Your mac is lying to you!

Exposing hidden security risks

By Oktay Sari and Somesh Pathak

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Boots on the Ground, Head in the Cloud - Just a digital Cowboy, Ridin' the Rains of Change!

Oktay Sari
Microsoft MVP · Security & Windows and Devices

Role
Self Employed, Modern Workplace Consultant
@All Things Cloud BV

Focus
Intune · Security · macOS · Windows 365 · CIS · NIST

https://allthingscloud.blog

https://www.linkedin.com/in/oktaysari/

Somesh Pathak
Microsoft MVP · Security

Role
Manager, Modern Workplace Engineering, Avanade

Focus
Intune · Security · Copilot · M365 Administration

www.intuneirl.com

in/someshpathak/

newsletters/life-in-tremors

FAST PACE
↳ UNCOMPROMISED
FOCUS

A NOTE FROM YOUR SPEAKER:

As someone living with Parkinson's, my speech can sometimes accelerate. My presentation is structured for clarity to ensure you stay on track, regardless of my speed.

Thank you for your support and understanding.

Psst... MOST OF THESE PICTURES WERE MADE BY AI!

DUHHHH... OBVIOUS, RIGHT?

Agenda

- All Fake news! Misleading
- Create a secure macOS Foundation
- Demo 1: Use script-based audits
- Demo 2: Bypass GateKeeper
- Demo 3: Tools & deploying Baselines

Are Macs Really Safer Than PCs?

The Myth

- macOS has a ‘secure by default’ reputation
- **Reality:** many defaults create hidden risk

Attackers rely on these assumptions

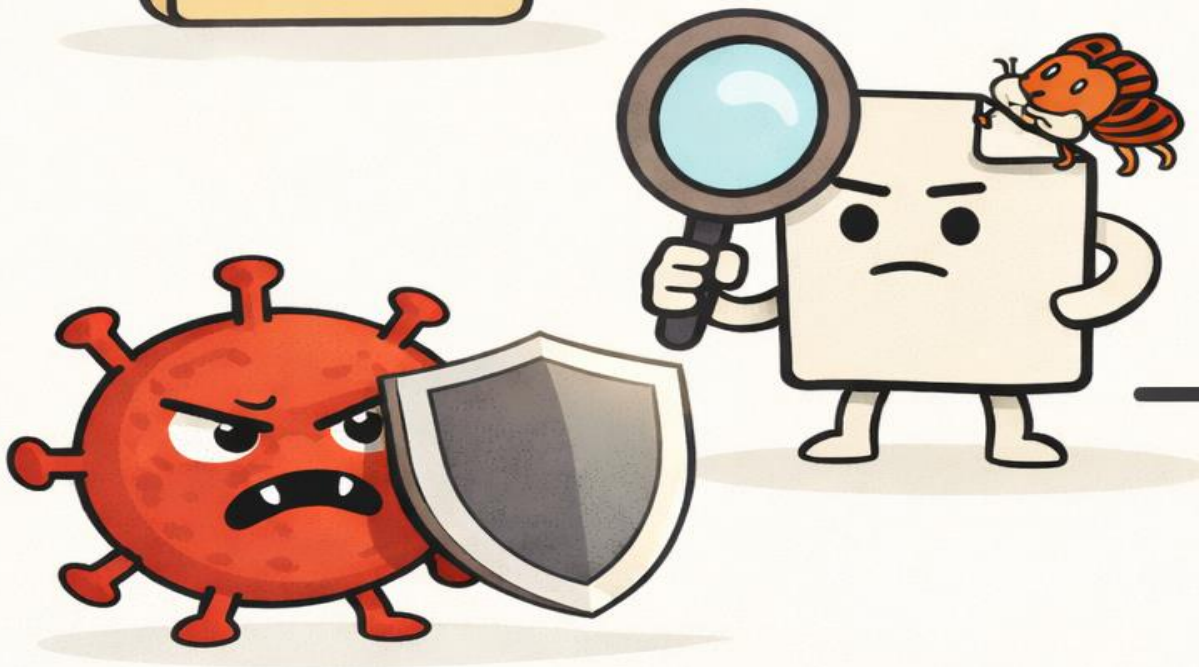

1: Learn which ‘secure’ settings are misleading, and how they can silently introduce risk into your environment.

What Makes macOS Secure (on paper)

Gatekeeper

→ **Blocks** unverified apps

(unless they wear a fake badge)



XProtect → Silent malware scanner, signature-based only

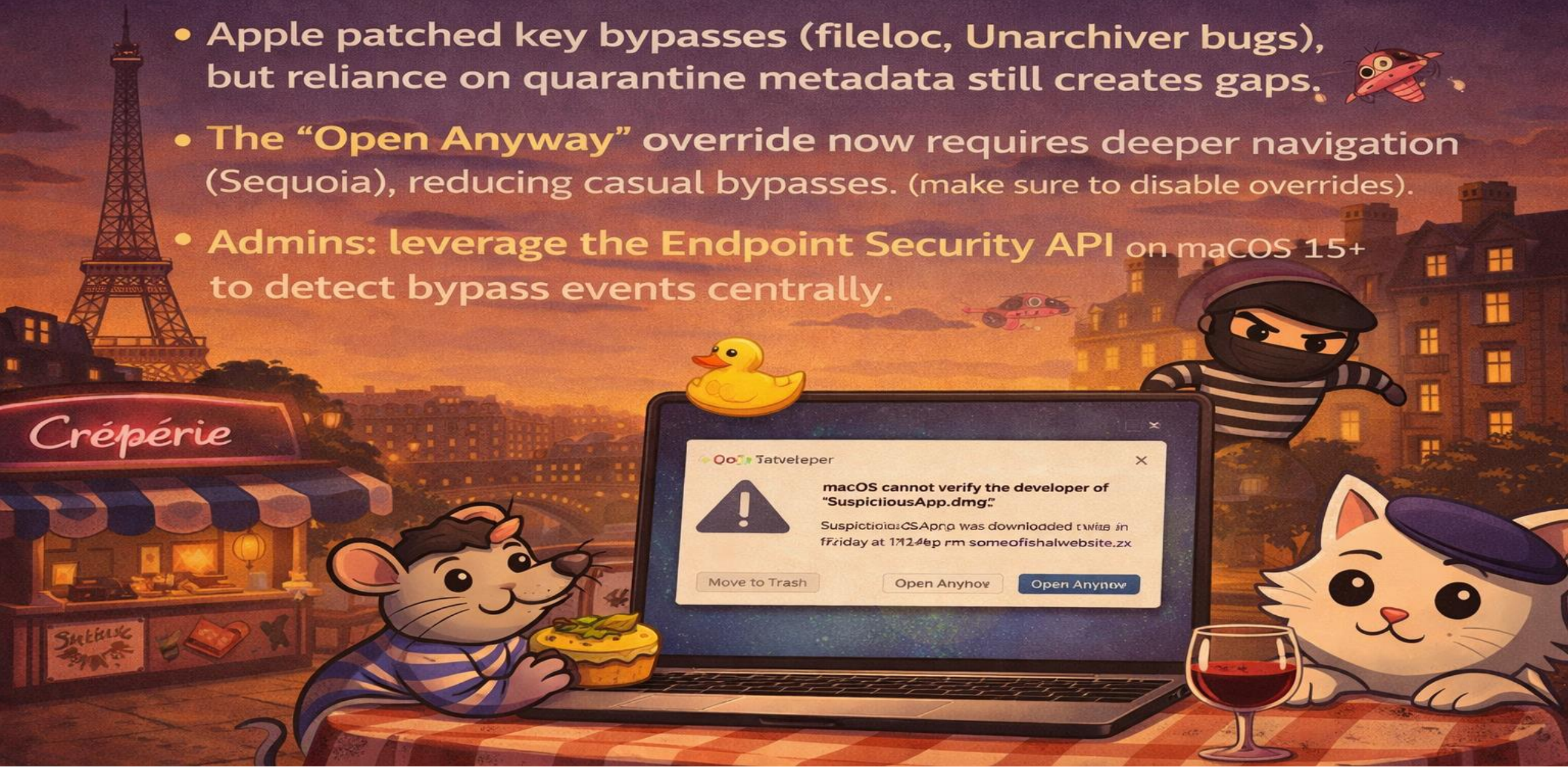
→ **System Integrity** Protection (SIP) → Shields critical system files

These features provide a solid foundation, but they're not perfect

Where it falls short

Gatekeeper: Still Strong, But With Caution

- Apple patched key bypasses (fileloc, Unarchiver bugs), but reliance on quarantine metadata still creates gaps.
- The “Open Anyway” override now requires deeper navigation (Sequoia), reducing casual bypasses. (make sure to disable overrides).
- Admins: leverage the Endpoint Security API on macOS 15+ to detect bypass events centrally.

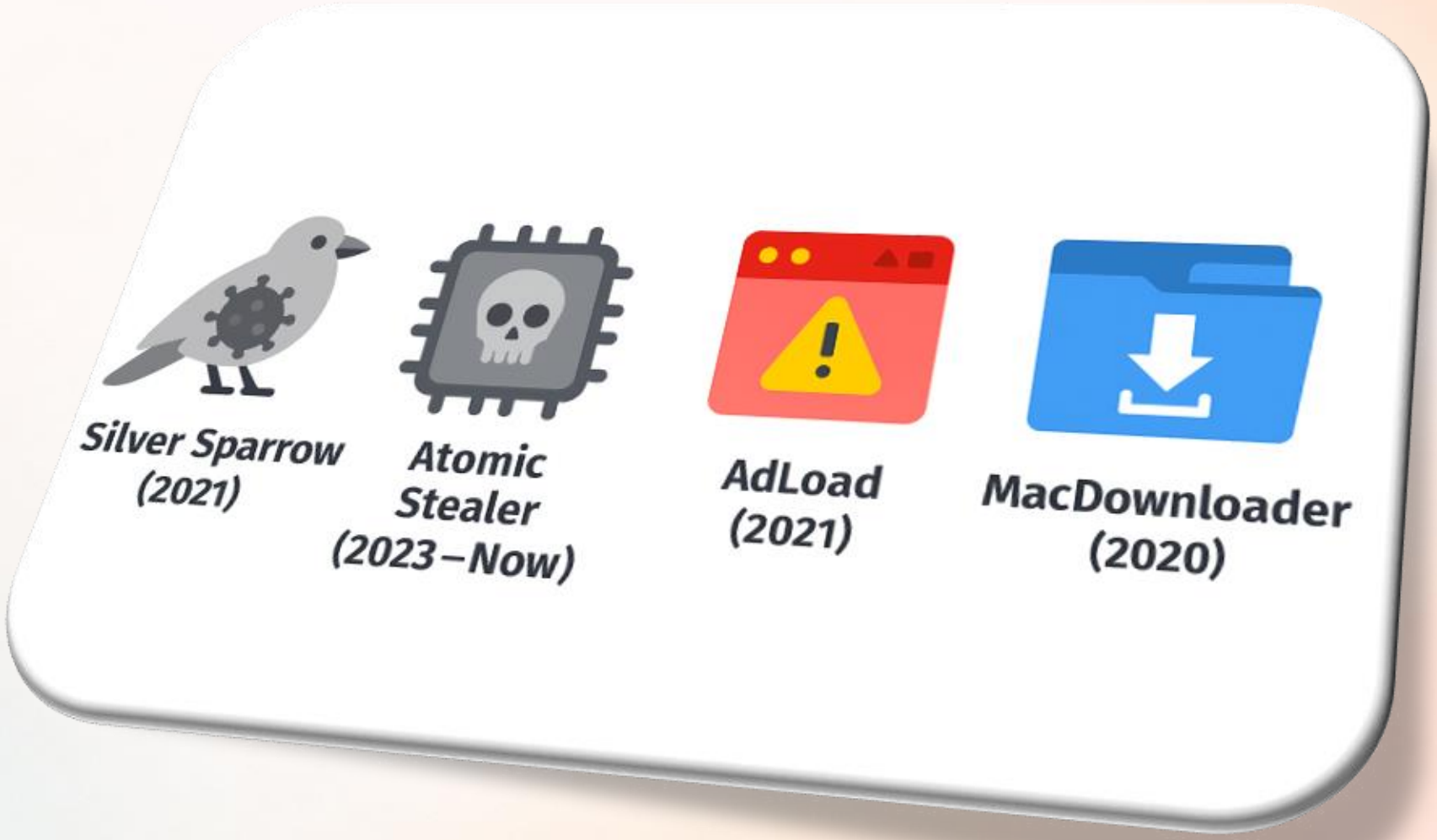


How Malware Targets Macs Today

- macOS no longer niche and attackers are actively adapting
- Malware evolves quickly to bypass Apple's defenses
- The myth of "Macs don't get viruses" makes users prime targets

Surge in macOS malware:
400% increase from 2023 to 2024

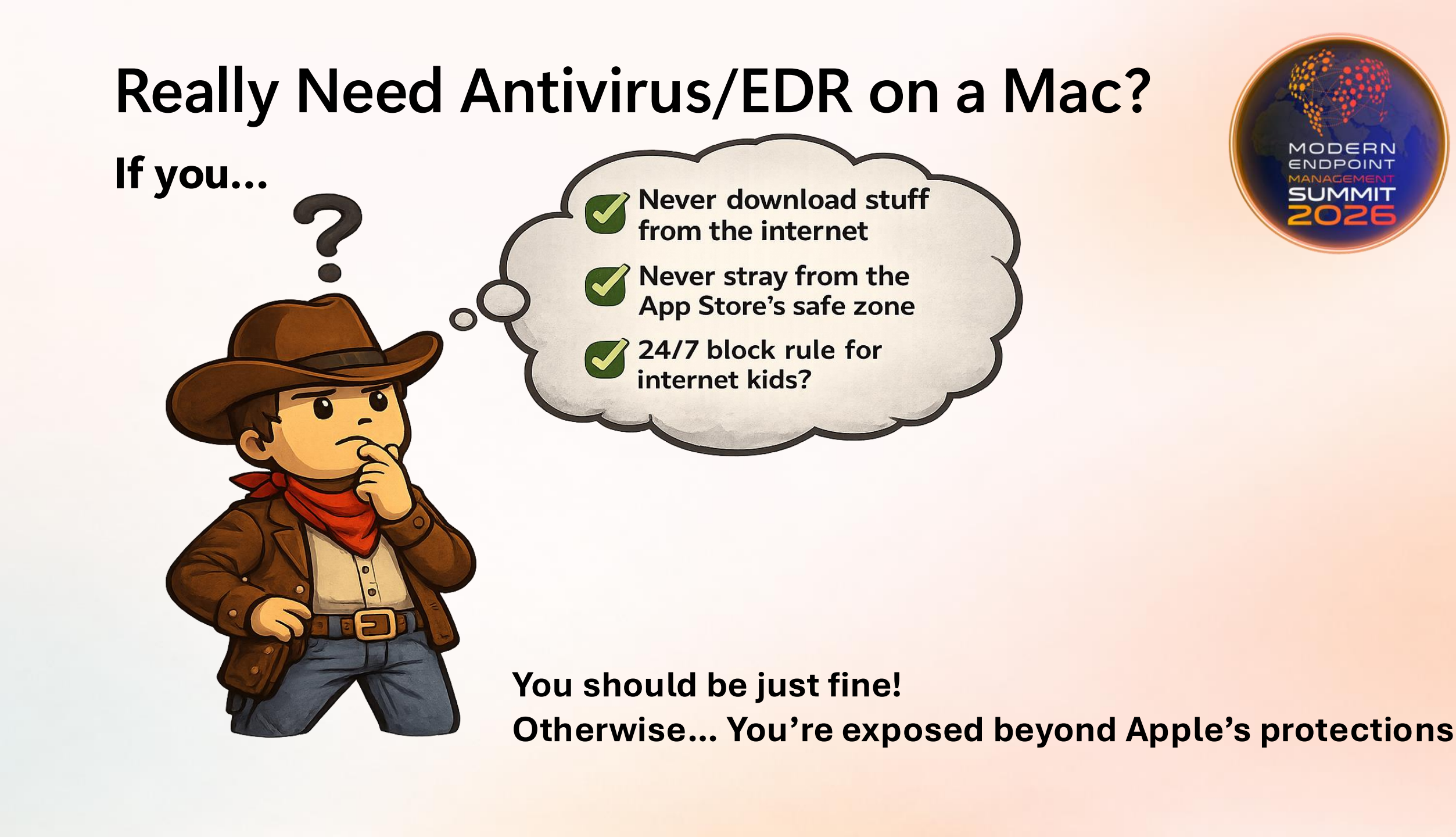
Real-World Malware Examples



Real-World Malware Examples


MOULIN ROGUE
Phishing
Zero-Day
Browser Hijacks
Infected Downloads
Weak Firewall
These threats slip past
Mac's default defenses

Really Need Antivirus/EDR on a Mac?



If you…

You should be just fine!

Otherwise… You're exposed beyond Apple's protections

What You Get When You Go Beyond Apple's Bubble

Microsoft Defender

Cross-Platform

Advanced Protection

Not advocating but....

Misleading...


Local Admin ≠ Local Safety
Admin rights granted.
More access = more attack surface.

Reality check...

Giving yourself root is like handing your dog the car keys... nothing good will happen!

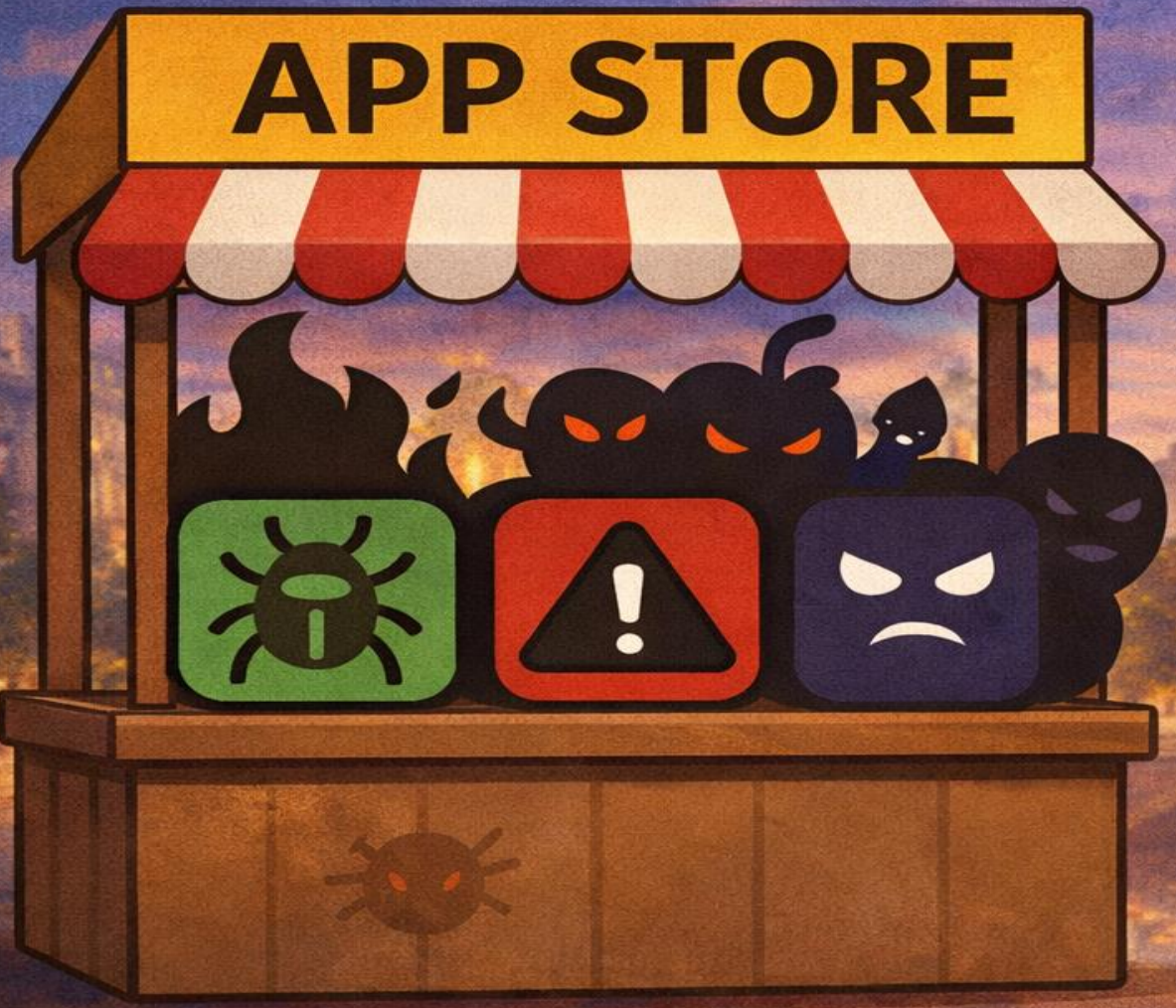
But we do it anyway...


All jokes aside...This SH$#& actually happened!!
BBC NEWS

3rd Party app stores

Not every store has security guards.

Why 3rd Party App Stores Are Risky

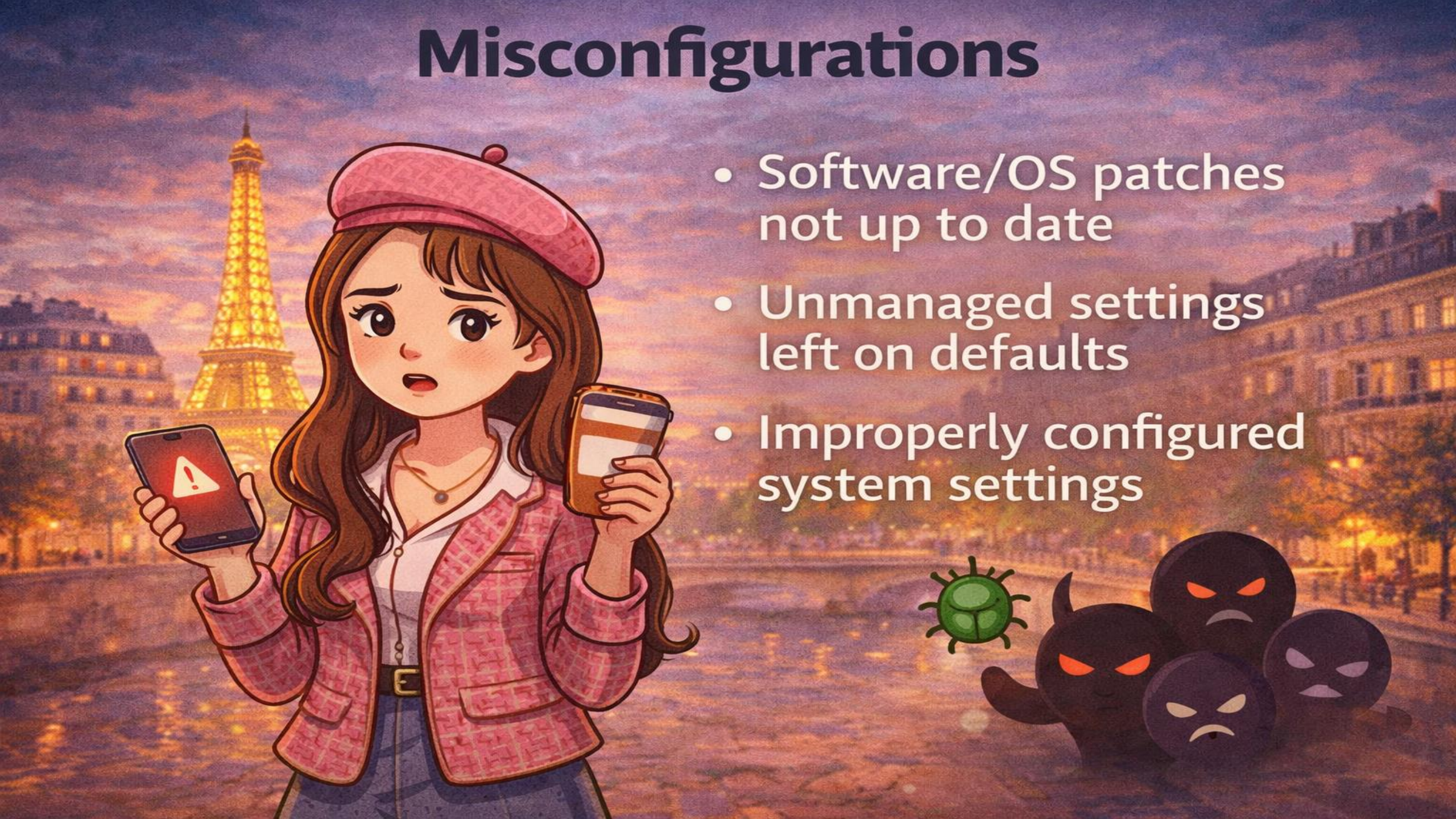


- No Apple review
  → More malware
- No vetting
  → Unknown apps
- Custom URLs
  → Apps from anywhere.

?

Not every app plays by the rules.

Misconfigurations



- Software/OS patches not up to date
- Unmanaged settings left on defaults
- Improperly configured system settings

Demo 1

Demo 1: Use script-based audits to surface services, risky permissions, and bad defaults.

Demo 2

Bypassing Gatekeeper

Demo 3

1. **Mac Beacon**
2. **Intune Log Reader**

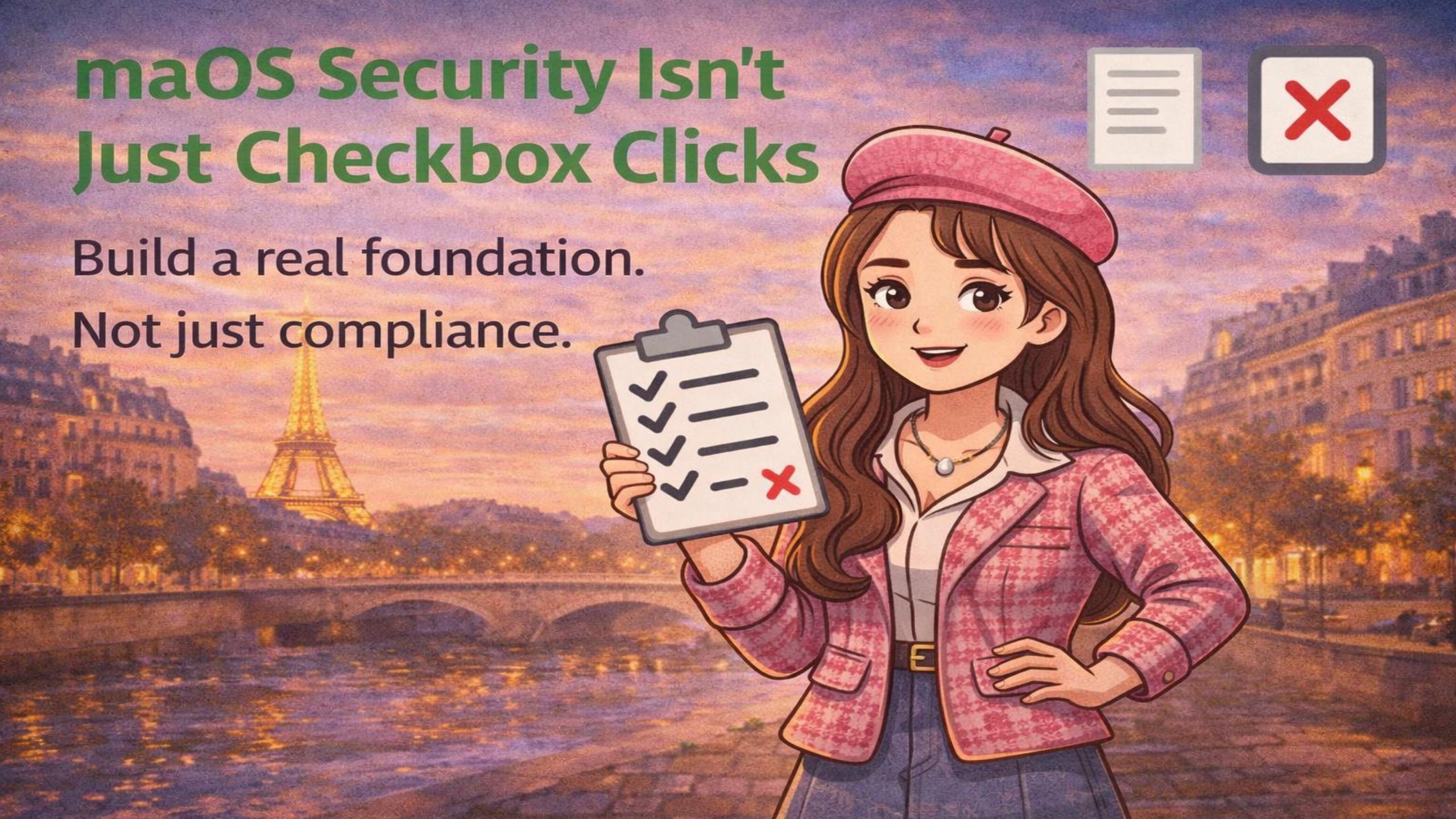
Demo 4

Security Baselines

maOS Security Isn't Just Checkbox Clicks

Build a real foundation.

Not just compliance.



Prepare for deployment

- Buy from an authorized reseller
- Pick an MDM provider
- Use ABM
- Link reseller & Set default MDM


MUST HAVES
MDM Provider
Compliance
Security Baseline

The Must haves...

- Enforce encryption
- Enforce screen to lock
- Enforce gatekeeper & disable bypass
- Enforce auto updates for OS & Apps
- Enforce password policy.
- Enforce hardening restrictions
- Disable icloud services
- Enable LAPS
- Enroll Macs with standard user rights

The Must haves...

- Move policies/configurations from MDM to DDM
- Use Platform SSO with Secure Enclave
- Standard User accounts!
- Disable 3rd party App stores
- Manage browser extensions using DDM
- Use Corporate EDR software!
- Block BETA updates in production
- Block Over The Air (OTA) profile installations


C’est parfait!
SECURE!
MDM
SIP
Compliance
Six
ENROLLED
ABM
SECURE!

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!