GRAHAM GILBERT / MACAD.UK 2025

ZERO TRUST FOR MAC ADMINS

The views expressed in this talk are my own and do not necessarily reflect those of my employer

HELLO!

- I’m Graham
- San Jose, California
- Client Engineering & Zero Trust at Airbnb
- Recovering open-sourcer

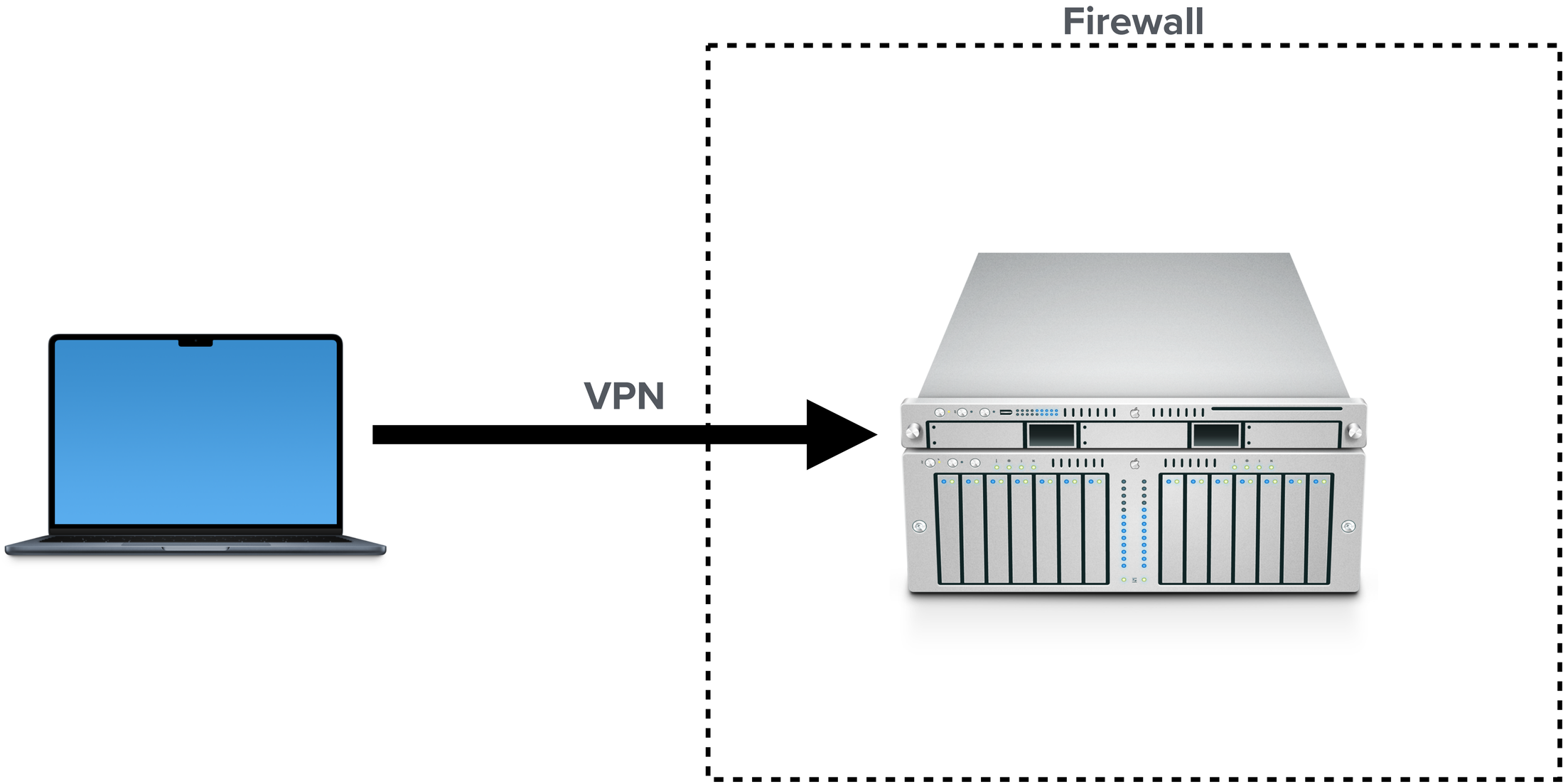
- July 10th @ Jamf London
- Looking for speakers!
- londonappleadmins.org.uk

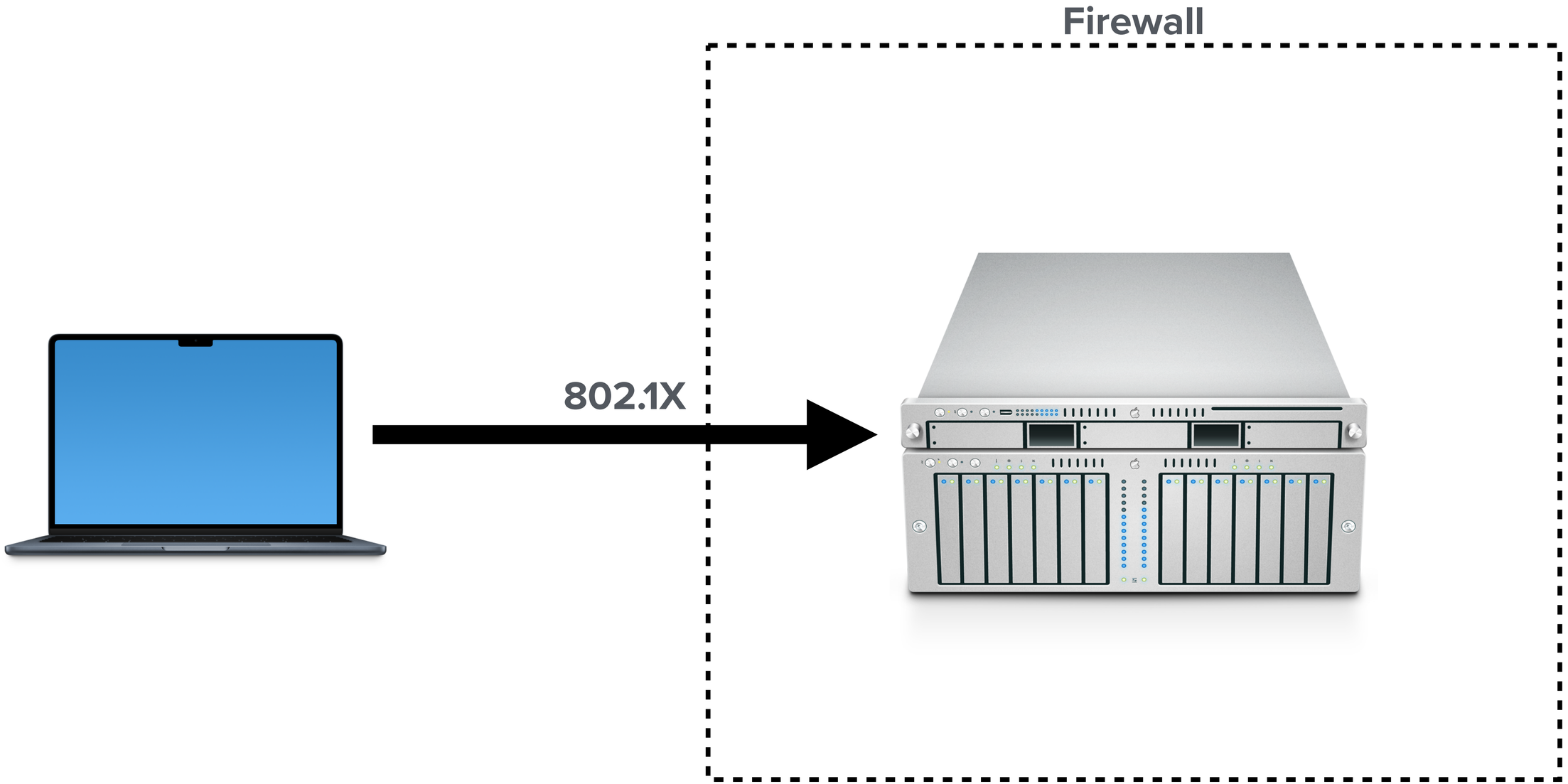
MAC ADMINS OPEN SOURCE

macadmins.io / github.com/sponsors/macadmins

GRAHAM.AT/MOVEMBER

ZERO WHAT?


Firewall
VPN


Firewall
802.1X

802.1X

Firewall

US GENERAL SERVICES ADMINISTRATION: ZERO TRUST

- Authenticate, monitor, and validate user identities and trustworthiness.
- Identify, monitor, and manage devices and other endpoints on a network.
- Control and manage access to data flows within networks.
- Secure and accredit applications within a technology stack.
- Automate security monitoring and connect tools across information systems.
- Analyze user behavior and other data to observe real-time events and proactively orient network defenses.
- Support IPv4 and IPv6.

$$\frac{\text{DEVICE} + \text{USER} + \text{CONTEXT}}{\text{POLICY}} = \text{ACCESS}$$

$$\frac{\text{DEVICE} + \text{USER} + \text{CONTEXT}}{\text{POLICY}} = \text{ACCESS}$$

USER IDENTITY; TLDR

- Cryptographic = good
- Non exportable = better
- Biometrics = useful
- Make sure you've got a good identity verification process

$$\frac{\text{DEVICE} + \text{USER} + \text{CONTEXT}}{\text{POLICY}} = \text{ACCESS}$$


GET ON
WITH IT!

THE DEVICE

THE MACOS DEVICE

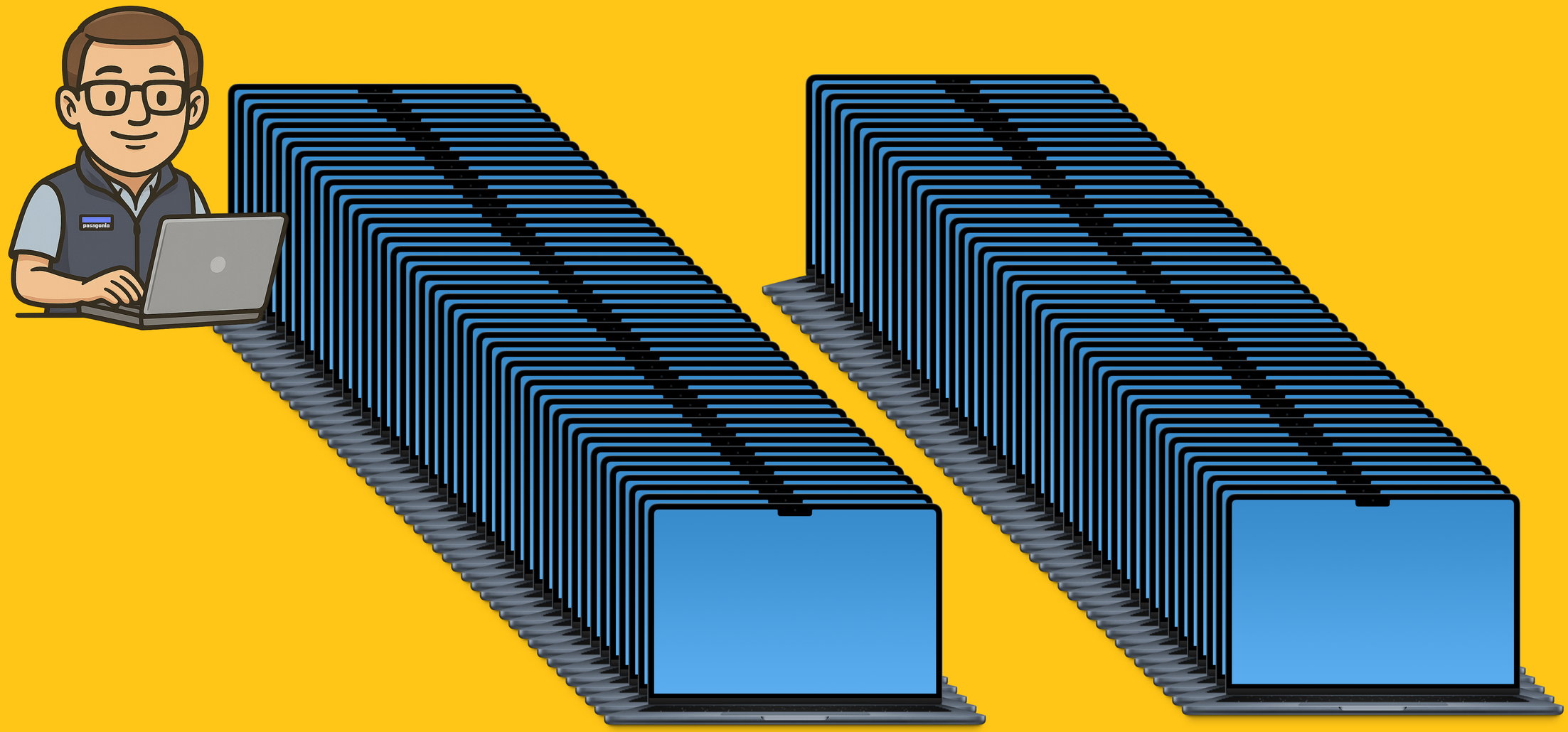
THE MACOS DEVICE (MOSTLY)

MDM ENROLLMENT?

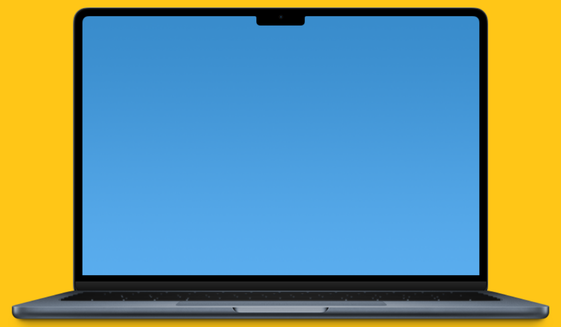
INVENTORY

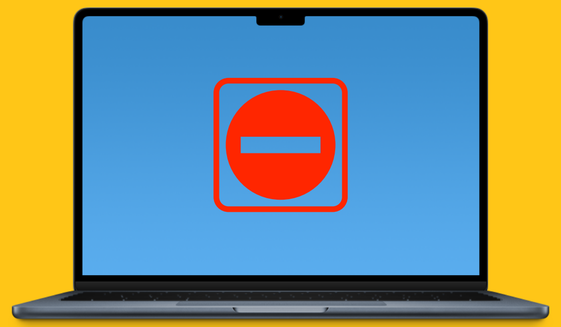
WHY DO I NEED INVENTORY?

- Device ownership
- Assigned user
- Device status


patagonia


patagonia





MDM ENROLLMENT

MACHINEINFO

https://developer.apple.com/documentation/devicemanagement/machineinfo

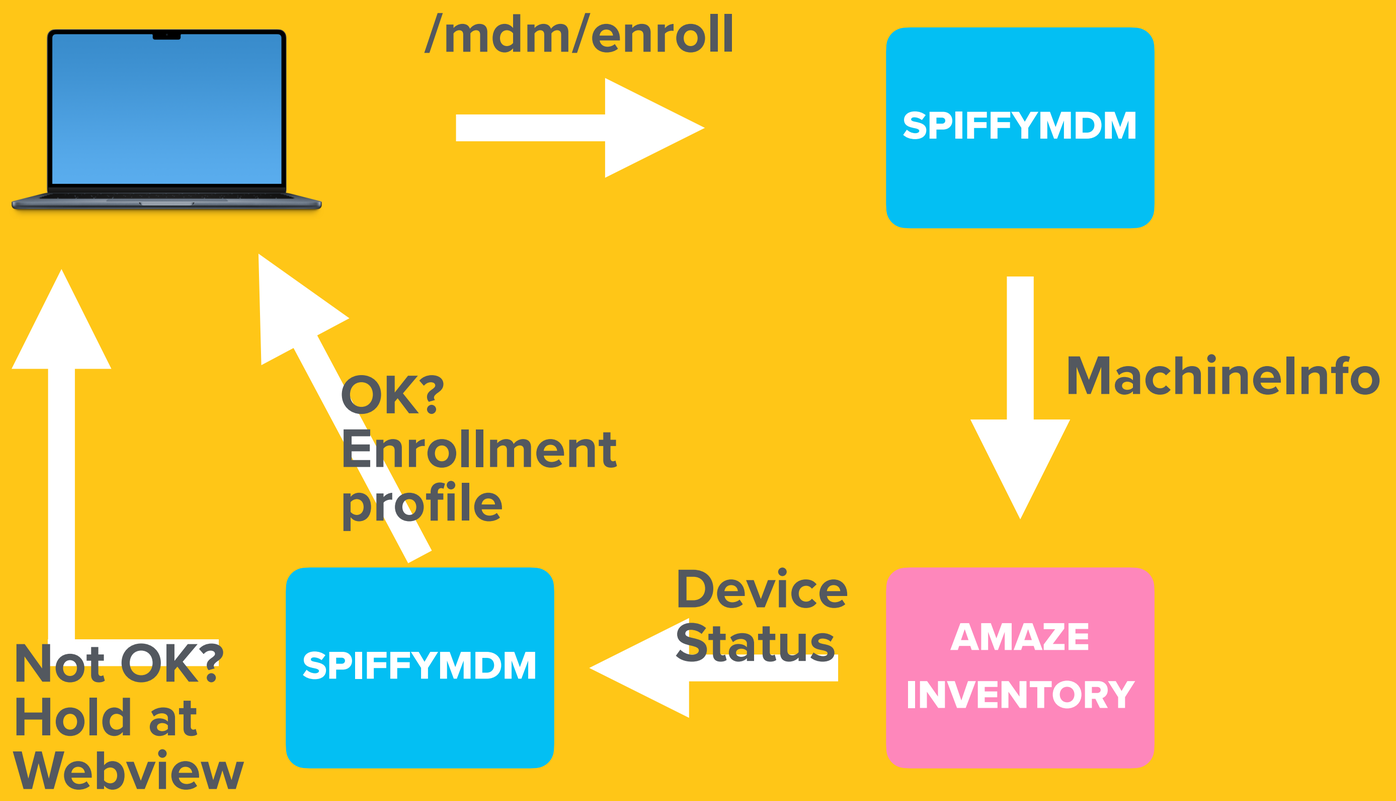
MACHINEINFO

- SERIAL
- UDID
- PRODUCT

https://developer.apple.com/documentation/devicemanagement/machineinfo

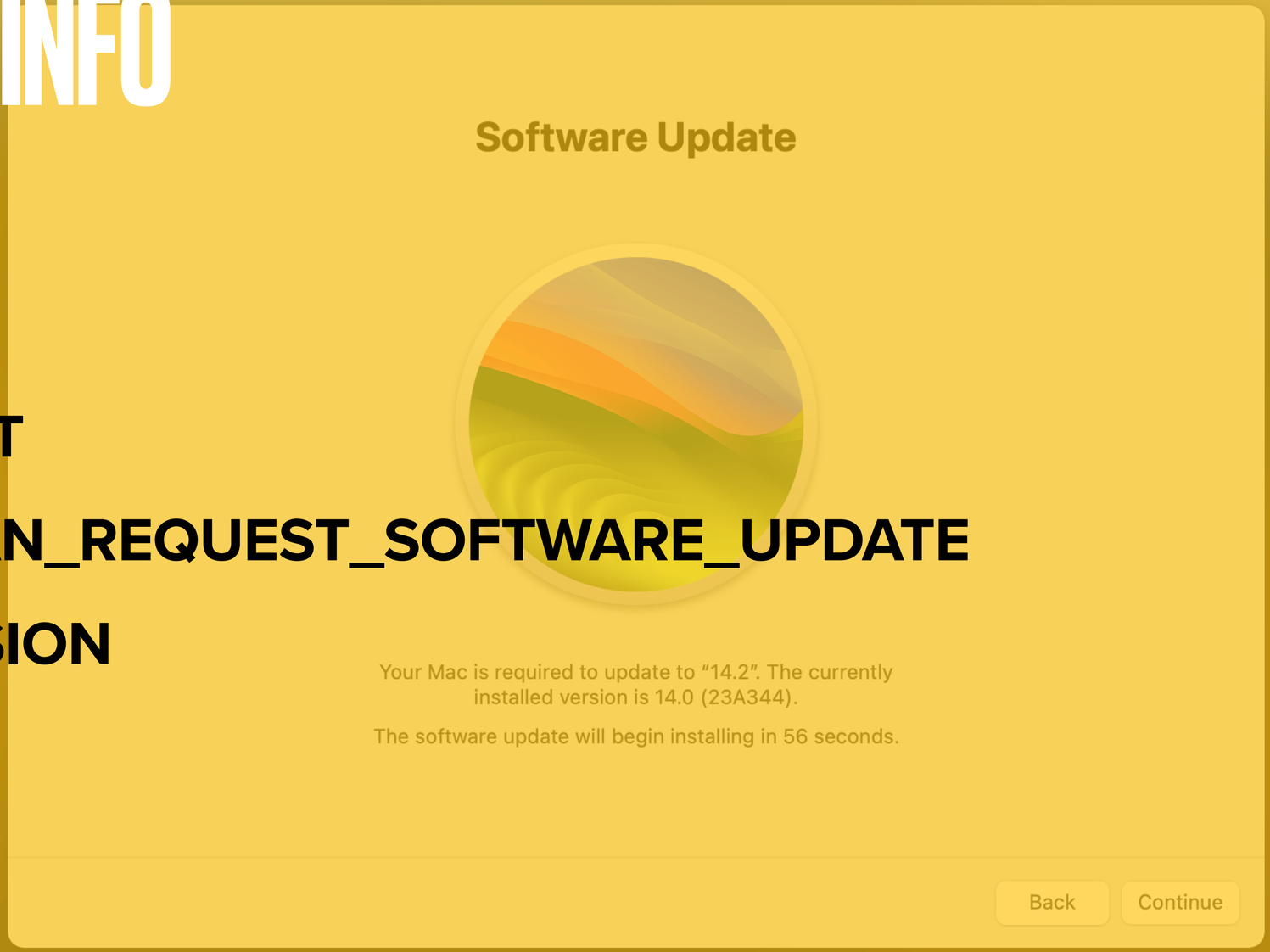
MACHINEINFO

- SERIAL
- UDID
- PRODUCT



MACHINEINFO

- SERIAL
- UDID
- PRODUCT
- MDM_CAN_REQUEST_SOFTWARE_UPDATE
- OS_VERSION



TELEMETRY

TELEMETRWHAT?

- macOS version
- FileVault status
- Screenlock status
- SIP
- EDR healthy and reporting
- MDM enrollment healthy and reporting
- DLP healthy and reporting
- Physical location

TELEMETRY SOURCES

- MDM
- Munki (via Sal or MunkiReport-PHP)
- EDR (Endpoint Detection & Response)
- VPN
- osquery

OSQUERY

```
osquery> select * from sip_config;
+----------------------------------+---------+---------------+
| config_flag                      | enabled | enabled_nvram |
+----------------------------------+---------+---------------+
| sip                              | 1       | 1             |
| allow_any_recovery_os            | 0       | 0             |
| allow_apple_internal             | 0       | 0             |
| allow_device_configuration       | 0       | 0             |
| allow_executable_policy_override | 0       | 0             |
| allow_kernel_debugger            | 0       | 0             |
| allow_task_for_pid               | 0       | 0             |
| allow_unapproved_kexts           | 0       | 0             |
| allow_unauthenticated_root       | 0       | 0             |
| allow_unrestricted_dtrace        | 0       | 0             |
| allow_unrestricted_fs            | 0       | 0             |
| allow_unrestricted_nvram         | 0       | 0             |
| allow_untrusted_kexts            | 0       | 0             |
+----------------------------------+---------+---------------+
osquery>
```

OSQUERY

- Lightweight
- Extensible (http://github.com/macadmins/osquery-extension)
- Flexible outputs
- On demand queries (with a TLS server such as Fleet DM)

DEVICE IDENTITY

MANAGED DEVICE ATTESTATION

Managed Device Attestation for Apple devices

Managed Device Attestation is a feature for devices with iOS 16, iPadOS 16.1, macOS 14, tvOS 16, or later. Managed Device Attestation provides strong evidence about which properties of a device can be used as part of a trust evaluation. This cryptographic declaration of device properties is based on the security of the Secure Enclave and the Apple attestation servers.

Managed device attestation helps protect against the following threats:

- A compromised device lying about its properties
- A compromised device providing an outdated attestation
- A compromised device sending a different device's identifiers
- Private key extraction for use on a rogue device
- An attacker hijacking a certificate request to trick the CA into issuing the attacker a certificate

For more information, see the WWDC22 video What's new in device management.

https://support.apple.com/guide/deployment/managed-device-attestation-dep28afbde6a/web

DEVICE OWNERSHIP MODELS

TO BYOD OR TO NOT BYOD?

“YOU SHOULD NEVER IMPLEMENT BYOD”

GRAHAM GILBERT, PRIOR TO 2016

APPROPRIATE DATA FOR APPROPRIATE DEVICE OWNERSHIP

“THE RIGHT ACCESS, ON THE RIGHT DEVICE, TO THE RIGHT IDENTITY, IN THE RIGHT CONTEXT”

A VERY SMART PERSON I WORK WITH

ENFORCEMENT LAYERS

ENFORCEMENT LAYERS

- MDM Commands
- Single Sign On
- Certificate Revocation

USER COMMS

Update Notifier APP

macOS 15.3.2 is avaïlable.

macOS 15.3.2 fixes multiple security ıulnerabilities, Please install all updates in System Settings. If you can't see this update in System Preferences, restart your computer and check again. For further help, please visit

Your Version:
macOS

Minimum Required Version:
macOS 15.3.2

Your Version:
15.3.1

Install Update By
April 2, 2025 1:00 PM PDT
(12 days from now)

Mute this version

About the security content of macOS Sequoia 15.3.2 - Apple Support
This document describes the security content of macOS Sequoia 15.3 'built-in apps, including Safari.

Hold Up!

Please fix the items below to avoid access disruption.

macOS 15.3.1 is available for your device

More Info

Access will be blocked in 6 days

Don't have time to fix every/thing right now?

Continue

macOS 15.3.1 is available for your device

Please update your macOS device to version 15.3.1 or newer to ensure your device is secure.

For instructions on installing the latest macOS update, follow this link.

If you have recently updated your device and are still seeing this message, you may need to perform an Endpoint Verification sync:

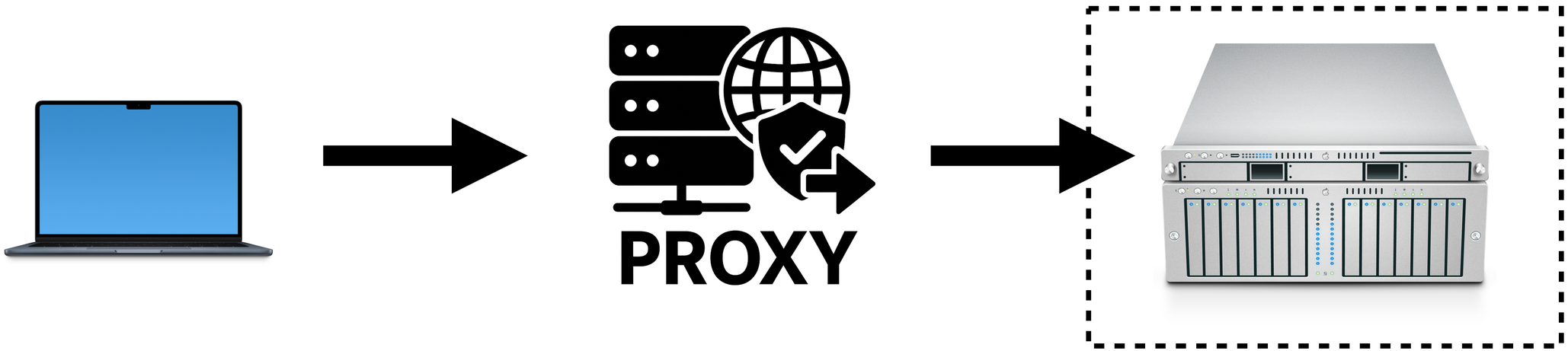
- Click on the “Endpoint Verification” extension (laptop icon) on the top right corner of your Google Chrome browser.
- Click on the “Sync Now” button to sync your device status.

CONTINUAL POLICY ENFORCEMENT

CONTINUAL POLICY ENFORCEMENT

- VPN
- Context Aware Access / Conditional Access
- Access Proxies

ACCESS PROXIES



BUT WON'T SOMEONE THINK OF THE SAAS APPS?

SHARED SIGNALS FRAMEWORK

WHY THIS IS THE MOST EXCITING THING TO COME OUT OF ZERO TRUST-Y THINGS EVER

BUT FIRST, SCIM

OKAY, WHY IS SSF COOL?

ROUNDUP

ROUNDUP

- Inventory is vital
- Independently control which devices can enroll in your MDM
- Telemetry, telemetry, telemetry
- Continual policy evaluation and enforcement
- Help your users understand what they need to do to be compliant

THANK YOU!

grahamgilbert.com
@grahamgilbert on Slack
graham.at/movember
graham@grahamgilbert.com