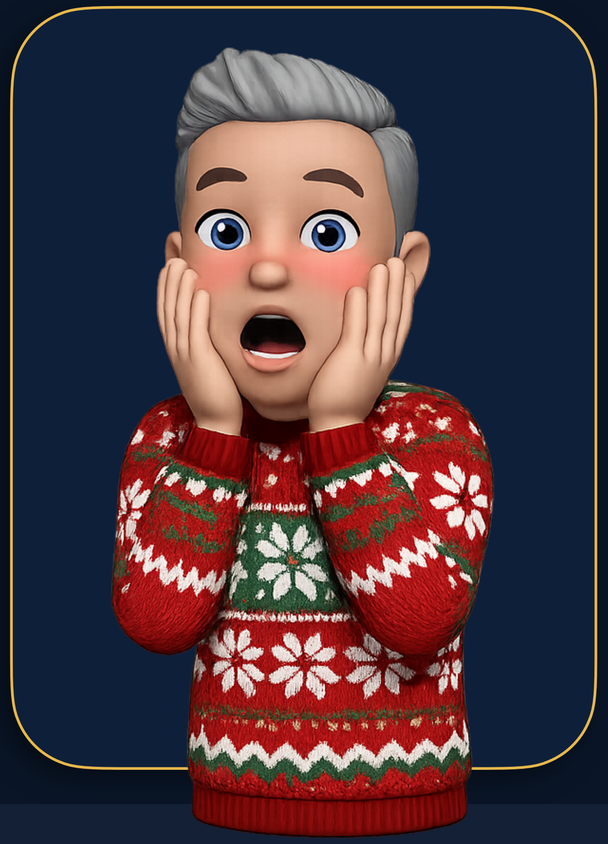

MacSysadmin 2026
YOU'RE NOT
HOME ALONe
with APPLE PLATFORM ZERO TRUST
Starring: Kenneth Villadsen & Ulrik Aabye-Hansen

Good afternoon...

Kenneth Villadsen



Ulrik Aabye-Hansen



Session materials & references available at yourenothomealone.com



disclaimer

This presentation makes use of references, imagery, and characters inspired by the popular movie "Home Alone"

References are employed strictly for satire, parody and educational purposes, and are not intended as copyright infringement on any copyrighted material.

All characters and names remain the property of their respective rights holders.

Kevin's Chores

5 acts. One very clever kid.

The Old World

Castle & Moat | perimeter trust and why it fails

Meet the Wet Bandits

Social engineering, reconnaissance, and the fatal flaw

Kevin is Home

Zero Trust : never trust, always verify

Apple's Five Layers

Hardware → Software → Device → Enrollment → User

Key takeaways

Practical steps for Mac admins today



The Old World

Castle & Moat • perimeter trust and why it fails

The Castle & Moat

One barrier. Everything inside is trusted.

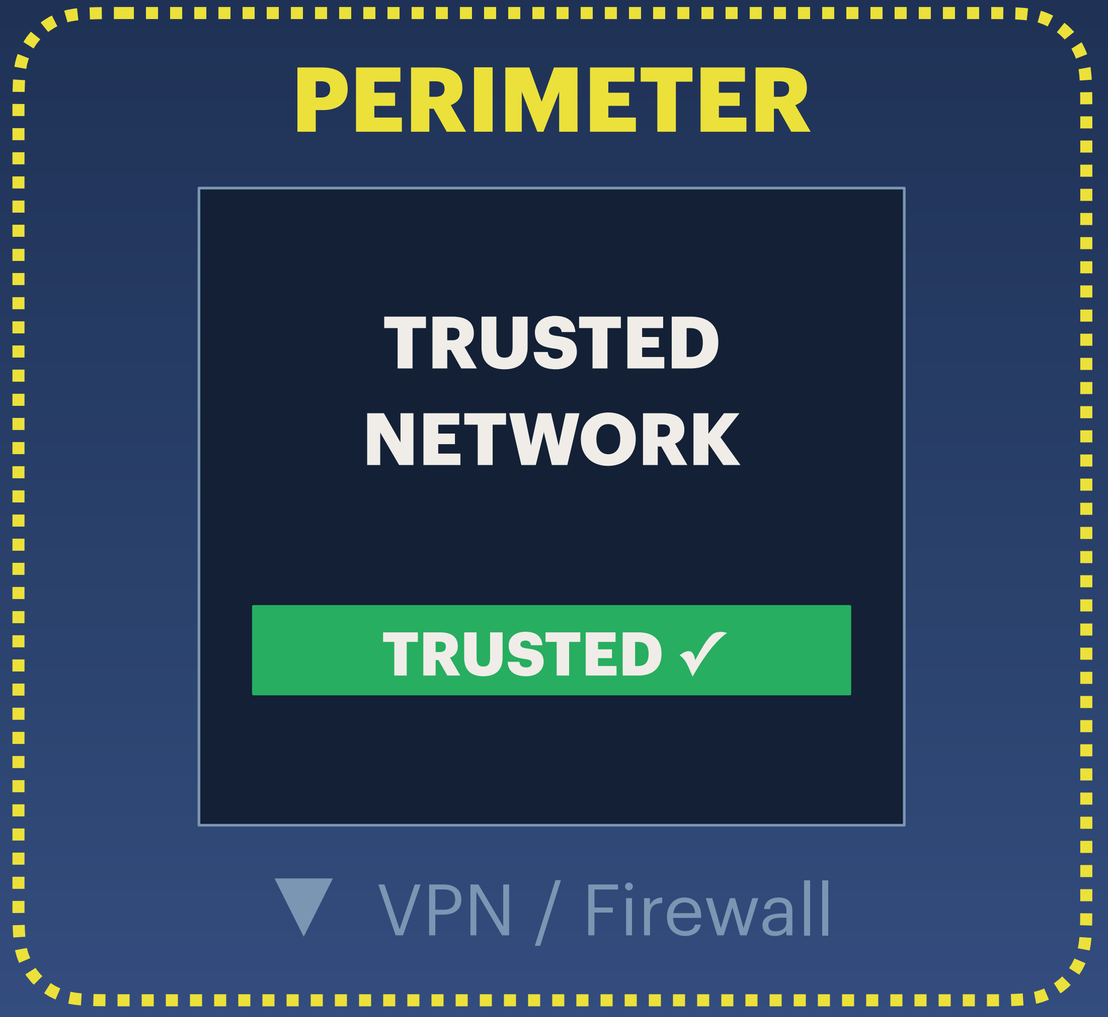
VPN grants full network access

On-prem resources trust the network join

Lateral movement is trivial once inside

Identity assumed, never re-verified

Devices never left the office...



Meet the Wet Bandits

HARRY LIME



The Mastermind

Disguises as police officer

Conducts 'security surveys' of homes

Maps targets, schedules, and weaknesses

Trusted once past the front door

MARV MERCHANTS



The Executor

Exploits open entry points

Moves freely inside trusted perimeter

Leaves a trail

Assumes the inside is always safe

Harry's Masterplan

A perfect social engineering attack — four steps



Impersonate

Dress as a police officer and establish authority and trust before asking a single question



Reconnaissance

Interview every family in the street. Who's home? When do they leave? What's the layout?



Target Selection

Choose the richest, emptiest house. Build the complete picture before the attack



Exploit

Cross the perimeter. Once inside, no further challenge. The castle is yours.



Once inside : fully trusted.

No re-verification. No continuous monitoring.

No second challenge.

The perimeter was the only lock on the door.



Kevin Is Home

All by himself, mistrusting by nature

"Never trust, always verify."

Verify Explicitly

Always authenticate & authorise based on all available data

Least Privilege

Limit access with just-in-time and just-enough access

Assume Breach

Minimise blast radius. Segment networks. Encrypt everything.

— NIST SP 800-207 Zero Trust Architecture

Apple's Five Defence Layers



User Identity Platform SSO · Passkeys



Deployment Trust Automated Device Enrollment



Device Identity Managed Device Attestation · ACME Protocol



Software Trust Signed System Volume, SIP



Hardware Trust Apple Silicon · Secure Enclave · Secure Boot



Hardware trust

Apple Silicon · Secure Enclave · Secure Boot

Apple silicon

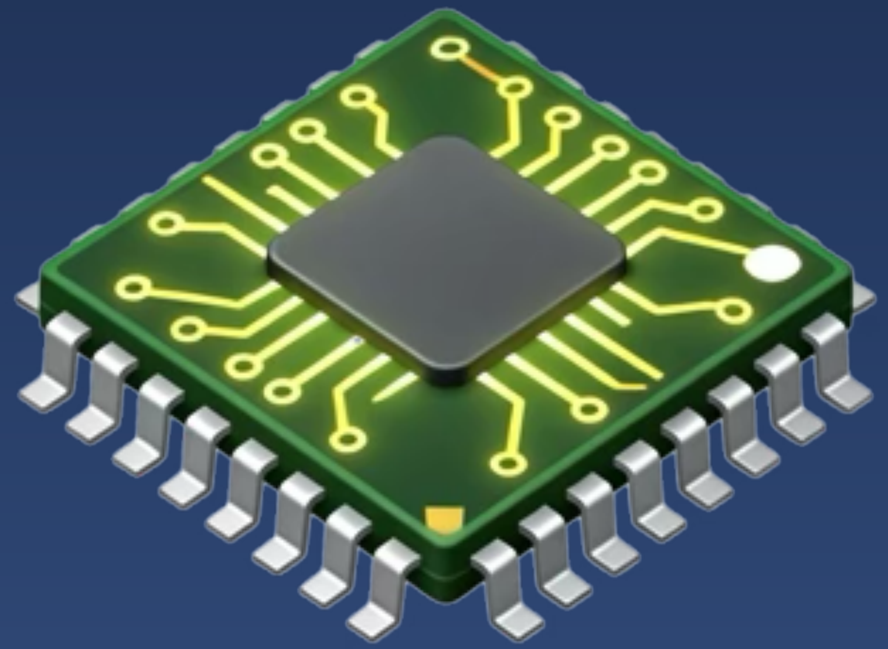
Where hardware trust begins

Secure Enclave

Secure boot

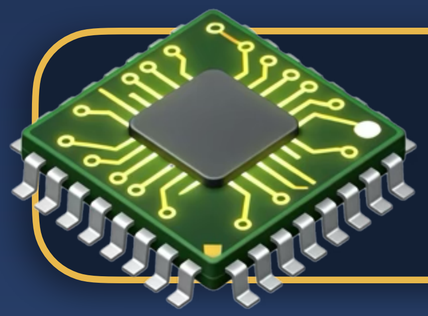
Automatic encryption

New security features



The Secure Enclave

A vault inside every Apple device — invisible to the OS



Unique Device ID



Biometrics



Key Storage

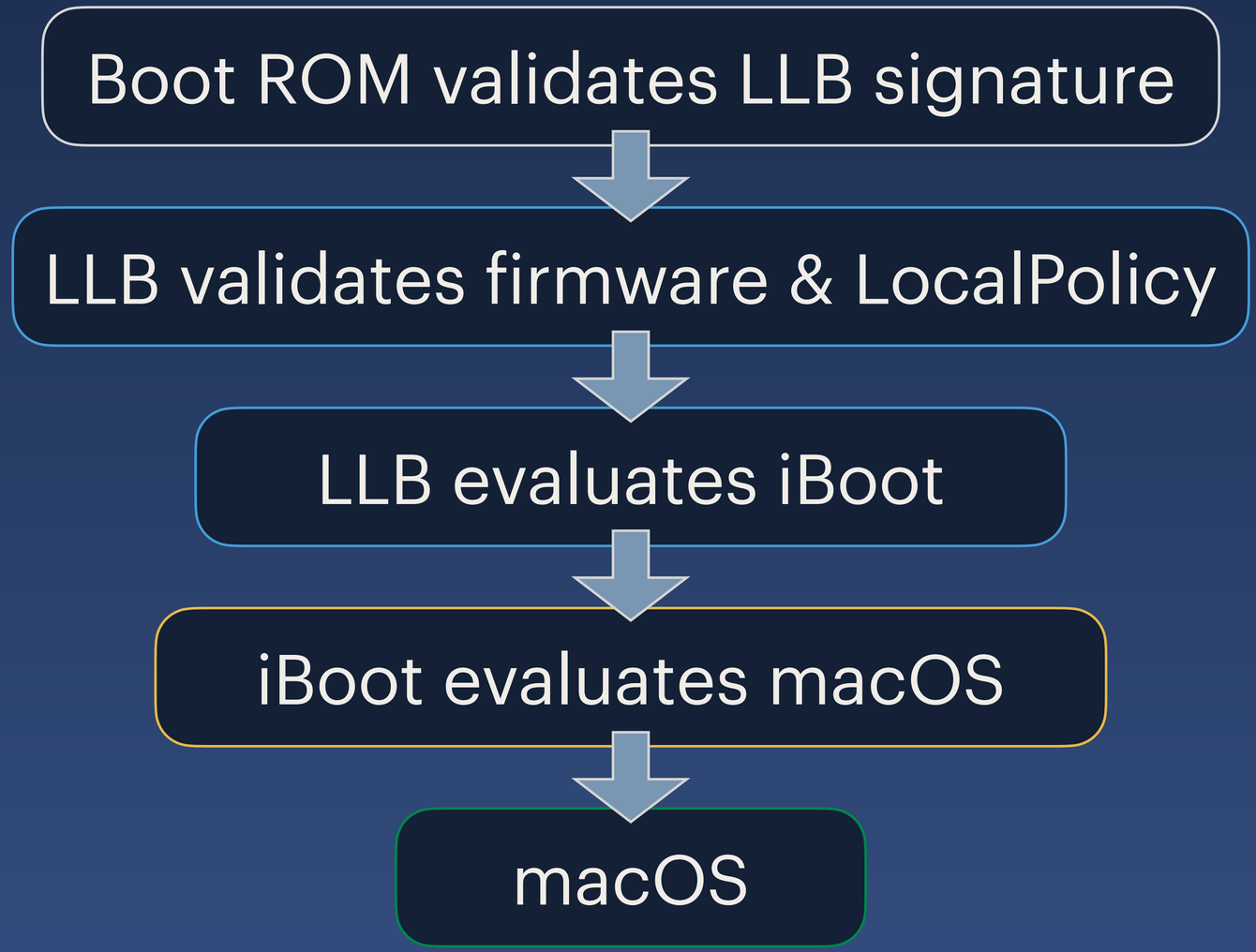


Data Protection



Secure Boot

The verified boot chain












PLEASE
UNARM.
1
2
3
4
5
6
7
8
9
0



Software trust

Signed System Volume • System Integrity Protection

System Integrity Protection

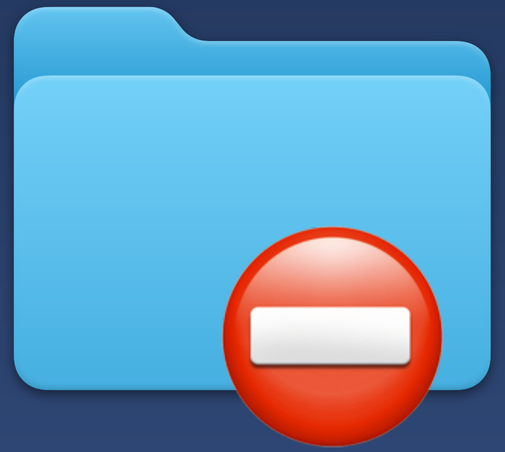
The basement is rigged

El Capitan 2015

Limits what even the root user can do

Denies write access to system files on disk

Prevents software to select a startup disk




Christmas

Signed System Volume

The treehouse rests upon a Merkle tree



Cryptographically signed system volume

macOS boots from snapshot

Improves macOS updates

No need for FileVault





System Installation

Re-installing System
“McCalister House”

Copying files...

91%

Cancel



Device Identity

Managed Device Attestation · ACME Protocol

Managed Device Attestation

The device proves it is what it claims to be — cryptographically, to your MDM

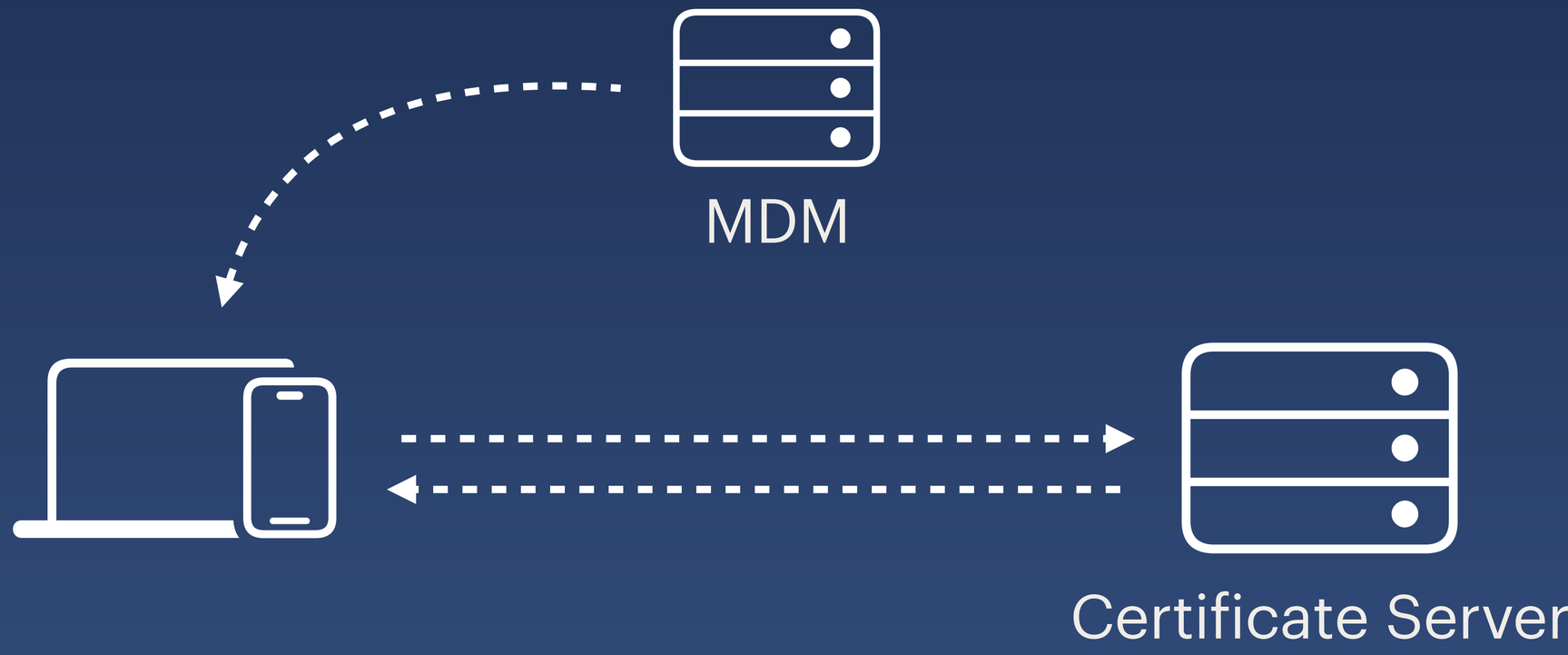
MDA attests:

- Genuine Apple hardware (not virtualised)
- Device identity (Serial and UDID)
- Software state (sepOS, LLB, iBoot, macOS)
- macOS state (SIP, kext auth, SecureBoot)
- Freshness (Live attestation vs old replay)

Managed Device Attestation

The device proves it is what it claims to be — cryptographically, to your MDM

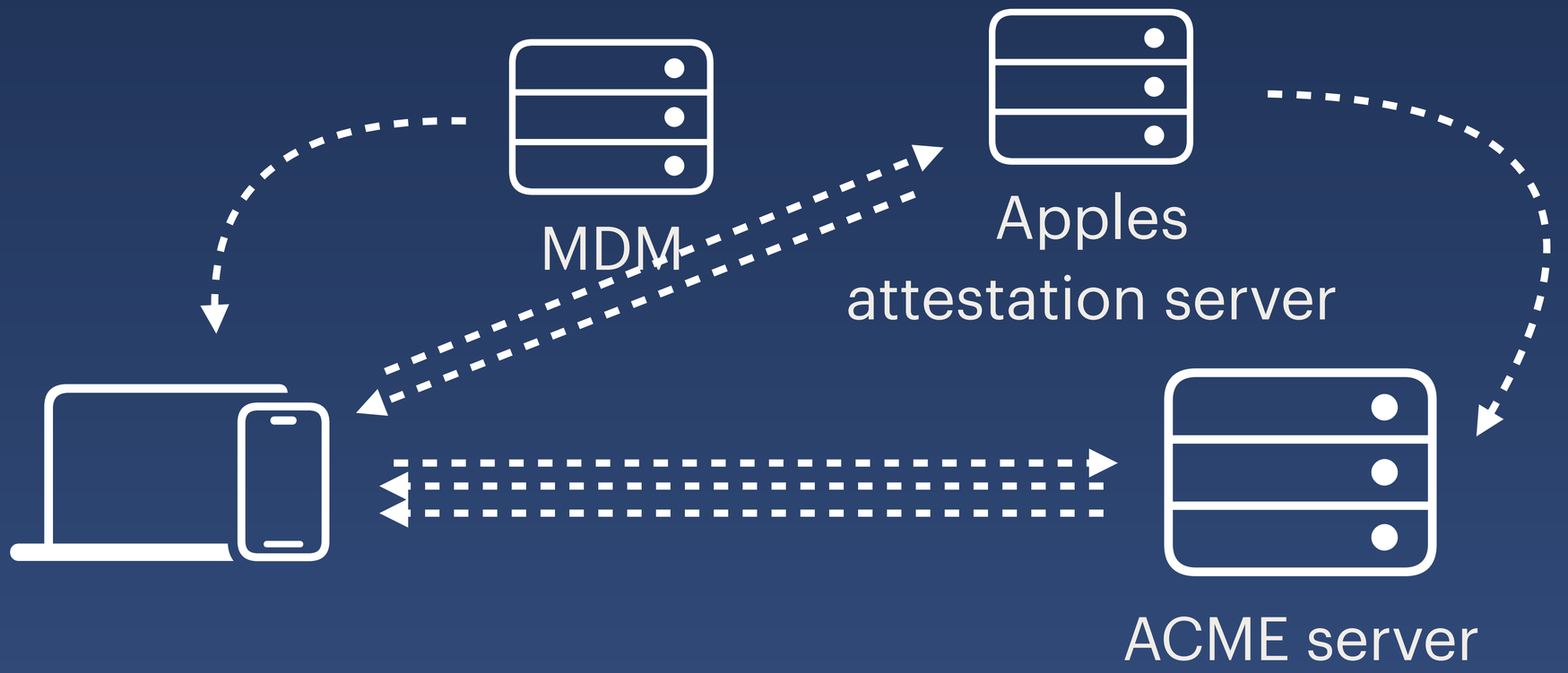
How it works (SCEP):



Managed Device Attestation

The device proves it is what it claims to be — cryptographically, to your MDM

How ACME works:




ACME
SLIPPERY
BANANAS


Little
Nero's
Pizza
CALL
555-8385
NO FIDDLIN'
AROUND
ANGELS
WITH
FILTHY SOULS



Deployment Trust

Automated Device Enrollment

Deployment Scenarios

Base device trust with Apple Business

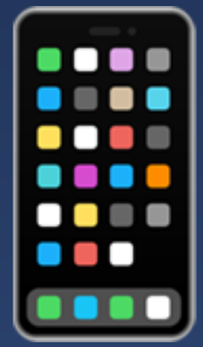


Corporate Owned

Automated Device Enrollment



Mac



Mobile / iPad

Account-driven Device Enrollment

Account-driven User Enrollment

Registered Automobiles

Belonging to the McCalister Household

- 1990 Buick LeSabre
- 1986 Buick Electra Estate Wagon





Unknown Vehicle

Denied Access

- 1986 Dodge RAM Van





User Identity

Platform SSO · Passkeys

Platform SSO & Passkeys

Phishing resistant IdP credentials

(Platform) SSO



Single system-wide extension

macOS integrated with your IdP

Login window auth → cloud identity

Token stored in Secure Enclave

Passkeys



Replaces passwords with key pairs

Private key lives in Secure Enclave

Biometric unlock — Touch ID / Face ID

Phishing-resistant by design





Takeaways

Final Thoughts...

The Bandits Are Still Out There.

Kevin adapted. So must you.



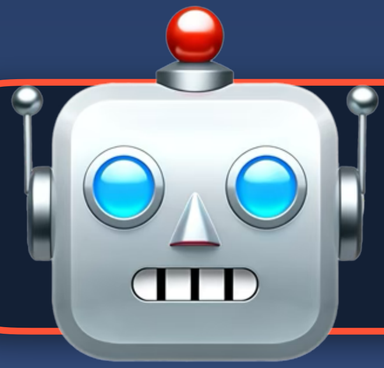
Phishing / Credential Theft



Supply Chain Attacks



Unmanaged Devices



AI Threats

Key Takeaways

1. Zero Trust is not a product — it's a mindset. Assume breach.
2. Apple's platform is a Zero Trust stack from the silicon up.
3. Managed Device Attestation is unique.
4. Platform SSO + Passkeys = phishing-resistant, hardware-bound user identity.
5. Start with Apple Business: own your devices.

Honorable Mentions

Gatekeeper



Codesigning



XProtect remediation



Thank you!

Thank you!