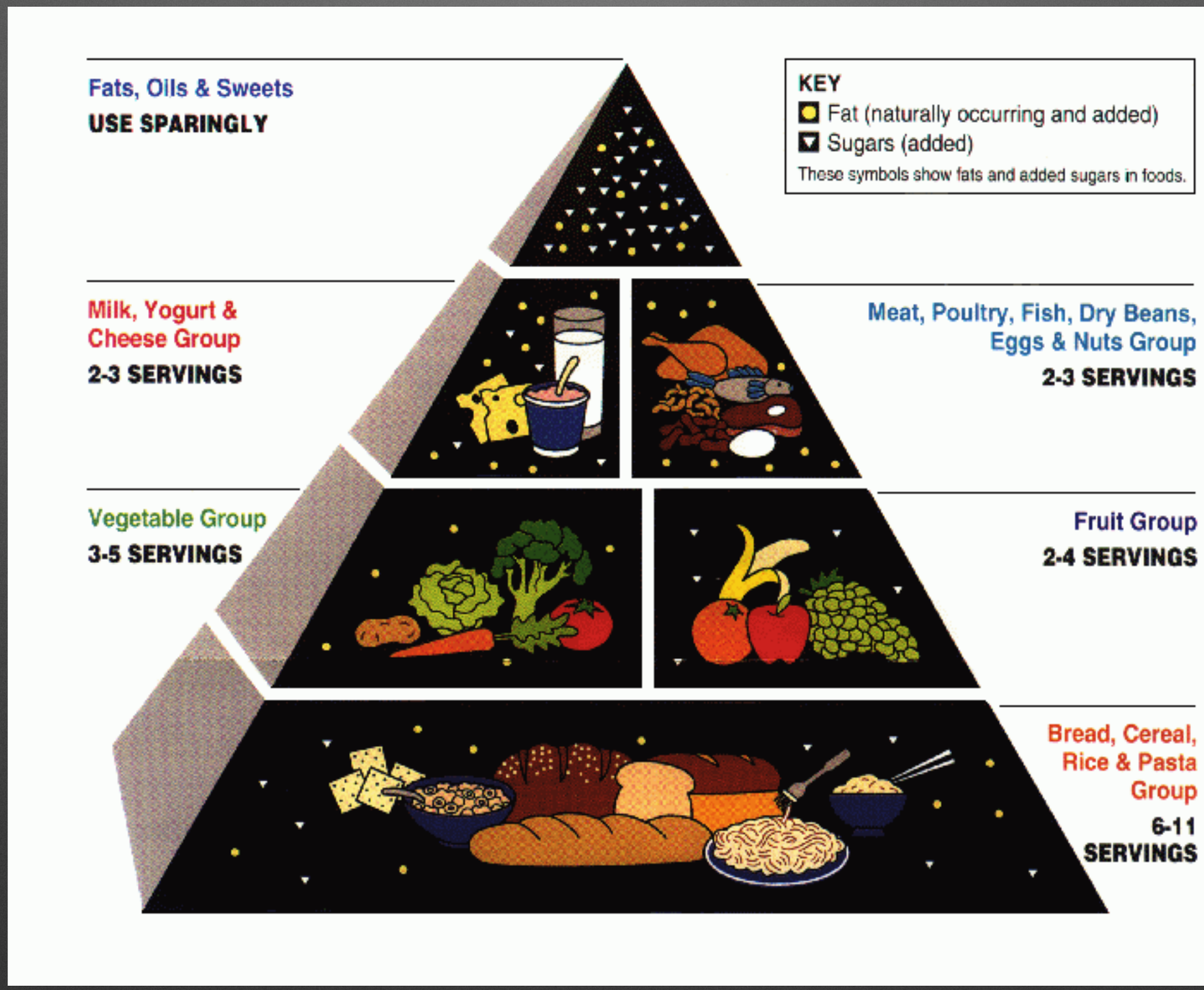
Puppet Uses

```
# Manages infrared Preferences
class osx_infrared::preferences {
  include macdefaults

  mac-defaults { 'Disable Apple IR Remote'  :
    domain       => '/Library/Preferences/
com.apple.driver.AppleIRController',
    key          => 'DeviceEnabled',
    value        => FALSE,
    type => 'bool',
  }
}
```

Puppet Uses

```
# disables icloud
class osx_disable_icloud::profiles {
  mac_profiles_handler::manage { 'com.afp548.disable_icloud' :
    ensure      => present,
    file_source => 'puppet:///modules/osx_disable_icloud/
com.afp548.disable_icloud.mobileconfig',
  }
}
```



Do not forget why they bought a Mac!

Q&A

http://www.afp548.com/2013/11/08/security-making-mavericks-work-for-you/