

Zero to Secure:

How We Secured our Environment Without Pain

^ MUCH

Yo!

I am John Mahlman

Mac Admin for 13 years

Mac Engineering Lead at Leidos



@jmahlman



yearofthegEEK.net


A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, while others are smaller and solid. The lines connecting them are thin and grey, creating a mesh-like structure.

Set Expectations

What this presentation is not...



Overview

- ◎ Background
 - ◎ The Plan
 - ◎ Implementation
 - ◎ Lessons Learned
 - ◎ ...
 - ◎ Profit?
- 

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

1.

Background

Who? What? Why?

End Goal

Ensure all Macs are
managed and secure.



Background - Why

- ◎ ~400-700 total Macs in the environment (?)
 - ~100 Enrolled in Jamf already
- ◎ Didn't know where the devices were/who had them
 - We had ways to find them...
- ◎ Need to secure devices for compliance **within ~~12~~⁸ months**
 - NIST 800-171
 - CMMC level 3/4
- ◎ Compliance required to win contracts
- ◎ Make life easier for users and admins

Background - Why

- ◎ Enterprise adding more controls for security
 - MFA
 - Application Controls
 - Certificate Verification
 - Blood samples
 - Retina scans
 - PIV Tokens

Background - How

- ◎ Legacy practices
- ◎ Legacy tools
- ◎ Macs not “in scope” for anything
- ◎ No enterprise-level support
- ◎ Users “fending for themselves”
- ◎ Business groups making their own compliance guidelines
- ◎ Animosity toward IT

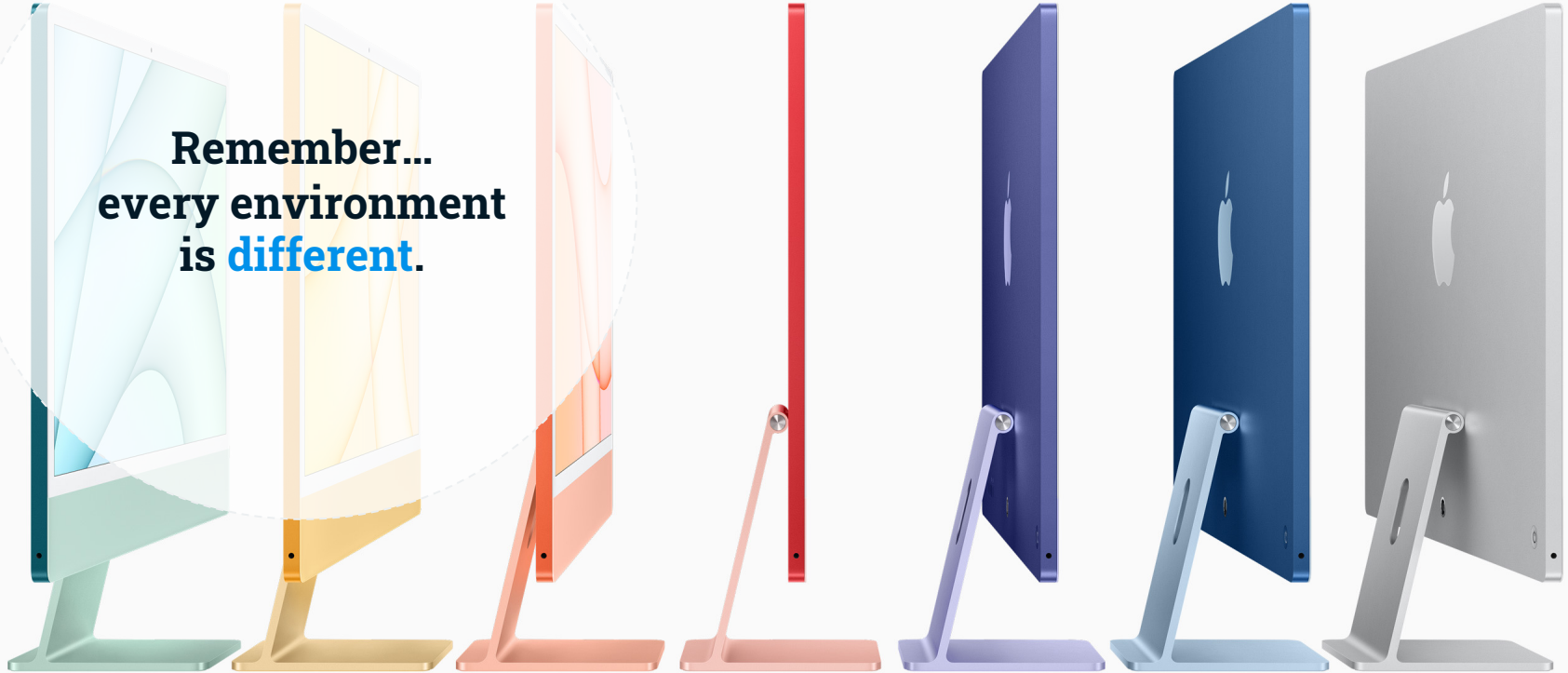
A decorative network diagram in the top-left corner, featuring a cluster of interconnected nodes. Some nodes are solid grey circles, while others are white circles with grey outlines. They are connected by thin grey lines, some of which are solid and others dashed.

2.

The Process

Make a plan, communicate it, do it

Remember...
every environment
is different.



Things to keep in mind...

- ◎ Most Mac users are developers
 - Pretty tech savvy
 - Doing development for customers (making \$\$\$ for business)
- ◎ Don't break the business
- ◎ Secure first, enhance after
- ◎ Not erasing devices

On not erasing devices...

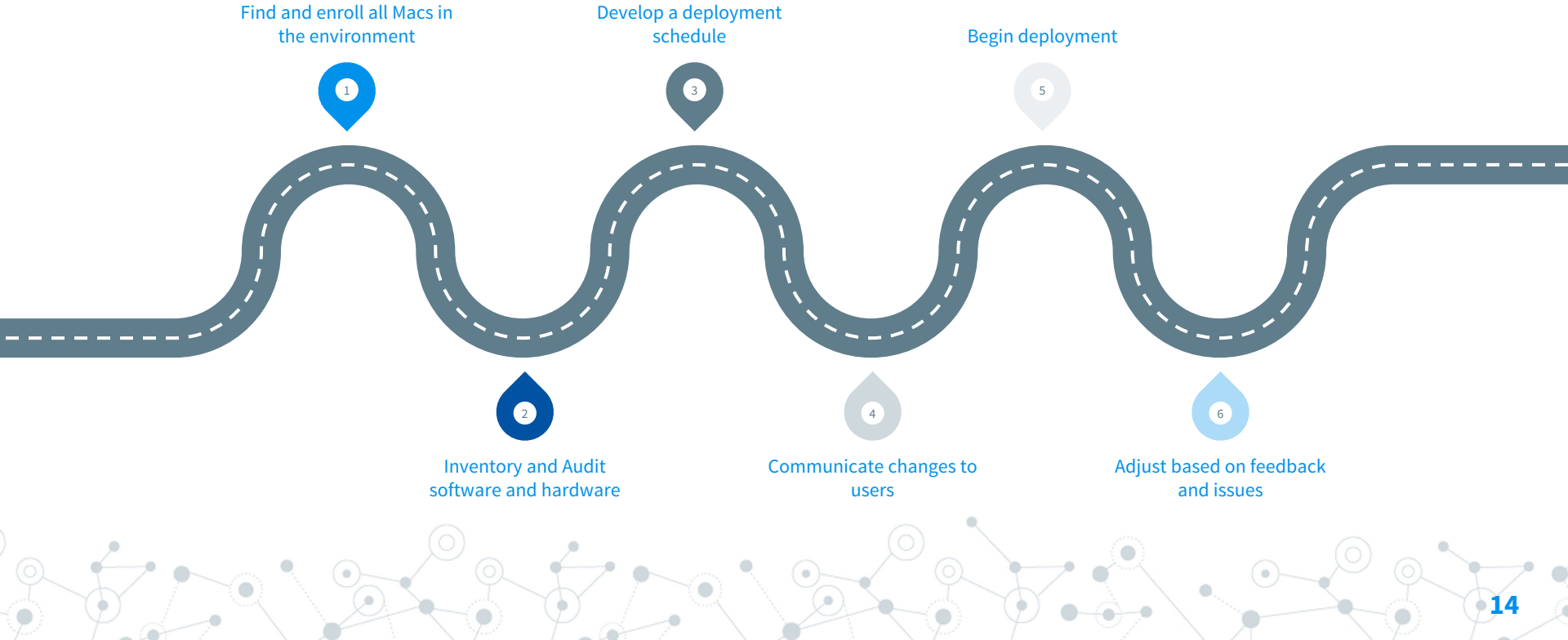
◎ Pros

- Won't stop work
- No need to collect machines
- Faster
- Will (hopefully) regain some trust with users
- Can always wipe if something goes wrong

◎ Cons

- Leave cruft on machines
- More prep
- Computers coming in unknown state

The Process (Simplified)



Find and enroll all Macs in the environment

- ◎ Used various methods to find the devices
 - Apple Business Manager
 - Purchase Records
 - VPN Logs
 - Anti-Virus Logs
 - Tickets
- ◎ Used various methods to enroll the devices
 - Blog/Forum/Newsletter Posts
 - Direct Emails to known users
 - Push with Anti-Virus server

Inventory and Audit software and hardware

- ◎ Collect application information
 - Identify known not-approved/problematic software
 - Find non-enterprise security software
- ◎ OS Inventory
- ◎ Hardware inventory
 - Do we need to retire any devices?
 - What kind of performance issues will we run into?
 - What models are “most popular”

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue.

Develop a deployment schedule

Why not just push a button?

Just Push everything out!



Why not just push a button?

	A	B	C	D	E
1	section #	recommendation #	title	status	assessment status
2	1		Install Updates, Patches and Additional Security Software	published	
3	1	1.7	Computer Name Considerations	published	Manual
4	2		System Preferences	published	
5	2.1		Bluetooth	published	
6	2.2		Date & Time	published	
7	2.3		Desktop & Screen Saver	published	
8	2.3	2.3.2	Secure screen saver corners	published	Automated
9	2.4		Sharing	published	
10	2.4	2.4.10	Disable Content Caching	published	Automated
11	2.4	2.4.11	Disable Media Sharing	published	Automated
12	2.5		Security & Privacy	published	
13	2.5	2.5.3	Enable Location Services	published	Automated
14	2.5	2.5.4	Monitor Location Services Access	published	Manual
15	2.5	2.5.5	Disable sending diagnostic and usage data to Apple	published	Automated
16	2.5	2.5.7	Camera Privacy and Confidentiality Concerns	published	Manual
17	2.5.1		Encryption	published	
18	2.5.2		Firewall	published	
19	2.6		iCloud	published	
20	2.6	2.6.1	iCloud configuration	published	Manual
21	2.6	2.6.2	iCloud keychain	published	Manual
22	2.6	2.6.3	iCloud Drive	published	Manual
23	2.6	2.6.4	iCloud Drive Document and Desktop sync	published	Manual
24	2.7		Time Machine	published	
25	2.7	2.7.1	Time Machine Auto-Backup	published	Automated
26	3		Logging and Auditing	published	
27	3	5.2	Configure Security Auditing Flags per local organizational requirements	published	Manual
28	3	5.7	Software Inventory Considerations	published	Manual
29	4		Network Configurations	published	
30	4	4.1	Disable Bonjour advertising service	published	Automated
31	4	4.3	Create network specific locations	published	Manual
32	4	4.6	Review Wi-Fi Settings	published	Manual
33	5		System Access, Authentication and Authorization	published	
34	5.1		File System Permissions and Access Controls	published	
35	5.1	5.1.4	Check Library folder for world writable files	published	Automated
36	5.2		Password Management	published	
37	5.2	5.2.3	Complex passwords must contain an Alphabetic Character	published	Manual
38	5.2	5.2.4	Complex passwords must contain a Numeric Character	published	Manual
39	5.2	5.2.5	Complex passwords must contain a Special Character	published	Manual
40	5.2	5.2.6	Complex passwords must uppercase and lowercase letters	published	Manual
41	5	5.4	Automatically lock the login keychain for inactivity	published	Manual
42	5	5.6	Ensure login keychain is locked when the computer sleeps	published	Manual
43	5	5.10	Ensure system is set to hibernate	published	Automated
44	5	5.14	Create a Login window banner	published	Automated
45	5	5.16	Disable Fast User Switching	published	Manual
46	5	5.17	Secure individual keychains and items	published	Manual
47	6		User Accounts and Environment	published	
48	6.1		Accounts Preferences Action Items	published	
49	7		Appendix: Additional Considerations	published	
50	7	7.1	Extensible Firmware Interface (EFI) password	published	Manual
51	7	7.2	FileVault and Local Account Password Reset using AppleID	published	Manual
52	7	7.4	App Store Password Settings	published	Manual
53	7	7.6	System information backup to remote computers	published	Manual

66	5.2	5.2.7	Password Age	published	Automated
67	5.2	5.2.8	Password History	published	Automated
68	5	5.3	Reduce the sudo timeout period	published	Automated
69	5	5.5	Use a separate timestamp for each user/tty combo	published	Automated
70	5	5.7	Do not enable the "root" account	published	Automated
71	5	5.8	Disable automatic login	published	Automated
72	5	5.9	Require a password to wake the computer from sleep or screen saver	published	Manual
73	5	5.11	Require an administrator password to access system-wide preferences	published	Automated
74	5	5.12	Ensure an administrator account cannot login to another user's active and locked session	published	Automated
75	5	5.13	Create a custom message for the Login Screen	published	Automated
76	5	5.15	Do not enter a password-related hint	published	Automated
77	5	5.18	System Integrity Protection status	published	Automated
78	5	5.19	Enable Library Validation	published	Automated
79	6		User Accounts and Environment	published	
80	6.1		Accounts Preferences Action Items	published	
81	6.1	6.1.1	Display login window as name and password	published	Automated
82	6.1	6.1.2	Disable "Show password hints"	published	Automated
83	6.1	6.1.3	Disable guest account login	published	Automated
84	6.1	6.1.4	Disable "Allow guests to connect to shared folders"	published	Automated
85	6.1	6.1.5	Remove Guest home folder	published	Automated
86	6	6.2	Turn on filename extensions	published	Automated
87	6	6.3	Disable the automatic run of safe files in Safari	published	Manual
88	7		Appendix: Additional Considerations	published	
89	7	7.3	Repairing permissions is no longer needed	published	Manual
90	7	7.5	Apple Watch features with macOS	published	Manual
91	7	7.7	Unified logging	published	Manual
92	7	7.8	AirDrop security considerations	published	Manual
93	7	7.9	Touch ID	published	Manual
94	7	7.10	Sidcar	published	Manual
95	7	7.11	Screen Time	published	Manual

Define Metrics



User Impact

How much impact will this cause to the user once implemented?



Ease of Deployment

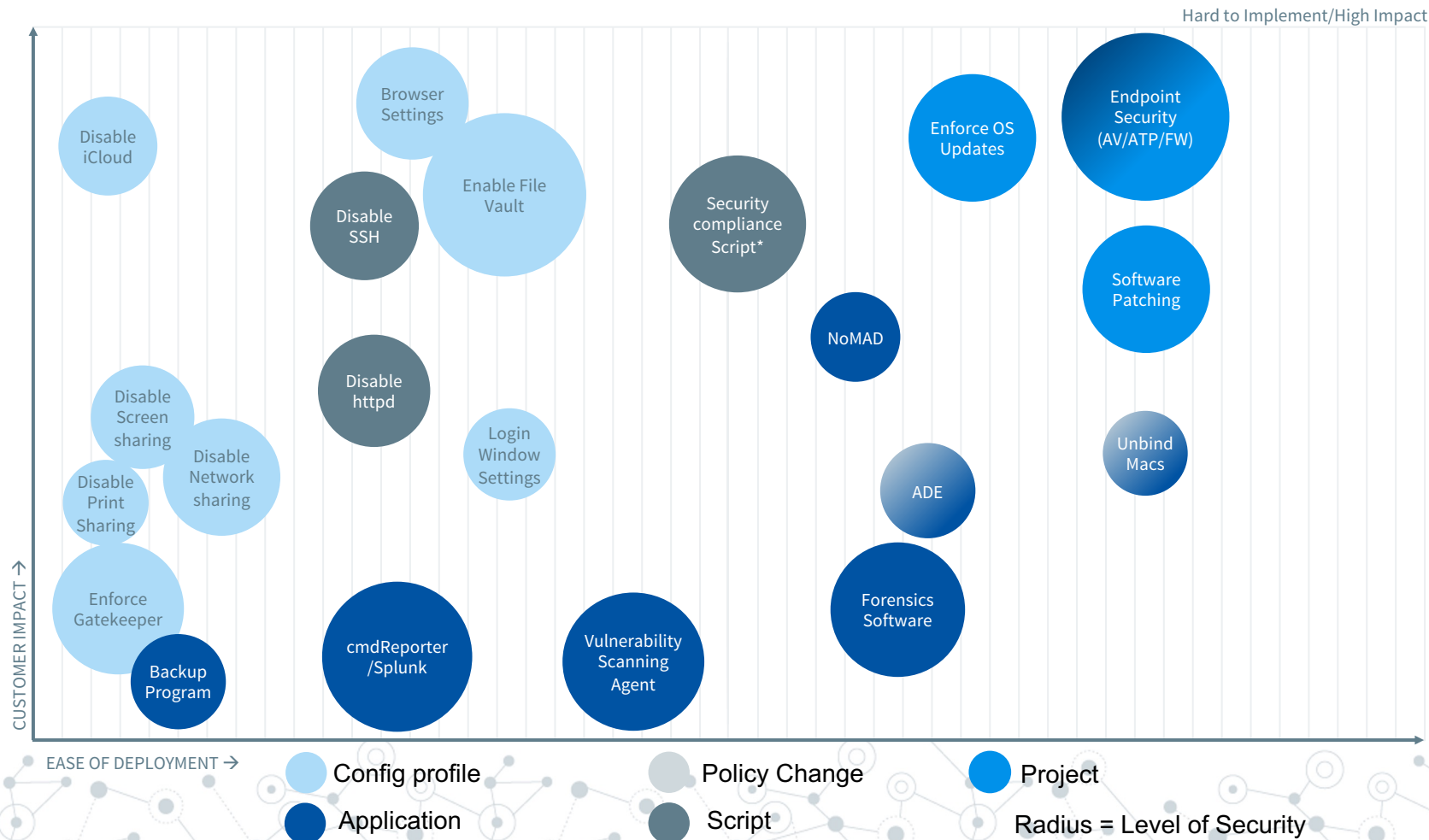
How easy is the control to deploy?



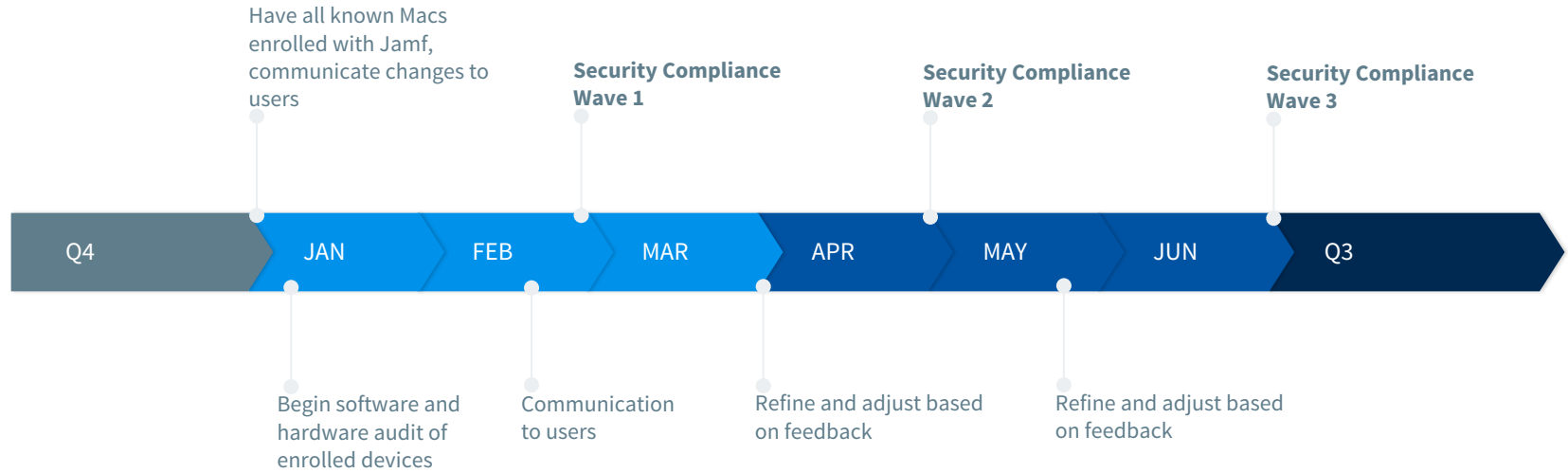
Level of Security

How much more secure does the change make the machine?

Deployment Graph



Timeline



Communication advice

- ◎ Let them know about things they will notice immediately
- ◎ Notify users about major policy changes
- ◎ Don't list every change
- ◎ Collect feedback
- ◎ Communicate using different mediums
- ◎ Don't use technical jargon
- ◎ Try to give the “positive impacts” of the changes
- ◎ Communicate every wave

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels or types of nodes. The lines are thin and gray, connecting the nodes in a non-linear fashion.

3.

Implementation

Do all of the things....in waves!

Deployment

- ◎ Tools used:
 - Jamf Pro
 - [Jamf CIS Scripts](#) (customized)
 - Config Profiles
 - Various scripts
 - Vendor provided packages and scripts

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are solid grey and others are hollow with a grey outline. The lines connecting them are thin and grey, creating a dense, organic structure.

So...

Who goes first?

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes being solid grey and others hollow with grey outlines. The overall shape is more triangular and less dense than the top-left diagram.

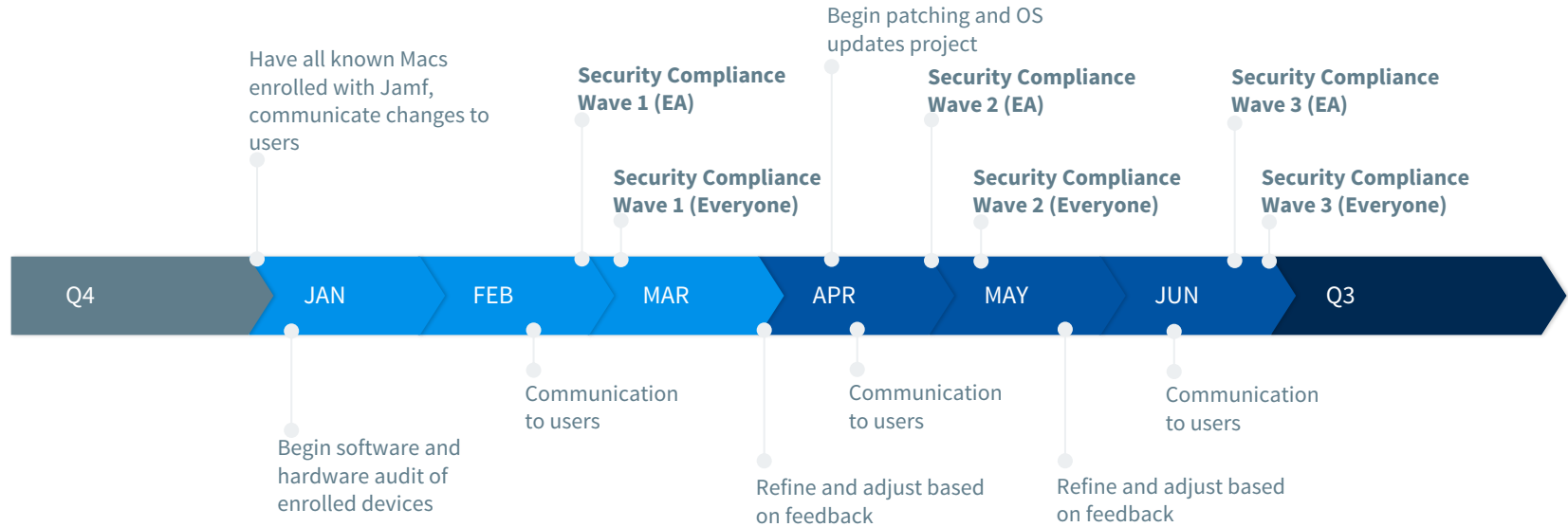
Early Adopters



Early Adopters

- ◎ Find them **early**
- ◎ Get a good mixture of user types
 - IT staff make great early adopters
- ◎ Communicate and follow-up

Timeline (Revised)





\$48,000


Under budget

1

Data loss incident

75%

Decrease in vulnerabilities per machine



Total Devices ▾	Low ▾	Medium ▾	High ▾	Critical ▾	Total ▾	Ratio (avg Vulns per Device) ▾
260	64	291	1131	243	1729	6.38
254	65	232	888	358	1543	6.07
259	62	219	1214	217	1712	6.61
223	63	905	2944	493	4405	19.75
280	248	929	3124	528	4830	17.25
284	333	1071	3116	528	5048	17.77
289	385	1055	3106	535	5081	17.58
291	375	632	1503	149	2659	9.14
302	390	285	1290	118	2083	6.90
302	393	229	1116	116	1854	6.14
299	382	176	1010	81	1649	5.52
288	407	292	908	56	1663	5.77
293	421	420	737	258	1836	6.27
297	417	298	154	62	931	3.13
299	418	163	160	153	894	2.99
299	418	163	160	153	894	2.99
297	415	133	255	210	1013	3.41
305	422	105	248	83	858	2.81
306	386	106	388	124	1004	3.28
294	368	190	330	221	1109	3.77
289	366	69	250	73	758	2.62
287	360	67	223	61	711	2.48
287	360	67	223	61	711	2.48
174	65	34	122	142	363	2.09
136	51	31	146	42	270	1.99
119	35	25	128	65	253	2.13
149	9	18	183	37	247	1.66
264	9	126	153	293	581	2.20
253	9	342	148	97	596	2.36
331	4	676	836	66	1582	4.78
331	4	676	836	66	1582	4.78
334	2	588	786	37	1413	4.23
341	2	596	750	105	1453	5.22
351	2	756	592	60	1410	4.02
346	2	771	551	110	1434	4.14
366	2	766	545	33	1346	3.68
371	20	654	560	116	1350	3.64
383	29	721	742	385	1877	4.90
387	30	848	809	84	1771	4.58
382	31	839	722	41	1633	4.27
392	31	913	690	31	1665	4.25

Lessons Learned

- ◎ Identify early adopters first
- ◎ Focus on patching separately
- ◎ Write more KBs and user support docs
 - Find support people to help
- ◎ It's better to be late than wrong
- ◎ Don't ignore Macs!






Thanks!

Any questions?

@jmahlman
yearothegeek.net



Resources

- © Jamf CIS Scripts: <https://github.com/jamf/CIS-for-macOS-Catalina-CP>
- © macOS Security Compliance Project: https://github.com/usnistgov/macOS_security
- © CMMC Website: <https://www.acq.osd.mil/cmmc/>
- © NIST 800-171 Rev. 2 Documentation: <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>