



MacAdmins Meeting — November 20, 2019



Brad Chapman

Systems Engineer

APNS + MDM

A technical update for elite squadrons
of Mac administrators

Outline

Looking Back...

To the Future!

See for Yourself

What's Possible



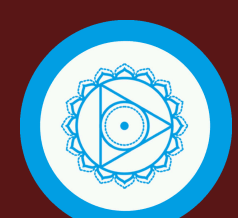

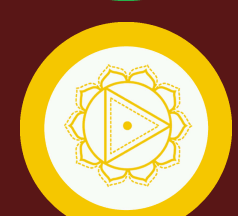
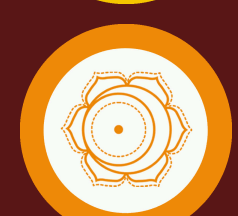

Last Words



Looking Back....



The 7 Principles of APNS

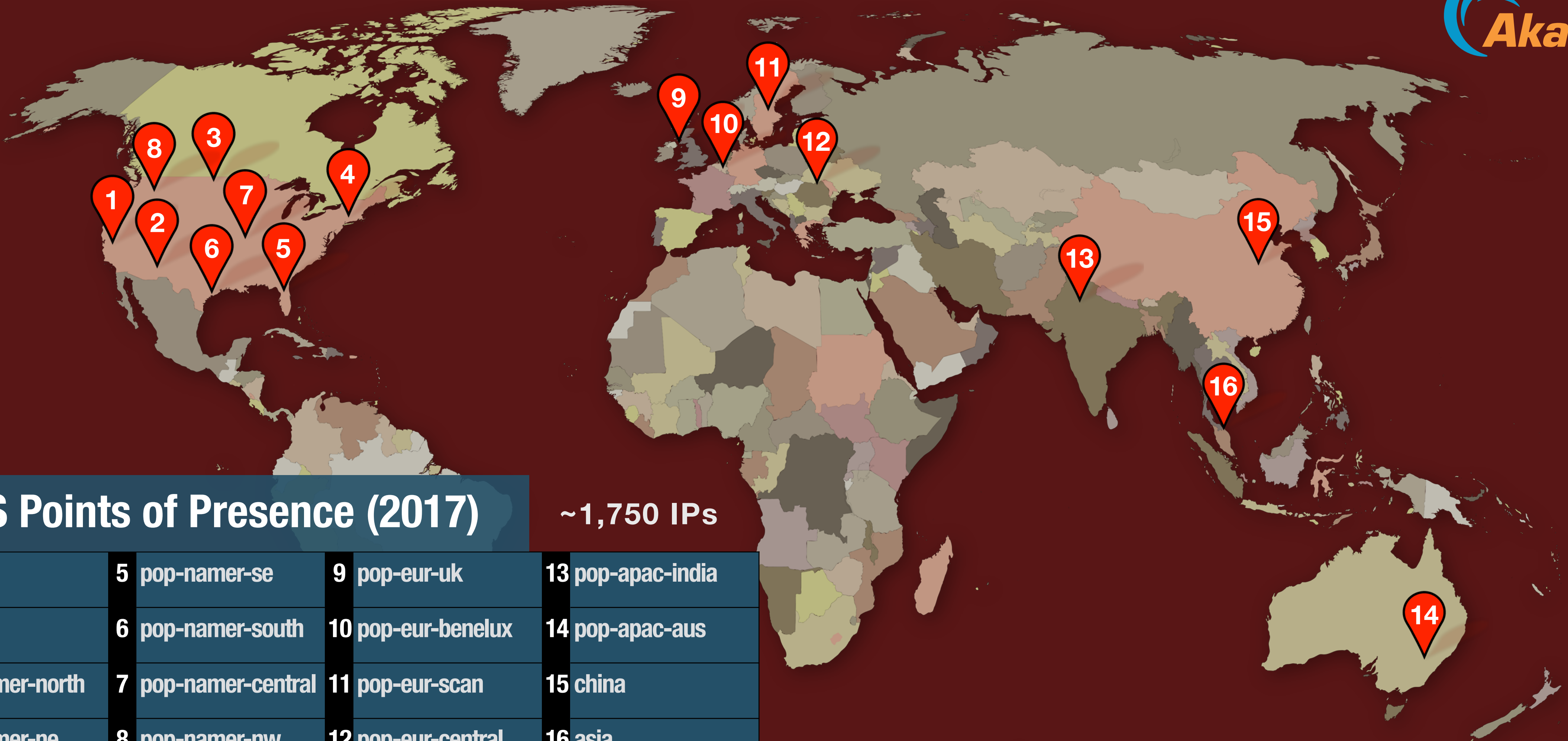
-  Push notifications are small packets of data with instructions for a device.
-  APNS uses Akamai Global Traffic Management for peak performance.
-  APNS has multiple security factors for integrity and authenticity.
-  APNS is required for secure delivery of configuration profiles.
-  Devices expect a direct, persistent path to the Internet.
-  You must permit outbound connections to Apple.
-  Apple does not make inbound connections.

APNS Hosts and Ports

Function	Server Address : Port
Sending Notifications	gateway.push.apple.com : 2195
Receiving Feedback	feedback.push.apple.com : 2196
Initialization (Devices)	init-p01st.push.apple.com : 80
Notifications (Devices)	##-courier.push.apple.com : 5223†
New http/2 API	api.push.apple.com : 443

† 443 is used as a fallback over Wi-Fi only. The protocol is HTTPS.

Looking Back...



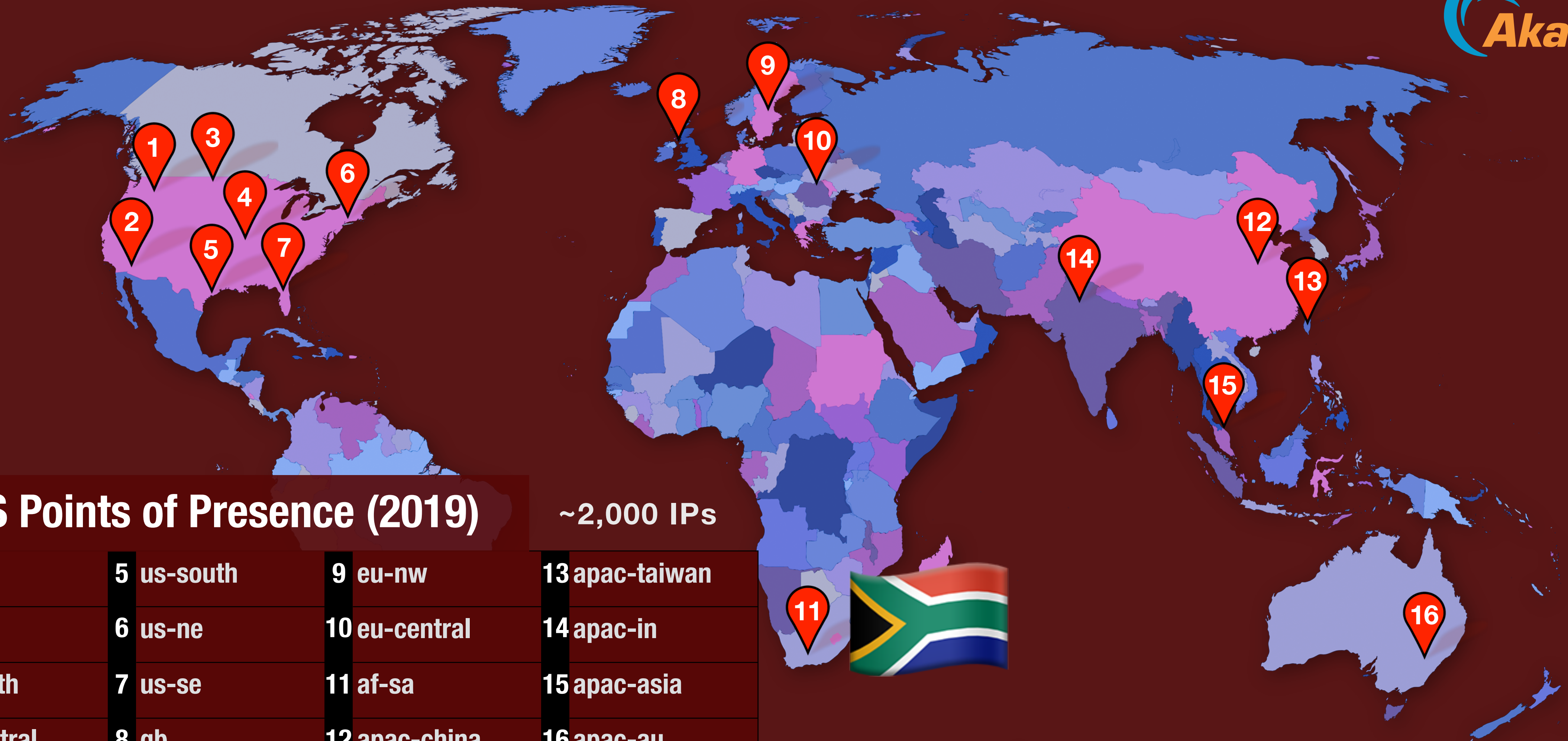
APNS Points of Presence (2017)

~1,750 IPs

1	sjc	5	pop-namer-se	9	pop-eur-uk	13	pop-apac-india
2	us	6	pop-namer-south	10	pop-eur-benelux	14	pop-apac-aus
3	pop-namer-north	7	pop-namer-central	11	pop-eur-scan	15	china
4	pop-namer-ne	8	pop-namer-nw	12	pop-eur-central	16	asia

[pop]-courier.push-apple.com.akadns.net

Looking Back...



APNS Points of Presence (2019)

~2,000 IPs

1 us-nw	5 us-south	9 eu-nw	13 apac-taiwan
2 us-sw	6 us-ne	10 eu-central	14 apac-in
3 us-north	7 us-se	11 af-sa	15 apac-asia
4 us-central	8 gb	12 apac-china	16 apac-au

[pop]-courier-4.push-apple.com.akadns.net

Rules of the road

Apple still owns 17.0.0.0/8

Apple services use **certificate pinning**

Jamf uses **APNS** binary (2195-2196)

Proxy support is mixed

apsd proxy support

transparent proxy	YES [†]
static http(s) proxy	YES [†]
proxy with PAC	NO
authenticated proxy	NO
proxy with SSL inspection	NO

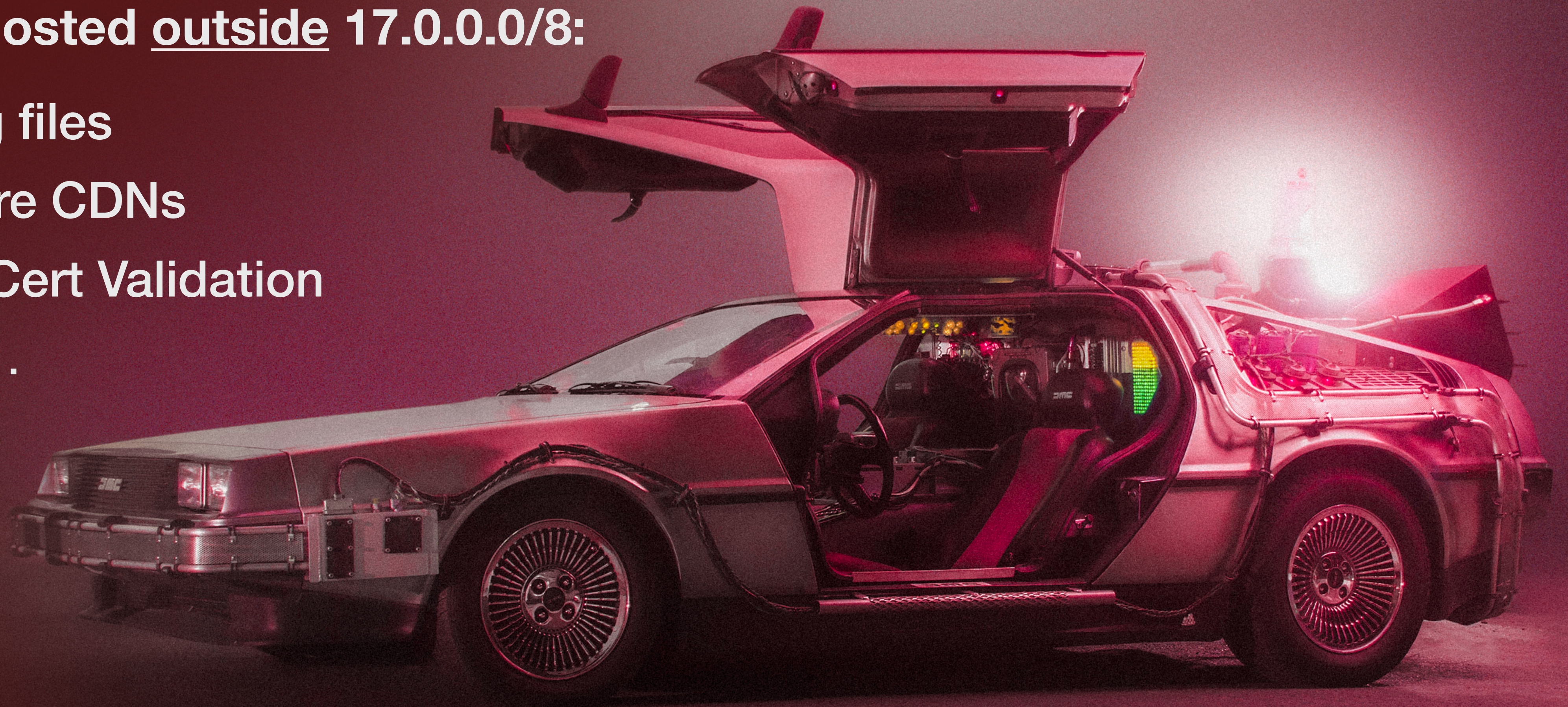
[†] All of *.push.apple.com must be whitelisted

Looking Back...

...we don't need roads

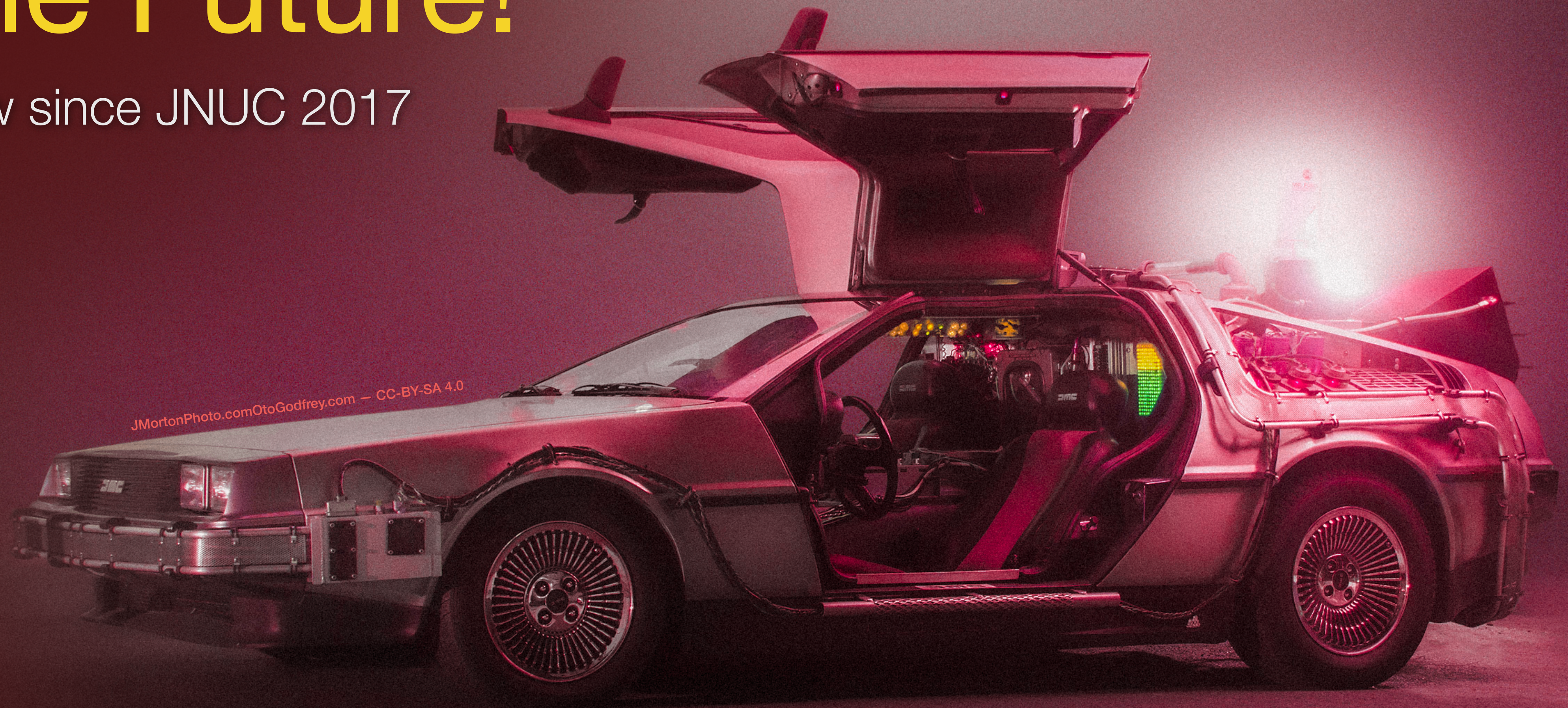
Services hosted outside 17.0.0.0/8:

- Init bag files
- Software CDNs
- OCSP Cert Validation
- others...



To the Future!

What's New since JNUC 2017



To the Future!



Big news about APNS!

Binary protocol ends **November 2020**

Move to HTTP/2-based API

- High speed, parallel processing
- Improved error handling
- Per-notification feedback



Apple Developer News: [Apple Push Notification Service Update](#)

To the Future!

What's new for Mac?



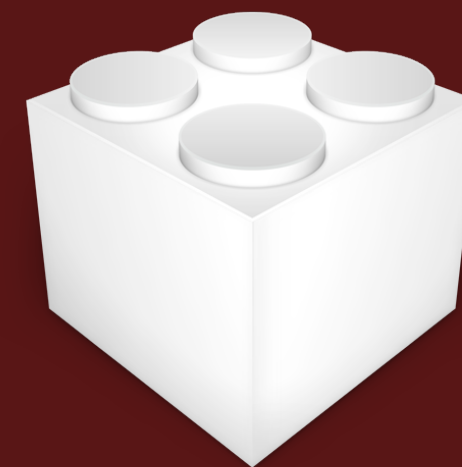
T2 Secure Boot



UAMDM



Jamf Pro 10.3



UAKEL



ABM/ASM



TCC + PPC



ARD



AppleSeed



Certification



Catalina

T2 Secure Boot

Complex, powerful security SOC

Plan deployments for “Full Security.”

[HT208330](#): Secure Boot

[HT208198](#): Secure Startup Utility

[PDF](#): T2 Security Chip Overview



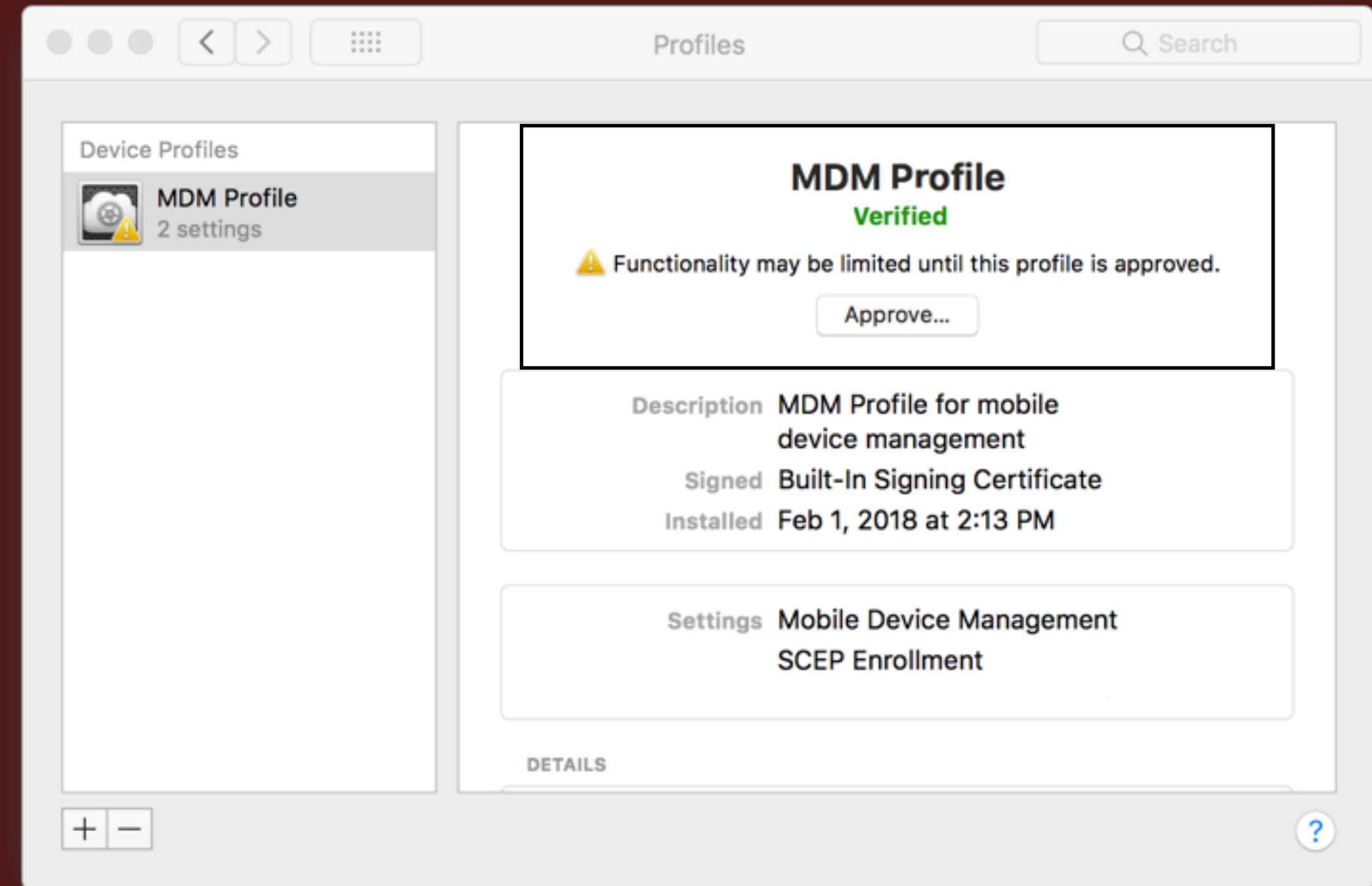
To the Future!

UAMDM

macOS 10.13.2

Manual MDM approval

Button can't be clicked remotely



HT208019: Prepare for changes ... in High Sierra

Jamf Pro 10.3

Enrollment loads CA + MDM profiles

APNS required to confirm enrollment

MDM is marked as **user-approved**

QuickAdd package is “deprecated”



To the Future!

UAKEL

KEXTs blocked by default

User has 30 min. to approve

Whitelisting requires **approved** profile



DerFlounder: Whitelisting third-party kernel extensions

ABM / ASM

Replaces Device Enrollment Program

Automated Device Enrollment

Multiple tokens / pre-stage workflows

MDM Profiles are **user-approved**

HT208817: Upgrade your organization to ABM

HT206960: Upgrade your institution to ASM



TCC + PPC

Users prompted once by every app requesting specific permissions.

Whitelist* with **user-approved** MDM



macOS User Guide: Change privacy preferences on Mac

JNUC 2018: PPC, TCC, User Data Protection and You

Remote Desktop

`kickstart` command

Control & observe was removed during 10.14 beta cycle

Enable with **user-approved** MDM



HT209161: Use the kickstart CLI in 10.14 and later

AppleSeed for IT

Invite testers via ABM / ASM

...or delegate to “Staff Admin.”

“Always be testing.”



MobCo: AppleSeed for IT is now available for everybody

Industrial Strength

ISO 27001:2013 (InfoSec Mgmt. Systems)

ISO 27018:2019 (Cloud / PII)

HT202739:

Security certifications, validations, guidance

ISO 27001, ISO 27018, T2 Firmware, SEP Key Store, macOS



Catalina

App Notarization

Mac supervision

New controls for TCC, Notifications

Activation Lock for **T2** Macs only

MDM can **only** bypass if Mac is **supervised**

HT202804: Use MDM to manage Activation Lock & Lost Mode



...to the Future!

Additional Reading

Apple: [MDM Settings for IT Administrators](#)

Apple: [Mac Deployment Overview](#)

Apple: [WWDC 2019 Session 303](#)

What's new in Managing Apple Devices



See for Yourself

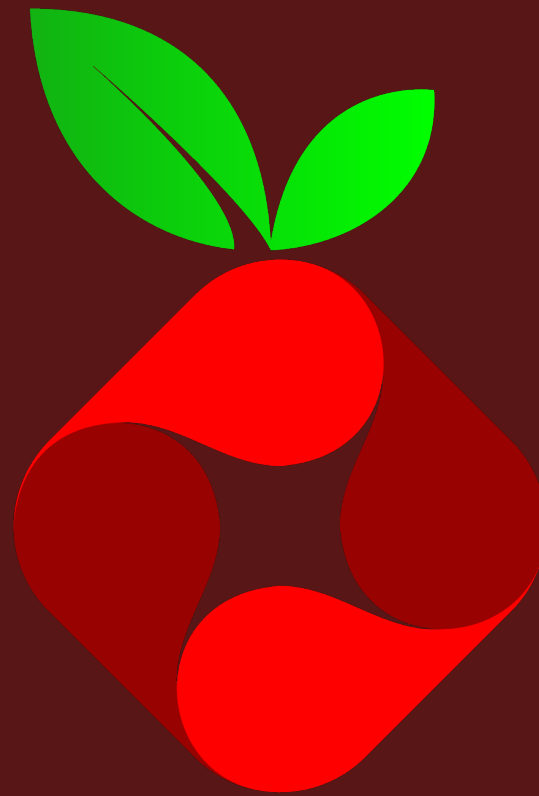
Discovering essential ports and services



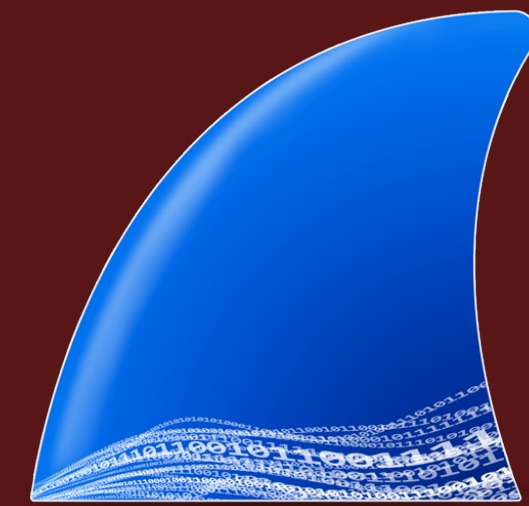
Analysis Tools



Little Snitch



Pi-Hole



Wireshark

Little Snitch

Exclusively for Mac : obdev.at

Rich UI with powerful filtering

Checks app code signatures

PCAP: Individual apps / services

OSI layers 3-7



See for Yourself



Pi-Hole

Ultra-compact DNS server

Built for the Raspberry Pi platform

Also works on VMs and Dockers

Great for SoHo & test networks

Black + white lists, detailed logging

Free & Open Source: pi-hole.net



See for Yourself

Pi-hole

Status

Active

Temp: 52.1 °C

Load: 0.06 0.05 0.07

Memory usage: 17.7%

MAIN NAVIGATION

Total queries (3 clients)

22,430

Queries Blocked

System

Blocklists

DNS

DHCP

API / Web interface

Privacy

Teleporter

Show10entries

Previous12345...10Next

Time	Type	Domain	Client	Status	Reply	Action
2019-11-02 15:06:34	A	login.microsoftonline.com	router.asus.com	OK (forwarded)	CNAME (23.5ms)	<div>Blacklist</div>
2019-11-02 15:06:34	A	outlook.office365.com	router.asus.com	OK (cached)	CNAME (0.2ms)	<div>Blacklist</div>
2019-11-02 15:06:30	A	time.apple.com	router.asus.com	OK (forwarded)	CNAME (18.6ms)	<div>Blacklist</div>
2019-11-02 15:06:25	A	mail.runbox.com	router.asus.com	OK (forwarded)	IP (17.3ms)	<div>Blacklist</div>
2019-11-02 15:06:22	A	client.dropbox.com	tardis.lan	OK (forwarded)	CNAME (1.5ms)	<div>Blacklist</div>
2019-11-02 15:06:22	AAAA	client.dropbox.com	tardis.lan	OK (forwarded)	N/A	<div>Blacklist</div>
2019-11-02 15:06:22	AAAA	client.dropbox-dns.com	tardis.lan	OK (forwarded)	IP (47.7ms)	<div>Blacklist</div>
2019-11-02 15:06:22	A	client.dropbox.com	router.asus.com	OK (cached)	CNAME (0.2ms)	<div>Blacklist</div>
2019-11-02 15:06:22	A	bolt.dropbox.com	router.asus.com	OK (forwarded)	CNAME (1.2ms)	<div>Blacklist</div>
2019-11-02 15:06:22	A	bolt.dropbox.com	tardis.lan	OK (cached)	CNAME (0.2ms)	<div>Blacklist</div>
Time	Type	Domain	Client	Status	Reply	Action

System Information

Network Interface:

eth0

Address:

192.168.11.9

Address:

Hostname:

raspberrypi

FTL Information

FTL version:

v4.3.1

Process identifier (PID):

608

Time FTL started:

Oct 01

User / Group:

pihole / pihole

Total CPU utilization:

0.1%

Memory utilization:

10.6%

Used memory:

95.87 MB

DNS cache size:

10000

DNS cache insertions:

211873

DNS cache evictions:

0

See also our [DNS cache documentation](#).

01:0004:0007:0010:0013:00

A (IPv4)

AAAA (IPv6)

Wireshark

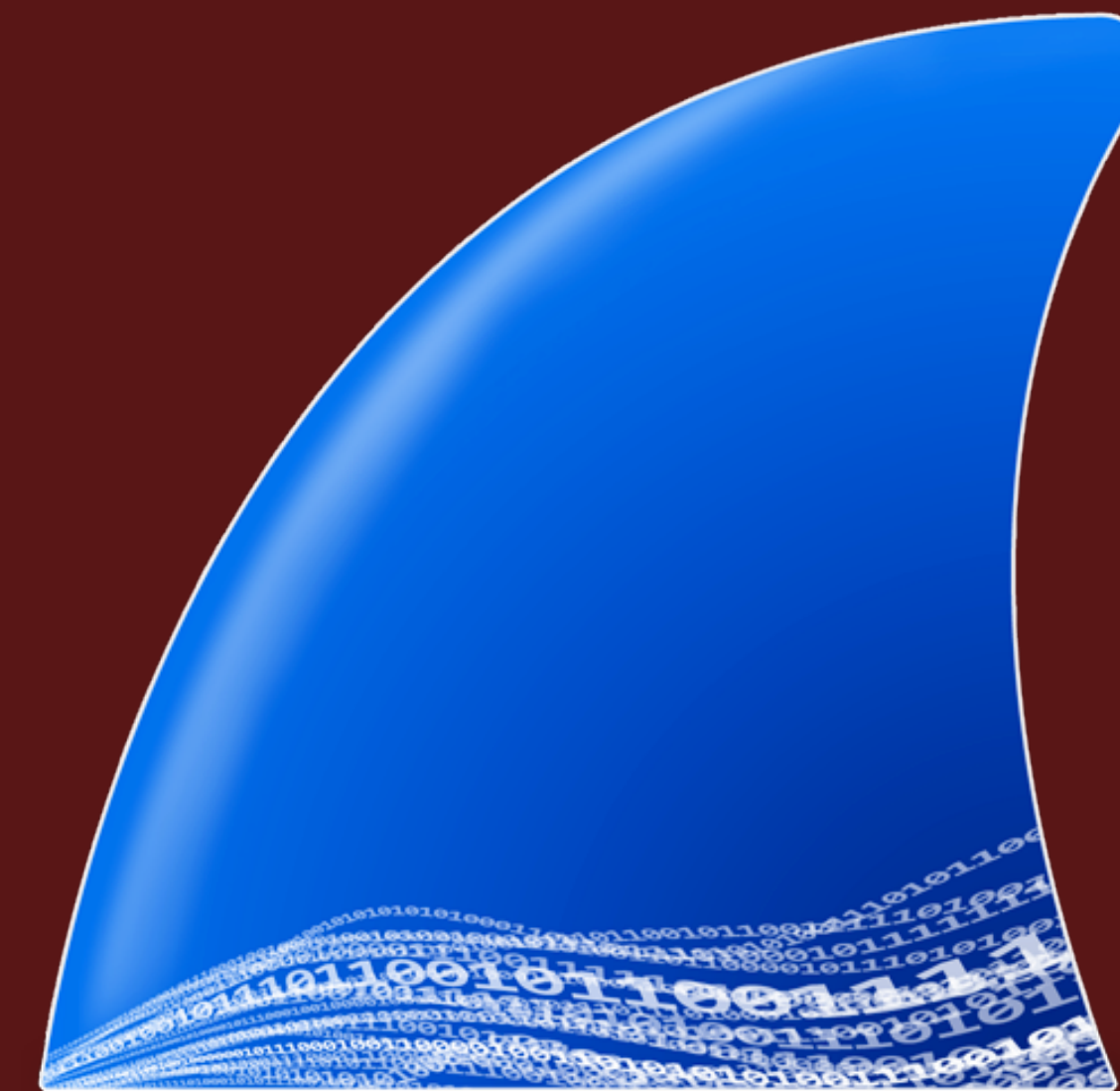
The ultimate packet inspector

Captures all traffic on an interface
(OSI Layers 2-7)

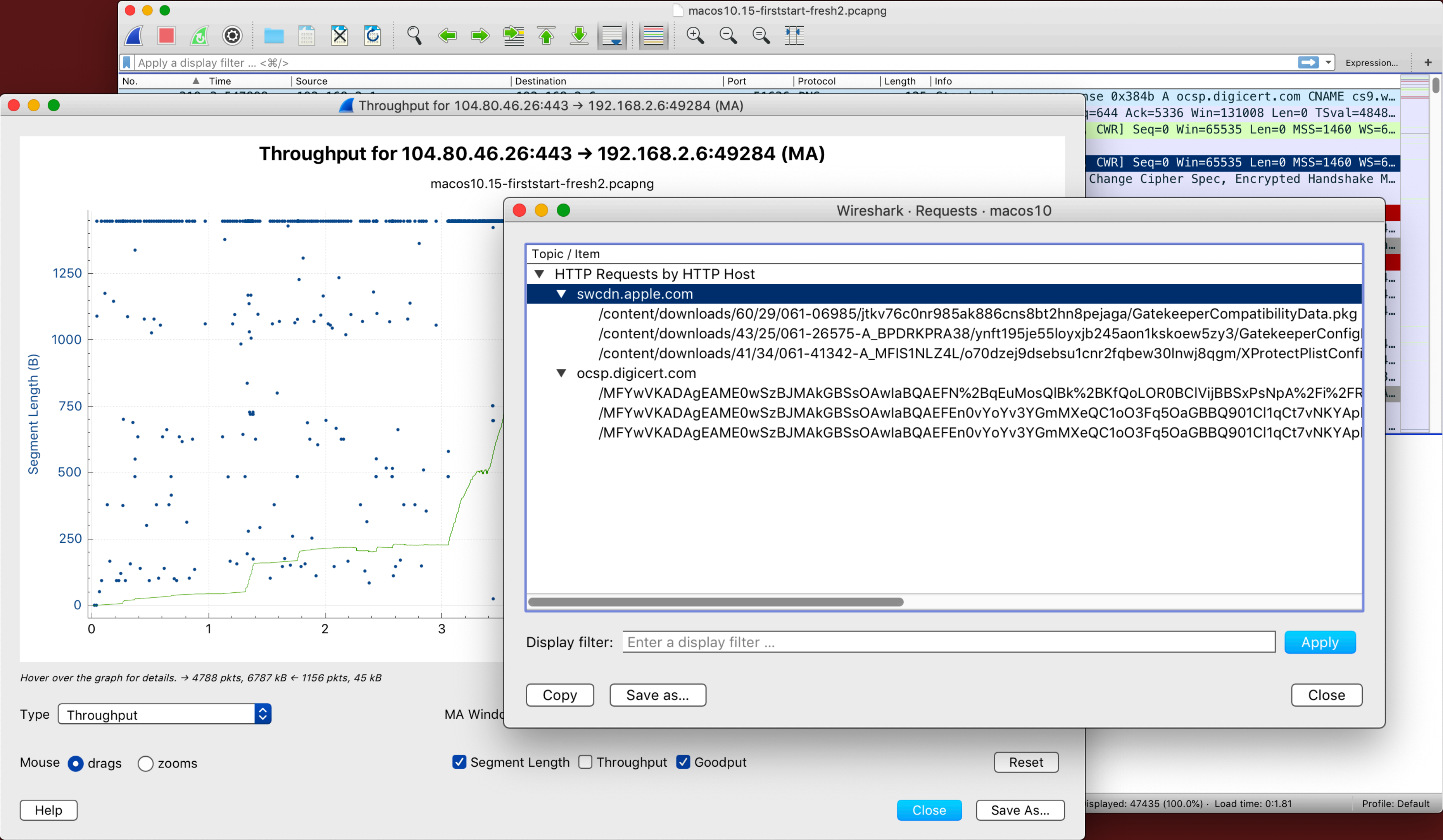
Detailed analysis & export functions

⚠ Can be overwhelming at first

Free & open source: www.wireshark.org



See for Yourself



Wireshark

GUI bogs down during long, heavy sessions

Use the CLI tools:

`/Applications/Wireshark.app/Contents/MacOS/`

```
dumpcap -D
```

```
dumpcap -i en# [-w outfile]
```

```
editcap -c ### infile outfile
```



See for Yourself

Demo

Show all DNS requests from a fresh macOS install

Wireshark Demo

1. Display Filter:

`dns and dns.flags.response == 0 and dns.qry.type == 1`

2. Export specified packets as a CSV file.

3. Process in Terminal for unique entries...

See for Yourself

```
awk -F", " '{ print $7 }' pcap.csv \
| sed 's_"__g' | cut -c 25- \
| awk '!x[$0]++' | grep -v .net
```

No.	Time	Source	Destination	Protocol	Length	Info
44	30:00.1	192.168.2.6	192.168.2.1	DNS	84	Standard query 0x15f9 A 1-courier.push.apple.com

See for Yourself

```
awk -F", " '{ print $7 }' pcap.csv \
| sed 's_"__g' | cut -c 25- \
| awk '!x[$0]++' | grep -v .net
```

No.	Time	Source	Destination	Protocol	Length	Info
44	30:00.1	192.168.2.6	192.168.2.1	DNS	84	Standard query 0x15f9 A 1-courier.push.apple.com

See for Yourself

```
awk -F", " '{ print $7 }' pcap.csv \  
| sed 's_""_g' | cut -c 25- \  
| awk '!x[$0]++' | grep -v .net
```

"Standard query 0x15f9 A 1-courier.push.apple.com"

See for Yourself

```
awk -F"," '{ print $7 }' pcap.csv \
| sed 's_""_g' | cut -c 25- \
| awk '!x[$0]++' | grep -v .net
```

Standard query 0x15f9 A 1-courier.push.apple.com

See for Yourself

```
awk -F"," '{ print $7 }' pcap.csv  
| sed 's_"__g' | cut -c 25- \  
| awk '!x[$0]++' | grep -v .net
```

```
rag.itunes.apple.com  
cf.iadsdk.apple.com  
iadsdk.apple.com  
itunes.apple.com  
init.push.apple.com  
14-courier.push.apple.com  
iprofiles-st.apple.com.akadns.net  
e673.dsce9.akamaiedge.net  
e673.dsce9.akamaiedge.net  
humb.apple.com.akadns.net  
iprofiles.apple.com.akadns.net  
e673.dsce9.akamaiedge.net  
appleid.apple.com  
e6858.dsce9.akamaiedge.net  
1-courier.push.apple.com  
14.courier-push-apple.com.akadns  
1.courier-sandbox-push-apple.com  
mesu.apple.com  
swdist.apple.com.edgekey.net  
gateway.fe.apple-dns.net  
gsa.apple.com.akadns.net  
radarsubmissions.apple.com  
swdist.apple.com.akadns.net  
a239.gi3.akamai.net  
init-p0lmd-lb.push-apple.com.aka  
setup.fe.apple-dns.net
```

See for Yourself

```
awk -F"," '{ print $7 }' pcap.csv \
| sed 's_"__g' | cut -c 25- \
| awk '!x[$0]++' | grep -v .net
```

swdist.apple.com
bag.itunes.apple.com
adsdk.apple.com
iadsdk.apple.com
init.push.apple.com
14-courier.push.apple.com
iprofiles-st.apple.com.akadns.net
humb.apple.com.akadns.net
iprofiles.apple.com.akadns.net
appleid.apple.com
e6858.dsce9.akamaiedge.net
1-courier.push.apple.com
mesu.apple.com
gateway.fe.apple-dns.net
gsa.apple.com.akadns.net
radarsubmissions.apple.com
swdist.apple.com.akadns.net
a239.gi3.akamai.net
init-p0lmd-lb.push-apple.com.aka
setup.fe.apple-dns.net
cf.iadsdk.apple.com
iadsdk.apple.com
gspe1-ssl.ls.apple.com

See for Yourself

```
awk -F", " '{ print $7 }' pcap.csv \
| sed 's_"__g' | cut -c 25- \
| awk '!x[$0]++' | grep -v .net
```

swdist.apple.com
bag.itunes.apple.com
cf.iadsdk.apple.com
iadsdk.apple.com
init.push.apple.com
14-courier.push.apple.com
appleid.apple.com
1-courier.push.apple.com
mesu.apple.com
radarsubmissions.apple.com
init-p01md-lb.push-apple.com.akad
cf.iadsdk.apple.com
iadsdk.apple.com
gspel-ssl.ls.apple.com

All DNS records - first 10 minutes (with enrollment)

*Not a complete list

www.apple.com
1-courier.push.apple.com
1-courier.sandbox.push.apple.com
gspe35-ssl.ls.apple.com
gspe1-ssl.ls.apple.com
appleid.apple.com
mesu.apple.com
swscan.apple.com
gsa.apple.com
radarsubmissions.apple.com
lcdn-locator.apple.com
pancake.apple.com
updates-http.cdn-apple.com
swdist.apple.com

gateway.icloud.com
bag.itunes.apple.com
g.symcd.com
ocsp.digicert.com
cf.iadsdk.apple.com
iadsdk.apple.com
humb.apple.com
ocsp.apple.com
init.ess.apple.com
init-p01md.apple.com
iprofiles.apple.com
setup.icloud.com
configuration.ls.apple.com
gspe21-ssl.ls.apple.com

init.push.apple.com
8-courier.push.apple.com
gspe64-ssl.ls.apple.com
itunes.apple.com
jamf.acme.com
updates-http.g.aaplimg.com
smp-device-content.apple.com
init.itunes.apple.com
api.apple-cloudkit.com
world-gen.g.aaplimg.com

Remember the Akamai...

Content distribution network

Follow DNS and whitelist accordingly

*.akamaiedge.net

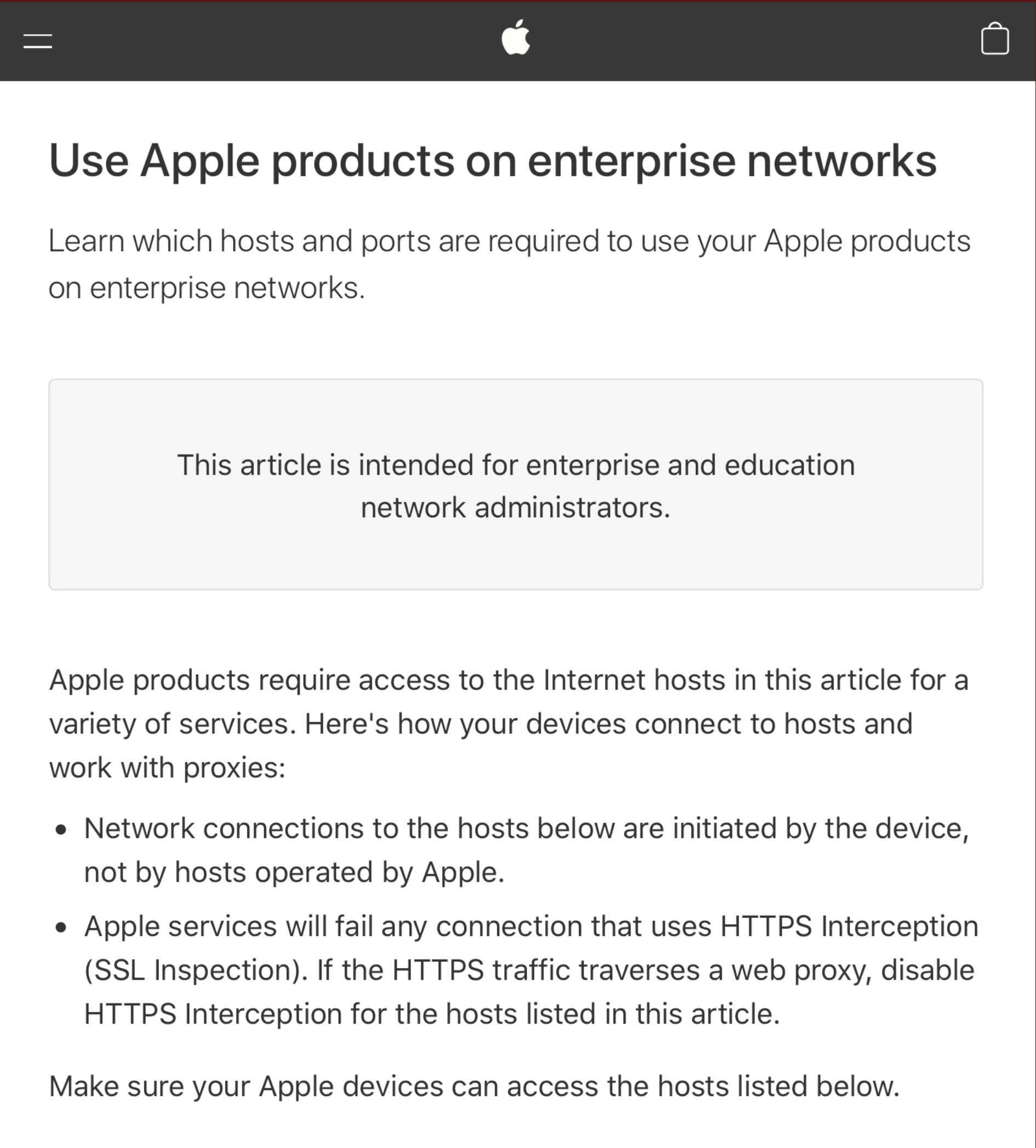
*.edgekey.net

*.edgesuite.net

Akamai: [Edge Hostnames API](#)

HT210060

**Use Apple products
on enterprise networks**



HT210060

Use Apple products on enterprise networks

See for Yourself

MacEval Utility

Apple + Mac Solutions Architects

Network evaluation readiness

Concise report + action items

Contact an Apple SE for details



Additional Reading

[A Deep Dive into macOS MDM](#)

Jesse Endahl & Max Bélanger

[Under the Hood: Device Enrollment](#)

Marcus Ransom, JNUC 2018

[Apple Device Management](#)

Charles Edge & Rich Trouton

Palo Alto [Applipedia](#)



What's Possible

...when everything works



Mac: the ultimate unboxing

Automatic enrollment & supervision

Rapid deployment of apps

Delightful user experiences

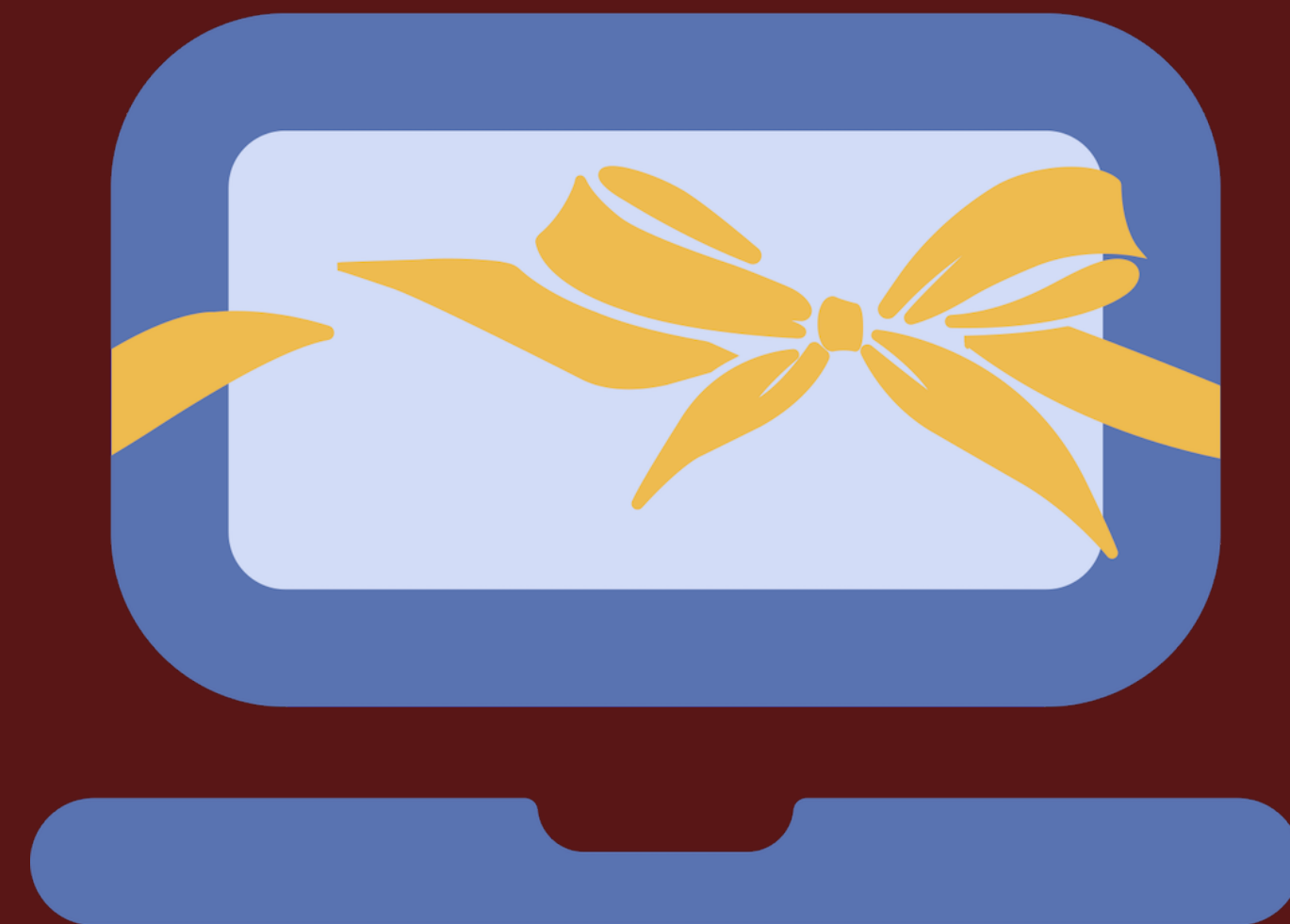
What's possible

Ceremony

Inspired by DEPNotify and Splashbuddy

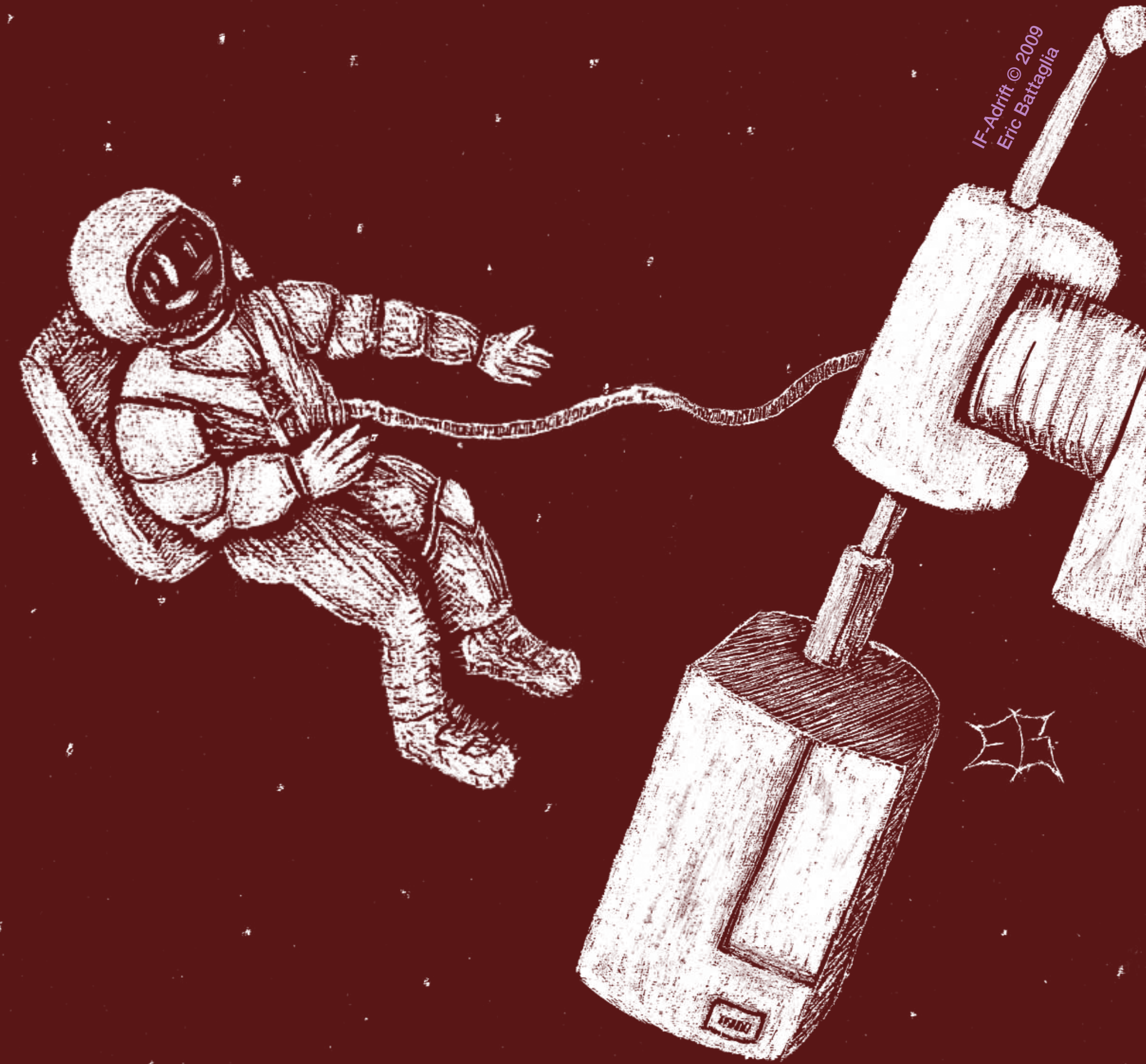
[GetCeremony.app](#)

Slack: [#ceremony](#)



Houston, we have a problem

When devices can't contact Apple



Impacted workflows



Auto Device Enrollment



Management actions



Manual enrollment



User experience



Security policies



Return to service



Software updates

Auto Device Enrollment

Can't reach activation servers...

Macs can skip remote management

Not enrolled & unsupervised



Manual Enrollment

Mac installs profiles...

...yet **fails** to validate via APNS

Enrollment **fails**.



Security policies

Enforced with profiles

Triggered by APNS

Sideloaded profiles are **not trusted**



Software Updates

T1 / T2: BridgeOS validation fails

Can't defer or force software updates

macOS updates cannot be verified

No background + critical updates

[HT207567](#): Make sure your MBP can connect...

[HT207005](#): About background updates



Management

Enable / disable:

- Remote desktop

- Bluetooth

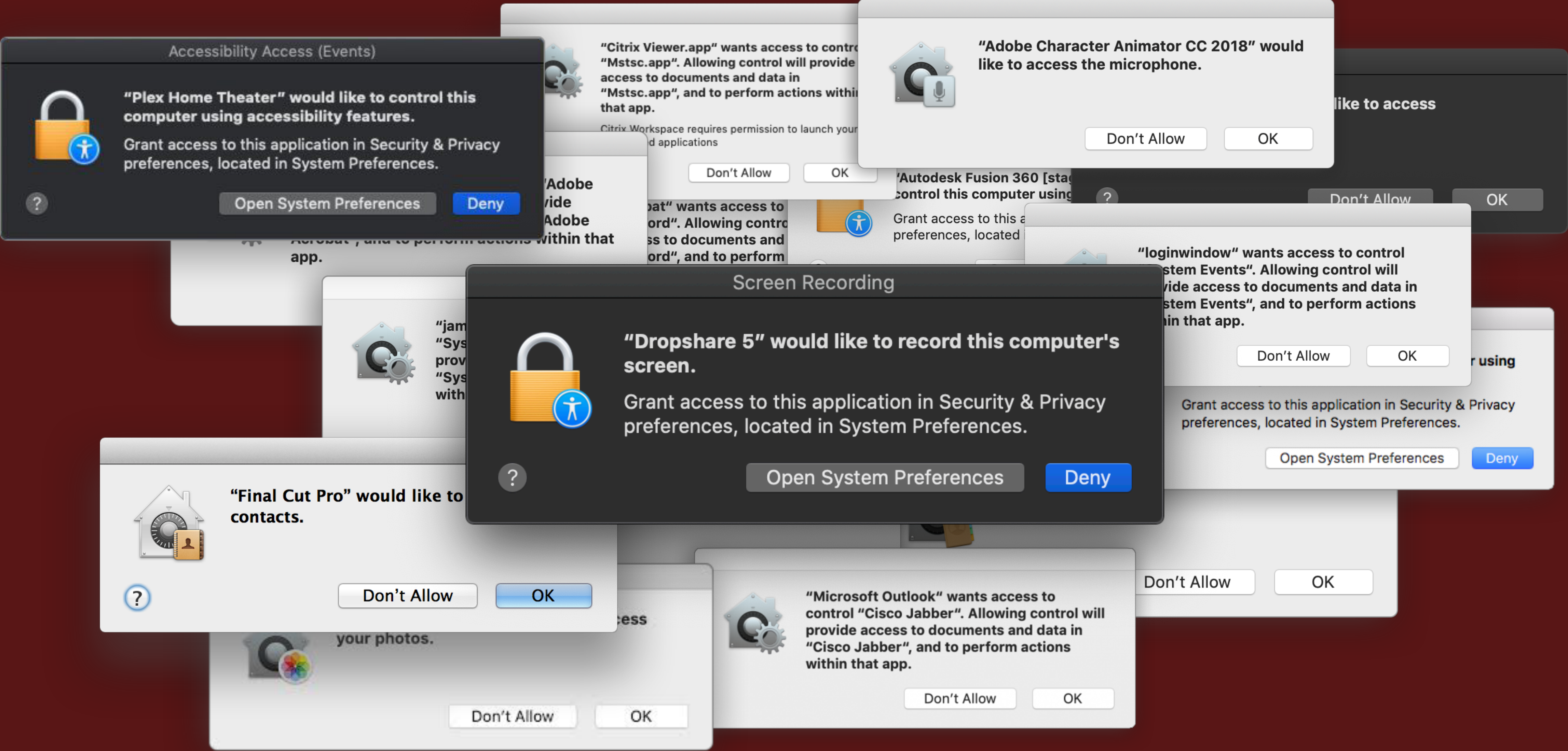
Remote lock and wipe

Override Activation Lock



Houston, we have a problem

U



User Experience

Can't manage privacy / notifications

No Self Service notifications

No remote notifications



Houston, we have a problem

Cloud Services

No VPP / App Store

No FaceTime or iMessage

No Continuity or Handoff



Return to Service

- macOS (Internet) Recovery
- 802.1X / RADIUS not supported
- Wi-Fi: WPA2-PSK or Open
- External DNS resolution
- No proxies or SSL decryption
- **Consider a limited 'deploy' SSID**



⚠ Error -2003F

Last Words



Devil's Advocate

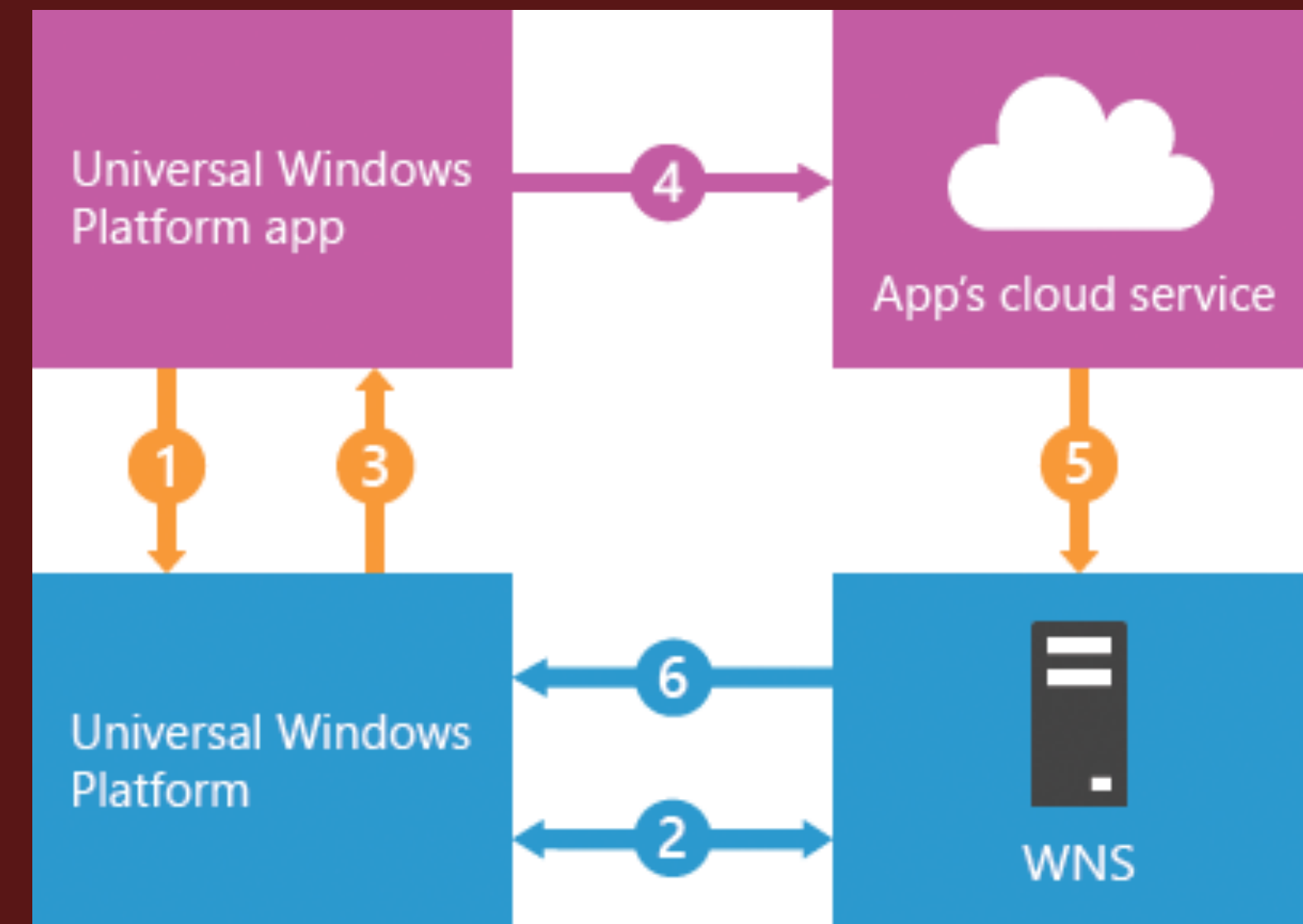
What if Microsoft told you to prepare for a
Windows Notification Service?

They did... in 2011.

WNS Overview

Firewall + Proxy Configuration

IP addresses for MPNS + WNS



A Warning:

**If you don't make changes to your network,
Jamf + Apple may be unable to support you.**



Prepare your institution

HT210060



Think global, not local

Set baseline security with MDM

Reinforce with education

Monitor at the perimeter

Avoid local security agents





Why care about MDM?

Consistent, delightful experiences

Streamlining support model

Empowering end users



Remember the Human

Trust people to do the right thing.

Assume positive intent.

People are awesome.



Apple means *business*

APNS = the gateway to MDM

MDM = great user experiences with Apple

Apple = the best tools for people



References

References

[Apple Push Notification Service Update](#)

[HT208330: Secure Boot](#)

[HT208198: Secure Startup Utility](#)

[PDF: T2 Security Chip Overview](#)

[HT208019: Prepare for changes to kernel extensions...](#)

[JN 499: Managing User Approved MDM](#)

[DerFlounder: Whitelisting third-party kernel extensions](#)

[HT208817: Upgrade your organization to ABM](#)

[HT206960: Upgrade your institution to ASM](#)

[HT209161: Use the kickstart CLI in 10.14 and later](#)

[MobCo: AppleSeed for IT is now available for everybody](#)

[macOS User Guide: Change privacy preferences on Mac](#)

[JNUC 2018: PPC, TCC, User Data Protection and You](#)

[HT202739: Security certifications, validations, guidance](#)

[ISO 27001](#), [ISO 27018](#), [T2 Firmware](#), [SEP Key Store](#), [macOS](#)

[HT202804: Use MDM to manage Activation Lock & Lost Mode](#)

[MDM Settings for IT Administrators](#)

[Mac Deployment Overview](#)

WWDC 2019 [Session 303](#) (Managing Apple Devices)

Little Snitch: [obdev.at](#)

Pi-Hole: [pi-hole.net](#)

WireShark: [www.wireshark.org](#)

Akamai: [Edge Hostnames API](#)

[HT210060: Use Apple products on Enterprise Networks](#)

Fleetsmith: [A Deep Dive into macOS MDM](#)

Marcus Ransom: [Device Enrollment Under the Hood](#)

Charles Edge & Rich Trouton: [Apple Device Management](#)

[Jamf Admin Guide: User-initiated enrollment](#)

[HT207567: Make sure your MBP can connect...](#)

[HT207005: About background updates](#)

[WNS Overview](#), [Firewall + Proxy Configuration](#)

IP addresses for [MPNS](#) + [WNS](#)

Palo Alto: [Applipedia](#)

Thank you!

Slack: @bradtchapman

Email: bradtchapman@gmail.com

github.com/bradtchapman/jnuc2019

