Michael Linde

Michael has been a Mac tech ever since breaking a brand new Quadra 950 in 1994. He spent 7 years as a software developer during the dot-com boom, 4 years with Apple as a Mac Genius, 3 years in a large healthcare organization in New England, and 7 years at Starz Entertainment in a variety of IT roles. He is currently a Solutions Engineer focusing on infrastructure solutions for creative design and post production.

Michael has been a lifeguard, ski instructor, nightclub DJ, pre-press technician, artist, and bike racer.

When not working, Michael spends time with his family and his bicycles.

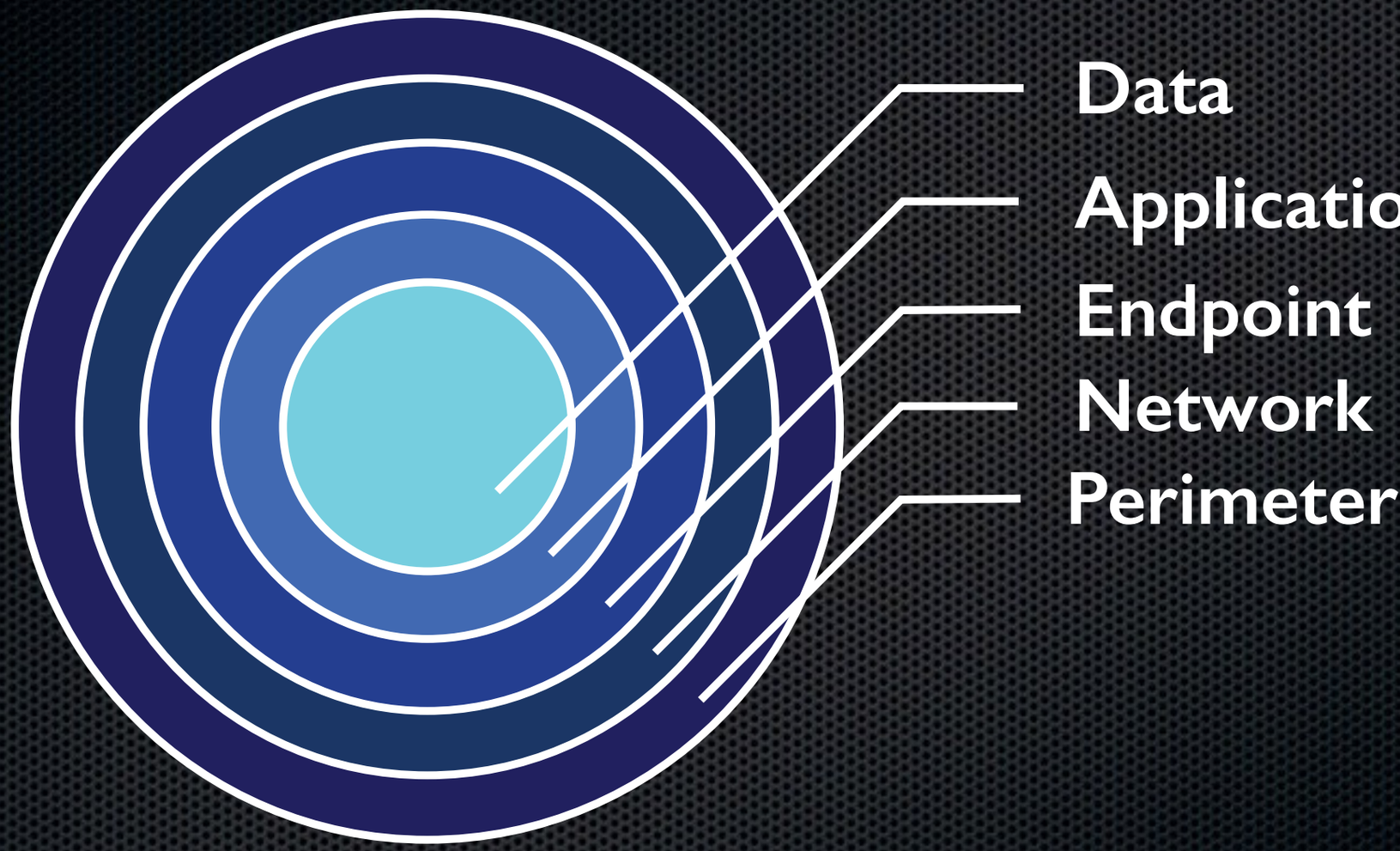
Security, Viruses, and Malware.
It's real. It's now.
You need to take it seriously

MACTECH PRO EVENTS

Practical Security

- Practical security is a trade off between convenience and safety.
- There is no single set of rules that are right for every situation.
- Balance your customers needs and wants with acceptable risk and security.
- Sometimes you have to tell them no.

Layers of Security



Perimeter & Network Security

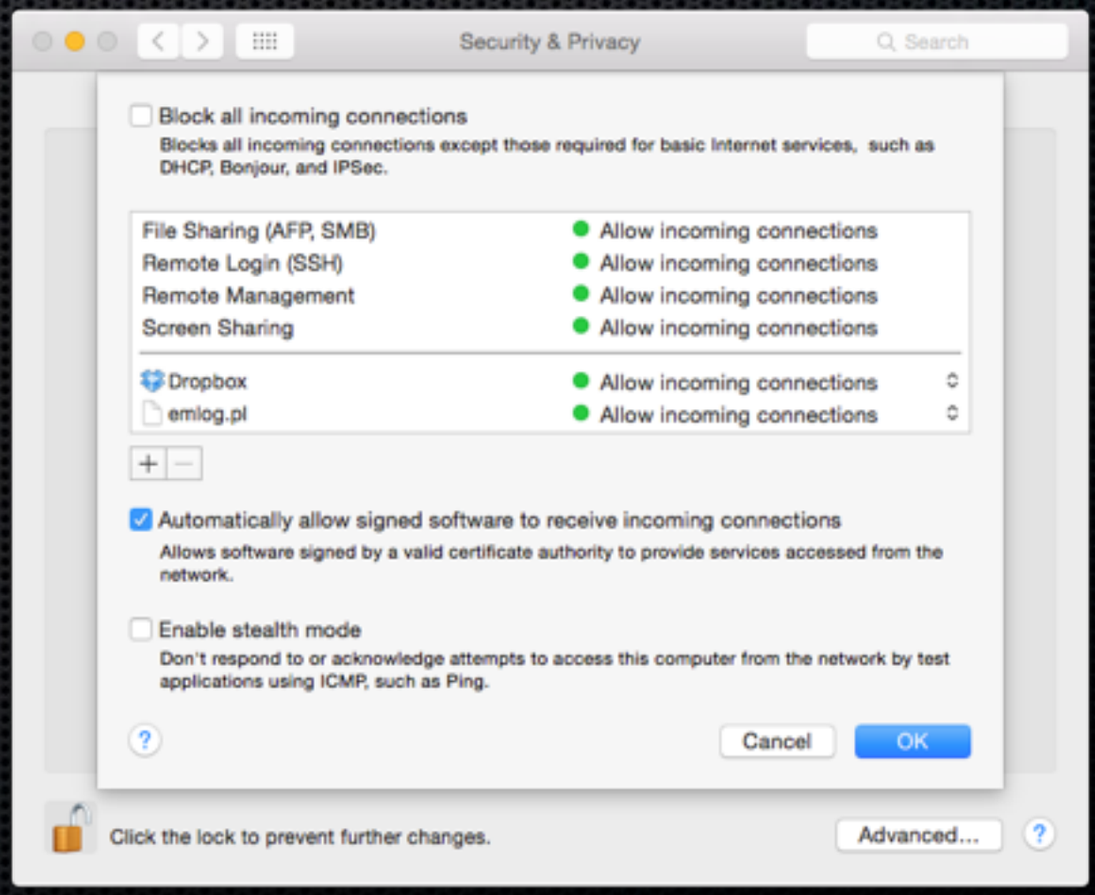
- Firewalls
  - How they work
  - Often a simple way to keep out the bad guys
- VPN
  - What and why?
- Simple solution: OS X Server
  - Offers a full suite of "edge" tools
  - Can be combined with a edge appliance to create a DMZ.

Endpoint Security

- OS X
  - Firewall
  - Passwords
  - FileVault
  - Adblockers and AntiVirus
- iOS
  - Passcode
  - VPN

OS X Firewall

- Built-in to OS X
- Simple setup
- Application Layer Firewall
- krypted.com for in depth articles to manage the firewall in OS X.



Password management

- Myths
  - Changing passwords every xxx days
  - Myth: You shouldn't use real words. Truth: You can if long enough
  - Myth: Don't write things in Apple Notes, OneNote or other note taking software.
- Reality and Best Practices:
  "My, you look lovely today!" vs. "mYy0ul00kl0v3ly"

Length is important.

- Go as long as you can 12, 15 and even 20+ characters - 14 is a good count.
- Use a password manager -- choose what matches you best
  - 1Password
  - LastPass
  - iCloud Keychain
- Ok to keep notes (but not passwords) in any SSL/ encryption protected app: Notes, OneNote, etc…
  - Some people even use secure notes in Keychain
  - Beware of "replacing" the keychain, however

FileVault

- Native Disk Encryption
- XTS-AES 128 bit encryption
- Requires the OS X Recovery volume
- User-specific access
- Recovery Keys are CRITICAL

iOS Security

- Built in hardware encryption
- Complex passcode + Touch ID
- Secure, sandboxed application environment
- VPN connectivity via 3PP application or network settings, including VPN on demand.

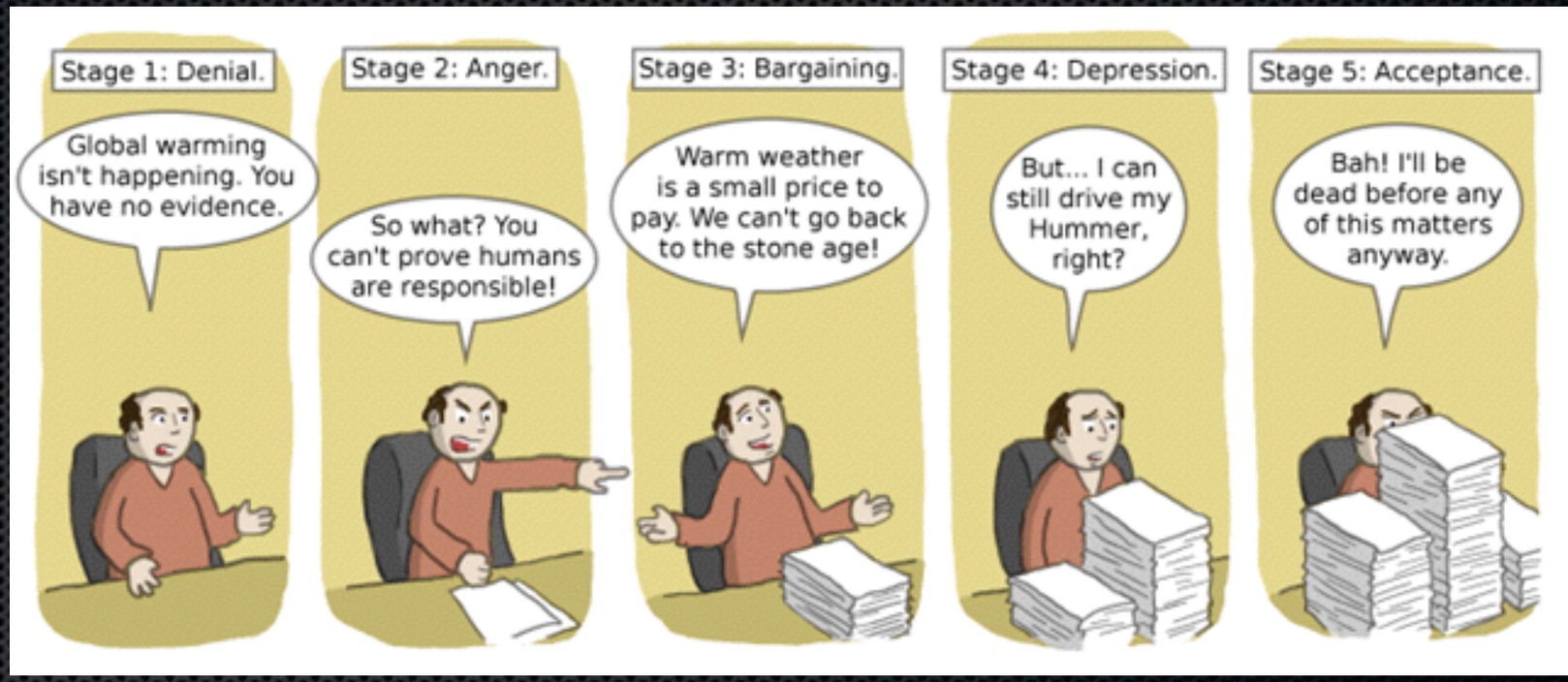
Application & Data Security

- Where possible, use SSO/authentication for application access to sensitive data.
- Secure application communications (https/ssl/vpn)
- Classify data and isolate sensitive or critical data
- Cloud data is public data (eventually)

Security Threats

5 Stages of Mac Security

- Denial
- Anger
- Bargaining
- Depression
- Acceptance



What's the difference?

- Viruses
- MalWare
- AdWare
- Trojans

Viruses, the history of viruses coming to our platform

- 1980's forward, Being an uninfected carrier
- 1990's forward, Word Macro Viruses
- AdWare: First appeared in 2012
- Malware: From the early 1980s.
- Trojan horses appeared on Mac in 2012 (Flashback Trojan)

Moving from complacent to vigilant one decade at a time

- Virus scanning software an Enterprise requirement
- Virus scanning software a best practice
- Virus scanning software, it may be necessary to protect productivity
- It finally really matters on a personal level

Modern Threats

- Mac users encountered an average of 9 threats in 2014
- Almost half of the top 20 are Adware
- Phishing
- Trojan keyloggers
- Data theft (of Mac and tethered iOS devices)
- Remote access backdoors
- Screen Scrapers

Statistics

- Estimated over 5% of iPhone users (globally) have jailbroken their devices
- Even non-jailbroken phones could be susceptible
- Millions of Macs are likely infected and people don't know (e.g., emails with Windows viruses).
- Likely a large portion of those Macs are infected and causing trouble
- Many Mac consultants think they know how to deal with viruses on a Mac but often don't

Developing a strategy

- There is no "singular solution" - every environment has different risks and needs.
- Identify the risks in your environment, and the environments you support.
- Research the tools to mitigate those risks and deploy the best solution for each environment
- Train your users.
- Bottom Line: Strategy is about risk management

Strategy: Securing Infrastructure

- Email
- Databases
- Websites
- Storage

Strategy: Email Continuity, Spam and Virus filtering

- MXlogic
- SpamSoap (now Nuvotera)
- eVitera
- Barracuda's ESS
- Appliances or Cloud Services

Strategy: Securing Data

- Web-based attacks
  - SQL injection attacks
  - Cross-site scripting attacks
  - OWASP Top 10
- Securing storage
  - Classifying data
  - Isolating sensitive data
  - Logging data access

Strategy: Virus Protection and Eradication

- AntiVirus options
  - Client-Server
  - Standalone

Strategy: Monitoring Systems

- Protection services
- Management software such as Watchman Monitoring detects malware and notifies you

Strategy: Users

- Users are the greatest threat and weakness in any security plan. They are also your greatest asset.
- Educate your users about security threats (social engineering, identity theft, data loss prevention).
- Treat them as partners in the security equation to gain their support and understanding

Strategy: Tools

- Watchman Monitoring - https://www.watchmanmonitoring.com
- Ghostery - https://www.ghostery.com/
- AdBlock - https://getadblock.com
- AdwareMedic (now Malware Bytes) - https://www.malwarebytes.org/antimalware/mac/
- Anti-Virus
  - BitDefender Virus Scanner: Free
  - Sophos
  - McAfee

Avoiding Adware Scanner Utilities

- How bad is Genieo?
  - Genieo virus
  - Hard to remove. Proceed with caution
  - Utilities for removal
- MacProtector
- MacKeeper
- Avoid good software from bad sources.

Educate yourself

- SANS.ORG
- “The Art of Deception” by Kevin Mitnick
- “The Basics of Hacking and Penetration Testing” by Patrick Engebretson
- “Security + Guide to Network Security Fundamentals” by Mark Ciampa
- Help Net Security weekly email

More Resources

- https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/
- http://www.thesafemac.com
- https://krypted.com
- https://net-security.com
- https://www.owasp.org/index.php/OWASP_Top_10
- http://www.intego.com/mac-security-blog/
- https://www.reddit.com/r/netsecstudents

Questions?

@mlinde
mlinde@gmail.com