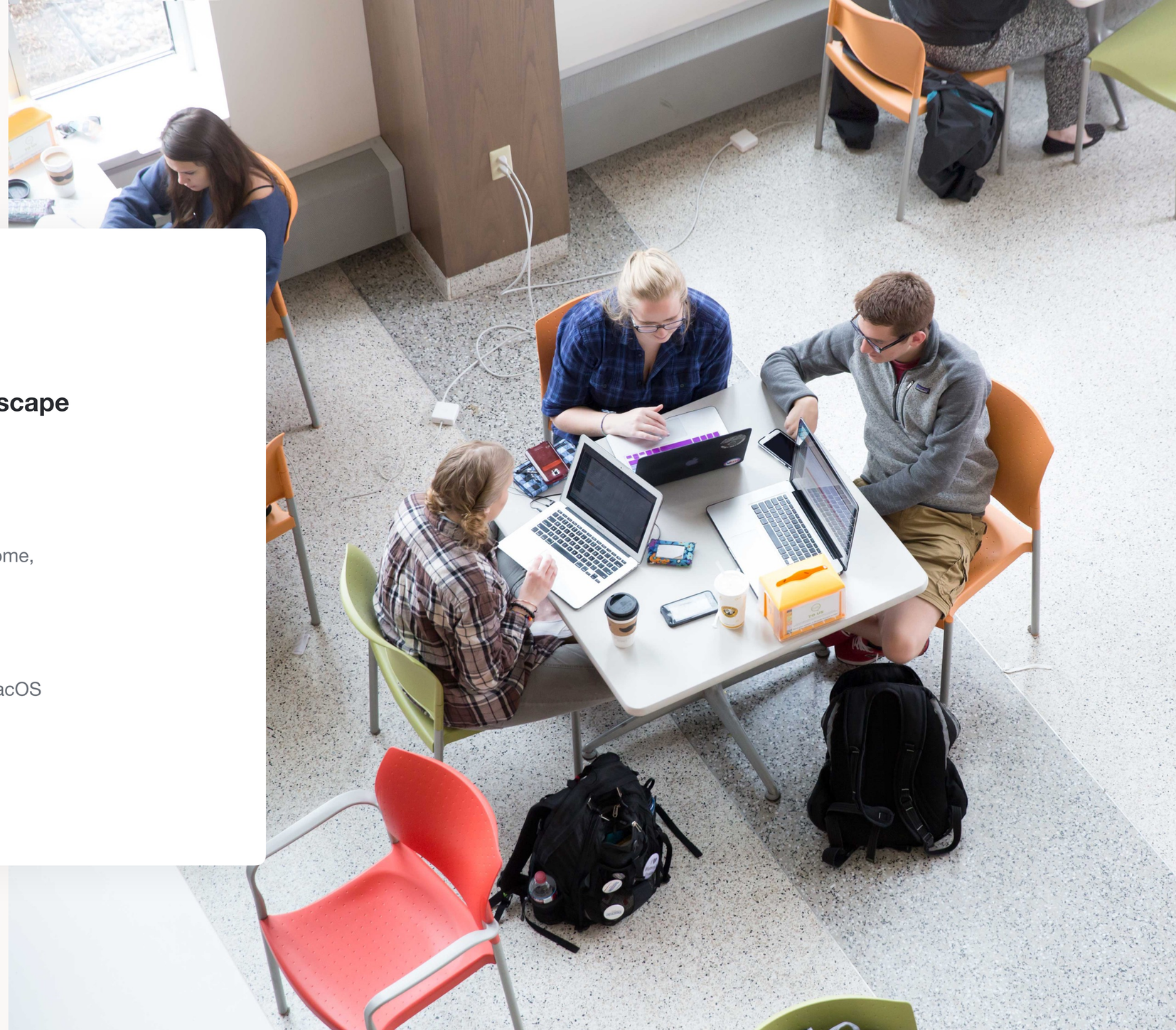
Securing Apple Devices in Education: Peeling back the Layers

JAMF NATION LIVE

Michael Thomson

Channel Sales Engineer
Jamf

Agenda



1 | Understanding the current landscape

Why do we need security in education?

2 | Identifying security layers

What are some of the ways we protect our home, family and personal belongings?

3 | Building a layered approach

How can we utilise the security features in macOS and enforce with Jamf?

Security Landscape in **Education**

Ransom requests totalling

$40M

Downtime due to ransomware attacks

1,387 days

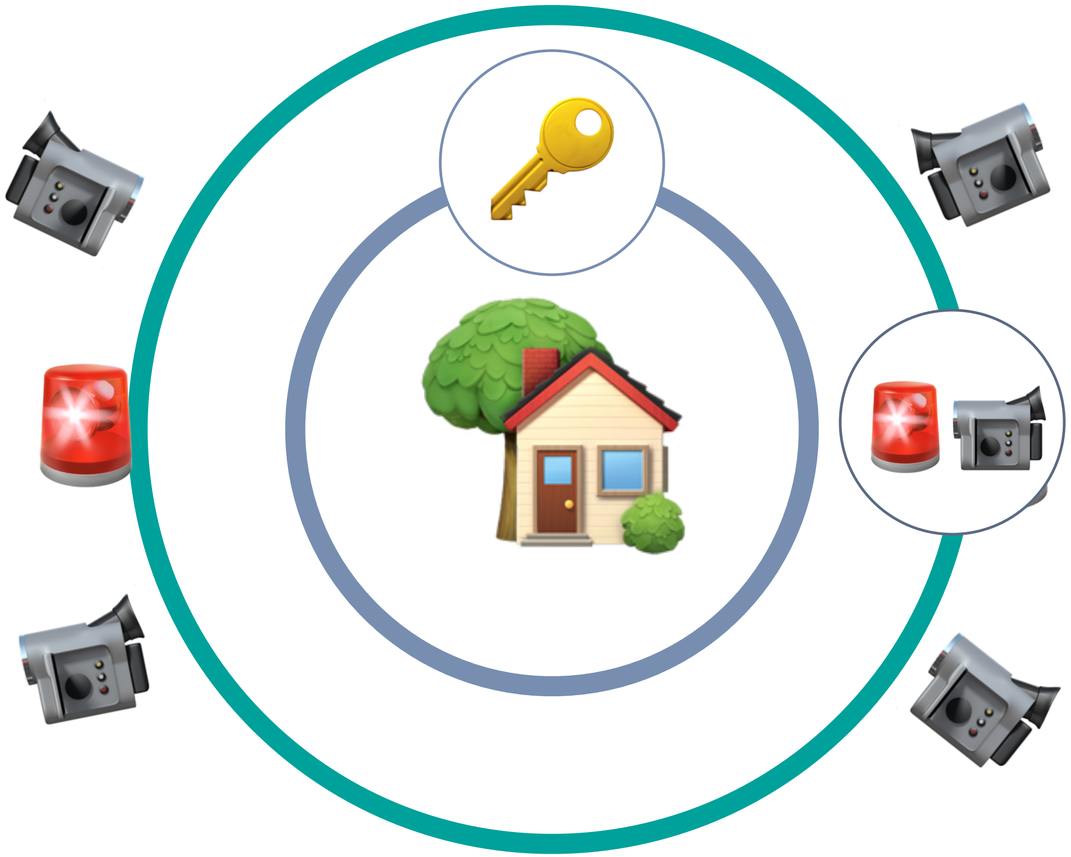
Affected schools & colleges

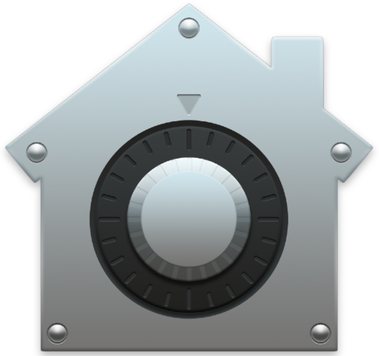
3,880

Students impacted

3.04M

Source: https://www.comparitech.com/blog/information-security/school-ransomware-attacks/

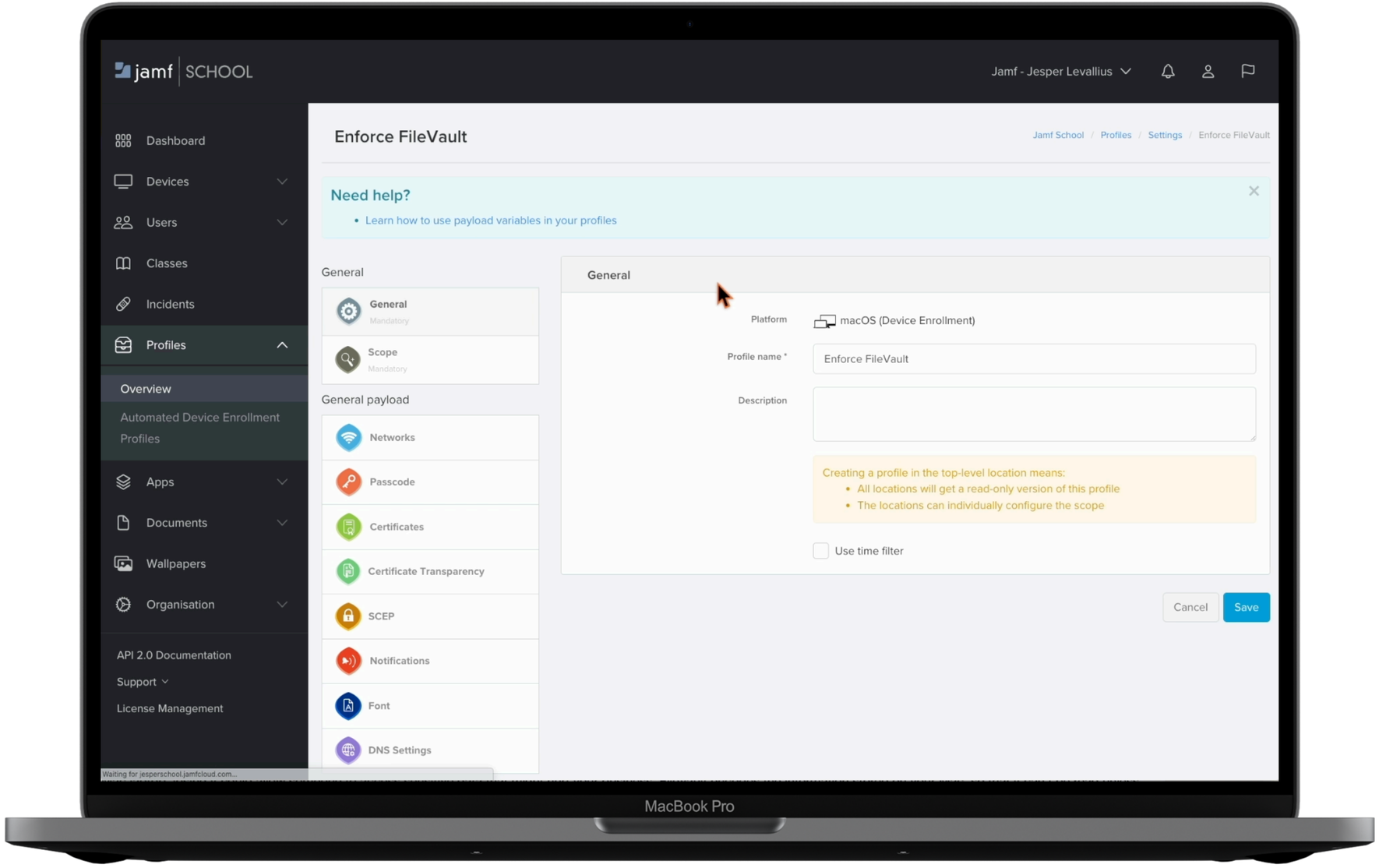




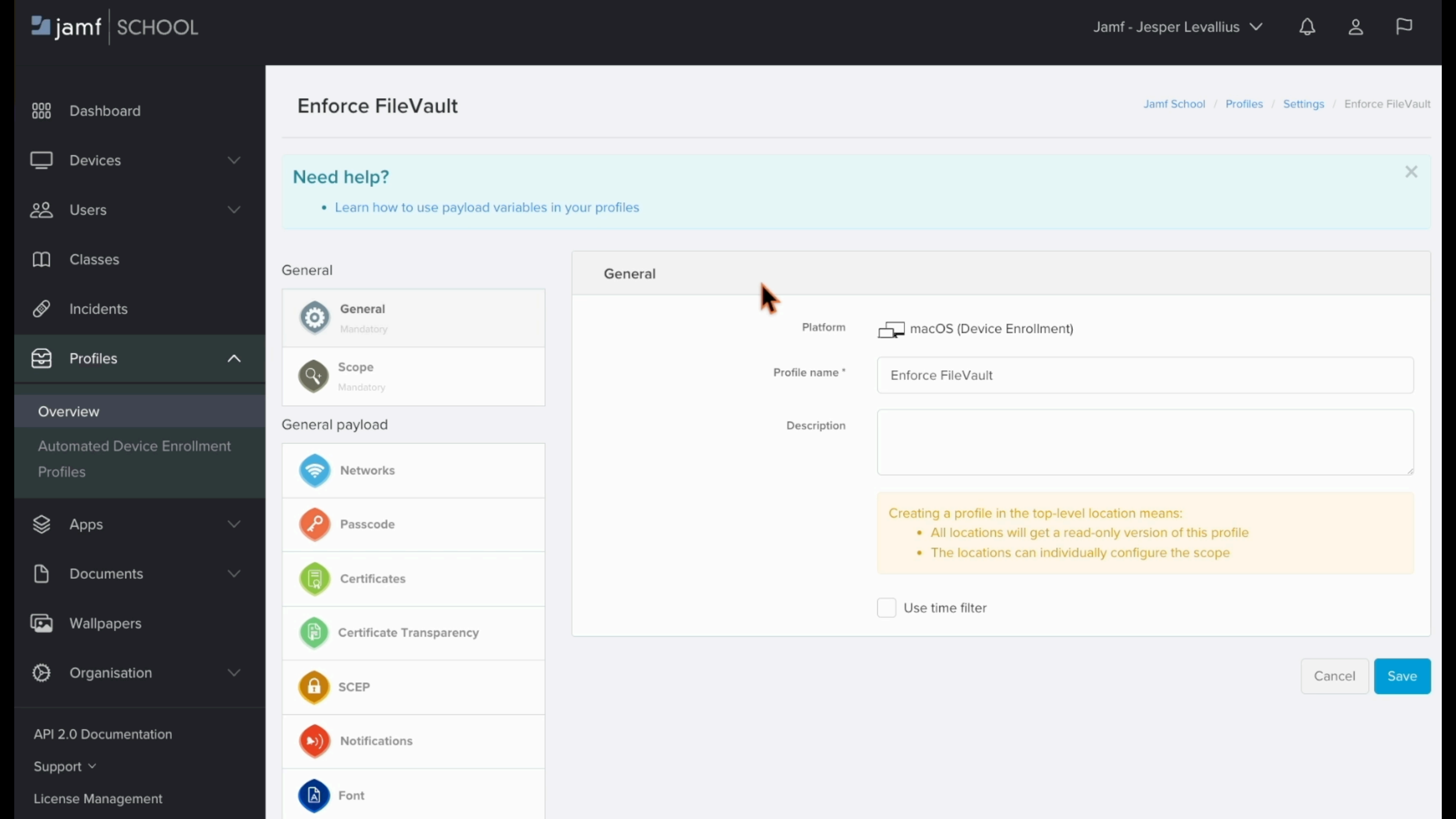
FileVault Encryption

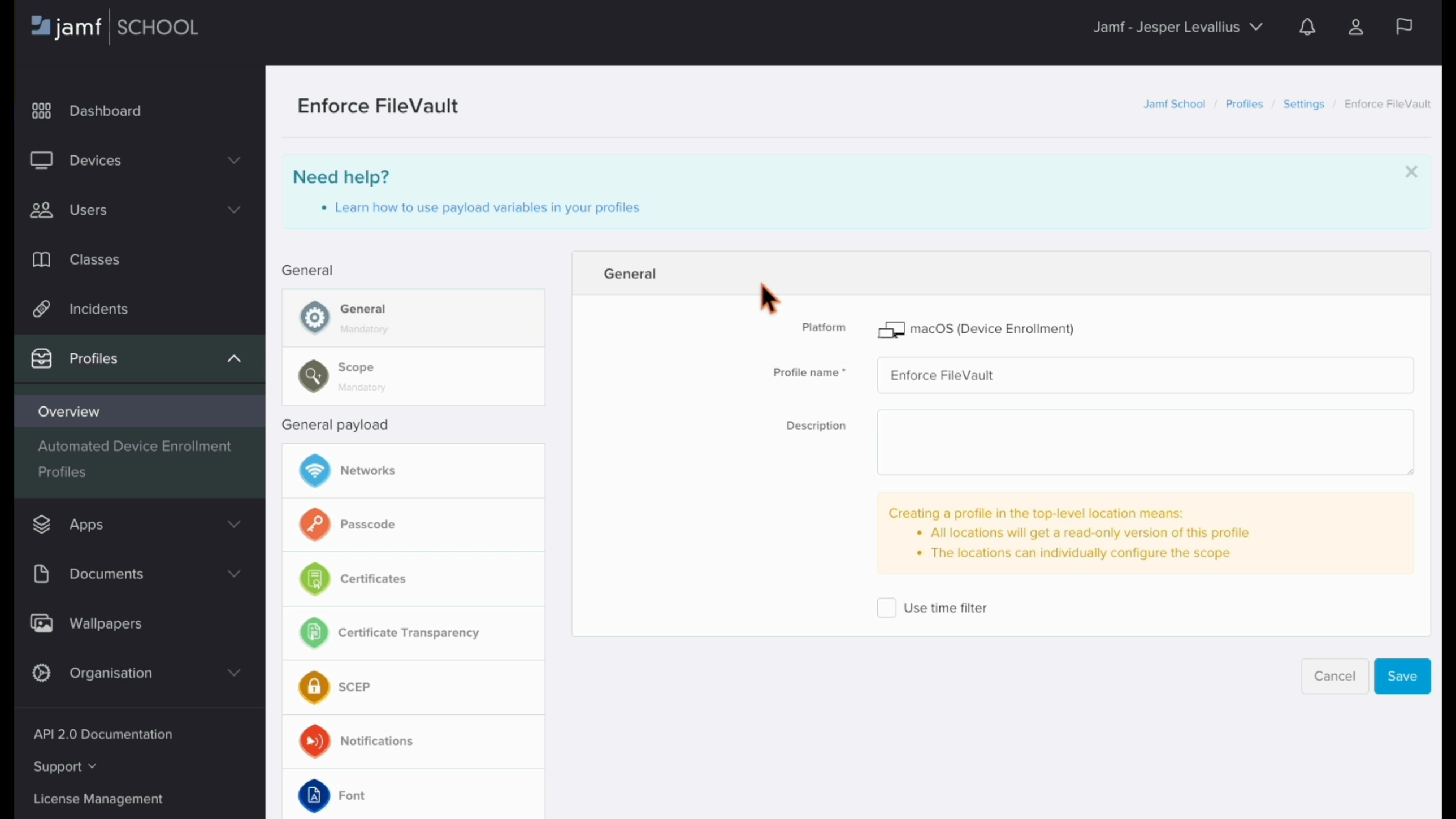
Turn off FileVault

Users can navigate to FileVault settings and turn off encryption



JAMF NATION LIVE

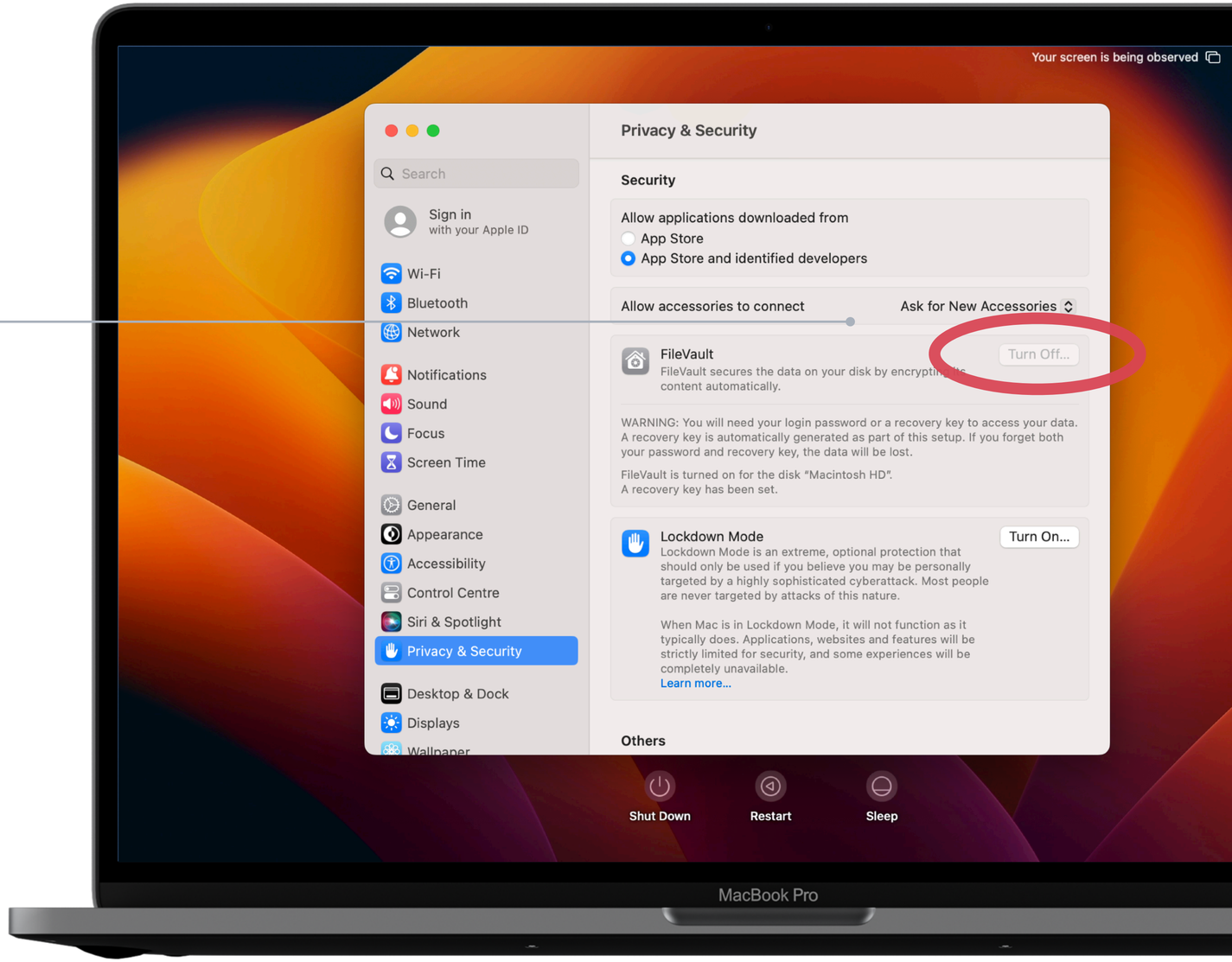

jamf SCHOOL
Jamf - Jesper Levallius
Dashboard
Devices
Users
Classes
Incidents
Profiles
Overview
Automated Device Enrollment
Profiles
Apps
Documents
Wallpapers
Organisation
API 2.0 Documentation
Support
License Management
Enforce FileVault
Jamf School / Profiles / Settings / Enforce FileVault
Need help?
Learn how to use payload variables in your profiles
General
General
Mandatory
Scope
Mandatory
General payload
Networks
Passcode
Certificates
Certificate Transparency
SCEP
Notifications
Font
General
Platform
macOS (Device Enrollment)
Profile name *
Enforce FileVault
Description
Creating a profile in the top-level location means:
All locations will get a read-only version of this profile
The locations can individually configure the scope
Use time filter
Cancel
Save


jamf SCHOOL
Jamf - Jesper Levallius
Dashboard
Devices
Users
Classes
Incidents
Profiles
Overview
Automated Device Enrollment
Profiles
Apps
Documents
Wallpapers
Organisation
API 2.0 Documentation
Support
License Management
Enforce FileVault
Jamf School / Profiles / Settings / Enforce FileVault
Need help?
Learn how to use payload variables in your profiles
General
General
Mandatory
Scope
Mandatory
General payload
Networks
Passcode
Certificates
Certificate Transparency
SCEP
Notifications
Font
General
Platform
macOS (Device Enrollment)
Profile name *
Enforce FileVault
Description
Creating a profile in the top-level location means:
All locations will get a read-only version of this profile
The locations can individually configure the scope
Use time filter
Cancel
Save

Jamf School
Enforce **FileVault**

FileVault

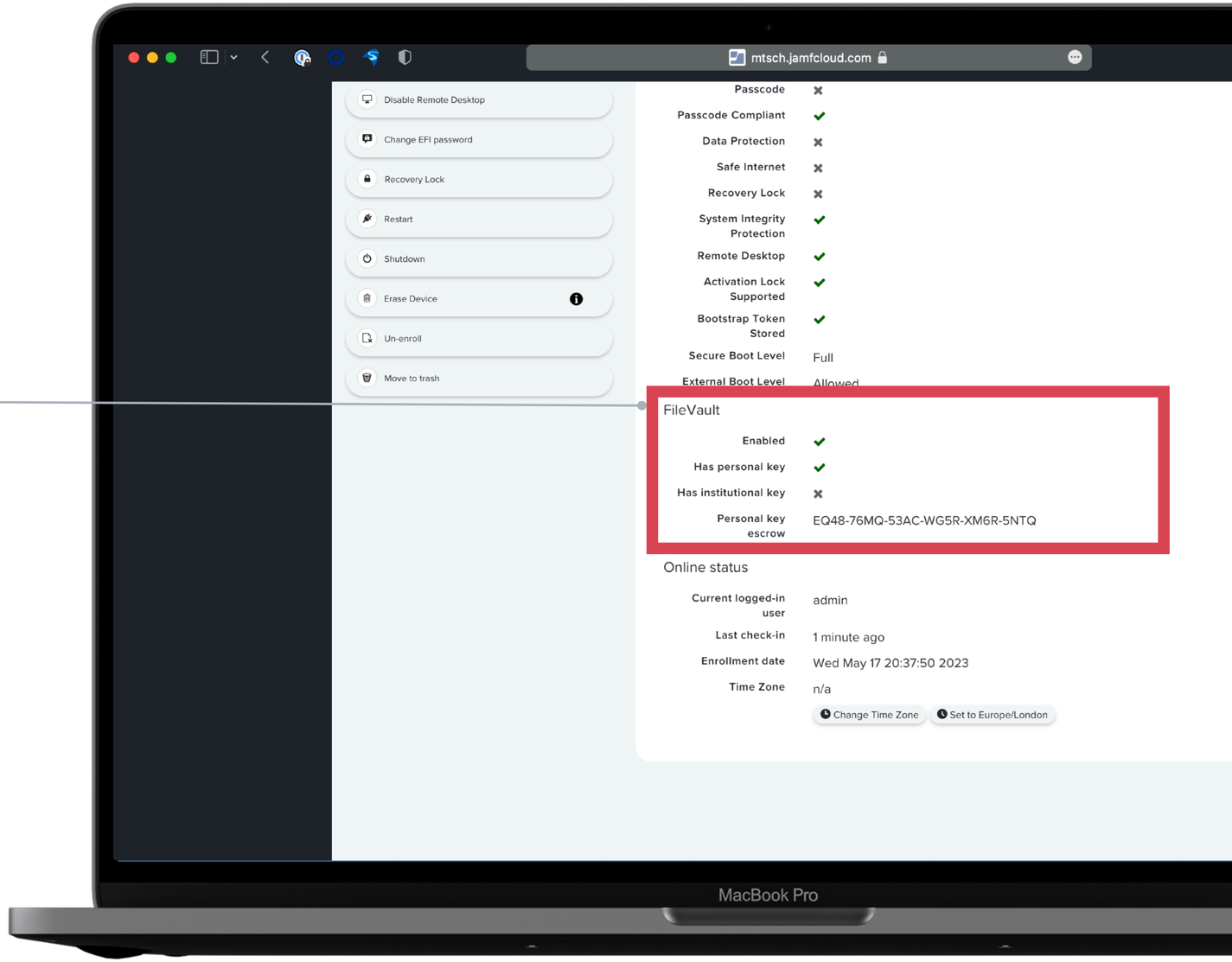
User can’t turn off FileVault once it’s enabled



Jamf School
Enforce **FileVault**

FileVault Status

See if FileVault is enabled and access to recovery key



JAMF NATION LIVE

FileVault

Password Policy

iCloud Storage

Declarative Device Management

USB connectivity

Defer Updates

Security Updates

Lock Device

Wi-fi policy

Activation lock

Lost Mode

Rapid Security Response

Passcode lock grace period

Remote wipe

Touch ID and Face ID

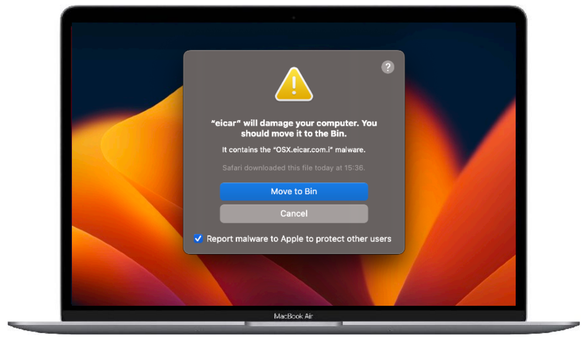
Apple Gatekeeper and XProtect

macOS has multiple built-in security tools to protect users out of the box

Gatekeeper

- Ensures that only trusted software runs on the Mac
- Verifies that apps are from a trusted developer, notarised and unaltered
- Requests user approval
- Feature enabled by default

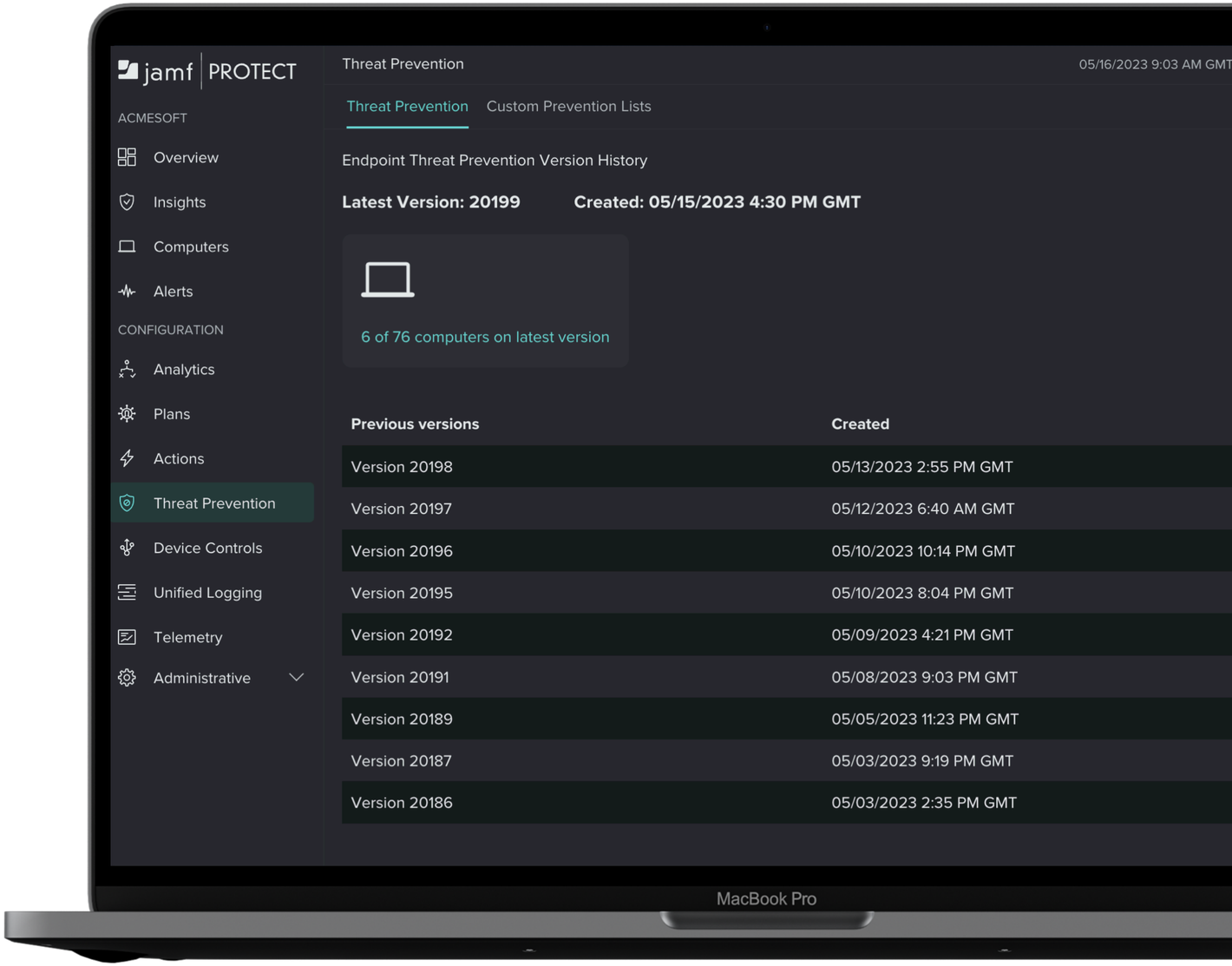
XProtect



- Uses signatures-based detection to block malware using YARA
- Signature database updated regularly by Apple
- Updates independent of software updates
- Software blocked and user notified

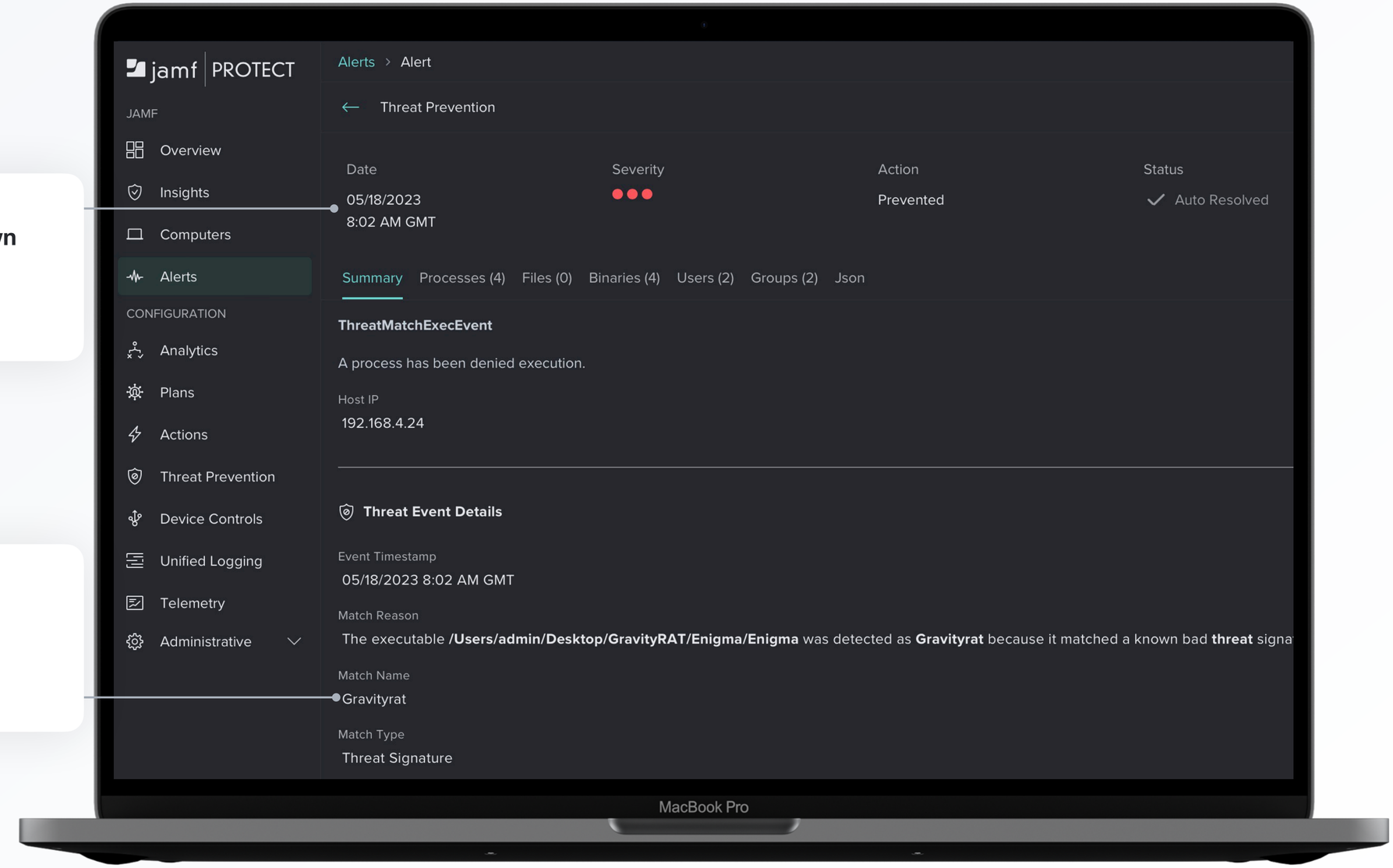
Protect against advanced attacks

- Broad protection against known macOS malware
- Extensible restrictions for unwanted applications
- Lightweight design



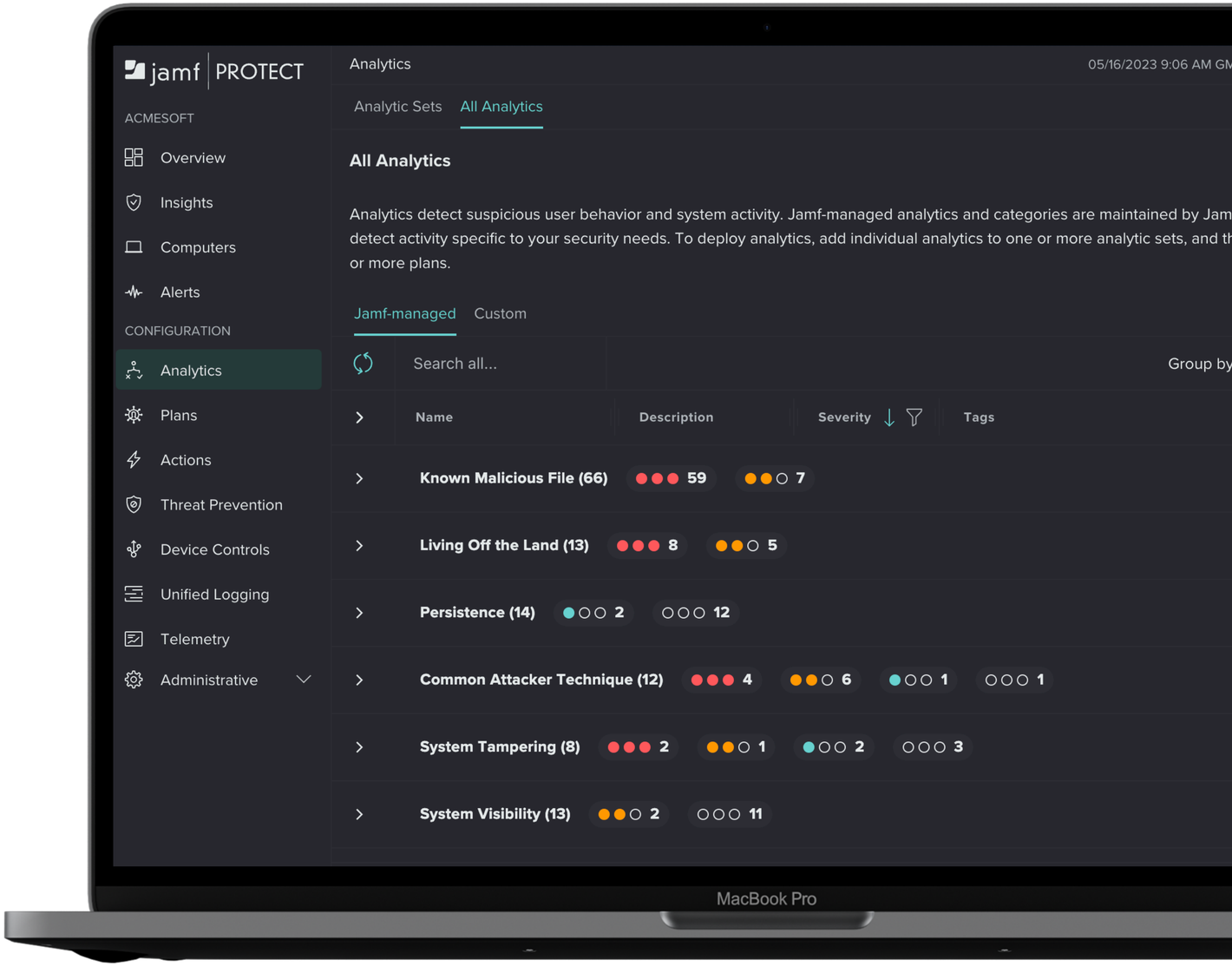
Be notified in real-time when known Mac threats are automatically prevented

Review matched threat signatures and contextual event data



Protect against advanced attacks

- Detect 150+ Mac-specific adversary techniques
- Powered by **Jamf Threat Labs** and **MITRE ATT&CK**
- **Comprehensive behavioural detection**



JAMF NATION LIVE

Malware Protection

Threat Prevention

Data Streaming

Security Visibility & Compliance

Removable Storage Controls

macOS Endpoint Security

Built-in Compliance Benchmarks

Unified Logging

Behavioural Analytics

Real-Time Insights

MITRE ATT&CK

Jamf Threat Labs

Endpoint Protection

Applications Controls

SIEM / SOAR Integrations

Jamf **Safe Internet**

Content **Filtering**….

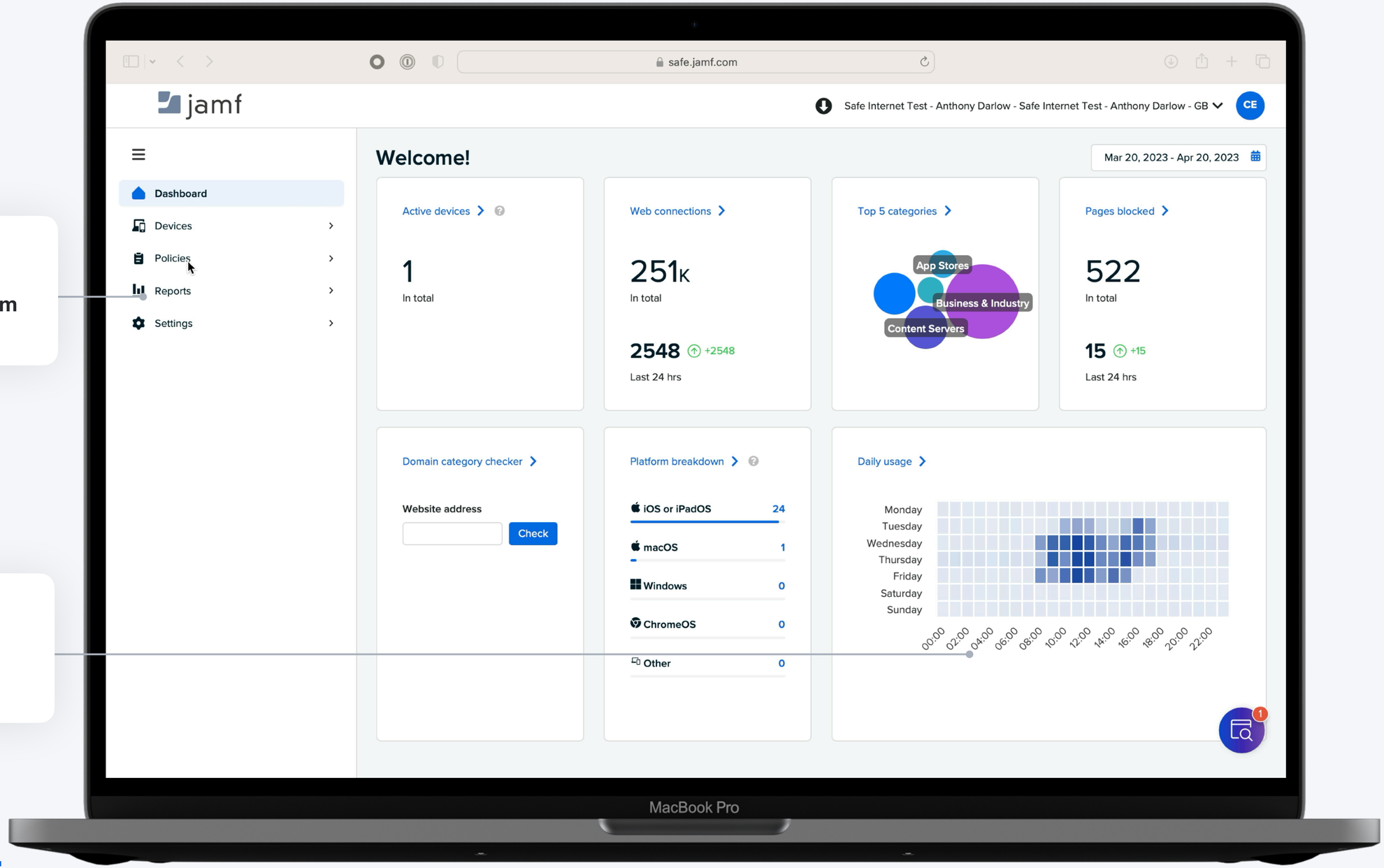
DNS over HTTPS Technology
Category Blocking
Google Safe Search Enforcement

Block Policy

Define content students and teachers can access to keep them safe online

Granular Categories

An extensive list of categories to build granular control



JAMF NATION LIVE

Block Policy

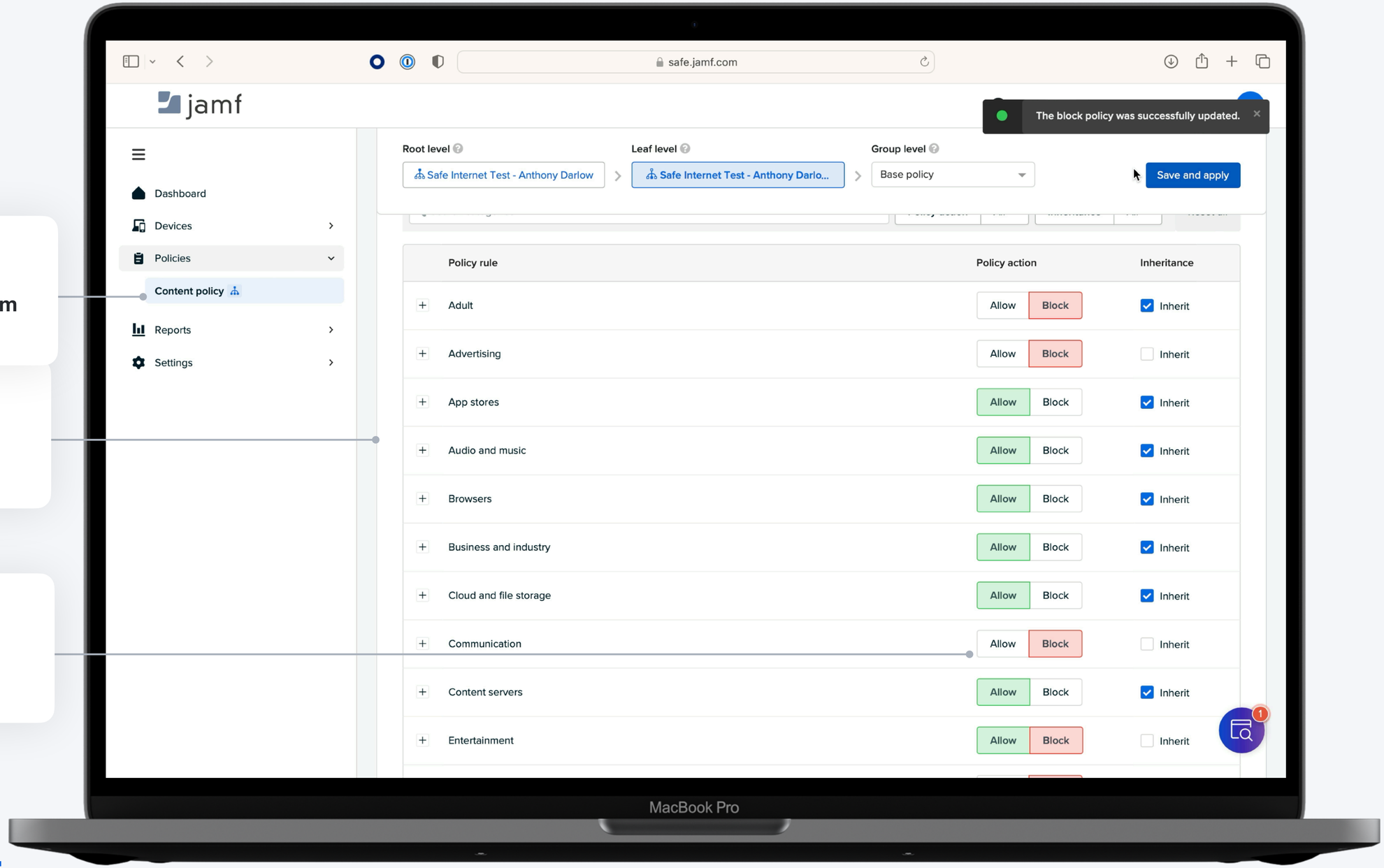
Define content students and teachers can access to keep them safe online

Safe Search & Restricted Mode

Enforce Google Safe Search and Youtube Restricted Mode for appropriate content

Granular Categories

An extensive list of categories to build granular control



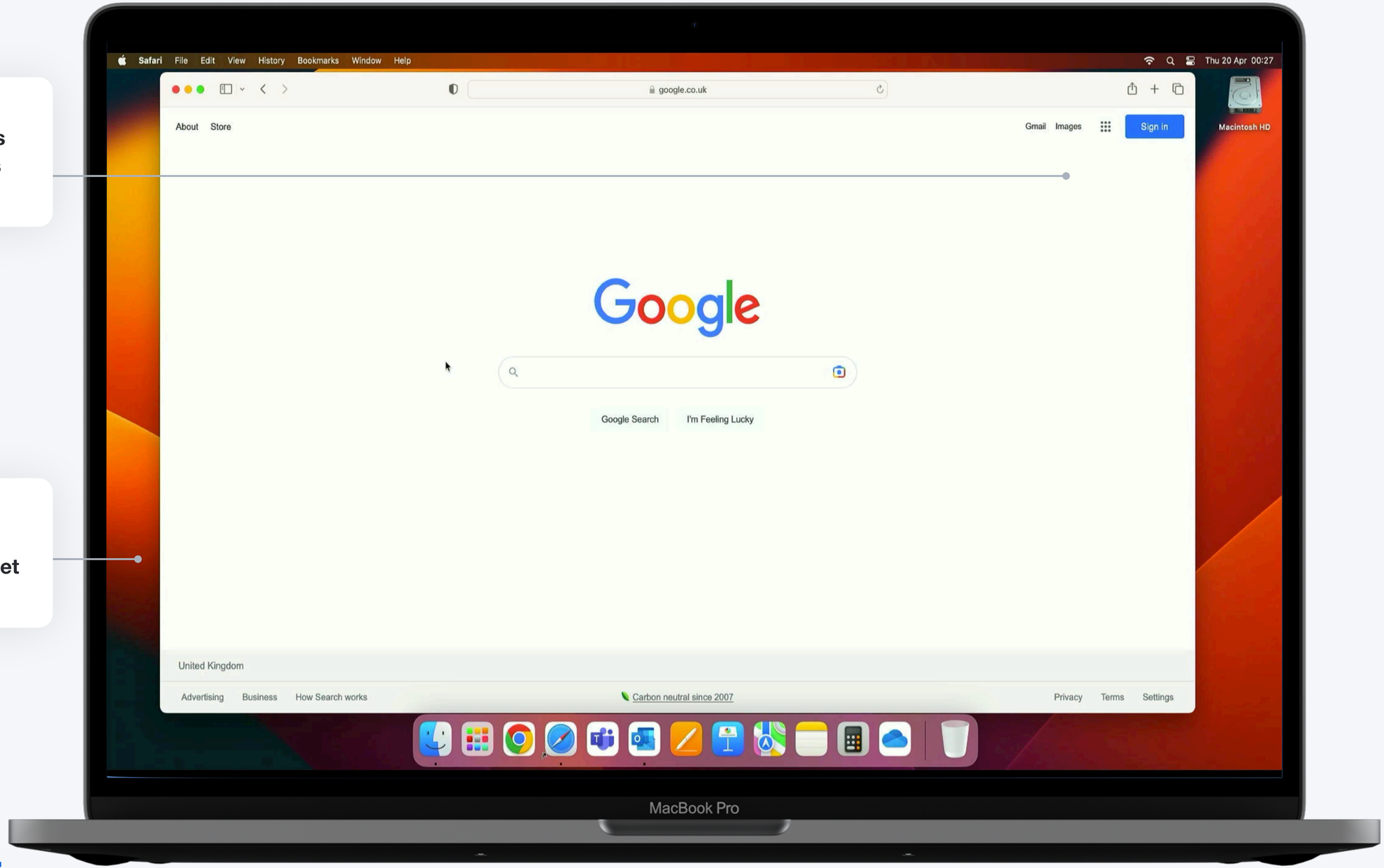
JAMF NATION LIVE

Google Safe Search

Notice that Google Safe Search is enforced as per the Search Rules policy in Safe Internet

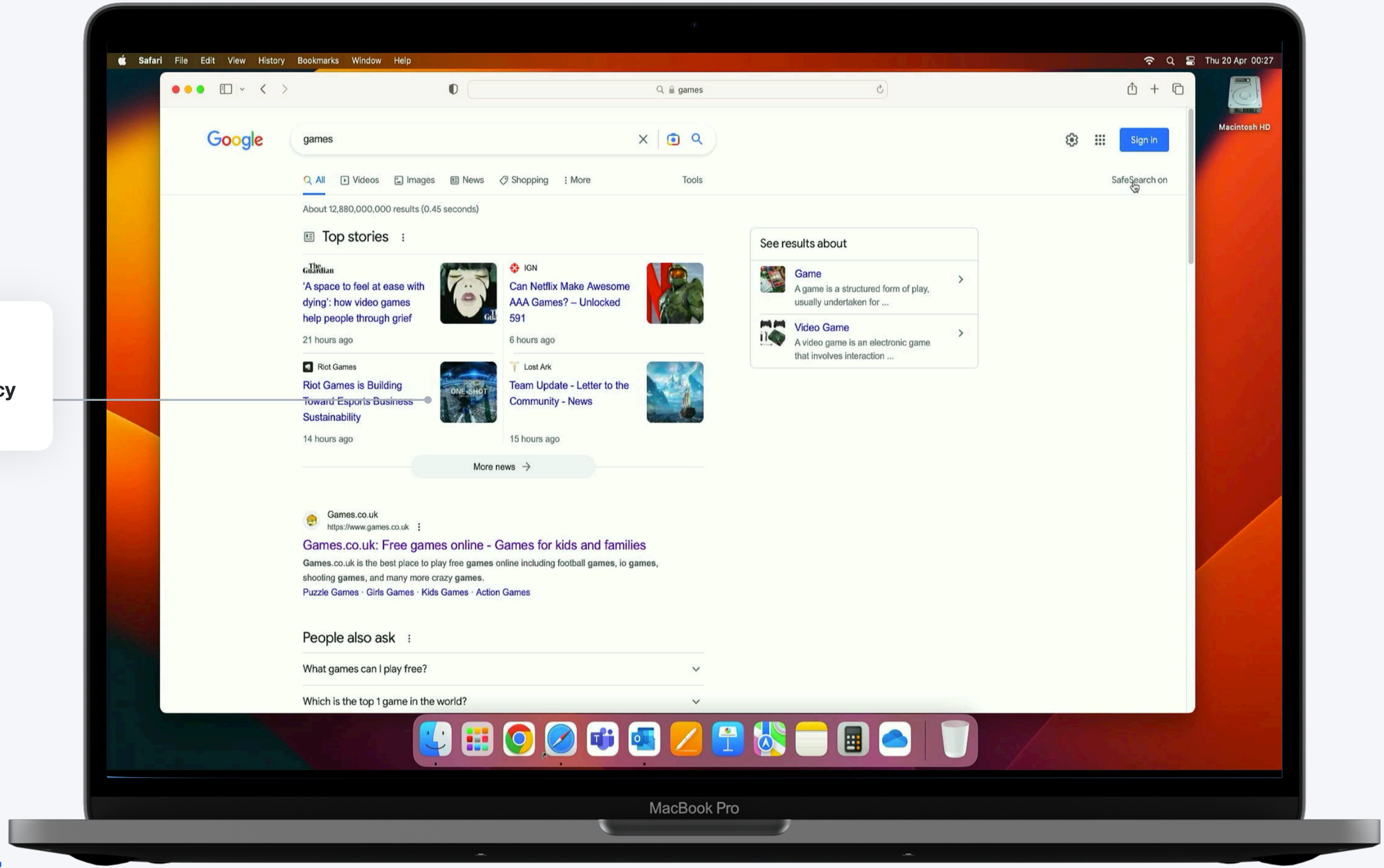
Student Device

Students will be students and try to do other things than the task set by the teacher



Enforced Safe Search

Users cannot edit or turn off safe search per the Search Rules policy in Safe Internet

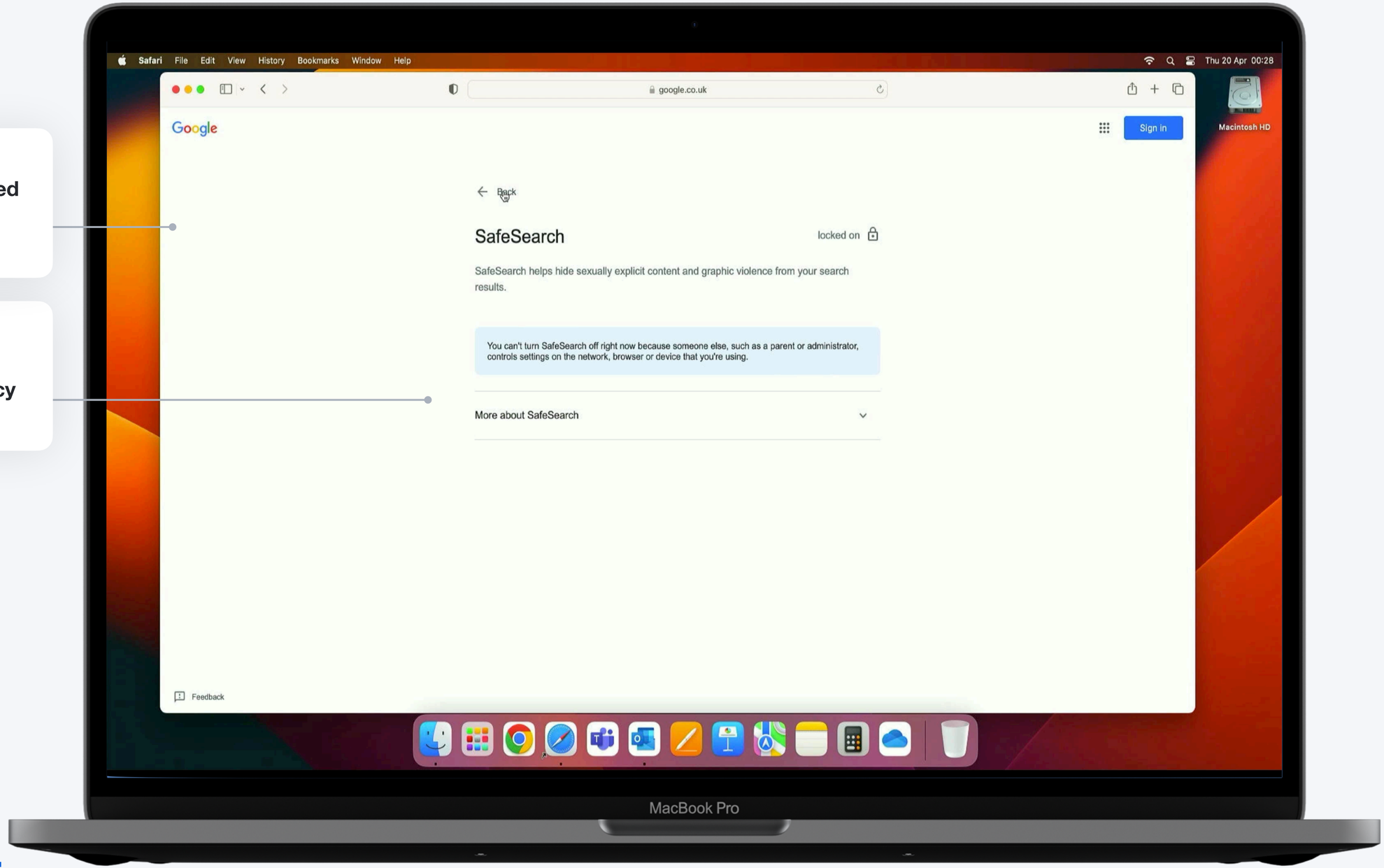


Blocked Content

No access to websites categorised as Games as per block policy in Safe Internet

Enforced Safe Search

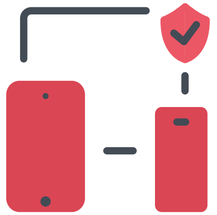
Users cannot edit or turn off safe search per the Search Rules policy in Safe Internet



Jamf **Safe Internet**

Content **Filtering**….

DNS over HTTPS Technology
Category Blocking
Google Safe Search Enforcement



Web-Based Threat Prevention…

Web-based Malware Traffic
Spam
Phishing

Email from IT Support

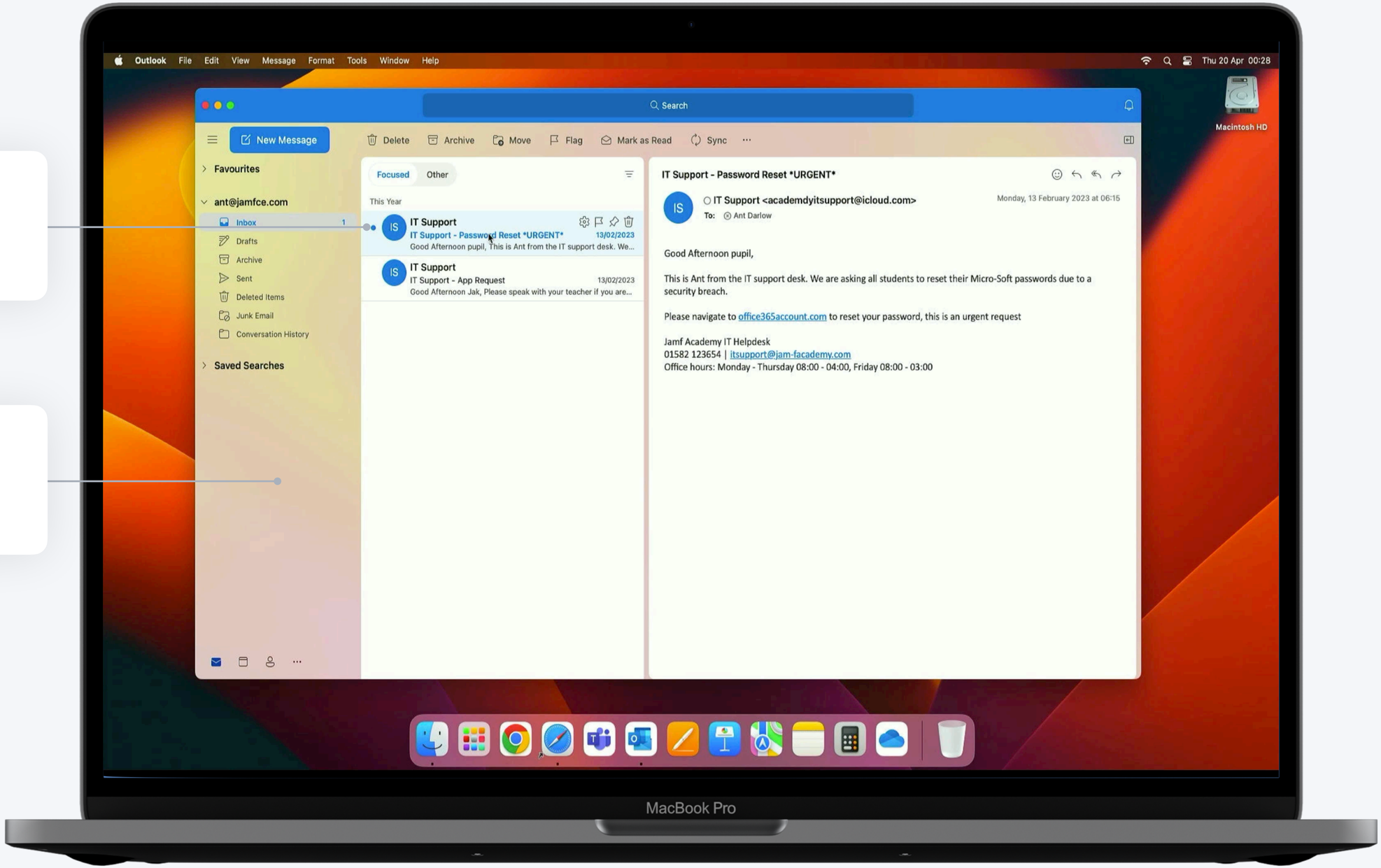
Asking for the student to reset their Microsoft password

Email from IT Support

Asking for the student to reset their Microsoft password

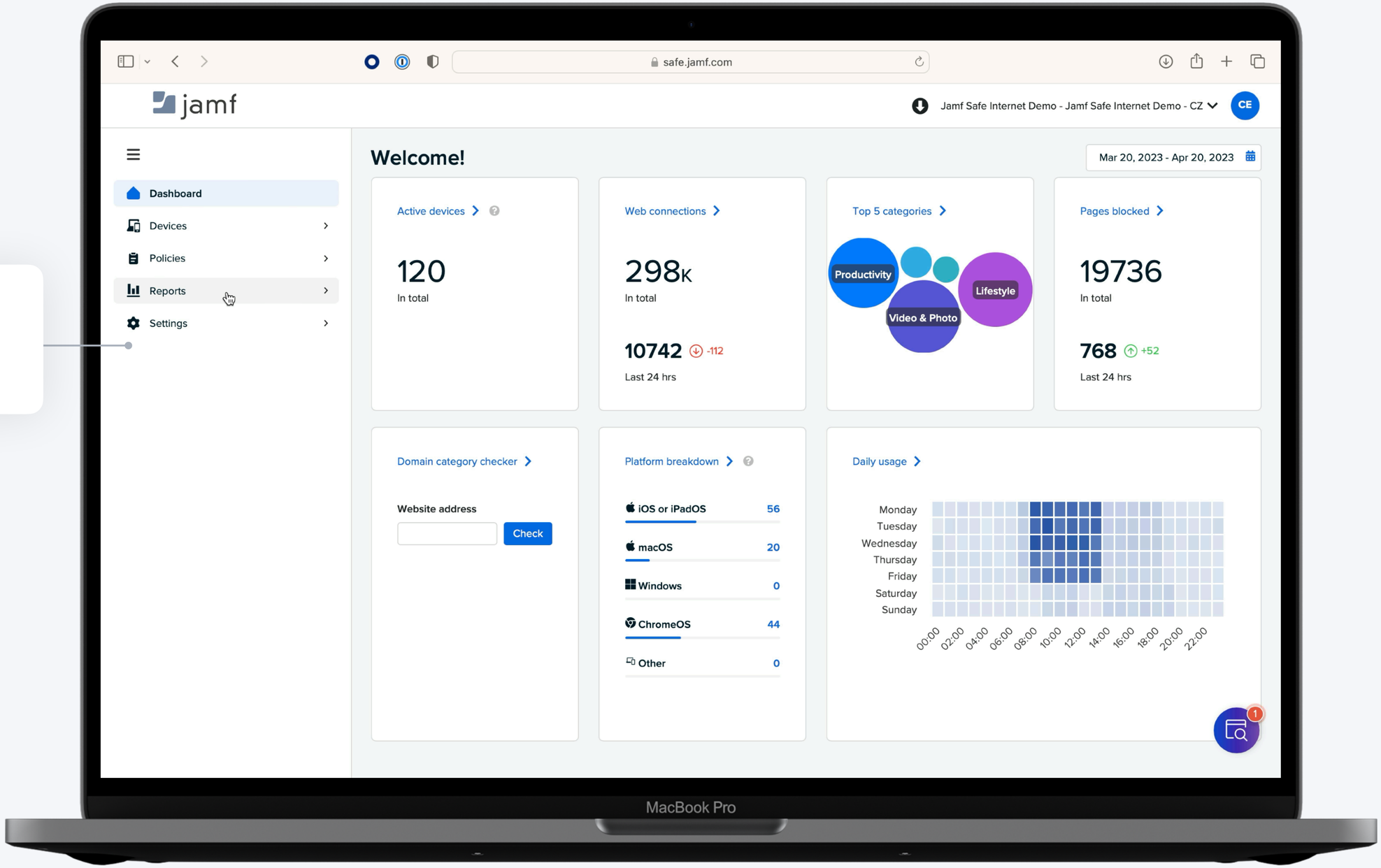
Web Based Threat Prevention

Protecting students against web-based malware, spam and phishing attacks



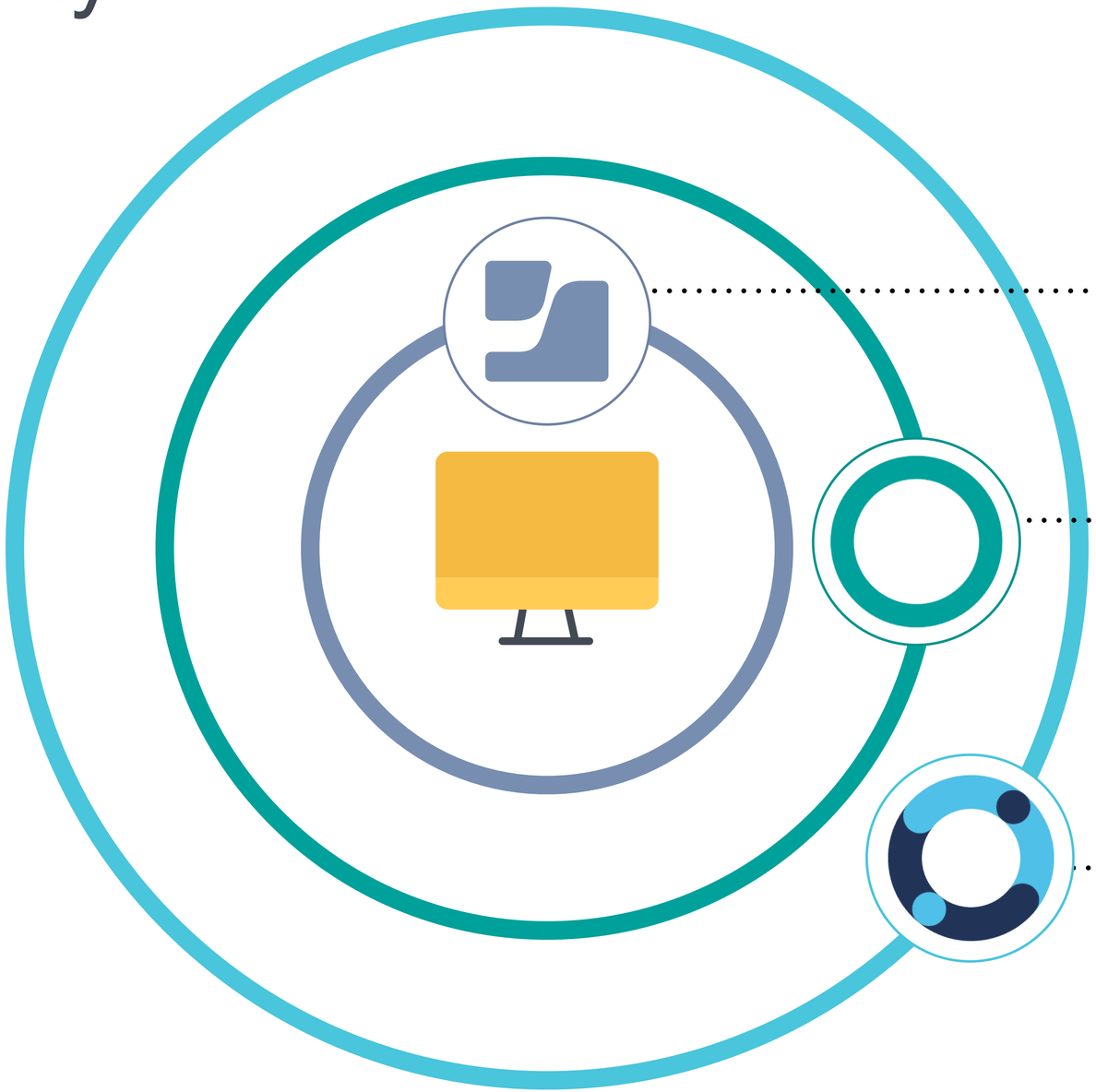
Security Reports

Data and reports showing Spam, Malware or Phishing traffic over time and the block destination



JAMF NATION LIVE

Layered Security



Jamf School
(MDM)

Jamf Protect
(Endpoint Security)

Jamf Safe Internet
(Web-Based Protection)

Thank You!

JAMF NATION LIVE